AIX Versió 7.2

Gestió de xarxes i de comunicacions

AIX Versió 7.2

Gestió de xarxes i de comunicacions

Nota

Abans d'utilitzar aquesta informació i el producte al qual dóna suport, llegiu la informació que apareix als apartats "Avisos" a la pàgina 689.

Aquesta edició s'aplica a AIX Versió 7.2 i a tots els releases posteriors d'aquest producte fins que no s'indiqui una altra cosa en noves edicions.

Contingut

Quant a aquest document

Aquest manual proporciona informació completa per als programadors d'aplicacions amb relació a l'habilitació de les aplicacions per a la globalització en el sistema operatiu AIX. També proporciona informació detallada per als administradors de sistema amb relació a l'habilitació d'entorns connectats en xarxa per a la globalització en el sistema operatiu AIX. Així doncs, els programadors i els administradors de sistema poden utilitzar aquest manual per conèixer les directrius i els principis relacionats amb la globalització. Entre els temes descrits s'inclouen els entorns locals, els conjunts de codis, el mètodes d'entrada, les subrutines, els convertidors, el mapatge de caràcters, informació específica de la cultura i recursos de missatges.

Ressaltat

En aquest document es fan servir els convenis tipogràfics següents:

Element	Descripció
Negreta	Identifica ordres, subrutines, paraules clau, fitxers, estructures, directoris i altres elements els noms dels quals estan predefinits pel sistema. També identifica objectes gràfics, com ara botons, etiquetes i icones que l'usuari selecciona.
Cursiva	Identifica paràmetres els noms o valors reals dels quals han de ser proporcionats per l'usuari.
`Monoespai`	Identifica exemples de valors de dades específics, exemples de text similars als que podeu veure a la pantalla, exemples de parts de codi del programa similars als que escriuríeu com a programador, missatges del sistema o informació que heu d'escriure.

Sensibilitat a minúscules i majúscules a l'AIX

El sistema operatiu AIX és sensible a les minúscules i majúscules. Això vol dir que distingeix entre la informació escrita en majúscules i minúscules. Per exemple, podeu executar l'ordre **ls** per veure una llista de fitxers. En canvi, si escriviu `LS`, el sistema us informarà que aquesta ordre `no s'ha trobat`. De la mateixa manera, **FITXER**, **FiTxer** i **fitxer** són tres noms de fitxers diferents, encara que estiguin al mateix directori. Per evitar equivocacions, escriviu sempre les majúscules i minúscules correctament.

ISO 9000

En el desenvolupament i fabricació d'aquest producte es van utilitzar els sistemes de qualitat ISO 9000 registrats.

Gestió de xarxes i de comunicació

Tant els administradors del sistema com els usuaris porten a terme una varietat de tasques de comunicacions de la xarxa. Els administradors del sistema poden buscar informació sobre el tema de com realitzar les tasques de configuració de valors TCP/IP, millora de la seguretat de la xarxa i supervisió del sistema. Els usuaris poden buscar informació completa sobre com dur a terme tasques d'utilització de les aplicacions de comunicacions i serveis pel sistema operatiu. Hi ha altra informació que explica com configurar i resoldre problemes de correu, problemes del gestor de missatges (MH), de l'NFS (Sistema de fitxers de xarxa), de l'HA-NFS (High Availability-NFS), Transmission Control Protocol/Internet Protocol (TCP/IP), BNU (Programes d'utilitat bàsics de la xarxa), dispositius de comunicacions en sèrie i dispositius TTY, Emulació de Terminal Asíncron (ATE) i SNMP (Simple Network Management Protocol). S'inclou informació sobre com rebre i enviar missatges i correu, com transferir fitxers (ordre **ftp**), com imprimir fitxers d'un sistema remot, com executar ordres en altres sistemes, com establir comunicació entre sistemes locals i remots i com personalitzar l'entorn de comunicacions. Aquest tema també està disponible en el CD de documentació que s'envia amb el sistema operatiu.

Novetats de la gestió de xarxes i de comunicació

Veieu les novetats que hi ha pel que fa la informació nova o modificada per a la col•lecció de temes de Gestió de xarxes i de comunicació.

Com veure les novetats i modificacions

En aquest fitxer de PDF, podeu veure les barres de revisió (|) al marge esquerre de la informació nova o canviada.

Octubre 2017

La informació següent és un resum de les actualitzacions realitzades en aquesta col•lecciló de temes:

- S'ha eliminat la informació obsoleta sobre el Mode de transferència asíncrona (ATM).

Abril de 2017

- S'ha actualitzat informació sobre l'eliminació d'un adaptador de l'EtherChannel al tema “Canvis a l'EtherChannel utilitzant el Dynamic Adapter Membership” a la pàgina 384.

Novembre de 2016

- S'ha actualitzat la informació sobre la instal•lació de la xarxa sobre l'EtherChannel en el tema “Consideracions sobre la configuració de l'EtherChannel” a la pàgina 373.

Comunicacions i xarxes

Darrera la descripció dels principis generals del treball en xarxa d'ordinadors hi ha un fonament conceptual. Els administrador del sistema que no estiguin familiaritzats amb els principis generals de treball en xarxa han de llegir aquesta secció. Aquells que ja estiguin familiaritzats amb el treball en xarxa UNIX poden saltar-se aquesta secció.

Una xarxa és la combinació de dos o més ordinadors i dels respectius enllaços de connexió. Una xarxa *física* és el maquinari (equipament com ara targetes adaptadores, cables i línies telefòniques) que forma la xarxa. El programari i el model conceptual formen la xarxa *lògica*. Els diferents tipus de xarxa i d'emuladors ofereixen diferents funcions.

Comunicacions

Les xarxes permeten nombroses funcions de comunicacions d'aplicació i d'usuari.

Per exemple, permeten que un usuari faci el següent:

- Envïi correu electrònic (e-mail)
- Emuli un altre terminal o inicïi la sessió en una altra màquina
- Transfereixi dades
- Executi programes que resideixen en un node remot.

Una de les aplicacions més conegudes per les xarxes d'ordinadors és el correu electrònic, el qual permet que un usuari enviï un missatge a un altre usuari. Els dos usuaris poden estar en el mateix sistema (en aquest cas no cal la xarxa de comunicacions), en sistemes diferents de diferents edificis o fins i tot a diferents països. Les capes subjacents de programari i maquinari, així com la xarxa física, permeten que l'usuari generi, enviï, rebi i processi missatges, cartes, memoràndums, invitacions i fitxers de dades. Aquestes comunicacions poden anar a qualsevol altre usuari que resideixi a la xarxa física o procedir-ne. El correu electrònic disposa de la possibilitat d'anotar missatges, ordenar-ne la seqüència, empaquetar-los, classificar dates i gestionar la carpeta de correu.

Mitjançant una xarxa de comunicacions, un ordinador pot *emular*, o simular, un altre ordinador i accedir a informació com si fos un tipus d'ordinador o terminal diferent. Les capacitats d'inici de sessió remot proporcionen als usuaris una interfície de la línia d'ordres interactiva per iniciar la sessió en un sistema remot i accedir als mateixos programes i arxius que si utilitzessin la màquina localment.

Les xarxes també permeten transferir dades d'un sistema a un altre. Es poden migrar fitxers, directoris i sistemes de fitxers sencers des d'una màquina a una altra a través d'una xarxa, habilitant la còpia de seguretat remota de les dades, així com assegurant-ne la redundància en el cas que es produís una anomalia a la màquina. Habitualment es proporciona protecció de paraula clau com a part del protocol. En una transferència de fitxers es dóna una relació de client/servidor entre l'usuari que inicia la sol•licitud i el sistema remot al qual està accedint l'usuari. Sovint els protocols de transferència de fitxers inclouen funcions de visualització i control, de manera que els usuaris amb accés de lectura/escriptura poden visualitzar, definir o suprimir fitxers i directoris.

Molts dels diferents protocols que hi ha permeten que els usuaris i les aplicacions d'un sistema invoquin procediments i aplicacions d'altres sistemes. Això pot ser útil per a un cert nombre d'entorns, incloent-hi la descàrrega de moltes rutines que requereixen una intensa utilització d'ordinadors en aplicacions científiques i d'enginyeria.

Xarxes

La complexitat de les xarxes d'ordinadors modernes han propiciat el naixement de models conceptuals per explicar el funcionament de les xarxes.

Un dels models més comuns d'aquest tipus es el model de referència es d'Interconnexió de Sistemes Oberts de l'International Standards Organization, també conegut com model de set capes OSI.

Les set capes del modelo OSI s'enumeren de la manera següent:

Element	Descripció
7	Aplicació
6	Presentació
5	Sessió
4	Transport
3	Xarxa
2	Enllaç de dades
1	Físic

Els nivells del 1 al 3 són específics de xarxa i varien en funció de la xarxa física que s'estigui emprant. Els nivells del 4 al 7 inclouen funciones de nivell superior i independents de xarxa. Cada capa descriu una funció determinada (enlloc d'un protocol específic) que es produeix a les comunicacions de dades. Les set capes funcionen des del nivell inferior (nivell de màquina) al nivell superior (nivell en el qual es produeix la major part de la interacció humana) de la manera següent:

Element	Descripció
Aplicació	Inclou les aplicacions que fan servir la xarxa.
Presentació	Garanteix que les dades es presenten a les aplicacions d'una manera coherent.
Sessió	Gestiona les connexions entre les aplicacions.
Transport	Garanteix la transmissió de dades sense errors.
Xarxa	Gestiona les connexions a altres màquines de la xarxa.
Enllaç de dades	Permet lliurar les dades de forma fiable a tota la capa física (la qual normalment és inherentment no fiable).
Físic	Descriu el suport d'emmagatzematge físic de la xarxa. Per exemple, el cable òptic de fibra necessari per la xarxa d'interfície de dades distribuïdes per fibra (FDDI) forma part de la capa física.

Nota: Encara que el model de referència OSI sigui útil per tractar conceptes de treball en xarxa, molts protocols de xarxa no segueixen estrictament el model OSI. Per exemple, al tractar el protocol TCP/IP (Transmission Control Protocol/Internet Protocol), es combinen les funcions de capa d'aplicació i de presentació, de la mateixa manera que es combinen les capes de sessió i de transport i les capes d'enllaç de dades i física.

Cada capa del model OSI es comunica amb la capa corresponent de la màquina remota, tal com es mostra a la figura del model de referència OSI.

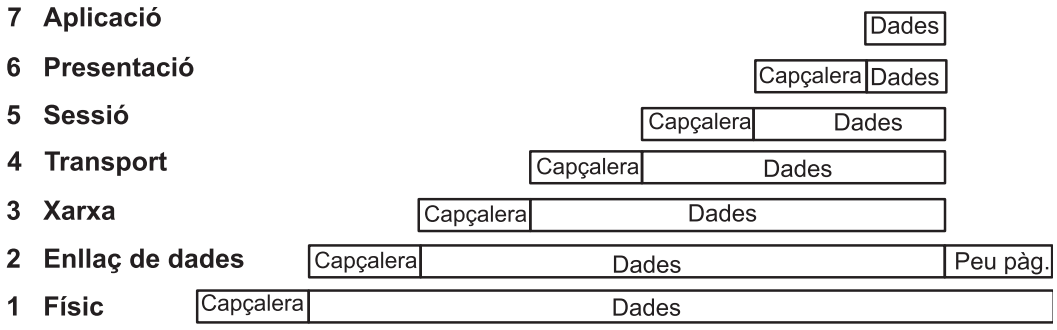


Figura 1. Model de referència OSI

Aquesta il•lustració mostra el diferents nivells de comunicació del model OSI tal com es descriuen en el text anterior.

Les capes passen les dades només a les capes immediatament superiors o inferiors. Cada capa afegeix la seva pròpia informació de capçalera (i informació de peu de pàgina, en el cas de l'enllaç de dades) i encapsula de forma efectiva la informació rebuda de les capes superiors.

Els usuaris individuals, així com les organitzacions fan servir xarxes per molts motius, els quals inclouen:

- Entrada de dades
- Consultes de dades
- Entrada de lot remota
- Compartició de recursos
- Compartició de dades
- Correu electrònic.

L'entrada de dades consta de l'entrada de dades directament a altres fitxers de dades locals o remotes. L'augment de l'exactitud i l'eficiència son conseqüències naturals de la transferència de dades en un sol pas. Les consultes de dades impliquen la cerca de fitxers de dades d'informació específica. L'actualització de dades implica l'alteració, l'afegiment o la supressió de les dades emmagatzemades en fitxers locals o remots. L'entrada de lot remota consta de l'entrada de lots de dades des d'una ubicació remota, una activitat que sovint es realitza de nit o durant períodes en els quals el nivell d'utilització del sistema és baix. Atès les diferents capacitats existents, les comunicacions i les xarxes no són només desitjables, sinó també necessàries.

La compartició de dades es una altra funció de les xarxes. Els usuaris poden compartir dades, així com programes, espai d'emmagatzematge de fitxers i dispositius perifèrics com impressores, mòdems, terminals i discos fixos. La compartició de recursos del sistema resulta econòmica perquè elimina els problemes de conservar vàries còpies de programes i manté les dades de forma coherent (en el cas que es comparteixi un programa o dades).

Xarxes físiques

La xarxa física consta de cables (cables coaxials, parells de trenat, fibra òptica i línies de telèfon) que connecten diferent maquinari que es troba a la xarxa, les targetes adaptadores utilitzades en ordinadors connectats a la xarxa (amfitrió) i qualsevol altre concentrador, repetidor, encaminador o pont utilitzat a la xarxa.

Les xarxes físiques varien en grandària i en el tipus de maquinari emprat. Les dues classes comunes de xarxa són les *xarxes d'àrea local* (LAN) i les *xarxes d'àrea ampla* (WAN). Una LAN es una xarxa en la qual les comunicacions estan limitades a un àrea geogràfica d'una grandària moderada de 1 a 10 km com, per exemple, un edifici d'oficines, magatzem o campus. Una WAN és una xarxa que proporciona la capacitat de comunicar dades a través d'àrees geogràfiques més grans que les proporcionades per les LAN com, per exemple, per un país o per continents. També existeix una classe intermèdia de xarxes anomenada *xarxa d'àrea metropolitana* (MAN). En aquesta guia no es distingeix entre les MAN i les WAN.

Les LAN normalment utilitzen l'Ethernet estàndard, IEEE 802.3 Ethernet, o el maquinari de token ring per la xarxa física, mentre que les WAN i les xarxes asíncrones utilitzen xarxes de comunicacions proporcionades per empreses de telecomunicacions comuns. El funcionament de la xarxa física en ambdós casos normalment es controla mitjançant estàndards de treball en xarxa d'organitzacions com, per exemple, Electronics Industry Association (EIA) o International Telecommunication Union (ITU).

Sistemes de xarxa

Totes les comunicacions en xarxa impliquen l'ús de maquinari i de programari. El suport de comunicacions de maquinari i de programari del sistema es determina mitjançant el maquinari que s'està utilitzant i el programari necessari per executar l'esmentat maquinari i la interfície amb la xarxa.

El *maquinari* consisteix en l'equipament físic connectat a la xarxa física. El *programari* consta de programes i programes de control de dispositiu que pertanyen al funcionament d'un sistema determinat. El maquinari del sistema consisteix en targetes adaptadores o altres dispositius que proporcionen un camí d'accés o una interfície entre el programari del sistema i la xarxa física. Una targeta adaptadora requereix una ranura de targeta d'entrada/sortida (E/S) al sistema. La targeta adaptadora connecta el DTE (*data*

terminal equipment) al DCE (*data circuit-terminating equipment*); és a dir, proporciona un adreçament local físic a un port DTE. Altres dispositius, com per exemple mòdems, poden adjuntar-se a un dels ports estàndard de l'ordinador.

Una targeta adaptadora prepara totes les dades d'entrada i de sortida, duu a terme cerques d'adreces, proporciona programes de control, receptors i protecció contra sobrecàrregues, dóna suport a diferents interfícies i, en general, relleva el processador del sistema de moltes de les tasques de comunicació. Les targetes adaptadores donen suport a les normes que requereix la xarxa física (per exemple, EIA 232D, Smartmodem, V.25 bis, EIA 422A, X.21 o V.35) i alhora dóna suport a *protocols* de programari, per exemple el control d'enllaços de dades síncrones (SDLC), el control d'enllaços de dades d'alt nivell (HDLC) i a protocols bisíncrons. Si l'adaptador no conté suport de programari, aquest suport haurà d'ésser proporcionat pel controlador de dispositiu de l'adaptador.

Protocolos

Tots els programaris de comunicació utilitzen *protocols*, conjunts de regles semàntiques i sintàctiques que determinen el comportament d'unitats funcionals a l'hora d'establir comunicacions.

Els protocols defineixen el mode en què es proporciona l'informació, com s'adjunta per arribar a la seva destinació de forma segura i quin camí d'accés segueix. Els protocols també coordinen el flux de missatges i els seus reconeixements.

Els protocols existeixen a diferents nivells dins del kernel i no es poden manipular de forma directa. De tota manera, es manipulen de forma indirecta segons el que l'usuari decideix fer al nivell de l'interfície de programació d'aplicació. Les opcions que un usuari fa en invocar programes de transferència de fitxers, d'inici de sessió remot o d'emulació de terminal defineixen els protocols que s'utilitzen en l'execució d'aquests programes.

Adreces

Les *adreces* s'associen amb el programari i el maquinari. Una adreça és el mode mitjançant el qual l'estació emissora o d'enviament selecciona l'estació on s'han d'enviar dades.

Les adreces identifiquen les ubicacions de rebuda o emmagatzematge. Una adreça física és un codi exclusiu assignat a un altre dispositiu o estació de treball connectats a una xarxa.

Per exemple, en una xarxa token ring, l'ordre **netstat -iv** mostra l'adreça de targeta token ring. Aquesta és l'adreça de xarxa física. L'ordre **netstat -iv** també mostra l'informació d'adreça de nivell de classe i d'usuari. Les adreces sovint es defineixen mitjançant el programari però també les pot crear l'usuari.

Dominis

Un aspecte de les adreces comú a moltes xarxes de comunicació és el concepte dels *dominis*. Els dominis col•loquen recursos de processament de dades a la xarxa sota un control comú.

Per exemple, l'estructura d'Internet mostra el mode en què els dominis defineixen l'adreça IP. Internet és una xarxa àmplia formada de diferents xarxes més petites. Per facilitar l'encaminament i l'adreçament, les adreces d'Internet s'estructuren de forma jeràrquica en dominis, amb categories molt àmplies en la part superior com, per exemple `com` pels usuaris comercials, `edu` per usuaris del món de l'educació i `gov` per usuaris del govern.

Dins del domini `com`, s'hi troben molts dominis més petits que corresponen a negocis individuals; per exemple, `ibm`. Dins del domini `ibm.com`, s'hi troben dominis fins i tot més petits que corresponen a adreces d'Internet de diferents ubicacions com, per exemple, `austin.ibm.com` o `raleigh.ibm.com`. En aquest nivell, es comencen a veure noms de *amfitrions*. Un amfitrió, en aquest context, és qualsevol ordinador connectat a la xarxa. Dins de `austin.ibm.com`, hi poden haver amfitrions amb els noms `hamlet` i `lear`, els quals tenen les adreces `hamlet.austin.ibm.com` i `lear.austin.ibm.com`.

Passarel•les i ponts

A Internet hi ha una àmplia varietat de xarxes, les quals sovint utilitzen maquinari diferent i executen programari diferent. Les *passarel•les* i els *ponts* permeten a aquestes diferents xarxes comunicar-se entre sí.

Un pont és una unitat funcional que connecta dos LAN que possiblement utilitzen el mateix procediment de control d'enllaços lògics com, per exemple, Ethernet, però procediments de control d'accés al medi diferents. Una passarel•la té un abast més ampli que un pont. Opera per sobre de la capa d'enllaços i, quan és necessari, converteix l'interfície i el protocol utilitzats per una xarxa en els que utilitza una xarxa completament diferent. Les passarel•les permet transferir dades per les diferents xarxes que constitueixen Internet.

Encaminament de dades

La utilització de noms de domini per l'adreçament i de passarel•les per la conversió facilita en gran mesura l'*encaminament* de les dades que es transfereixen. L'encaminament és l'assignació d'un camí d'accés gràcies al qual un missatge arriba a la seva destinació.

El nom de domini defineix de forma efectiva la destinació del missatge. En una xarxa gran com Internet, l'informació s'encamina des d'una xarxa de comunicacions a la següent fins que l'informació arriba a la seva destinació. Cada xarxa de comunicacions comprova el nom de domini i, segons els dominis amb els quals estigui familiaritzada la xarxa, encamina l'informació a la següent aturada lògica. D'aquesta manera, cada xarxa de comunicació que rep les dades contribueix al procés d'encaminament.

Nodes locals i remots

Els amfitrions que es troben utilitzen la xarxa física on es troben. Cada amfitrió és un *node* de la xarxa. Un node és una ubicació a la qual es pot fer referència en una xarxa de comunicacions que proporciona serveis de processament d'amfitrió. L'intercomunicació d'aquests diferents nodes es defineix com a *local* o *remota*.

Local pertany a un dispositiu, fitxer o sistema al qual s'accedeix directament des del sistema, sense utilitzar una línia de comunicació. *Remot* pertany a un dispositiu, fitxer o sistema al qual s'accedeix per una línia de comunicacions. Els fitxers locals es troben al sistema, mentre que els fitxers remots es troben en un servidor de fitxers o en un altre node amb el qual us podeu comunicar utilitzant una xarxa física com, per exemple, Ethernet, token ring o les línies de telèfon.

Client i servidor

Un *servidor* és un ordinador que conté dades o proporciona recursos als quals es pot accedir des d'altres ordinadors de la xarxa. Un *client* és un ordinador que sol•licita serveis o dades d'un servidor.

Els tipus de servidors comuns són els servidors de fitxers, els quals emmagatzemen fitxers; els servidors de noms, els quals emmagatzemen noms i adreces; els servidors d'aplicacions, els quals emmagatzemen programes i aplicacions i els servidors d'impressió, els quals programen i dirigeixen treballs d'impressió a la seva destinació.

Un client pot sol•licitar un codi de programa actualitzat o l'ús d'aplicacions des d'un servidor de codis. Per obtenir un nom o una adreça, el client es posa en contacte amb un servidor de noms. Un client també pot sol•licitar fitxers i dades per l'entrada de dades, la demanda o l'actualització d'enregistraments des d'un servidor de fitxers.

Comunicació amb altres sistemes operatius

Es poden connectar diferents tipus de màquines en una xarxa. Les màquines poden procedir de fabricants diferents o poden ser models diferents del mateix fabricant. Els programes de configuració creen ponts entre les diferències de sistema operatiu de dos o més tipus d'ordinadors.

De vegades, aquests programes requereixen que s'hagi instal•lat un altre programa anteriorment a la xarxa. És probable que altres programes requereixin que hi hagi a la xarxa protocols de connectivitat de comunicacions com ara TCP/IP (Transmission Control Protocol/Internet Protocol) o SNA (Systems Network Architecture).

Aplicacions d'emulació de l'amfitrió

Un *emulador* és una aplicació de programari que permet que el sistema funcioni com si s'estigués utilitzant un terminal o una impressora diferent.

Un *emulador de terminal* es connecta amb un amfitrió per accedir a dades o a aplicacions. Alguns emuladors de terminal faciliten un recurs de transferència de fitxers a l'amfitrió i des del mateix. Altres faciliten una API (interfície de programació d'aplicacions) per permetre la comunicació programa a programa i l'automatització de les tasques de l'amfitrió.

Un *emulador d'impressora* permet que l'amfitrió imprimeixi fitxers en una impressora local o els emmagatzemi en format imprimible per imprimir-los o editar-los posteriorment.

Moltes aplicacions estan disponibles perquè el sistema pugui emular altres tipus de terminals. Aquest tema proporciona informació sobre els emulador de terminal o d'impressora.

Nota: L'ordre **bterm** emula terminals en modalitat BIDI (bidireccional).

Ordres TCP/IP d'emulació

El programari del Transmission Control Protocol/Internet Protocol inclou les ordres **telnet** i **rlogin**, que permeten la connexió i l'accés a un sistema TCP/IP remot.

Element	Descripció
telnet	Permet que un usuari iniciï la sessió en un amfitrió remot en implementar el protocol **TELNET**. És diferent de l'ordre **rlogin** en el sentit que es tracta d'una ordre fiable. Una ordre *fiable* és la que satisfà tots els nivells de seguretat configurats de la màquina. Els sistemes que requereixen mesures de seguretat extraordinàries només haurien de permetre ordres fiables. El Departament de Defensa dels Estats Units estableix i manté les normes sobre ordres, processos i programes fiables.
tn	Duu a terme la mateixa funció que l'ordre **telnet**.
rlogin	Permet que un usuari iniciï la sessió en un amfitrió remot. La diferència és que l'ordre **telnet** es considera una ordre *no fiable* i es pot inhabilitar si el sistema necessita més seguretat.

Per obtenir més informació sobre **TCP/IP**, consulteu l'apartat "Transmission Control Protocol/Internet Protocol" a la pàgina 102.

Ordres BNU d'emulació

El programari Basic Networking Utilities (BNU) inclou les ordres **ct**, **cu** i **tip**, cosa que permet efectuar la connexió amb un sistema remot que utilitzi el sistema operatiu AIX.

Element	Descripció
ct	Permet que un usuari d'un terminal remot, com ara un 3161, es comuniqui amb un altre terminal a través d'una línia telefònica. L'usuari del terminal remot pot aleshores iniciar la sessió i treballar en l'altre terminal. L'ordre **ct** és semblant a l'ordre **cu** però no és tan flexible. Per exemple, no és possible executar ordres al sistema local mentre s'està connectat a un sistema remot mitjançant l'ordre **ct**. No obstant això, es poden donar instruccions a l'ordre **ct** perquè continuï marcant fins que s'estableixi la connexió o perquè especifiqui més d'un número de telèfon cada vegada.
cu	Connecta el terminal a un altre terminal connectat a un sistema UNIX o no UNIX. Un cop s'ha establert la connexió, podeu iniciar la sessió en tots dos sistemes alhora, executant ordres en un dels dos sense deixar anar l'enllaç de comunicació dels BNU. Si el terminal remot també funciona en UNIX, podeu transferir fitxers ASCII entre el dos sistemes. També podeu utilitzar l'ordre **cu** per connectar diversos sistemes i, aleshores, es poden executar ordres en qualsevol dels sistemes connectats.

Element	Descripció
tip	Connecta el terminal a un terminal remot i permet treballar al terminal remot com si s'hi hagués iniciat la sessió directament. Es pot utilitzar l'ordre **tip** per transferir fitxers al sistema remot i des del mateix. Es poden utilitzar seqüències per enregistrar les converses que manteniu mitjançant l'ordre **tip**. **Nota:** Cal que inicieu una sessió al sistema remot per utilitzar l'ordre **tip**.

Per obtenir més informació sobre els BNU, consulteu l'apartat "Basic Networking Utilities (BNU)" a la pàgina 432.

Emulació de Terminal Asíncron

El programa ATE (Emulació de terminal asíncron) permet que el terminal es connecti a la majoria de sistemes que donen suport als terminals asíncrons, incloent-hi els sistemes que donin suport a les connexions RS-232C o RS-422A.

L'ATE permet que el sistema remot es comuniqui amb el terminal com a pantalla asíncrona o com a terminal DEC VT100.

L'ATE permet executar ordres al sistema remot, enviar i rebre fitxers i comprovar la integritat de les dades dels fitxers transferits entre sistemes. Es pot utilitzar també un fitxer de captura per enregistrar, o *capturar*, dades entrants del sistema remot. L'ATE és un programa dirigit per menús i utilitza subordres.

Quan s'instal•la, només poden accedir a l'ATE els usuaris que s'han enregistrat com a membres del grup UUCP mitjançant un usuari amb autorització root.

Per obtenir més informació sobre l'ATE, consulteu l'apartat "Emulació de terminal asíncron" a la pàgina 629.

Ordres del sistema de comunicacions

En aquest apartat es descriuen ordres disponibles per mostrar informació que identifiqui els usuaris del sistema, el sistema que s'està utilitzant i els usuaris que han iniciat la sessió en altres sistemes.

Consulteu els temes següents si voleu veure les diverses ordres que s'utilitzen per tal d'oferir informació del sistema i de l'usuari.

Visualització del nom d'inici de sessió

Utilitzeu l'ordre **whoami** per determinar el nom d'inici de sessió.

Per visualitzar el nom de l'usuari actual, escriviu:

```
whoami
```

Apareix una pantalla similar a la següent:

```
nuria
```

En aquest exemple, el nom d'inici de sessió és `núria`.

Visualització del nom del sistema

Utilitzeu l'ordre **uname** per determinar el nom del sistema.

1. Per visualitzar el nom del vostre sistema si us trobeu en una xarxa, escriviu:

   ```
   uname -n
   ```

   Apareix una pantalla similar a la següent:

   ```
   bernat
   ```

En aquest exemple, el nom del sistema és bernat.

2. Per saber el nom de node d'un altre sistema, heu de demanar que un usuari d'aquell sistema escrigui l'ordre **uname -n**.

Determinació de si es pot accedir al sistema

Utilitzeu **host** per determinar si el sistema té accés a informació que defineix l'altre sistema.

Per accedir a un altre sistema de la xarxa, el sistema local ha de tenir accés a la informació que defineix l'altre sistema. Per tal de determinar si el sistema local disposa d'aquesta informació, escriviu l'ordre **host** amb el nom de l'altre sistema.

Per tal de determinar si el sistema local disposa de la informació d'encaminament per al sistema zeus, escriviu:

```
host zeus
```

Si el vostre sistema disposa de la informació correcta, apareixerà una pantalla similar a la següent:

```
zeus és 192.9.200.4  (300,11,310,4)
```

Aleshores podeu enviar un missatge al sistema zeus. El sistema utilitza l'adreça 192.9.200.4 per encaminar el correu. Si el vostre sistema no disposa d'aquesta informació, apareixerà una pantalla similar a la següent:

```
zeus: sistema principal desconegut
```

Si rebeu un missatge del tipus amfitrió desconegut, aleshores el nom del sistema sobre el qual es fa la sol•licitud:

- No és correcte (comproveu que l'adreça s'hagi escrit correctament)
- És a la vostra xarxa, però no s'ha definit per al vostre sistema (poseu-vos en contacte amb la persona responsable de la configuració de la xarxa)
- És en una altra xarxa (consulteu l'apartat "Adreçament de correu a usuaris d'una xarxa diferent" a la pàgina 23) i necessita un adreçament més detallat
- No està connectat a la vostra xarxa

També es pot rebre un missatge del tipus amfitrió desconegut si la xarxa no està en funcionament i el sistema local depèn d'un sistema remot per tal de subministrar adreces de xarxa.

Visualització d'informació sobre usuaris que han iniciat la sessió

Utilitzeu l'ordre **finger** o **f** per tal de mostrar informació sobre els usuaris actuals d'un amfitrió especificat.

Aquesta informació pot incloure el nom d'inici de sessió de l'usuari, nom complet, i el nom del terminal, així com la data i l'hora de l'inici de sessió.

1. Per veure informació sobre tots els usuarios que han iniciat la sessió a l'amfitrió @alcatraz, escriviu:

   ```
   finger @alcatraz
   ```

   Apareix una pantalla similar a la següent:

   ```
   salines  Consola  15 mar 13:19
   sola       pts0     15 jn 13:01
   alos       tty0       15 jn 13:01
   ```

   L'usuari puig ha iniciat la sessió a la consola; l'usuari prat, des de la línia d'un pseudoterminal pts0, i l'usuari pujol, des d'un terminal tty0.

2. Per tal d'obtenir informació sobre l'usuari puig de l'exemple anterior, escriviu:

   ```
   finger puig@alcatraz
   ```

o

```
finger puig
```

Apareix una pantalla similar a la següent:

```
Nom d'inici de sessió: puig
A la vida real: Marta Puig
Directori:/home/puig    Shell: /bin/ksh
Activat des del 8 maig 07:13:49 a la consola
Sense planificació.
```

Gestió del correu

El recurs de correu proporciona un mètode per intercanviar correu electrònic (e-mail) amb usuaris del mateix sistema o de diversos sistemes connectats mitjançant una xarxa. A continuació es descriu el sistema de correu, la interfície d'usuari de correu estàndard, l'**Internet Message Access Protocol (IMAP)** i el **protocol d'oficina de correus (POP - Post Office Protocol)**.

El sistema de correu és un recurs de lliurament de correu d'internetwork que consta d'una interfície d'usuari, un programa d'encaminament de missatges i un programa de lliurament de correu (o aplicació de correu - mailer). El sistema de correu retransmet els missatges d'un usuari a un altre del mateix amfitrió, entre amfitrions i a diferents límits de la xarxa. També porta a terme una quantitat limitada d'edició de capçaleres de missatges per donar al missatge un format que sigui adequat per a l'amfitrió receptor.

Una *interfície d'usuari* de correu permet que els usuaris creïn i enviïn missatges, que rebin missatges d'altres usuaris. El sistema de correu proporciona dues interfícies d'usuari, **mail** i **mhmail**. L'ordre **mail** és la interfície d'usuari de correu estàndard que hi ha disponible a tots els sistemes UNIX. L'ordre **mhmail** és la interfície d'usuari del gestor de missatges (MH), una interfície d'usuari ampliada que s'ha dissenyat per a usuaris experts.

Un *programa d'encaminament de missatges* encamina els missatges a les seves destinacions pertinents. El programa d'encaminament de missatges del sistema de correu és el programa **sendmail**, que forma part del BOS (sistema operatiu base) i que s'instal•la amb el BOS. El programa **sendmail** és un daemon que utilitza informació del fitxer `/etc/mail/sendmail.cf` i del fitxer `/etc/mail/aliases` per dur a terme l'encaminament necessari.

Segons el tipus de camí cap a la destinació, l'ordre **sendmail** utilitza diferents *aplicacions de correu* per lliurar els missatges.

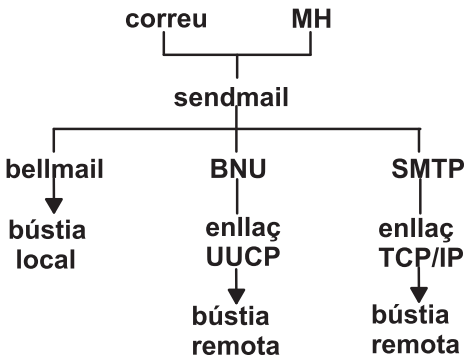


Figura 2. Aplicacions de correu (mailers) que utilitza l'ordre sendmail

Aquesta il•lustració és un tipus de gràfic organitzatiu en sentit vertical amb el correu i l'MH a dalt de tot. D'ell en pengen el bellmail, els BNU i l'SMTP. Per sota del nivell anterior hi ha el respectiu enllaç a la bústia local, l'enllaç UUCP i l'enllaç **TCP/IP**. Per sota de l'enllaç UUCP hi ha la bústia remota i per sota de l'enllaç **TCP/IP** hi ha la bústia remota.

La il•lustració mostra:

- Per lliurar un correu local, el programa **sendmail** encamina els missatges al programa **bellmail**. El programa **bellmail** lliura tot el correu local afegint missatges a la bústia del sistema d'usuaris, que es troba al directori /var/spool/mail.
- Per lliurar correu a través d'un enllaç UUCP (Programa de còpia UNIX a UNIX), el programa **sendmail** encamina els missatges utilitzant els BNU (Programes d'utilitat bàsics de la xarxa).
- Per lliurar correu encaminat mitjançant **Transmission Control Protocol/Internet Protocol (TCP/IP)**, l'ordre **sendmail** estableix una connexió **TCP/IP** al sistema remot i, aleshores, utilitza el **Simple Mail Transfer Protocol (SMTP)** per transferir el missatge al sistema remot.

Programes agent d'usuari de correu

Abans que pugueu utilitzar el sistema de correu, heu de seleccionar un programa agend d'usuari. Podeu triar un programa de correu (**mail**), un gestor de missatges (**mh**) o l'ordre **bellmail**.

Un programa agent d'usuari proporciona recursos per crear, rebre, enviar i arxivar correu. A banda d'això, cal disposar d'un programa agent de transport, **sendmail**, que distribueixi el correu o els paquets que entren procedents d'altres sistemes, que distribueixi cada element de correu de sortida i que el transmeti a un programa semblant d'un o més sistemes remots.

> **Nota:** Els programes **mail** i **mh** són incompatibles pel que fa a la manera d'emmagatzema el correu. Heu de triar un gestor de correu o l'altre.

Interfície de programa de correu (mail)

El programa **mail** us facilita una interfície d'usuari per gestionar correu cap a i des d'un usuari de xarxa local i cap a i des d'un usuari de sistema remot.

Un missatge de correu pot ser de text, escrit mitjançant un editor, o un fitxer ASCII. A més d'un missatge escrit o un fitxer, es poden enviar:

Element	Descripció
missatge del sistema	Informa els usuaris que s'ha produït una actualització del sistema. Un missatge del sistema és semblant a un missatge de difusió però s'envia només a la xarxa local.
correu confidencial	S'utilitza per enviar informació classificada. Els missatges de correu secret estan encriptats. El destinatari ha d'especificar una paraula clau per llegir-los.
missatge de vacances	Informa els usuaris que esteu de vacances. Quan el sistema rep correu mentre no hi sou, envia un missatge de tornada a l'origen. El missatge anuncia que esteu de vacances. Qualsevol missatge que rebeu mentre esteu de vacances també es pot reenviar.

Quan es rep el correu mitjançant les subordres **mail**, es pot:

- Deixar el correu a la bústia del sistema.
- Llegir i suprimir el correu.
- Reenviar el correu.
- Afegir comentaris al correu.
- Emmagatzemar el correu a la bústia personal (mbox).
- Emmagatzemar el correu en una carpeta que hàgiu creat.
- Crear i mantenir un fitxer d'àlies o un fitxer de distribució, el qual direcciona el correu i els missatges de correu.

La instal•lació de **sendmail** és automàtica.

Per obtenir més informació sobre el programa **mail**, consulteu l'apartat “Funcions del correu” a la pàgina 13.

Gestor de missatges (mh)

El programa **mh** és una recopilació d'ordres que permet dur a terme totes les funcions de processament de correu des de la línia d'ordres.

Aquestes ordres proporcionen una gamma més amplia de funcions que les subordres de **mail**. A més, com que es poden executar en qualsevol moment en què aparegui l'indicador d'ordres, s'obté més potència i flexibilitat a l'hora de crear correu i processar el correu rebut. Per exemple, es pot llegir un missatge de correu, cercar un fitxer o executar un programa a fi de trobar una solució concreta i contestar el missatge, tot això dins el mateix intèrpret d'ordres.

El programa **mh** permet crear, distribuir, rebre, veure, processar i emmagatzemar missatges a través de les següents ordres:

Element	Descripció
ali	Llista àlies de correu i les seves adreces.
anno	Anota missatges.
ap	Analitza i torna a formatar adreces.
burst	Divideix resums en missatges.
comp	Inicia un editor per crear o modificar un missatge.
dist	Redistribueix un missatge a adreces addicionals.
dp	Analitza i torna a formatar dates.
folder	Selecciona i llista carpetes i missatges.
folders	Llista totes les carpetes i els missatges del directori de correu.
forw	Reenvia missatges.
inc	Incorpora el nou correu en una carpeta.
mark	Crea, modifica i mostra seqüències de missatges.
mhl	Genera una llista formatada de missatges.
mhmail	Envia o rep correu.
mhpath	Imprimeix els noms complets del camí d'accés de missatges i de carpetes.
msgchk	Comprova si hi ha missatges nous.
msh	Crea un intèrpret d'ordres de gestor de correu (mh).
next	Mostra el missatge següent.
packf	Comprimeix el contingut d'una carpeta en un fitxer.
pick	Selecciona missatges per contingut i crea i modifica seqüències.
prev	Mostra el missatge anterior.
refile	Desplaça fitxers entre carpetes.
repl	Contesta un missatge.
rmf	Elimina carpetes i els missatges que contenen.
rmm	Elimina missatges de l'estat actiu.
scan	Genera un llistat escanejable que conté un missatge per línia.
send	Envia un missatge.
show	Mostra missatges.
sortm	Classifica missatges.
vmh	Inicia una interfície visual que cal utilitzar amb les ordres **mh**.
whatnow	Inicia una interfície d'indicador per veure un esborrany.
whom	Manipula adreces de l'**mh**.

Per obtenir més informació sobre les ordres **mh**, consulteu la publicació *Commands Reference, Volume 3*.

Ordre bellmail

L'ordre **bellmail** és l'ordre original de correu AT&T UNIX que gestiona el correu dels usuaris d'un mateix sistema i també dels usuaris de sistemes remots als quals es pot accedir mitjançant els BNU (Basic Network Utilities), de vegades anomenats UUCP (UNIX-to-UNIX Copy Program).

Aquests programes donen suport només a xarxes de sistemes connectats per línies de comunicació de marcatge o punt a punt llogades. L'ordre obre un intèrpret d'ordres les subordres de la qual permeten:

- Prendre dades de l'entrada estàndard (escrites en un fitxer existent o redireccionades des d'aquest fitxer), afegir una o més adreces (subministrades com a arguments a la mateixa ordre) i una indicació de l'hora i, tot seguit, afegir una còpia als fitxers de bústia del sistema de cadascun dels destinataris (`/var/spool/mail/`*`ID_usuari`*).
- Llegir elements de correu del fitxer de la bústia del sistema.
- Afegir elements de correu al fitxer de bústia personal (`$HOME/mbox`) o a un fitxer especificat.
- Enviar correu mitjançant els BNU a un usuari d'un altre sistema.
- Redireccionar automàticament tot el correu de la bústia del sistema a una d'un altre sistema mitjançant l'addició d'una sentència *.forward* al començament del fitxer de bústia del sistema.

De tota manera, cal que tingueu certs coneixements d'UNIX abans de poder utilitzar plenament aquest gestor de correu. Per obtenir més informació, consulteu l'ordre **bellmail** ala publicació *Commands Reference, Volume 1*.

Funcions del correu

En aquest apartat s'expliquen les funcions del programa **mail**.

El programa **correu** permet rebre, crear i enviar correu a usuaris d'un sistema local o remot.

Emmagatzematge de correu

El correu s'emmagatzema de diferents maneres, en funció de la situació específica.

Quan s'envia correu a una adreça, aquest correu s'emmagatzema en un directori del sistema que és específic per al correu. Aquest directori del sistema conté un fitxer per a cada usuari del sistema local. Aquest directori conserva el correu fins que se'n fa alguna cosa.

Bústia de sistema:

La bústia del sistema és semblant a una bústia d'una oficina de correus: l'oficina de correus lliura cartes adreçades a la persona a qui pertany aquesta bústia.

De la mateixa manera, la bústia del sistema és un fitxer en el qual es lliuren missatges a un usuari concret. Si aquest fitxer no existeix quan arriba el correu, es crea. Se suprimeix el missatge quan s'han eliminat tots els missatges.

Les bústies del sistema resideixen al directori `/var/spool/mail`. Cada bústia del sistema rep el nom que li assigna l'ID d'usuari que hi està associat. Per exemple, si l'ID d'usuari és `ester`, la bústia del sistema serà:

```
/var/spool/mail/ester
```

Bústia personal per defecte:

La bústia personal és semblant a una cubeta d'una oficina. El correu es deixa a la cubeta després de rebre'l però abans d'haver-lo arxivat.

Cada usuari té una bústia personal. Quan es llegeix correu de la bústia del sistema i si no s'ha marcat per suprimir-lo o per desar-lo en un fitxer, s'enregistra a la bústia personal, `$HOME/mbox` (`$HOME` és el directori d'inici de sessió). El fitxer `mbox` només existeix quan conté un missatge.

Fitxer dead.letter per a missatges incomplets:

Si cal interrompre un missatge que s'està creant per completar altres tasques, el sistema desa els missatges incomplets al fitxer `dead.letter` del directori `$HOME`.

Si el fitxer `dead.letter` no existeix, es crea. Més tard, es podrà editar el fitxer per completar el missatge.

> **Atenció:** No utilitzeu el fitxer `dead.letter` per emmagatzemar missatges. El contingut d'aquest fitxer se sobreescriu cada vegada que s'emet una interrupció per desar un missatge parcial al fitxer `dead.letter`.

Carpetes de correu:

Les carpetes permeten desar missatges de manera organitzada. Gràcies al programa de correu, es pot posar en una carpeta un missatge procedent de la bústia del sistema, d'una bústia personal o d'una altra carpeta.

Cada carpeta és un fitxer de text. Cada carpeta se situa al directori que s'especifiqui al fitxer `.mailrc` amb l'opció **set folder**. Cal crear aquest directori abans d'utilitzar carpetes per emmagatzemar missatges. Quan el directori existeix, el programa de correu crea les carpetes en aquest directori. Si no especifiqueu un directori al fitxer `.mailrc`, les carpetes es creen al directori actual. Consulteu l'apartat "Organització del correu" a la pàgina 19.

> **Nota:** Hi ha molts programes disponibles per enviar i rebre correu, inclosos l'HM (Gestor de missatges) i el programa **bellmail**. El programa que s'utilitzi dependrà del que hi hagi instal•lat i configurat al sistema. Per obtenir informació sobre la configuració del sistema, poseu-vos en contacte amb l'administrador del sistema.

Manipulació i recepció de correu

El programa **mail** permet examinar cada missatge d'una bústia i després suprimir-lo o arxivar-lo en un directori personal de correu.

L'intèrpret d'ordres d'ordres notifica que ha arribat correu. Aquesta notificació apareix abans del següent indicador, sempre que la variable d'entorn **MAIL** estigui establerta i hagi transcorregut l'interval especificat per **MAILCHECK** des de la darrera vegada que l'intèrpret d'ordres hagi comprovat l'arribada de correu. El missatge de notificació és el valor de la variable d'entorn **MAILMSG**. En funció de l'intèrpret d'ordres que s'estigui utilitzant (els intèrprets d'ordress bourne, korn o C), la notificació serà semblant a la següent:

```
TENIU CORREU NOU
```

Inici de la bústia:

Utilitzeu l'ordre **mail** per llegir i eliminar missatges de la bústia de correu.

No utilitzeu la bústia del sistema per emmagatzemar missatges. Emmagatzema missatges a la bústia personal i a les carpetes de correu.

Comprovació del correu a la bústia del sistema:

Utilitzeu l'ordre **mail** per comprovar si hi ha correu a la vostra bústia del sistema.

Escriviu l'ordre **mail** a l'indicador de la línia d'ordres del sistema:

```
mail
```

Si no hi ha correu a la bústia del sistema, el sistema respon amb un missatge:

```
No hi ha correu per El vostre ID
```

Si hi ha correu a la bústia, el sistema mostra una llista dels missatges que hi ha a la bústia del sistema:

```
Correu Escriviu ? per a l'ajuda.
"/usr/mail/lluis": 3 missatges 3 nous
  >N       1 carme dm 27 abr 16:10 12/321 "Reunió departament"
   N       2 laura dm 27 abr 16:50 10/350 "Notícies del sistema"
   N       3 pere  dm 27 abr 17:00 11/356 "Eines disponibles"
```

El missatge actual sempre va precedit d'un signe major que (>). Cada entrada en línia mostra els següents camps:

Element	Descripció
estat	Indica la classe del missatge
número	Identifica la part de correu al programa de correu.
emissor	Identifica l'adreça de la persona que ha enviat el correu.
data	Especifica la data de recepció del missatge.
grandària	Defineix el nombre de línies i caràcters continguts al missatge (la capçalera inclosa).
tema	Identifica el tema del missatge, si en té.

L'estat pot ser un dels següents:

Element	Descripció
N	Un nou missatge.
P	Un missatge que es conservarà a la bústia del sistema.
U	Un missatge no llegit. Es tracta d'un missatge que ha estat llistat a la bústia la darrera vegada que s'ha utilitzat el programa de correu però el contingut del qual no s'ha examinat.
*	Un missatge que ha estat desat o escrit en un fitxer o carpeta.

Un missatge sense indicador d'estat és un missatge que s'ha llegit però que no s'ha suprimit o desat.

Comprovació del correu a la bústia personal o a la carpeta de correu:

Podeu utilitzar l'ordre **mail** per comprovar si hi ha correu a la vostra bústia personal o carpeta de correu.

Es pot utilitzar l'ordre **mail** a l'indicador de la línia d'ordres segons els passos següents:

1. Per tal de visualitzar un llistat dels missatges de la bústia personal, `$HOME/mbox`, escriviu:
   ```
   mail -f
   ```
   Si no hi ha correu a la bústia personal, el sistema respon amb un missatge similar al següent:
   ```
   "/u/jordi/mbox": 0 missatges
   ```
   o
   ```
   Un fitxer o directori del camí d'accés no existeix
   ```
2. Per tal de visualitzar un llistat dels missatges de la carpeta `dept`, escriviu:
   ```
   mail -f +dept
   ```
   Si no hi ha correu a la vostra carpeta de correu, el sistema respon amb un missatge similar al següent:
   ```
   Un fitxer o directori del camí d'accés no existeix
   ```

Opcions de visualització del contingut de la bústia:

Es poden escriure subordres de bústia, des de l'indicador de la bústia, per gestionar-ne el contingut.

`Prerequisits`

1. El programa de correu ha d'estar instal•lat al sistema.
2. S'ha d'iniciar el programa de correu.
3. Cal que hi hagi correu a la bústia.

Grups de missatges:

Utilitzeu la subordre (**h**) per veure un missatge que forma part d'una llista de missatges que heu determinat per tal que no hàgiu d'examinar tots els missatges.

Es pot utilitzar la subordre **h** a l'indicador de la bústia, segons els següents exemples:

Element	Descripció
h	Es mostren aproximadament 20 missatges alhora. El nombre real de missatges que apareix està determinat pel tipus de terminal que s'està utilitzant i per l'opció **set screen** del fitxer `.mailrc`. Si torneu a escriure la subordre **h**, apareix el mateix grup de missatges.
h `21`	Apareix el missatge núm. 21 i els següents, fins a i incloent-hi el missatge núm. 40 (si hi ha aquest nombre de missatges a la bústia). Continueu especificant la subordre **h** amb el subsegüent número de missatge fins que hagin aparegut tots els missatges.
h `1`	Per tornar al primer grup de 20 missatges, escriviu un número de l'1 al 20.

Desplaçament per la bústia:

Utilitzeu la subordre **z** per desplaçar-se per la bústia.

Es pot utilitzar la subordre **z** a l'indicador de la bústia, segons els següents exemples:

Element	Descripció
z	Es mostren aproximadament 20 missatges alhora. El nombre real de missatges que apareix està determinat pel tipus de terminal que s'està utilitzant i per l'opció **set screen** del fitxer `.mailrc`. Torneu a escriure la subordre **z** per desplaçar-vos als 20 missatges següents.
z +	L'argument de signe més (**+**) us desplaça als 20 missatges següents. Apareix el missatge núm. 21 i els següents, fins a i incloent-hi el missatge núm. 40 (si hi ha aquest nombre de missatges a la bústia). Continueu escrivint la subordre **z+** fins que hagin aparegut tots els missatges. El sistema respondrà amb el següent missatge: `A la darrera pantalla de missatges.`
z -	L'argument de signe menys (**-**) us desplaça als 20 missatges anteriors. Quan arribeu al primer conjunt de missatges, el sistema respondrà amb el següent missatge: `A la primera pantalla de missatges.`

Filtrat de missatges amb informació específica:

Es pot utilitzar la subordre **f** a l'indicador de bústia, segons els següents exemples per tal de filtrar missatges en funció de la informació que desitgeu.

Element	Descripció
f	Mostra informació de capçalera del missatge actual.
f `1 4 7`	Mostra informació de capçalera dels missatges específics números 1, 4 i 7.
f `1-10`	Mostra informació de capçalera del grup de missatges de l'1 a 10.
f `*`	Mostra tots els missatges.

f `pau`	Apareixen els missatges, si n'hi ha, procedents de l'usuari `pau`. Els caràcters escrits per a una adreça no cal que coincideixin exactament amb l'adreça. Per tant, la sol•licitud de l'adreça `pau` en majúscules o en minúscules coincideix amb totes les adreces següents:
	`PaU`
	`pau@topdog`
	`hpau`
	`pAu`

f`meet`	Apareixeran els missatges, si n'hi ha, que tinguin el camp **Tema:** els caràcters `reunió`. Els caràcters introduïts per a un patró no cal que coincideixin exactament amb el camp **Tema:**. Cal que només estiguin continguts al camp **Tema:** en majúscules o minúscules. Per tant, la sol•licitud del tema `reunió` coincideix amb tots els temes següents:
	`Reunió de dijous`
	`Tenim una reunió demà`
	`MEET ME IN ST. LOUIS`

Nombres dels missatges actuals:

La subordre **=** mostra els números dels missatges.

Es pot utilitzar la subordre **=** a l'indicador de la bústia segons el següent exemple:

Element	Descripció
=	Apareix el número del missatge actual.

Nombre total de missatge a la bústia:

Utilitzeu la subordre **folder** per comprovar quants missatges hi ha a la bústia.

Es pot utilitzar la subordre **folder** a l'indicador de la bústia, segons el següent exemple:

Element	Descripció
folder	Llista informació sobre la carpeta o bústia. El sistema respondrà amb un missatge semblant al següent: `"/u/lluis/mbox": 29 missatges.`

Opcions de lectura de correu:

Es pot llegir el correu de diverses maneres diferents. En aquest apartat veiem exemples de tots els mètodes.

Trieu el mètode amb el qual us sentiu més còmode i utilitzeu-lo per llegir el correu. Abans d'intentar llegir el correu, assegureu-vos que es compleixen les condicions següents:

1. El programa de correu ha d'estar instal•lat al sistema.
2. S'ha d'iniciar el programa de correu.
3. Cal que hi hagi correu a la bústia.

Lectura de missatges a la bústia:

Utilitzeu la subordre **t** o **p** per llegir els missatges de la vostra bústia.

Es poden utilitzar les subordres **t** o **p** a l'indicador de la bústia, segons els següents exemples:

Element	Descripció
`3`	Si utilitzeu el número del missatge, per defecte, apareixerà el text del missatge.
t	Si utilitzeu la subordre **t**, per defecte, apareixerà el text del missatge actual.
t `3`	Apareix el text del missatge 3.
t `2 4 9`	Apareix el text dels missatges 2, 4 i 9.
t `2-4`	Apareix el text del grup de missatges del 2 al 4.
t	Si utilitzeu la subordre **p**, per defecte, apareixerà el text del missatge actual.
p `3`	Apareix el text del missatge 3.
p `2 4 9`	Apareix el text dels missatges 2, 4 i 9.
p `2-4`	Apareix el text del grup de missatges del 2 al 4.

Lectura del següent missatge de la bústia:

Utilitzeu la subordre **n** per llegir el següent missatge de la vostra bústia.

Podeu utilitzar les subordres (**n**)ext o signe més (+) a l'indicador de la bústia segons el següent exemple:

Element	Descripció
n o **+**	Mostra el text del següent missatge i aquest missatge es converteix en el missatge actual.

També es pot prémer la tecla Intro per fer aparèixer el text del següent missatge.

Lectura del missatge anteror de la bústia:

Utilitzeu la subordre **-** per llegir el missatge anterior.

Es pot utilitzar la subordre **-** a l'indicador de la bústia segons el següent exemple:

Element	Descripció
-	Apareix el text del missatge anterior.

Supressió del correu:

Si es vol suprimir un missatge, es pot suprimir el missatge actual, suprimir un missatge específic o suprimir un grup de missatges.

També es pot suprimir el missatge actual i fer aparèixer el següent missatge mitjançant la combinació de subordres. Assegureu-vos que s'acompleixin les condicions següents:

1. El programa de correu ha d'estar instal•lat al sistema.
2. Cal que hi hagi correu a la bústia.
3. S'ha d'iniciar el programa de correu.

Suprimir missatges:

Utilitzeu els diferents formularis de la subordre **d** per tal de suprimir missatges.

Es pot utilitzar la subordre (**d**)elete a l'indicador de la bústia, segons els següents exemples:

Element	Descripció
d	Se suprimeix el missatge actual.
dp o **dt**	El missatge actual se suprimeix i apareix el següent missatge. Això també es pot acomplir incloent l'opció **set autoprint** al fitxer `.mailrc`, que establirà la subordre **d** perquè funcioni com la combinació de la subordre **dp** o **dt**.
d `4`	Suprimeix el missatge específic 4.
d `4-6`	Suprimeix el grup de missatges del 4 al 6.
d `2 6 8`	Suprimeix els missatges 2, 6 i 8.

Desfer supressió de missatges:

Utilitzeu la subordre **u** per desfer missatges.

Es pot utilitzar la subordre **u** a l'indicador de la bústia, segons els següents exemples:

Element	Descripció
u	Es desfà la supressió del missatge actual.
u 4	Es desfà la supressió del missatge específic 4.
u 4-6	Es desfà la supressió del grup de missatges del 4 al 6.
u 2 6 8	Es desfà la supressió dels missatges 2, 6 i 8.

Sortida del programa de correu:

Assegureu-vos que es donin els requisits següents abans de sortir del programa de correu.

1. El programa de correu ha d'estar instal•lat al sistema.
2. Cal que hi hagi correu a la bústia.
3. S'ha d'iniciar el programa de correu.

Sortir del correu i desar els canvis:

Utilitzeu la subordre **q** per sortir del correu i desar els canvis.

Si sortiu de la bústia del sistema:

Element	Descripció
q	La subordre **q** deixa la bústia del sistema i torna al sistema operatiu. Quan es deixa la bústia, tots els missatges marcats per suprimir-los s'eliminen de la bústia i no es poden recuperar. El programa de correu desa els missatges que es llegeixen a la bústia personal (**mbox**). Si no s'ha llegit cap dels missatges de correu, resten a la bústia del sistema fins que no s'hi realitza alguna acció.

Si sortiu de la bústia personal o de la carpeta de correu:

Element	Descripció
q	Si s'utilitza la subordre **q** de la bústia personal o d'una carpeta de correu, els missatges llegits i no llegits restaran a la bústia personal o en una carpeta de correu fins que no s'hi realitzi alguna acció.

Sortir del correu sense desar els canvis:

Utilitzeu la subordre **x** o **ex** per sortir del correu sense dur a terme els canvis de bústia.

Element	Descripció
x o **ex**	La subordre **x** o **ex** permet deixar la bústia i tornar al sistema operatiu sense canviar el contingut original de la bústia. El programa ignora totes les sol•licituds que s'han fet abans de la sol•licitud **x**; si s'ha desat un missatge en una altra carpeta, es desarà de tota manera.

Organització del correu:

Utilitzeu carpetes per desar missatges de manera organitzada.

Es poden crear tantes carpetes com se'n necessitin. Assigneu a cada carpeta un nom que coincideixi amb el tema dels missatges que conté, de manera semblant a les carpetes de fitxers d'un sistema de fitxers d'oficina. Cada carpeta és un fitxer de text situat al directori que especifiqueu al fitxer `.mailrc` amb l'opció **set folder**. Cal crear aquest directori abans d'utilitzar carpetes per emmagatzemar missatges. Quan el directori existeix, el programa de correu crea les carpetes en aquest directori. Si no especifiqueu un directori amb l'opció **set folder** al fitxer `.mailrc`, la carpeta es crea al directori actual. Gràcies al programa de correu, es pot posar en una carpeta un missatge procedent de la bústia del sistema, d'una bústia personal o d'una altra carpeta.

El contingut d'un missatge es pot afegir a un fitxer o carpeta mitjançant les subordres **s** o **w**. Totes dues subordres afegeixen informació a un fitxer existent o creen un nou fitxer si no existeix. La informació que

es troba al fitxer actualment no es destrueix. Si deseu un missatge de la bústia del sistema en un fitxer o carpeta, el missatge se suprimeix de la bústia del sistema i es transfereix al fitxer o a la carpeta especificada. Si deseu un missatge de la bústia personal o d'una carpeta a un altre fitxer o carpeta, el missatge no se suprimeix de la bústia personal sinó que es copia al fitxer o a la carpeta especificats. Si s'utilitza la subordre **s**, es pot llegir la carpeta com si fos una bústia, perquè els missatges i la informació de capçalera s'afegeixen al final de la carpeta. Si s'utilitza la subordre **w**, es pot llegir la carpeta com si fos un fitxer perquè el missatge s'afegeix sense informació de capçalera al final del fitxer.

Abans d'organitzar el correu, assegureu-vos que es donin els requisits següents:

1. El programa de correu ha d'estar instal•lat al sistema.
2. Cal que hi hagi correu a la bústia del sistema, a la bústia personal o en una carpeta que hàgiu definit.
3. S'ha d'iniciar el programa de correu.

Creació d'un directori de bústia de cartes per emmagatzemar missatges en carpetes:

Els missatges es poden desar en una carpeta del directori de la bústia utilitzant la subordre **set folder**.

Utilitzeu el procediment següent per emmagatzemar missatges en carpetes:

1. Per comprovar si l'opció **set folder** ha estat habilitada al fitxer `.mailrc`, escriviu la subordre següent a l'indicador de la bústia:

   ```
   set
   ```

   La subordre **set** mostra una llista d'opcions de correu habilitades del fitxer `.mailrc`.

   Si l'opció **set folder** ha estat habilitada, el sistema respon amb un missatge semblant al següent:

   ```
   folder /home/jordi/cartes
   ```

   En aquest exemple, `cartes` és el directori en el qual s'emmagatzemaran les carpetes de correu.
2. Si l'opció **set folder** no ha estat habilitada, afegiu una línia similar a la següent al fitxer `.mailrc`:

   ```
   set folder=/home/jordi/cartes
   ```

   En aquest exemple, `/home/jordi` és el directori d'inici d'en Jordi i `cartes` és el directori en el qual s'emmagatzemaran les carpetes de correu. L'opció **set folder** permet utilitzar l'anotació abreujada del signe més (+) a l'indicador de la bústia per desar missatges al directori `cartes`.
3. Cal crear un directori `cartes` al directori d'inici. Escriviu a l'indicador de la línia d'ordres del sistema del directori d'inici:

   ```
   mkdir cartes
   ```

Desar missatges amb capçaleres:

La subordre **s** desa missatges amb capçaleres.

Utilitzeu la subordre **s** segons els següents exemples:

Element	Descripció
s `1-4 notes`	Desa els missatges `1`, `2`, `3` i `4` amb la informació de capçalera a una carpeta anomenada `notes` del directori actual. El programa de correu respondrà amb el següent missatge: `"notes" [Afegit] 62/1610`
s `+admin`	Desa el missatge actual en una carpeta existent anomenada `admin` del vostre directori de carpetes. Si el directori de carpetes es defineix com a `/home/jordi/cartes` al fitxer `.mailrc`, el sistema respon amb: `"/home/jordi/cartes/admin" [Afegit] 14/321`

Element	Descripció
s 6 +admin	Desa el missatge 6 a una carpeta existent anomenada admin del vostre directori de carpetes. Si el directori de carpetes es defineix com a /home/jordi/cartes al fitxer .mailrc, el sistema respon amb: "/home/jordi/cartes/admin" [Afegit] 14/321

Desar missatges sense capçaleres:

Utilitzeu la subordre **w** per desar un missatge com a fitxer en lloc de com a carpeta.

Per llegir o editar un fitxer desat amb la subordre **w**, cal utilitzar l'editor **vi** o algun altre editor de text. A l'indicador de la bústia, podeu utilitzar la subordre **w** segons els exemples següents:

Element	Descripció
w 6 pass	Desa només el text del missatge 6 a un fitxer anomenat pass del directori actual. Si el fitxer pas encara no existeix, el sistema respon amb el següent missatge: "pas" [Nou fitxer] 12/30 Si el fitxer pas existeix, el sistema respon amb el següent missatge: "pas" [Afegit] 12/30
w 1-3 segur	Desa només el text dels missatges específics 1, 2 i 3 a un fitxer anomenat segur al directori actual. El text dels missatges d'aquests exemples s'afegiran un rere l'altre en un fitxer. I el fitxer segur encara no existeix, el sistema respon amb el següent missatge: "segur" [Nou fitxer] 12/30

Determinació de la bústia o carpeta actual:

Utilitzeu la subordre **folder** per tal de determinar la bústia o carpeta actual.

Encara que l'ordre **mail** mostra el nom de la bústia actual quan s'inicia, es pot perdre la pista de la bústia on us trobeu. A l'indicador de la bústia, podeu utilitzar la subordre **folder** segons l'exemple següent:

Element	Descripció
folder	Troba el nom de la bústia o carpeta actuals. Si la bústia actual és /home/lluis/mbox, apareix el següent: /home/lluis/mbox: 2 missatges 1 suprimit Aquest missatge indica que /home/lluis/mbox és la bústia en la qual us trobeu en aquest moment, conté dos missatges i un d'aquests missatges se suprimirà quan acabeu d'utilitzar aquesta bústia.

Canviar a una altra bústia:

Canviar a una altra bústia és com sortir d'una bústia o una carpeta.

Els missatges que hàgiu marcat per suprimir-los se suprimiran quan deixeu aquesta bústia. Els missatges suprimits no es poden recuperar. A l'indicador de la bústia, podeu utilitzar la subordre **file** o **folder** segons els exemples següents:

Element	Descripció

folder +projecte	Un cop s'ha iniciat el programa de correu amb una bústia, utilitzeu les subordres **file** o **folder** per canviar a una altra bústia.
	
	Si canvieu del fitxer mbox a la carpeta mbox i heu suprimit tots els missatges del fitxer mbox, el programa de correu mostra:
	`/home/dee/mbox removed`
	`+projecte: 2 missatges 2 nous`
	
	seguit d'una llista dels missatges de la carpeta projecte.

Creació i enviament de correu

Es pot utilitzar el programa **mail** per crear, enviar, contestar i adreçar missatges a altres usuaris o per enviar fitxers ASCII a altres usuaris.

Un fitxer ASCII pot ser, per exemple, un document que s'ha escrit mitjançant un editor preferit i un fitxer d'origen d'un programa.

Es podem enviar missatges i fitxers a un usuari del sistema local, de la xarxa o a un usuari d'una altra xarxa connectada. No cal que el destinatari estigui connectat al sistema quan envieu la informació. El correu s'envia a una adreça d'usuari.

Adreçament del correu:

El correu s'envia a una adreça d'usuari. L'adreça, que conté el nom d'inici de sessió i el nom del sistema, direcciona el lliurament del missatge de correu.

En general, per enviar un missatge a un altre usuari, cal que escriviu l'ordre **mail** i l'adreça tal com s'indica a continuació:

`mail` *`Usuari@Adreça`*

El format del paràmetre *Adreça* depèn de la ubicació del destinatari. El concepte és semblant al d'enviar una nota a un company de feina. Per enviar una nota a en Joan, que treballa en un petit departament de sis a vuit persones, podeu escriure el nom en un sobre i deixar-lo al sistema de correu de l'oficina. De tota manera, si en Joan és en un altre departament, és probable que calgui especificar més informació al sobre:

```
Joan
Trias
```

Si en Joan es troba en una altra ubicació geogràfica, és probable que necessiteu més informació per assegurar-vos que li arriba el missatge:

```
Joan
Trias
Cerdanyola
```

Per enviar correu electrònicament, utilitzeu una progressió d'adreçament semblant:

Element	Descripció
mail joan	Per enviar correu a un usuari del sistema local, el nom d'inici de sessió és l'única part obligatòria de l'adreça.
mail joan@tybalt	Per enviar correu a un usuari de la xarxa local, escriviu l'adreça (node) completa del sistema.
mail joan@mars.aus.dbm.com	Per enviar correu a un usuari en una altra xarxa connectada, escriviu les adreces completes del sistema i de la xarxa.
mail dept71	Es pot enviar correu a un grup específic de persones utilitzant un àlies o una llista de distribució. Per fer-ho, cal crear un àlies o una llista de distribució al fitxer .mailrc. Si us cal informació sobre la manera d'enviar àlies, consulteu l'apartat "Àlies i llistes de distribució" a la pàgina 38.

Adreçament de correu a més d'un usuari:

Per adreçar correu a més d'un usuari a la vegada, separeu cada nom d'usuari mitjançant un espai.

Per exemple:

```
joan@tybalt susanna@julius gbadia@ophelia
```

Adreçament de correu a usuaris en el sistema local:

Per enviar un missatge a un usuari del sistema local (a algú el nom d'inici de sessió del qual està llistat al fitxer `/etc/passwd`), utilitzeu el nom d'inici de sessió de l'adreça.

Es pot utilitzar l'ordre **mail** a l'indicador de la línia d'ordres del sistema segons el següent exemple:

```
mail nom_inici_sessió
```

Element	Descripció
mail `joan`	Si en Joan és al sistema i té el nom d'inici de sessió `joan`, aquesta ordre activa el programa de correu, permet crear un missatge i mira d'enviar el missatge al nom d'inici de sessió local `joan`. Si el missatge s'ha lliurat satisfactòriament, no es rep cap notificació. Si en Joan no és al sistema, el sistema de correu torna un missatge d'error i torna el missatge no enviat a la bústia del sistema.

Adreçament de correu als usuaris de la xarxa:

Utilitzeu l'ordre **mail** per enviar un missatge a usuaris de la vostra xarxa. Incloeu el nom d'inici de sessió de l'usuari i el nom del sistema a l'adreça.

Per enviar un missatge a través d'una xarxa local a un usuari d'un altre sistema, escriviu:

Element	Descripció
mail *Nom_inici_de_sessió@Nom_sistema*	Per exemple, si en Joan és al sistema `zeus`, utilitzeu la següent ordre per crear un missatge i enviar-l'hi: `mail joan@zeus` Aquesta ordre activa el programa de correu, permet crear un missatge i mira d'enviar el missatge al nom d'inici de sessió `joan` del sistema `zeus`. Si el missatge s'ha lliurat satisfactòriament, es rep l'indicador del sistema sense notificació. Si l'adreça de correu és incorrecta, rebreu un missatge d'error.

> **Nota:** Per enviar un missatge a través d'una xarxa local a un usuari d'un altre sistema, cal que conegueu el nom d'inici de sessió i el nom de l'altre sistema. Per obtenir més informació sobre com visualitzar la informació que identifica els usuaris, consulteu l'apartat "Ordres del sistema de comunicacions" a la pàgina 8.

Adreçament de correu a usuaris d'una xarxa diferent:

Si la xarxa està connectada a altres xarxes, es pot enviar correu als usuaris de les altres xarxes.

Els paràmetres d'adreça difereixen en funció del mode amb què la vostra xarxa i les altres xarxes s'adrecen mútuament i del mode en què estan connectades. En funció de la configuració de la xarxa, porteu a terme una d'aquestes accions:

- Si esteu utilitzant una base de dades de noms i adreces central, utilitzeu l'ordre **mail** que apareix a l'exemple següent:

  mail *Nom_inici_de_sessió@Nom_sistema*

  Si les xarxes utilitzen una base de dades central de noms, no cal informació addicional per enviar correu als usuaris de les xarxes connectades. Utilitzeu el mateix format d'adreçament que per als usuaris de la xarxa local.

Aquest tipus d'adreçament funciona bé quan la naturalesa de la xarxa permet el manteniment d'una base de dades central de noms.

- Si la vostra xarxa fa servir l'adreçament de noms de domini, utilitzeu l'ordre **mail** que es mostra a l'exemple següent:

  mail *nom_inici_sessió@nom_sistema.nom_domini*

  Per a les xarxes que exploren grans xarxes no relacionades a ubicacions esteses no és possible una base de dades central de noms. El paràmetre *nom_domini* defineix la xarxa remota, relativa a la xarxa local, dins l'estructura definida per al grup més gran de xarxes interconnectades.

  Per exemple, si escriviu l'ordre següent:

  ```
  mail begonya@merlin.odin.valryanl
  ```

  el correu s'envia a l'usuari `begonya` del sistema `merlin`, que es troba en una xarxa local anomenada `odin` que està connectada a una segona xarxa el domini de la qual s'anomena `valryanl`.

Adreces de correu a través d'un enllaç BNU o UUCP:

Podeu enviar missatges a usuaris d'un altre sistema a través d'un enllaç BNU (Basic Networking Utilities - Programes d'utilitat bàsics de la xarxa) o UUCP (UNIX-to-UNIX Copy Program - Programa de còpia UNIX a UNIX).

Per enviar un missatge a un usuari d'un altre sistema connectat al vostre sistema mitjançant el BNU o una altra versió de l'UUCP, cal que sapigueu:

- El nom d'inici de sessió
- El nom de l'altre sistema
- El camí físic a aquest altre sistema

La persona responsable de connectar el sistema a altres sistemes ha de poder facilitar informació d'encaminament per adreçar l'altre sistema.

Si el sistema té un enllaç BNU o UUCP: utilitzeu l'ordre **mail** a l'indicador de línies d'ordre del sistema, segons els següents exemples:

Element	Descripció
mail *camí_UUCP*!*nom_inici_sessió*	Si el sistema local té una connexió dels BNU o d'UUCP que es pot utilitzar per arribar al sistema remot, utilitzeu el format d'aquest exemple per adreçar un missatge. La variable *nom_inici_sessió* és el nom d'inici de sessió del sistema remot per al destinatari del missatge. La variable *camí_UUCP* descriu el camí físic que el missatge ha de seguir al llarg de la xarxa UUCP. Si el vostre sistema està connectat al sistema remot sense cap sistema UUCP intermedi, aquesta variable és el nom del sistema remot.
mail`arthur!lancelot!merlin!quim`	Si el missatge ha de viatjar a través d'un o més sistemes UUCP intermedis abans d'arribar al sistema remot desitjat, aquesta variable és una llista de cadascun dels sistemes intermedis. La llista s'inicia amb el sistema més proper i continua fins al sistema més llunyà, separats per un signe d'exclamació (!). Es pot seguir aquest exemple, si el missatge ha de viatjar a través dels sistemes `artur` i `lancelot` (en aquest ordre) abans d'arribar a `merlin`.
mail `merlin!quim`	Si el sistema local té un enllaç UUCP amb un sistema anomenat `merlin` i no hi ha cap altre sistema UUCP entre el vostre sistema i `merlin`, es pot enviar un missatge a `quim` d'aquest sistema.

Si l'enllaç dels BNU o d'UUCP és en un altre sistema: en un entorn de xarxa d'àrea local o àmplia, és probable que un dels sistemes de la xarxa tingui un BNU o un altre tipus de connexió UUCP amb un sistema remot. Es pot utilitzar aquesta connexió UUCP per enviar un missatge a un usuari d'aquest sistema UUCP. Podeu utilitzar l'ordre **mail** a l'indicador de la línia d'ordres del sistema segons el següent exemple:

mail @artur:merlin!quim
Envia correu a quim del sistema UUCP merlin des del sistema d'Internet artur. El delimitador @ serveix per a l'adreçament d'Internet, el delimitador ! serveix per a l'adreçament d'UUCP i el delimitador : connecta les dues adreces. Tingueu en compte que en aquest format no s'envia correu a un usuari d'un dels sistemes intermedis, de manera que cap nom d'inici de sessió no precedeix l'@ a l'adreça de domini.

mail @artur:odin!acct.dept!begonya
Envia correu a begonya del sistema UUCP acct.dept a través del sistema odin des del sistema d'Internet artur.

mail@odin.uucp:@dept1.UUCP:@dept2:pere@dept3
Envia correu a pere@dept3 a través dels enllaços UUCP odin i dept1 i, a continuació, a través de l'enllaç de la xarxa local entre els sistemes dept2 i dept3. El fitxer /etc/sendmail.cf s'ha d'anotació d'adreça UUCP. Consulteu l'administrador del sistema per obtenir-ne informació.

Si s'envia correu sovint a usuaris d'altres xarxes, la creació d'àlies que incloguin adreces d'usuaris pot estalviar temps. Consulteu l'apartat "Àlies i llistes de distribució" a la pàgina 38.

Inici de l'editor de correu:

El programa **mail** proporciona un editor orientat a línies per crear missatges.

1. El programa de correu ha d'estar instal•lat al sistema.
2. S'ha d'iniciar el programa de correu.

Aquest editor permet escriure cada línia del missatge, prémer la tecla Intro per obtenir una nova línia i escriure més text. No podeu canviar una línia un cop hagueu fet clic a la tecla Intro. De tota manera, abans de prémer la tecla Intro, podeu canviar la informació d'aquesta línia utilitzant les tecles Retrocés i Suprimir per esborrar. També podeu utilitzar les subordres d'editor de correu per especificar un editor a pantalla completa i canviar el missatge.

Quan es crea correu amb l'editor de correu, el sistema completa els camps **data:** i **de:** automàticament. Teniu l'opció de completar els camps **tema:** i **cc:**. Aquests camps són semblants al cos d'una carta comercial estàndard.

L'editor de correu inclou moltes subordres de control que permeten dur a terme altres operacions en un missatge. Cal que escriviu cadascuna d'aquestes subordres en una nova línia i que comenci amb el caràcter d'*escapament*. Per defecte, el caràcter d'escapament és una titlla (~). Podeu canviar-lo per qualsevol altre caràcter incloent l'opció **set escape** al fitxer .mailrc.

Es pot utilitzar l'ordre **mail** a l'indicador de la línia d'ordres del sistema, segons els següents exemples:

Element	Descripció
mail *Usuari@Adreça*	Executeu aquesta ordre des de l'indicador de la línia d'ordres. El missatge s'adreça a *Usuari@Adreça*. El paràmetre *Adreça* depèn de la ubicació del destinatari.
m*Usuari@Adreça*	Executeu aquesta subordre des de l'indicador de la bústia. El missatge s'adreça a *Usuari@Adreça*. El paràmetre *Adreça* depèn de la ubicació del destinatari.

L'editor de correu també s'activa, si utilitzeu les subordres **R** o **r** per respondre un missatge. Per obtenir més informació sobre la manera de respondre un missatge, consulteu l'apartat "Enviament del correu" a la pàgina 30 i "Resposta del correu" a la pàgina 31.

Edició de missatges:

Dins la bústia, podeu afegir informació a un missatge existent escrivint la subordre (**e**)dit o (**v**)isual a l'indicador de la bústia.

Dins l'editor de correu, no es pot canviar la informació d'una línia un cop s'ha fet clic a la tecla Intro i heu anat a la línia següent. Es pot canviar el contingut del missatge abans d'enviar-lo mitjançant l'edició del missatge amb un altre editor.

Abans d'editar un missatge en un altre editor, assegureu-vos que es compleixen les condicions següents:

1. El programa de correu ha d'estar instal•lat al sistema.
2. L'editor alternatiu ha d'estar definit al fitxer `.mailrc` amb:

   `set EDITOR=`*`Nom_via_accés`*

   Això defineix l'editor que activeu amb la subordre **~e**. El valor de *nom_via_accés* ha de ser el nom de camí d'accés sencer del programa editor que voleu utilitzar. Per exemple, la definició `set EDITOR=/usr/bin/vi` defineix l'editor **vi** perquè s'utilitzi amb la subordre **~e**.
3. Per afegir informació a un missatge de la bústia, cal que s'hagi iniciat l'ordre **mail** per llegir correu a la bústia del sistema, a una altra bústia o a una carpeta.
4. Per iniciar un editor alternatiu mentre es crea un missatge, cal que estigueu a l'indicador de l'editor de correu.

Afegir informació a un missatge específic de la bústia:

Per afegir informació a un missatge de la bústia, escriviu la subordre (**e**) o la subordre (**v**), seguida del número del missatge.

Es poden utilitzar les subordres **e** o **v** a l'indicador de la bústia, segons els següents exemples:

Element	Descripció
e 13	Per afegir una nota al missatge 13 mitjançant l'editor **e** (o qualsevol altre editor que estigui definit al fitxer `.mailrc`).
v 15	Per afegir una nota al missatge 15 mitjançant l'editor **vi** (o qualsevol altre editor que estigui definit al fitxer `.mailrc`).

Si no especifiqueu un número de missatge, l'ordre **mail** activa l'editor mitjançant el missatge actual. Quan deixeu l'editor, torneu a l'indicador de la bústia per continuar processant els missatges a la bústia.

Canvi del missatge actual dins l'editor de correu:

Al començament d'una línia dins l'editor de correu, podeu utilitzar la subordre **~e** o la subordre **~v**, segons els següents exemples.

Element	Descripció
~e	Activa l'editor **e** o un altre editor que es defineixi al fitxer `.mailrc`.
~v	Activa l'editor **vi** o un altre editor que es defineix al fitxer `.mailrc`.

Això permet editar el text del missatge actual. Quan deixeu l'editor diferent, torneu a l'editor de correu.

Visualització de línies d'un missatge dins l'editor de correu:

Utilitzeu la subordre **~p** per visualitzar les línies del missatge dins l'editor de correu.

1. El programa de correu ha d'estar instal•lat al sistema.
2. Per veure un missatge dins l'editor de correu, cal que s'hagi iniciat l'editor de correu. Si us cal obtenir-ne informació, consulteu l'apartat "Inici de l'editor de correu" a la pàgina 25.

Al començament d'una línia dins l'editor de correu, utilitzeu la subordre **~p** segons el següent exemple:

Element	Descripció
~p	L'editor mostra el contingut del missatge, incloent-hi la informació de capçalera del missatge. El text es desplaça cap a dalt des de la part inferior de la pantalla. El final del missatge va seguit per l'indicador (`Continuar`) de l'editor de correu.

Si el missatge és més gran que una pantalla i no s'ha establert la grandària de la pàgina del terminal mitjançant l'ordre **stty**, el text surt de la pantalla fins que s'acaba. Per veure el contingut de textos grans, utilitzeu les subordres de l'editor de correu per veure el missatge amb un altre editor. Si us cal obtenir-ne informació, consulteu l'apartat "Edició de missatges" a la pàgina 25.

Sortir de l'editor de correu:

Per sortir de l'editor de correu sense enviar el missatge, utilitzeu la subordre **~q** o la seqüència de tecles d'interrupció (normalment les seqüències Alt-Pausa o Control-C).

1. El programa de correu ha d'estar instal•lat al sistema.
2. Per veure un missatge dins l'editor de correu, cal que s'hagi iniciat l'editor de correu. Si us cal obtenir-ne informació, consulteu l'apartat "Inici de l'editor de correu" a la pàgina 25.

Si heu escrit text, l'ordre **mail** desa el missatge al fitxer `dead.letter`.

Al començament d'una línia dins l'editor de correu, podeu utilitzar la subordre **~q** segons el següent exemple:

Element	Descripció
~q	Surt de l'editor de correu i no s'envia el missatge. El missatge es desa al fitxer `dead.letter` del directori d'inici, excepte si no s'ha escrit cap text. Apareix l'indicador del sistema.

Control-C	Per sortir de l'editor mitjançant una seqüència de tecles d'interrupció, feu clic a la seqüència de trencament (seqüència de tecles Control-C) o la seqüència d'interrupció (seqüència de tecles Alt-Pausa). Apareix el següent missatge:
	`(Interrupció -- una més per eliminar la carta)`
	
	Torneu a prémer les seqüències de trencament o d'interrupció:
	`(Darrera interrupció -- carta desada a dead.letter)`
	
	El missatge no s'envia. El missatge es desa al fitxer `dead.letter` del directori d'inici, excepte si no s'ha escrit cap text. Apareix l'indicador del sistema.

Nota: Quan se surt de l'editor de correu sense enviar el missatge, el contingut anterior del fitxer `dead.letter` se substitueix pel missatge incomplet. Per recuperar el fitxer, consulteu l'apartat "Opcions per afegir un fitxer i un missatge específic dins un misstge".

Opcions per afegir un fitxer i un missatge específic dins un misstge:

Cal que es donin tota una sèrie de requisits abans d'afegir un fitxer i un missatge específic dins un missatge de correu.

Prerequisits

1. El programa de correu ha d'estar instal•lat al sistema.
2. Cal que sapigueu el nom i l'adreça del destinatari del correu.
3. S'ha d'iniciar l'editor de correu.

Inclusió de fitxers en un missatge:

Utilitzeu la subordre **~r** per afegir fitxers a un missatge.

Al començament d'una línia dins l'editor de correu, podeu utilitzar la subordre **~r** segons el següent exemple:

Element	Descripció
~r `horari`	On `horari` és el nom del fitxer que es vol incloure. En aquest exemple, la informació del fitxer `horari` està inclosa al final actual del missatge que s'està escrivint.

Inclusió d'un missatge específic dins un missatge:

Utilitzeu la subordre **~f** o **~m** per tal d'incloure un missatge específic dins el missatge.

Al començament d'una nova línia dins l'editor de correu, podeu utilitzar les subordres **~f** o **~m**, segons els següents exemples:

Element	Descripció
~f *`llista_missatges`*	Afegeix el missatge o missatges indicats al final del missatge actual, però *no* sagna el missatge afegit. Utilitzeu aquesta subordre per afegir missatges per consultar quins marges són massa amples per incorporar-los amb la subordre **~m**. **Nota:** El paràmetre *llista_missatges* és una llista d'enters que es refereix a números de missatges vàlids de la bústia o carpeta que està gestionant el correu. També podeu introduir grups simples de números. Per exemple: **~f 1-4** Afegeix els missatges 1, 2, 3 i 4 al final del missatge que s'està escrivint. Aquests missatges s'alineen amb el marge esquerre (no sagnat).
~m `2`	Afegeix el missatge indicat al final del missatge actual. El missatge inclòs se sagna un tabulador des del marge esquerre normal del missatge. En aquest exemple, el missatge 2 s'afegeix al missatge actual.
~m `1 3`	Afegeix el missatge 1 i, a continuació, el missatge 3 al final del missatge que s'està escrivint, sagnant un tabulador des del marge esquerre.

Addició el contingut del fitxer dead.letter al missatge actual:

Utilitzeu la subordre **~d** per afegir contingut del tipus `dead.letter` al vostre missatge.

Al començament d'una nova línia dins l'editor de correu, podeu utilitzar la subordre **~d** segons el següent exemple:

Element	Descripció
~d	Recupera i afegeix el contingut del fitxer `dead.letter` al final del missatge actual. A l'indicador (`Continuar`), podeu seguir incorporant informació al missatge o podeu enviar-lo.

Edició de la informació de capçalera:

La capçalera d'un missatge conté informació d'encaminament i una breu frase sobre el tema. Cal especificar, si més no, un destinatari del missatge.

1. El programa de correu ha d'estar instal•lat al sistema.
2. Inicieu l'editor de correu i comenceu a editar un missatge. Per obtenir més informació, consulteu l'apartat Inici de l'editor de correu.

La resta de la informació de la capçalera no és obligatòria. La informació de la capçalera pot incloure el següent:

Element	Descripció
Per a:	Conté l'adreça o adreces per enviar el missatge.
Tema:	Conté un breu resum de l'assumpte del missatge.
Cc:	Conté l'adreça o adreces dels destinataris a qui es vol enviar còpia del missatge. El contingut d'aquest camp és part del missatge enviat a tots els qui reben el missatge.
Bcc:	Conté l'adreça o adreces dels destinataris a qui es vol enviar una còpia *oculta* del missatge. Aquest camp *no* s'inclou com a part del missatge enviat a tots els qui reben el missatge.

Es pot personalitzar el programa de correu perquè demani automàticament la informació d'aquests camps col•locant entrades al fitxer `.mailrc`. Per obtenir més informació, consulteu l'apartat "Opcions de personalització del programa de correu" a la pàgina 35.

Establir o tornar a establir el camp Tema::

Utilitzeu la subordre **~s** per establir el camp **Tema:** en una frase o oració completa.

Si utilitzeu aquesta subordre se substitueix el contingut anterior (si n'hi ha) del camp **Tema:**. Al començament d'una nova línia dins l'editor de correu, podeu utilitzar la subordre **~s** segons el següent exemple:

Element	Descripció

`~s Excursió de pesca`	Això canvia el camp **Tema:** actual:
	`Tema: Vacances`
	
	Pel següent:
	`Tema: Excursió de pesca`
	Nota: No es pot afegir res al camp **Tema:** amb aquesta subordre. Utilitzeu la subordre **~h**, com es descriu a l'apartat "Edició de la informació de capçalera" a la pàgina 28.

Addició d'usuaris als camps Per a:, Cc:, i Bcc::

Utilitzeu la subordre **~t**, **~c** o **~b** per afegir usuaris als camps de capçalera.

Al començament d'una nova línia dins l'editor de correu, podeu utilitzar les subordres **~t**, **~c** , o **~b**, segons els següents exemples:

Element	Descripció

`~t leo@austin xavi@gtwn`	Això canvia el camp **Per a:** actual:
	`Per a: marc@austin`
	
	per la següent:
	`Per a: marc@austin leo@austin xavi@gtwn`

`~c leo@austin xavi@gtwn`	Això canvia el camp **Cc:** actual:
	`Cc: marc@austin carles`
	
	per la següent:
	`Cc: marc@austin carles leo@austin xavi@gtwn`

`~b leo@austin xavi@gtwn`	Això canvia el camp **Bcc:** actual:
	`Bcc: marc@austin`
	
	per la següent:
	`Bcc: marc@austin leo@austin xavi@gtwn`

Nota: No es poden utilitzar les subordres **~t**, **~c**, o **~b** per canviar o suprimir el contingut dels camps **Per a:**, **Cc:** i **Bcc:**. Utilitzeu la subordre **~h**, com es descriu a l'apartat "Edició de la informació de capçalera" a la pàgina 28.

Donar nou format a un missatge dins l'editor de correu:

Després d'escriure el missatge i abans d'enviar-lo, podeu tornar a formatar el missatge per millorar-ne l'aspecte mitjançant el programa d'intèrpret d'ordres **fmt**.

Abans de tornar a formatar un missatge, assegureu-vos que es compleixen les condicions següents:

1. El programa de correu ha d'estar instal•lat al sistema.
2. Cal que l'ordre **fmt** estigui instal•lada al sistema.

Al començament d'una nova línia dins l'editor de correu, es pot utilitzar l'ordre **fmt** segons el següent exemple:

Element	Descripció
~| fmt	Canvia l'aspecte del missatge ajustant la informació de cada paràgraf dins dels marges definits (cal que cada paràgraf estigui separat per una línia en blanc). La subordre de barra vertical (|) condueix el missatge a l'entrada estàndard de l'ordre i substitueix el missatge per la sortida estàndard d'aquesta ordre.

Atenció: No utilitzeu l'ordre **fmt** si el missatge conté missatges incrustats o informació preformatada de fitxers externs. L'ordre **fmt** torna a formatar la informació de capçalera dels missatges incrustats i és probable que canviï el format de la informació preformatada. Utilitzeu, en lloc d'aquesta ordre, la subordre **~e** o **~v** per escriure en un editor de pantalla completa i tornar a formatar el missatge.

Comprovar l'ortografia dins l'editor de correu:

L'ordre **spell** comprova l'ortografia del missatge.

Abans de comprovar si hi ha faltes d'ortografia en un missatge, assegureu-vos que es compleixen les condicions següents:

1. El programa de correu ha d'estar instal•lat al sistema.
2. Els programes de formatatge de text han d'estar instal•lats al sistema.

Utilitzeu l'ordre **spell** per comprovar si hi ha paraules mal escrites al missatge, des de l'editor de correu:

1. Escriviu el missatge en un fitxer temporal. Per exemple, per escriure el missatge al fitxer `checkit`, escriviu:

   ```
   ~w checkit
   ```

2. Executeu l'ordre **spell** mitjançant el fitxer temporal com a entrada. Escriviu:

   ```
   ~! spell checkit
   ```

   En aquest exemple, el signe d'exclamació (!) és la subordre que inicia un intèrpret d'ordres, executa una ordre i la torna a la bústia. L'ordre **spell** respon amb una llista de paraules que no es troben a la seva llista de paraules conegudes, seguida d'un signe d'exclamació (!) per indicar-vos que heu tornat al programa de correu.
3. Examineu la llista de paraules. Determineu si us cal utilitzar un editor per efectuar correccions.
4. Escriviu el següent per suprimir el fitxer temporal:

   ```
   ~! rm checkit
   ```

Enviament del correu:

Utilitzeu aquest procediment per enviar un missatge després de crear-lo.

- El programa de correu ha d'estar instal•lat al sistema.
- Cal que sapigueu el nom i l'adreça del destinatari del correu.

1. Escriviu l'ordre **mail** a la línia d'ordres, seguida del nom i de l'adreça del destinatari (o destinataris) del missatge. Per exemple:

```
>mail jan@prat
```

El sistema respon amb:

```
Tema:
```

2. Escriviu el tema del missatge. Per exemple:

```
Tema: Reunió Dept.
```

i feu clic a Intro. Ara podeu escriure el cos del text.

3. Escriviu el missatge. Per exemple:

```
Hi haurà una petita reunió del departament aquesta tarda
al meu despatx. No hi faltis.
```

4. Per enviar un missatge que heu escrit amb l'editor de correu, feu clic al caràcter de final de text, que normalment és la seqüència de tecles Control-D o un punt (**.**), mentre sigueu al començament d'una nova línia dins el missatge.

   El sistema mostra el camp **Cc:**:

```
Cc:
```

5. Escriviu els noms i les adreces dels usuaris que han de rebre còpies del missatge. Per exemple:

```
Cc: ester@palau claudi@creus
```

   Nota: Si no voleu enviar còpies, feu clic a Intro sense escriure res.

Quan feu clic a la tecla Intro, el missatge es lliura a l'adreça especificada.

Nota: Si escriviu una adreça que el sistema no coneix o que no s'ha definit en una llista d'àlies o de distribució, el sistema respon amb el nom d'inici de sessió seguit per un missatge d'error: `[ID d'usuari]... Usuari desconegut`

Resposta del correu:

A l'indicador de la bústia es poden utilitzar les subordres **r** i **R**, segons els següents exemples.

1. El programa de correu ha d'estar instal•lat al sistema.
2. Cal que hi hagi correu a la bústia.

Element	Descripció
r	Crea un nou missatge que està adreçat a l'emissor del missatge seleccionat i una còpia del qual s'enviï a les persones que apareixen a la llista **Cc:** (si n'hi ha). El camp **Tema:** del nou missatge fa referència al missatge seleccionat. El valor per defecte de la subordre **r** és el missatge actual. Aquest valor per defecte es pot alterar temporalment escrivint el número del missatge després de la **r**.
R	Inicia una resposta només per a l'emissor del missatge. El valor per defecte de la subordre **R** és el missatge actual.

R 4	Inicia una resposta només per a l'emissor del missatge. Podeu alterar temporalment el missatge actual escrivint el número de missatge després de la **R**. En aquest exemple s'inicia una resposta al missatge 4. El sistema respon amb un missatge semblant al següent:
	`Per a: marta@prats`
	`Tema: Re: Reunió Departament`
	
	A continuació, podeu escriure la vostra resposta:
	`Hi seré.`
	
	Quan hàgiu acabat d'escriure el missatge, premeu el punt (**.**) o la seqüència de tecles Control-D per enviar el missatge. Després d'enviar la contestació, torneu a l'indicador de la bústia.

Creació d'un nou missatge dins la bústia:

A l'indicador de la bústia podeu utilitzar la subordre **m** tal com s'indica a l'exemple següent per crear missatges nous.

Element	Descripció
m *Adreça*	El paràmetre *Adreça* és qualsevol adreça d'usuari correcta. Aquesta subordre inicia l'editor de correu i permet crear un nou missatge dins la bústia. Quan s'envia el missatge, tornareu a l'indicador de la bústia.

Reenviament del correu:

Mentre llegiu el correu, és probable que vulgueu reenviar una nota específica a un altre usuari.

1. El programa de correu ha d'estar instal•lat al sistema.
2. Si s'està reenviant un missatge seleccionat, inicieu el recurs de correu amb l'ordre **mail**. Preneu nota del número del missatge de correu que voleu reenviar.

Aquesta tasca es pot acomplir mitjançant les subordres **~f** i **~m**.

Si heu de sortir de la vostra adrea de xarxa habitual, podeu fer que el vostre correu el rebeu a una altra adreça de xarxa si creeu el fitxer `.forward`. Consulteu l'apartat “Fitxers .forward” a la pàgina 33. La nova adreça pot ser qualsevol adreça de correu vàlida de la vostra xarxa o d'una xarxa connectada a la vostra. Pot ser l'adreça d'un company de feina que gestioni els vostres missatges mentre sou fora. Si decidiu reenviar el vostre correu de xarxa, no rebeu còpia del correu que entra a la vostra bústia. Tot el correu es reenvia directament a l'adreça o adreces que heu especificat.

Reenviament de missatges seleccionats des de la bústia:

Utilitzeu aquest procediment per tornar a enviar missatges específics de correu dins la mateixa bústia.

Per tornar a enviar missatges de correu específics:

1. Creeu un nou missatge mitjançant la subordre **m** i especifiqueu un destinatari escrivint el següent a l'indicador de la bústia:

   ```
   m Usuari@Sistema_Principal
   ```

   en què *Usuari* es refereix al nom d'inici de sessió d'un altre usuari i *Sistema_Principal* és el nom del sistema de l'usuari. Si l'usuari és al vostre sistema, podeu ometre la part `@Sistema_Principal` de l'adreça.
2. Escriviu un nom de tema a l'indicador **Tema:**.
3. Per especificar el número del missatge de correu que voleu reenviar, escriviu:

   ```
   ~f número_missatge
   ```

   O

   ```
   ~m número_missatge
   ```

   número_missatge identifica el missatge de correu que cal enviar.

   L'ordre **mail** mostra un missatge semblant al següent:

   ```
   Interpolant: 1
   (continuar)
   ```
4. Per sortir del missatge, escriviu un punt (`.`) en una línia en blanc. A l'indicador **Cc:**, escriviu tots els noms de les persones a les quals desitgeu reenviar un missatge de correu.

Reenviament de tot el correu:

Utilitzeu aquest procediment per tornar a enviar el vostre correu a una altra persona.

Per tornar a enviar tot el vostre correu a una altra persona:

1. Escriviu l'ordre **cd** sense paràmetres per assegurar-vos que sou al vostre directori d'inici. Per exemple, escriviu el següent per al nom d'inici de sessió `marta`:

```
cd
pwd
```

El sistema respon amb:

```
/home/marta
```

2. Creeu un fitxer `.forward` al vostre directori d'inici. Consulteu l'apartat "Fitxers .forward".

   Nota: No rebreu cap correu fins que no suprimiu el fitxer `.forward`.

Fitxers .forward:

El fitxer `.forward` conté l'adreça o adreces de xarxa que rebrà el correu de xarxa reenviat.

Les adreces han de tenir el format *Usuari@Sistema_Principal*. *Usuari* es refereix al nom d'inici de sessió d'un altre usuari i *Sistema_principal* és el nom del sistema de l'usuari. Si l'usuari és al vostre sistema, podeu ometre la part `@Sistema_Principal` de l'adreça. L'ordre **cat** es pot utilitzar per crear un fitxer `.forward` de la manera següent:

```
cat > .forward
marc
pep@saturn
[END OF FILE]
```

`[END OF FILE]` representa el caràcter de final de fitxer, que és la seqüència Control-D a la majoria de terminals. Cal que escriviu això en una línia en blanc.

El fitxer `.forward` conté les adreces dels usuaris a qui voleu reenviar el vostre correu. El vostre correu es reenviarà a `marc` del vostre sistema local i a `pep` del sistema `saturn`.

Aquest fitxer ha de contenir adreces vàlides. Si és un fitxer nul (longitud zero), el vostre correu no es reenvia i s'emmagatzema a la bústia.

Nota: No rebreu cap correu fins que no suprimiu el fitxer `.forward`.

Anul•lació del correu tornat a enviar:

Per deixar de reenviar correu, esborreu el fitxer `.forward` tal com s'indica a continuació.

Utilitzeu l'ordre **rm** per eliminar el fitxer `.forward` del directori d'inici:

```
rm .forward
```

Enviament d'una nota de missatge de vacances:

Utilitzeu aquest procediment per preparar i enviar un avís de missatge de vacances.

El programa de correu ha d'estar instal•lat al sistema.

1. Per inicialitzar el missatge de vacances, escriviu al vostre directori `$HOME` (inici de sessió):

   ```
   vacation -I
   ```

   Això crea un fitxer `.vacation.dir` i un fitxer `.vacation.pag` en què es conserven els noms de les persones que envien missatges.

2. Modifiqueu el fitxer `.forward`. Per exemple, `eva` escriu la següent sentència al fitxer `.forward`:

   ```
   eva, |"/usr/bin/vacation eva"
   ```

   La primera entrada `eva` és el nom d'usuari al qual es reenvia el correu. La segona entrada `eva` és el nom d'usuari de l'emissor del missatge de vacances. L'emissor del missatge de correu rep un missatge de vacances d'`eva` cada setmana, sense tenir en compte quants missatges s'envien a `eva` des de

l'emissor. Si heu fet que alguna altra persona reenviï el vostre correu, el missatge de correu de l'emissor es reenvia a la persona que s'especifica al fitxer `.forward`.

Utilitzeu el senyalador **-f** per canviar els intervals de freqüència amb què s'envia el missatge. Per exemple, `eva` escriu la següent sentència al fitxer `.forward`:

```
eva, |"/usr/bin/vacation -f10d eva"
```

L'emissor dels missatges de correu rep un missatge de vacances d'`eva` cada deu dies, sense tenir en compte quants missatges s'envien a `eva` des de l'emissor.

3. Per enviar un missatges a cada persona que us enviï correu, creeu el fitxer `$HOME/.vacation.msg` i el vostre missatge en aquest fitxer. Aquest és un exemple de missatge de vacances:

```
De: eva@odin.austin (Eva Sala)
Tema: Estic de vacances.
Estic de vacances fins a l'1 d'octubre. Si hi ha res d'urgent,
poseu-vos en contacte amb en Ramon Duran <ramon@zeus.valhalla>.
  --eva
```

L'emissor rep el missatge que hi ha al fitxer `$HOME/.vacation.msg` o, si el fitxer no existeix, l'emissor rep el missatge per defecte que es trobi al fitxer `/usr/share/lib/vacation.def`. Si no existeix cap dels dos, no s'envia cap resposta automàtica a l'emissor del missatge de correu i no es genera cap missatge d'error.

Per anul•lar el missatge de vacances, elimineu el fitxer `.forward`, el fitxer `.vacation.dir`, el fitxer `.vacation.pag` i el fitxer `.vacation.msg` del directori `$HOME` (inici de sessió) tal com s'indica a continuació:

```
rm .forward .vacation.dir .vacation.pag .vacation.msg
```

Enviament i recepció de correu confidencial:

Per enviar correu confidencial, a l'indicador de la línia d'ordres, utilitzeu l'ordre **xsend** de la manera que s'indica a l'exemple següent.

1. El programa de correu ha d'estar instal•lat al sistema.
2. S'ha d'haver establert una paraula clau mitjançant l'ordre **enroll**.

Element	Descripció
xsend `francesc`	En aquest exemple, el correu confidencial s'està adreçant al nom d'inici de sessió `francesc`. Si feu clic a Intro, s'utilitza un editor de línia única per escriure el text del missatge. Quan hàgiu acabat d'escriure el missatge, premeu la seqüència de tecles Control-D o un punt (.) per sortir de l'editor de correu i enviar el missatge. L'ordre **xsend** xifra el missatge abans d'enviar-lo.

1. Per rebre correu confidencial, a l'indicador de la línia d'ordres, escriviu:

```
mail
```

El sistema mostra la llista de missatges de la bústia del sistema. El programa de correu confidencial us envia una notificació que heu rebut correu confidencial. La línia del missatge serà semblant a la següent:

```
Correu [5.2 UCB] Escriviu ? per a l'ajuda.
"/usr/spool/mail/elena": 4 missatges 4 nous
>N 1 robert dm 14 abr 15:23 4/182 "correu confidencial de robert@Zeus"
```

El text del missatge us fa llegir el correu confidencial al vostre amfitrió mitjançant l'ordre **xget**.

2. A l'indicador de la línia d'ordres, escriviu:

```
xget
```

Se us sol•licita la paraula clau que s'ha establert anteriorment mitjançant l'ordre **enroll**. Després d'escriure la paraula clau, apareixerà l'indicador d'ordres **xget** seguit d'una llista de tot el correu confidencial. El programa de correu s'utilitza per mostrar tot el correu confidencial. Heu d'escriure la subordre **q** si voleu deixar els missatges llegits i no llegits de la bústia de correu confidencial i evitar que l'ordre **xget** suprimeixi els missatges.

Información d'ajuda de correu

Es pot obtenir informació d'ajuda sobre com utilitzar el programa de correu mitjançant les ordres **?**, **man**, o **info**.

Element	Descripció
Per obtenir ajuda a la bústia	Escriviu `?` o `help` a l'indicador de la bústia. Les subordres **?** i **help** mostren un resum de les subordres de bústia comunes. També podeu visualitzar una llista de totes les subordres de bústia (sense resum) indicant la subordre **(l)**ist.
Per obtenir ajuda dins l'editor de correu	Escriviu `~?` a l'indicador de l'editor de correu. La subordre **~?** mostra un resum de les subordres comunes de l'editor de correu.
Per obtenir ajuda en el correu confidencial	Escriviu `?` a l'indicador de l'editor de correu. Les subordres **?** mostra un resum de les subordres comunes del correu confidencial.
Per obtenir ajuda en l'ús de pàgines manuals	Escriviu `man mail` en l'indicador de línia d'ordres del sistema. En aquest exemple, `mail` és el nom de l'ordre que s'està cercant. El sistema us facilitarà documentació ASCII sobre l'ordre **mail**. Quan aparegui el marcador de continuació (:), feu clic a Intro per veure la resta del document. L'ordre **man** proporciona informació en format ASCII per consultar temes sobre ordres, subrutines i arxius.

Opcions de personalització del programa de correu

Les ordres i opcions dels fitxers `.mailrc` i `/usr/share/lib/Mail.rc` es poden personalitzar perquè s'adaptin a les vostres necessitats de correu personals.

Vegeu l'apartat "Habilitació i inhabilitació de les opcions de correu" a la pàgina 36 per obtenir més informació sobre les opcions de correu.

Les característiques d'una sessió de correu que es poden personalitzar són:

- **Sol•licituds del tema d'un missatge.** Si escriviu l'ordre **mail**, el programa us demanarà que completeu el camp **Tema:**. Quan aparegui aquesta sol•licitud, podeu emplenar un resum del tema del missatge. Aquest resum s'inclou al començament del missatge quan el destinatari el llegeix. Consulteu l'apartat "Sol•licituds de camp Tema: i còpia (Cc:)" a la pàgina 37.
- **Sol•licituds d'enviament de còpies d'un missatge a usuaris.** El fitxer `.mailrc` es pot personalitzar perquè, quan s'enviï un missatge, el programa de correu sol•liciti els noms dels altres usuaris que han de rebre còpies del missatge. Consulteu l'apartat "Sol•licituds de camp Tema: i còpia (Cc:)" a la pàgina 37.
- **Àlies o llistes de distribució.** Si s'envia correu en una xarxa gran o s'envia sovint el mateix missatge a un gran nombre de persones, haver d'escriure les llargues adreces de cadascun dels receptors pot resultar pesat. A fi de simplificar aquest procés. Creeu un àlies o una llista de distribució al vostre fitxer `.mailrc`. Un *L'àlies* és un nom definit que es pot utilitzar per comptes d'una única adreça d'usuari. Una *llista de distribució* és un nom definit que es pot utilitzar en lloc d'un grup d'adreces d'usuari. Consulteu l'apartat "Àlies i llistes de distribució" a la pàgina 38.

- **Nombre de línies que apareixen quan es llegeixen els missatges.** Podeu canviar el nombre de línies de les capçaleres dels missatges o del text dels missatges que es desplacen per la pantalla. Consulteu l'apartat "Canvia el nombre de capçaleres de missatge o de línies de text de missatge que apareixen al programa de correu." a la pàgina 39.
- **Informació llistada als missatges.** Podeu fer que no apareguin les capçaleres dels missatges, com ara el camp `Id missatge` establert per la màquina. Consulteu l'apartat "Visualització d'informació d'un missatge" a la pàgina 40.
- **Directori de carpetes per emmagatzemar missatges.** Podeu crear un directori especial per emmagatzemar missatges. Podeu utilitzar la subordre abreujada de signe més (+) per designar aquest directori si voleu emmagatzemar missatges o consultar les carpetes. Consulteu l'apartat "Creació de carpetes per defecte per emmagatzemar missatges" a la pàgina 42.
- **Fitxer d'enregistrament per enregistrar els missatges de sortida.** Podeu donar instruccions al programa **mail** perquè enregistri tots els missatges de sortida en un fitxer o en un subdirectori del directori d'inici. Consulteu l'apartat "Creació de carpetes per defecte per emmagatzemar missatges" a la pàgina 42.
- **Editors per escriure missatges.**. A més de l'editor de correu, podeu triar dos editors diferents per editar missatges. Consulteu l'apartat "Editors de textos per escrire missatges" a la pàgina 42.

Per obtenir més informació sobre com personalitzar el programa de correu, consulteu els temes següents.

Habilitació i inhabilitació de les opcions de correu:

Les opcions poden ser binàries o amb un valor.

Les opcions binàries són **set** o **unset**, mentre que les opcions amb un valor es poden establir (**set**) en un valor específic.

> **Nota:** La forma **unset** *opció* equival a **set no** *opció*.

Utilitzeu l'ordre **pg** per veure el fitxer `/usr/share/lib/Mail.rc`. El contingut del fitxer `/usr/share/lib/Mail.rc` defineix la configuració del programa de correu. Modifiqueu la configuració del sistema del programa de correu creant un fitxer `$HOME/.mailrc`. Quan executeu l'ordre **mail**, les subordres del fitxer **.mailrc** alteren temporalment les ordres semblants del fitxer `/usr/share/lib/Mail.rc`. Les opcions de `.mailrc` es poden personalitzar i són vàlides cada vegada que s'utilitza el programa de correu.

Per executar les ordres de correu que s'emmagatzemen en un fitxer, utilitzeu la subordre **source**.

`Prerequisits`

El programa de correu ha d'estar instal•lat al sistema.

Habilitació de les opcions de correu:

Les subordres de bústia que més s'utilitzen per modificar les característiques d'una sessió de correu son:

Element	Descripció
set	Habilita opcions de correu.
source	Habilita opcions de correu que s'emmagatzemen en un fitxer. Quan llegiu el correu, podeu executar aquesta subordre a l'indicador de la bústia: `source nom_via_accés` en què *nom_via_accés* és el camí d'accés i el fitxer que contenen les ordres de correu. Les ordres d'aquest fitxer alteren temporalment els valors anteriors d'ordres semblants durant la sessió actual. També podeu modificar les característiques de la sessió de correu actual escrivint ordres a l'indicador de la bústia.

Podeu establir aquestes opcions dins la bústia o efectuant entrades al fitxer `.mailrc`.

Veure opcions de correu habilitades:

Quan llegiu el correu, escriviu la subordre **set** sense arguments a fi de llistar totes les opcions `.mailrc` habilitades.

També podeu veure en aquesta llista si s'ha seleccionat un directori de carpetes i si s'ha configurat un fitxer de registre per tal que enregistri els missatges que surten.

Escriviu a l'indicador de la bústia:

```
set
```

Apareix un missatge semblant al següent:

```
ask
metoo
toplines 10
```

En aquest exemple, les dues opcions binàries estan habilitades: **ask** i **metoo**. No hi ha cap entrada **askcc** a la llista. Això indica que l'opció **askcc** no està habilitada. S'ha assignat el valor `10` a l'opció **toplines**. Les opcions **ask**, **metoo**, **askcc** i **toplines** es descriuen a l'apartat Format del fitxer .mailrc del manual *Files Reference*.

Inhabilitació de les opcions de correu:

Les subordres de bústia que més s'utilitzen per modificar les característiques d'una sessió de correu son:

Element	Descripció
unset	Inhabilita les opcions de correu.
unalias	Suprimeix els noms d'àlies especificats.
ignore	Suprimeix els camps de capçalera de missatge.

Podeu establir aquestes opcions dins la bústia o efectuant entrades al fitxer `.mailrc`.

> **Nota:** La forma **unset** *opció* equival a **set no** *opció*.

Sol•licituds de camp Tema: i còpia (Cc:):

Quan s'editen les sol•licituds de camp **Tema:** i **Cc:**, s'han d'acomplir els prerequisits següents.

```
Prerequisits
```

El programa de correu ha d'estar instal•lat al sistema.

Habilitar o inhabilitar la sol•licitud del Tema::

Utilitzeu les ordres **set** i **unset** per habilitar i inhabilitar el camp **Tema:**.

Podeu habilitar o inhabilitar el camp **Tema:** segons els següents exemples:

Element	Descripció
set ask	La sol•licitud **Tema:** s'habilita editant l'opció `ask` del fitxer `.mailrc`.
unset ask	La sol•licitud **Tema:** s'habilita editant l'opció `ask` del fitxer `.mailrc`.

Habilitar o inhabilitar la sol•licitud del camp de còpia (Cc:):

Utilitzeu les ordres **set** i **unset** per habilitar o inhabilitar el camp **Cc:**.

Podeu habilitar o inhabilitar el camp **Cc:** segons els següents exemples:

Element	Descripció
set askcc	La asol•licitud del camp de còpia (**Cc:**) s'habilita editant l'opció `askcc` del fitxer `.mailrc`.
unset askcc	La sol•licitud del camp de còpia (**Cc:**) s'habilita editant l'opció **askcc** del fitxer `.mailrc`.

Àlies i llistes de distribució:

Quan creeu àlies i llistes de distribució, podeu gestionar els destinataris i les adreces que feu servir normalment amb més facilitat.

Abans de crear un àlies o una llista de distribució, assegureu-vos que es compleixen les condicions següents:

1. El programa de correu ha d'estar instal•lat al sistema.
2. Cal que sapigueu els noms i les adreces dels usuaris que voleu incloure a la llista d'àlies o de distribució.

Podeu crear un àlies o una llista de distribució segons els següents exemples:

Element	Descripció

alias	`bego begonya@gtwn`
	
	En aquest exemple, s'ha llistat un àlies `bego` per a l'usuari `begonya` a l'adreça `gtwn`. Quan hàgiu afegit aquesta línia al fitxer `$HOME/.mailrc`, per enviar un missatge a Begonya, escriviu el següent a l'indicador de la línia d'ordres:
	`mail bego`
	
	Ara ja podeu enviar correu a Begonya mitjançant l'àlies `bego`.

alias	`dept pep@merlin anna@anchor jaume@zeus pere rosa`
	
	Després d'haver afegit aquesta línia al fitxer `$HOME/.mailrc`, escriviu el següent a l'indicador de la línia d'ordres per enviar un missatge al vostre departament:
	`mail dept`
	
	El missatge que acabeu de crear i enviar anirà a `pep` del sistema `merlin`, `anna` del sistema `anchor`, `jaume` del sistema `zeus` i a `pere` i `rosa` del sistema local.

Si voleu una llista dels àlies i de les llistes de distribució, escriviu el següent a l'indicador de la bústia:

```
alias
```

O

```
a
```

Apareixerà una llista d'àlies i llistes de distribució.

Canvia el nombre de capçaleres de missatge o de línies de text de missatge que apareixen al programa de correu.:

Si canvieu el fitxer `.mailrc` podreu personalitzar la capacitat de desplaçament a través de les llistes de la bústia o a través dels missatges reals.

Per tal de realitzar aquestes modificacions, el programa de correu ha d'estar instal•lat al sistema.

Canvi del nombre de línies que apareixen a la llista de missatges:

Cada missatge de la bústia té una capçalera d'una línia a la llista de missatges. Si teniu més de 24 missatges, les primeres capçaleres de la llista de missatges es desplacen fora de la part superior de la pantalla. L'opció **set screen** controla la quantitat de línies de la llista que apareixen alhora.

Per canviar el nombre de línies que apareixen a la llista de missatges alhora, escriviu el següent al fitxer **$HOME/.mailrc**:

```
set screen=20
```

En aquest exemple, el sistema mostrarà 20 capçaleres de missatge alhora. Utilitzeu la subordre **h** o la subordre **z** per veure grups addicionals de capçaleres. També podeu escriure aquesta subordre a l'indicador de la bústia.

Canvi del nombre de línies que apareixen en un missatge llarg:

Si visualitzeu un missatge amb més de 24 línies, les primeres línies del missatge es desplacen fora de la part superior de la pantalla. Podeu utilitzar l'ordre **pg** des del correu per examinar missatges llargs si heu inclòs l'opció **set crt** al fitxer `.mailrc`.

L'opció **set crt** controla la quantitat de línies que un missatge ha de contenir abans que s'iniciï l'ordre **pg**.

Per exemple, si utilitzeu la subordre **t** per llegir un missatge llarg, només apareix una pantalla (o pàgina). Després de la pàgina apareixen dos punts fer-vos saber que hi ha més pàgines. Premeu la tecla tecla Intro per visualitzar la pàgina següent del missatge. Després que aparegui la darrera pàgina del missatge, apareix un indicador semblant al següent:

```
EOF:
```

Podeu escriure qualsevol subordre **pg** vàlida a l'indicador. Podeu visualitzar les pàgines anteriors, cercar sèries de caràcters als missatges o deixar de llegir el missatge i tornar a l'indicador de la bústia.

L'opció **set crt** s'escriu al fitxer `.mailrc` com a:

set crt=*Línies*

Per exemple:

```
set crt=20
```

especifica que un missatge ha de tenir 20 línies abans que s'iniciï l'ordre **pg**. L'ordre **pg** s'inicia quan llegiu missatges de més de 20 línies.

Canvi del nombre de línies que apareixen a la part superior d'un missatge:

La subordre **top** permet explorar un missatge sense haver-lo de llegir sencer.

Podeu controlar la quantitat de línies d'un missatge que apareixen establint l'opció **toplines** de la manera següent:

set toplines=*Línies*

En aquesta subordre, la variable *Línies* és el nombre de línies, a partir de la part superior i incloent-hi tots els camps de capçalera, que apareixen amb la subordre **top**.

Per exemple, si l'usuari `Carles` té la següent línia al fitxer `.mailrc`:

```
set toplines=10
```

quan en Carles executi l'ordre **mail** per llegir els missatges nous, es mostrarà el text següent:

```
Correu Escriviu ? per a l'ajuda.
"/usr/mail/carles": 2 missatges 2 nous>
N  1 jordi   dm 6 gen  9:47  11/257 "Reunió Dept."
N  2 marc    dm 6 gen 12:59  17/445 "Planificació projecte"
```

Quan en Carles utilitza la subordre **top** per examinar els seus missatges, es mostra el següent missatge parcial:

```
top 1
Missatge 1:
De jordi dm 6 gen 9:47 CST 1988
Rebut: per zeus
    ID AA00549; dm 6 gen 88 9:47:46 CST
Data: dm 6 gen 88 9:47:46 CST
De: jordi@zeus
ID de missatge: <8709111757.AA00178>
Per a: carles@zeus
Tema: Reunió Dept.
Apunta't a l'agenda que dilluns hi haurà una reunió del departament
a les 13:30 a la sala de conferències. Parlarem del
```

El missatge es visualitza en part perquè **toplines** s'estableix en 10. Només apareixen les línies de la 1 (el camp **Rebut:**) a la 10 (la segona línia del cos del missatge). La primera línia, `De jordi dm 6 gen 9:47 CST 1988`, sempre està present i no compta a l'opció **toplines**.

Visualització d'informació d'un missatge:

Si canvieu el fitxer `.mailrc`, podeu controlar quina informació de capçalera apareix en un missatge.

És probable que alguna informació de capçalera ja s'hagi desactivat. Examineu el fitxer `/usr/share/lib/Mail.rc` per obtenir els camps de capçalera que s'han passat per alt.

`Prerequisits`

El programa de correu ha d'estar instal•lat al sistema.

Evitar que es visualitzin les capçaleres Data, De i Per a:

Cada missatge té diversos camps de capçalera a la part superior. Aquests camps de capçalera es visualitzen quan es llegeix un missatge. Podeu utilitzar la subordre **ignore** per suprimir la visualització de camps de capçalera si es llegeix un missatge.

El format de la subordre **ignore** és:

`ignore [`*`llista_camps`*`]`

El valor de *llista_camps* pot consistir en el nombre de noms de camps que voleu passar per alt quan visualitzeu un missatge. Per exemple, si l'usuari Carles inclou la següent línia al fitxer `.mailrc`:

```
ignore date from to
```

i el fitxer `/usr/share/lib/Mail.rc` té la línia:

```
ignore received message-id
```

el resultat que donarà la subordre **t** és:

```
t 1
Missatge 1:
De jordi dm 6 gen 9:47 CST 1988
Tema: Reunió Dept.
Apunta't a l'agenda que dilluns hi haurà una reunió del departament
a les 13:30 a la sala de conferències. Parlarem del
nous mètodes d'utilització del programa de planificació
de projectes desenvolupat pel nostre departament.
```

Els camps **Rebut:**, **Data:**, **De:**, **ID de missatge:** i **Per a:** no es mostren. Per visualitzar aquests camps, utilitzeu la subordre **T** o **P** o bé la subordre **top**.

> **Nota:** A l'exemple, apareix la línia **De**. No és la mateixa que la del camp **De:** que apareix al valor *llista_camps* de la subordre **ignore**.

Llistat de camps de capçalera ignorats:

Utilitzeu la subordre **ignore** per llistar camps de capçalera que has estat obviats.

Per obtenir una llista dels camps de capçalera passats per alt actualment, escriviu a l'indicador de la bústia:

```
ignore
```

Apareix una llista de totes les capçaleres passades per alt en aquest moment. Per exemple:

```
mail-from
message-id
return-path
```

Restablir els camps de capçalera:

Per restablir els camps de capçalera, utilitzeu la subordre **retain**.

Per exemple:

```
retain date
```

Llistat de camps de capçalera conservats:

Utilitzeu aquesta subordre **retain** per llistar camps de capçalera conservats.

Per veure quins camps de capçalera estan retinguts en aquest moment, escriviu la subordre **retain** sense paràmetre de camp de capçalera.

Evitar que aparegui la línia informativa:

La línia informativa del programa de correu és la línia que apareix per sobre de la llista de missatges i que mostra el nom del programa de correu quan executeu l'ordre **mail**.

És semblant a la línia següent:

```
Correu [5.2 UCB] [Workstation 3.1] Escriviu ? per a l'ajuda.
```

Per evitar que la línia informativa del programa de correu aparegui quan inicieu el programa de correu, afegiu la línia següent al fitxer `$HOME/.mailrc`:

```
set quiet
```

Una altra opció per suprimir la línia informativa del programa **mail** és:

```
set noheader
```

Amb aquesta opció del fitxer `.mailrc`, no apareix la llista de missatges de la bústia. Quan inicieu el programa **mail**, l'única cosa que apareixerà és l'indicador de la bústia. Podeu obtenir una llista de missatges escrivint la subordre (**h**)eader.

Combinació de les ordres delete i print:

Utilitzeu l'opció autoprint per combinar les subordres delete i print.

Després de llegir un missatge, podeu suprimir-lo amb la subordre **d**. Podeu visualitzar el següent missatge amb la subordre **p**. Combineu aquestes subordres escrivint la següent línia al fitxer `.mailrc`:

```
set autoprint
```

Amb l'opció **set autoprint** del fitxer `.mailrc`, la subordre **d** suprimeix el missatge actual i en mostra el següent.

Creació de carpetes per defecte per emmagatzemar missatges:

Les carpetes per defecte us permeten emmagatzemar missatges.

El programa de correu ha d'estar instal•lat al sistema.

Utilitzeu el procediment següent per crear un directori de bústies amb lletres on s'emmagatzemin els missatges en carpetes:

1. Per comprovar si l'opció **set folder** ha estat habilitada al fitxer `.mailrc`, escriviu el següent a l'indicador de la bústia:

   ```
   set
   ```

   Si l'opció **set folder** ha estat habilitada, el sistema respon amb el següent:

   ```
   folder /home/jordi/cartes
   ```

   En aquest exemple, `cartes` és el directori en el qual s'emmagatzemaran les carpetes de correu.
2. Si no s'ha habitlitat l'opció **set folder**, afegiu una entrada **set folder** al fitxer `.mailrc`:

   ```
   set folder=/home/george/letters
   ```

   En aquest exemple, `/home/jordi` és el directori d'inici d'en Jordi i `cartes` és el directori en el qual s'emmagatzemaran les carpetes de correu. L'opció **set folder** permetrà utilitzar l'anotació abreujada de signe més (+) per desar missatges en el directori `cartes`.
3. Si no existeix un directori `cartes`, cal crear un directori `cartes` al directori d'inici. Des del directori d'inici, escriviu a la línia d'ordres del sistema:

   ```
   mkdir cartes
   ```

Utilitzeu el procediment següent per conservar un enregistrament de missatges enviats a altres persones:

1. Escriviu la següent sentència al fitxer `.mailrc`:

   ```
   set record=cartes/mailout
   ```
2. Si no existeix un directori `cartes`, cal crear un directori `cartes` al directori d'inici. Des del directori d'inici, escriviu a la línia d'ordres del sistema:

   ```
   mkdir cartes
   ```
3. Si voleu llegir les còpies dels missatges que heu enviat a altres persones, escriviu:

   ```
   mail -f +mailout
   ```

   En aquest exemple, el fitxer `mailout` conté còpies dels missatges que heu enviat a altres persones.

Editors de textos per escrire missatges:

Utilitzeu l'opció **set EDITOR=***nom_vía_accés* per definir l'editor de textos amb el qual escriviu els missatges.

El programa de correu ha d'estar instal•lat al sistema.

Element	Descripció
set EDITOR=*nom_via_accés*	Aquesta opció del fitxer `.mailrc` defineix l'editor que activeu amb la seqüència de tecles **~e**. El valor del *nom_via_accés* ha de ser el nom de camí d'accés sencer del programa editor que voleu utilitzar. Per canviar a l'editor e dins el programa de correu, escriviu: `~e` Aquesta seqüència activa l'editor e o un altre editor que hàgiu definit al fitxer `.mailrc`. Editeu el missatge de correu mitjançant aquest editor.
set VISUAL=*nom_via_accés*	Aquesta opció dle fitxer `.mailrc` defineix l'editor que activeu amb la seqüència de tecles **~v**. El valor de *nom_via_accés* ha de ser el nom de camí d'accés sencer del programa editor que voleu utilitzar. El valor per defecte és `/usr/bin/vi`. Per canviar a l'editor vi dins el programa de correu, escriviu: `~v` Aquesta seqüència activa l'editor vi o un altre editor que hàgiu definit al fitxer `.mailrc`. Editeu el missatge de correu mitjançant aquest editor.

Subordres de l'ordre mail

L'ordre **mail** utilitza diverses subordres que duen a terme diferents funcions.

Aquest tema s'utilitza com a referència per l'ordre **mail** i les seves subordres.

Ordres per executar el correu:

Utilitzeu aquestes ordres del sistema per executar el correu.

Element	Descripció
mail	Mostra la bústia del sistema.
mail -f	Mostra la bústia personal (**mbox**).
mail -f +*folder*	Mostra una carpeta de correu.
mail *usuari@adreça*	Adreça un missatge a l'usuari especificat.

Subordres de bústia en el programa de correu:

Quan el programa de correu està processant una bústia, mostra l'indicador de bústia per assenyalar que està esperant una entrada.

L'indicador de bústia és un ampersand (&)e que apareix al començament d'una nova línia. Podeu escriure a l'indicador qualsevol de les subordres de bústia.

Subordres de control del programa de correu:

Utilitzeu aquestes subordres per controlar el programa de correu.

Element	Descripció
q	Surt del programa i aplica les subordres de bústia especificades durant aquesta sessió.
x	Surt del programa i restaura la bústia al seu estat original.
!	Inicia un intèrpret d'ordres, executa una ordre i torna a la bústia.
cd *dir*	Canvia el directori per `dir` o `$HOME`.

Subordres de visualització del programa de correu:

Utilitzeu aquestes subordres per controlar la visualització del programa de correu.

Element	Descripció
t	Mostra els missatges de *llista_msg* o el missatge actual.
n	Mostra el missatge següent.
f *llista_msg*	Mostra les capçaleres dels missatges de *llista_msg* o del missatge actual si no es proporciona *llista_msg*.
h *número*	Mostra les capçaleres de grups que contenen el missatge que té el número indicat per *número*.
top *número*	Mostra part d'un missatge.
set	Mostra una llista de totes les opcions **.mailrc** habilitades.
ignore	Mostra una llista de tots els camps de capçalera passats per alt.
folder	Mostra el nombre de missatges de la carpeta actual amb el nom del camí d'accés de la carpeta.

Gestió de missatges:

Utilitzeu aquestes subordres per editar, suprimir, tornar a cridar, afegir o conservar els missatges.

Element	Descripció
e *número*	Edita el missatge *número* (l'editor per defecte és l'e).
d *llista_msg*	Suprimeix els missatges de *llista_msg* o el missatge actual.
u *llista_msg*	Crida els missatges suprimits de la *llista_msg*.
s *llista_msg* **+***fitxer*	Afegeix missatges (amb capçaleres) a *fitxer*.
w *llista_msg* **+***fitxer*	Afegeix missatges (només text) a *fitxer*.
pre *llista_msg*	Conserva missatges a la bústia del sistema.

Subordres de correu nou:

Utilitzeu aquestes subordres per crear missatges de correu nou.

Element	Descripció
m*llista_adreces*	Crea un nou missatge i l'envia a les adreces de *llista_adreces*.
r*llista_msg*	Envia una contestació a emissors i destinataris dels missatges.
R*llista_msg*	Envia una contestació només als emissors dels missatges.
a	Mostra una llista d'àlies i les seves adreces.

Subordres de l'editor de correu:

Quan es processa l'editor de correu, aquest mostra l'indicador de l'editor de correu per indicar que està esperant una entrada.

Podeu escriure a l'indicador qualsevol de les subordres de l'editor de correu.

Subordres de control de l'editor de correu:

Utilitzeu les subordres següents per controlar l'editor de correu.

Element	Descripció
~q	Surt de l'editor sense desar ni enviar el missatge actual.
~p	Mostra el contingut del buffer de missatges.
~: *mcmd*	Executa una subordre de bústia (*mcmd*).
EOT	Envia un missatge (Control-D en molts terminals).
.	Envia el missatge actual.

Subordre afegir a capçalera:

Utilitzeu aquestes subordres per afegir diferents elements de capçalera als missatges.

Element	Descripció
~h	Afegeix una entrada als camps **Per a:**, **Tema**:, **Cc:** i **Bcc:**.
~t *llista_adreces*	Afegeix les adreces d'usuari de *llista_adreces* al camp **Per a:**.
~s *tema*	Estableix el camp **Tema** en la sèrie especificada mitjançant *subject*.
~c *llista_adreces*	Afegeix les adreces d'usuari de *llista_adreces* al camp **Cc:** (amb còpia a).
~b *llista_adreces*	Afegeix les adreces d'usuari de *llista_adreces* al camp `Bcc:` (amb còpia oculta).

Subordres afegir a missatge:

Utilitzeu aquestes subordres per afegir contingut a un missatge.

Element	Descripció
~d	Afegeix el contingut de `dead.letter` al missatge.
~r *nom_fitxer*	Afegeix el contingut de *nom_fitxer* al missatge.
~f *llista_núm*	Afegeix el contingut de *llista_núm* dels números dels missatges.
~m*llista_núm*	Afegeix i sagna el contingut de la *llista_núm* dels números dels missatges.

Subordres de canvi de missatge:

Utilitzeu aquestes subordres per editar missatges.

Element	Descripció
~e	Edita el missatge mitjançant l'editor e (per defecte és l'e).
~v	Edita el missatge mitjançant l'editor vi (per defecte és vi).
~w*nom_fitxer*	Escriu el missatge a *nom_fitxer*.
ordre **~!**	Inicia un intèrpret d'ordres, executa l'*ordre* i torna a l'editor.
ordre **~|**	Condueix el missatge a l'entrada estàndard de l'*ordre* i substitueix el missatge amb la sortida estàndard d'aquesta ordre.

Subordres de correu confidencial:

Quan el programa de correu confidencial processa una bústia confidencial, mostra l'indicador de la bústia confidencial per assenyalar que està esperant una entrada.

L'indicador de la bústia confidencial és un signe d'interrogació (?) que apareix al començament d'una nova línia. Podeu escriure a l'indicador qualsevol de les subordres de la bústia confidencial.

Subordres de correu confidencial:

Utilitzeu les subordres següents per enviar correu confidencial.

Element	Descripció
xsend `francesc`	Adreça un missatge a l'usuari especificat.
xget	Mostra la bústia confidencial.

Tasques de la bústia:

Les subordres següents ing subcommands porten a terme diferents tasques de la bústia.

Element	Descripció
q	Surt i deixa els missatges sense llegir.
n	Suprimeix el missatge actual i mostra el següent.
d	Suprimeix el missatge actual i mostra el següent.
Intro	Suprimeix el missatge actual i mostra el següent.
!	Executa una ordre d'intèrpret d'ordres.
s	Desa el missatge al fitxer amb nom o a `mbox`.
w	Desa el missatge al fitxer amb nom o a `mbox`.

Tasques de la gestió de correu

El gestor de correu és responsable de les tasques següents.

1. Configurar el fitxer `/etc/rc.tcpip` de manera que el daemon **sendmail** s'iniciï quan s'engegui el sistema. Consulteu l'apartat "Configuració del fitxer /etc/rc.tcpip per iniciar el daemon sendmail".
2. Personalitzar el fitxer de configuració `/etc/mail/sendmail.cf`. El fitxer per defecte `/etc/mail/sendmail.cf` es configura de manera que es pugui lliurar correu local i correu TCP/IP. Per tal de lliurar el correu mitjançant un BNU, cal que personalitzeu el fitxer `/etc/mail/sendmail.cf`. Consulte el fitxer sendmail.cf a *Files Reference* per obtenir més informació.
3. Definir els àlies de correu de tot el sistema i de tot el domini al fitxer `/etc/mail/aliases`. Vegeu l'apartat "Àlies de correu" per obtenir més informació.
4. Gestionar la cua del correu. Vegeu l'apartat "Cua del correu" a la pàgina 49 per obtenir més informació.
5. Gestionar l'enregistrament de correu. Vegeu l'apartat "Registre de al correu" a la pàgina 53 per obtenir més informació.

Configuració del fitxer /etc/rc.tcpip per iniciar el daemon sendmail

Per configurar el fitxer `/etc/rc.tcpip` per tal que s'iniciï el daemon **sendmail** al moment d'engegar el sistema, feu servir aquest procediment.

1. Editeu el fitxer `/etc/rc.tcpip` amb el vostre editor de textos preferit.
2. Busqueu la línia que comença per `start /usr/lib/sendmail`. Per defecte, aquesta línia hauria d'estar descomentada, és a dir, no hi ha d'haver el signe signe diesi (#) al principi de la línia. No obstant això, si està comentada, suprimiu-ne el signe diesi.
3. Deseu el fitxer.

Amb aquest canvi, el sistema iniciarà el daemon **sendmail** al moment de l'engegada.

Àlies de correu

Els àlies mapen noms a les llistes d'adreces utilitzant fitxers d'àlies personals, de tot el sistema i de tot el domini.

Podeu definir tres tipus d'àlies:

Element	Descripció
personal	El defineixen els usuaris individuals al fitxer d'usuari `$HOME/.mailrc`.
sistema local	El defineix l'administrador del sistema de correu al fitxer `/etc/mail/aliases`. Aquests àlies corresponen al correu que gestiona el programa **sendmail** al sistema local. Els àlies del sistema local rarament s'han de canviar.
tot el domini	Per defecte, l'ordre **sendmail** llegeix `/etc/alias` per resoldre els àlies. Per tal d'alterar temporalment el valor per defecte i utilitzar el NIS, editeu o creeu `/etc/netsvc.conf` i afegiu-hi la línia: `aliases=nis`

Fitxer /etc/mail/aliases

En aquest apartat es descriuen els propietats, el contingut i la ubicació del fitxer `/etc/mail/aliases`.

El fitxer `/etc/mail/aliases` consta d'una sèrie d'entrades en el format següent:

Àlies`:` *Nom1*`,` *Nom2*`, ...` *NomX*

en què *Àlies* pot ser qualsevol sèrie alfanumèrica que trieu (que no inclogui els caràcters especials, com ara @ o !). Des de *Nom1* fins *NomX* és una sèrie d'un o més noms de destinatari. La llista de noms es pot estendre a una o més línies. Cada línia continuada comença amb una espai o tabulador. Les línies en buides i les línies que comencen amb # (signe de diesi) són línies de comentaris.

El fitxer `/etc/mail/aliases` ha de tenir els tres àlies següents:

Element	Descripció
MAILER-DAEMON	L'ID de l'usuari que ha de rebre missatges adreçats al daemon de l'aplicació de correu. Aquest nom s'assigna inicialment a l'usuari root: `MAILER-DAEMON: root`
postmaster	L'ID de l'usuari responsable del funcionament del sistema de correu local. L'àlies **postmaster** defineix una sola adreça de la bústia que és vàlida en cada sistema d'una xarxa. Aquesta adreça permet que els usuaris enviïn demandes a l'àlies **postmaster** de qualsevol sistema, sense haver de saber l'adreça correcta d'un usuari del sistema. Aquest nom s'assigna inicialment a l'usuari root: `postmaster: root`
nobody	L'ID que ha de rebre missatges dirigits a programes com ara **news** i **msgs**. Aquest nom s'assigna inicialment a `/dev/null`: `nobody: /dev/null` Per rebre aquests missatges, definiu aquest àlies perquè sigui un usuari vàlid.

Sempre que canvieu aquest fitxer, heu de recopilar-lo en un format de base de dades que l'ordre **sendmail** pugui utilitzar. Consulteu l'apartat "Muntatge de base de dades d'àlies" a la pàgina 48.

Creació d'un àlies local per al correu

La creació d'un àlies local per al correu permet crear grups de llistes de distribució per enviar-los correu.

En aquest escenari, `geo@medussa`, `mark@zeus`, `ctw@athena`, i `dsf@plato` s'afegiran a l'àlies de correu `testers`. Després de crear l'àlies `testers`, s'atorgarà la propietat de l'àlies a glenda@hera.

Quan l'àlies `testers` s'afegeix al fitxer `/etc/mail/aliases`, la base de dades d'àlies es torna a compilar per mitjà de l'ordre **sendmail**. Un cop s'ha compilat la base de dades, es pot enviar un correu electrònic a l'àlies `testers`.

Informació que cal tenir en compte

- La informació d'aquest cas s'ha provat amb versions específiques de l'AIX. Els resultats obtinguts poden variar força segons la versió i el nivell de l'AIX.

Realitzeu els passos següents per crear un àlies de correu local:

1. Obriu el fitxer `/etc/mail/aliases` amb l'editor de textos que vulgueu.

2. En una línia en blanc, afegiu el nom de l'àlies seguit per dos punts (:) i una llista de destinataris separats per comes. Per exemple, l'entrada següent defineix l'àlies `testers`:

   ```
   testers: geo@medussa, mark@zeus, ctw@athena, dsf@plato
   ```

3. Creeu un propietari per a l'àlies. Si l'ordre **sendmail** no aconsegueix enviar el correu a l'àlies, enviarà un missatge d'error al propietari.

   Afegiu una línia al fitxer `/etc/mail/aliases` per especificar el propietari. El format d'aquesta línia ha de ser `owner-`*nom_grup*`:` *propietari*, en què *nom_grup* és el nom de l'àlies i *propietari* l'adreça de correu electrònic del propietari. En aquest exemple, `glenda@hera` s'assigna com a propietària de l'àlies `testers`:

   ```
   testers: geo@medussa, mark@zeus, ctw@athena, dsf@plato owner-testers: glenda@hera
   ```

4. Després de crear l'àlies, executeu l'ordre **sendmail -bi** per tornar a compilar la base de dades d'àlies. Haureu d'executar aquesta ordre cada vegada que actualitzeu el fitxer `/etc/mail/aliases`.

Ara podeu enviar un correu electrònic a l'àlies `testers`.

Muntatge de base de dades d'àlies

L'ordre **sendmail** no utilitza directament les definicions d'àlies del fitxer del sistema local `/etc/mail/aliases`. En canvi, l'ordre **sendmail** llegeix una versió del gestor de bases de dades (dbm) del fitxer `/etc/mail/aliases`.

Podeu compilar la base de dades d'àlies fent servir un d'aquests mètodes:

- Executeu l'ordre `/usr/sbin/sendmail` utilitzant el senyalador **-bi**.
- Executeu l'ordre **newaliases**. Aquesta ordre fa que l'ordre **sendmail** llegeixi el fitxer `/etc/mail/aliases` del sistema local i crea un fitxer nou que conté la informació de la base de dades dels àlies. Aquest fitxer està en el format Berkeley més eficient:

  ```
  /etc/mail/aliases.db
  ```

- Executeu l'ordre **sendmail** utilitzant el senyalador de **Tornar a crear àlies**. D'aquesta manera es torna a crear automàticament la base de dades d'àlies quan està obsoleta. L'acció de tornar a crear automàticament la base de dades pot ser perillosa en màquines que estiguin molt carregades i amb fitxers d'àlies grans. Si aquesta acció hagués de durar més del temps d'espera de tornar a crear (normalment cinc minuts), es pot fer que diversos processos simultàniament iniciïn el procés de tornar a crear la base de dades.

Nota:

1. Si no existeixen els fitxers, l'ordre **sendmail** no pot processar el correu i generarà un missatge d'error.
2. Si heu especificat diverses bases de dades d'àlies, el senyalador **-bi** tornarà a crear tots els tipus de bases de dades que entengui (per exemple, pot tornar a crear bases de dades Network Database Management (NDBM) però no podrà crear bases de dades NIS).

El fitxer `/etc/netsvc.conf` conté la sol•licitud dels serveis del sistema. Per tal d'especificar la sol•licitud del servei d'àlies, afegiu la línia següent:

```
aliases=service, service
```

en què `service` pot ser `files` o `nis`. Per exemple:

```
aliases=files, nis
```

indica a l'ordre **sendmail** que provi primer el fitxer d'àlies local i, si aquest falla, que provi `nis`. Si `nis` s'ha definit com un servei, hauria de funcionar.

Per obtenir més informació sobre el fitxer `/etc/netsvc.conf`, vegeu *Files Reference*.

Cua del correu

La cua del correu és un directori que emmagatzema dades i controla fitxers pel que fa als missatges de correu que lliura l'ordre **sendmail**. Per defecte, la cua del correu és `/var/spool/mqueue`.

Els missatges de correu es poden posar en cua per diversos motius.

Per exemple:

1. L'ordre **sendmail** es pot configurar per processar la cua a uns intervals determinats, per comptes de fer-ho immediatament. Si és així, els missatges de correu s'han d'emmagatzemar temporalment.
2. Si un amfitrió remot no respon una sol•licitud d'una connexió de correu, el sistema de correu posa el missatge en cua i ho torna a provar més tard.

Impresió de la cua del correu

El contingut de la cua es pot imprimir utilitzant l'ordre **mailq** (o especificant el senyalador **-bp** amb l'ordre **sendmail**).

Aquestes ordres generen un llistat dels ID de les cues, de les grandàries dels missatges, de les dates en què els missatges han entrat a la cua i dels emissors i destinataris.

Fitxers de la cua del correu

Cada missatge de la cua té un nombre de fitxers associats.

Els fitxers s'anomenen segons els convenis següents:

TipusfID

essent *ID* un ID de la cua de missatges exclusiu i *Tipus* una de les lletres següents que indica el tipus de fitxer:

Element	Descripció
`d`	El fitxer de dades que conté el cos del missatge sense informació de la capçalera.
`q`	El fitxer de control de cua. Aquest fitxer conté la informació necessària per processar el treball.
`t`	Un fitxer temporal. Aquest fitxer és una imatge del fitxer `q` quan s'està tornant a crear. Es canvia de nom ràpidament pel fitxer `q`.
`x`	Un fitxer de transcripció que existeix mentre dura una sessió i mostra tot el que passa durant la sessió.

Por exemple, si un missatge té un ID de cua `AA00269`, es crearan i es suprimiran els fitxers següents del directori de la cua del correu mentre l'ordre **sendmail** mira de lliurar el missatge:

Element	Descripció
`dfAA00269`	Fitxer de dades
`qfAA00269`	Fitxer de control
`tfAA00269`	Fitxer temporal
`xfAA00269`	Fitxer de transcripció

Fitxer de control q:

El fitxer de control `q` conté una sèrie de línies que comencen amb una lletra de codi.

Element	Descripció
B	Especifica el `tipus de cos`. La resta de la línia és una sèrie de text que defineix el `tipus de cos`. Si falta tot el camp sencer, el `tipus de cos` serà, per defecte, de 7 bits i no s'intentarà cap processament especial. Els valors vàlids són **7BIT** i **8BITMIME**.
C	Conté l'usuari de control. Per adreces de destinataris que són un fitxer o un programa, **sendmail** du a terme un lliurament en qualitat de propietari del fitxer o del programa. L'usuari de control serà el propietari del fitxer o programa. Les adreces dels destinataris que es llegeixen d'un fitxer **.forward** o **:include:** també tenen l'usuari de control establert com a propietari del fitxer. Quan **sendmail** lliura correu a aquests destinataris, el lliura com si fos l'usuari de control i es torna a convertir en root.
F	Conté senyaladors de sobre. Els senyaladors són una combinació de **w**, que estableix el senyalador **EF_WARNING**; **r**, que estableix el senyalador **EF_RESPONSE**; **8**, que estableix el senyalador **EF_HAS8BIT**; i **b**, que estableix el senyalador **EF_DELETE_BCC**. Les altres lletres s'obvien tàcitament.
H	Conté una definició de capçalera. Hi poden haver vàries línies d'aquestes. L'ordre en què apareixen les línies **H** determina l'ordre al missatge final. Aquestes línies utilitzen la mateixa sintaxi que les definicions de capçalera del fitxer de configuració `/etc/mail/sendmail.cf`.
I	Especifica informació d'inodes i dispositius pel fitxer `df`. Es pot utilitzar per recuperar la cua de correu quan s'ha produït una caiguda de disc.
K	Especifica l'hora (en segons) del darrer intent de lliurament.
M	Quan un missatge es posa en cua perquè s'ha produït un error durant l'intent de lliurament, la naturalesa de l'error s'emmagatzema a la línia **M**.
N	Especifica el nombre total d'intents de lliurament.
O	Especifica el valor original MTS (sistema de transferència de missatges) de l'ESMTP. S'utilitza només per les notificacions d'estat del lliurament.
P	Conté la prioritat del missatge actual. La prioritat es fa servir per sol•licitar la cua. Vuit números són per les prioritats inferiors. La prioritat augmenta a mesura que el missatge s'estableix a la cua. La prioritat inicial dependrà de la classe i grandària del missatge.
Q	Conté el destinatari original segons s'ha especificat al camp `ORCPT=` en una transacció ESMTP. Utilitzat exclusivament per les notificacions d'estat del lliurament. Només s'aplica a la línia **R** que va immediatament després.
R	Conté una adreça de destinatari. Hi ha una línia per cada destinatari.
S	Conté l'adreça del remitent. Només hi ha una línia d'aquestes.
T	Conté l'hora de creació del missatge utilitzada per calcular quan s'esgotarà el temps d'espera del missatge.
V	Especifica el número de versió del format del fitxer de cua utilitzat per permetre que els binaris nous de **sendmail** llegeixin fitxers de cua creats en versions anteriors. El valor per defecte és la versió **zero**. Si n'hi ha, ha de ser la primera línia del fitxer.
Z	Especifica l'ID del sobre original (de la transacció ESMTP). S'utilitza només per les notificacions d'estat del lliurament.
$	Conté una definició de macro. Els valors de determinades macros (**$r** i **$s**) es passen a la fase d'execució de la cua.

El fitxer `q` per un missatge enviat a `amy@zeus` seria similar al següent:

```
P217031
T566755281
MDeferred: Connection timed out during user open with zeus
Sgeo
Ramy@zeus
H?P?return-path: <geo>
Hreceived: by george (0.13 (NL support)/0.01)
        id AA00269; Thu, 17 Dec 87 10:01:21 CST
H?D?date: Thu, 17 Dec 87 10:01:21 CST
H?F?From: geo
Hmessage-id: <8712171601.AA00269@george>
HTo: amy@zeus
Hsubject: test
```

En què:

Element	Descripció
P217031	És la prioritat del missatge
T566755281	És l'hora d'enviament en segons
MDeferred: Connection timed out during user open with zeus	És el missatge d'estat
Sgeo	És l'ID del remitent
Ramy@zeus	És l'ID del receptor
H *línies*	És la informació de capçalera del missatge

Valors de temps a sendmail

Per establir el temps d'espera del missatge i l'interval de processament de cua, heu d'utilitzar un format específic pel valor de temps.

El format del valor de temps és:

-q*UnitatTemps*

on *Número* és un valor enter i *Unitat* és una lletra d'unitat. *Unitat* pot tenir un dels valors següents:

Element	Descripció
s	Segons
m	Minuts
h	Hores
d	Dies
w	Setmanes

Si no s'especifica *Unitat*, el daemon **sendmail** utilitza minuts (**m**) per defecte. A continuació, es mostren tres exemples que il•lustren l'especificació del valor de temps:

```
/usr/sbin/sendmail -q15d
```

Aquesta ordre indica al daemon **sendmail** que processi la cua cada 15 dies.

```
/usr/sbin/sendmail -q15h
```

Aquesta ordre indica al daemon **sendmail** que processi la cua cada 15 hores.

```
/usr/sbin/sendmail -q15
```

Aquesta ordre indica al daemon **sendmail** que processi la cua cada 15 minuts.

Cues de correu obturades

En alguns casos, potser veureu que la cua està obturada per algun motiu. Podeu forçar l'execució de la cua utilitzant el senyalador **-q** (sense valors).

També podeu utilitzar el senyalador **-v** (explicatiu) per veure què passa:

```
/usr/sbin/sendmail -q -v
```

També podeu limitar els treballs als que tenen un identificador de cua, un remitent o destinatari particular utilitzant un dels modificadors de cua. Per exemple, **-qRdora** restringeix l'execució de la cua a treballs que tinguin la sèrie `dora` en una de les adreces de destinataris. De forma similar, **-qS***sèrie* limita l'execució a uns remitents en particular, i **-qI***sèrie* ho limita a uns identificadors de cua particulars.

Establiment de l'interval de processament de cues

El valor del senyalador **-q** quan s'inicia el daemon determina l'interval en què el daemon **sendmail** processa la cua de correu.

El daemon **sendmail** el sol iniciar el fitxer `/etc/rc.tcpip` quan s'engega el sistema. El fitxer `/etc/rc.tcpip` conté una variable anomenada interval de processament de cues (QPI), que utilitza per

especificar el valor del senyalador **-q** quan inicia el daemon **sendmail**. Per defecte, el valor de **qpi** és de 30 minuts. Per especificar un interval de processament de cues:

1. Editeu el fitxer `/etc/rc.tcpip` amb el vostre editor preferit.
2. Busqueu la línia que assigna un valor a la variable *qpi*, com ara:
   ```
   qpi=30m
   ```
3. Canvieu el valor assignat a la variable *qpi* pel valor de temps que vulgueu.

Aquests canvis entraran en vigor quan es torni a engegar el sistema. Si voleu que els canvis entrin en vigor immediatament, atureu i reinicieu el daemon **sendmail**, especificant el nou valor del senyalador **-q**. Consulteu els apartats "Aturada del daemon sendmail" a la pàgina 53 i "Inici del daemon sendmail" per obtenir més informació.

Trasllat de la cua del correu

Quan un amfitrió s'apaga durant una estona, els missatges encaminats a aquest amfitrió poden estar emmagatzemats a la cua del correu. Per tant, l'ordre sendmail triga molt de temps en classificar la cua, fent minvar dràsticament el rendiment del sistema. Si traslladeu la cua a un lloc temporal i creeu una cua nova, la cua vella es podrà executar més tard quan l'amfitrió torni a prestar servei.

Per traslladar la cua a un lloc temporal i crear una cua nova:

1. Atureu el daemon **sendmail** seguint les instruccions que trobareu a l'apartat "Aturada del daemon sendmail" a la pàgina 53.
2. Traslladeu tot el directori de la cua escrivint:
   ```
   cd /var/spool
   mv mqueue omqueue
   ```
3. Reinicieu el daemon **sendmail** seguint les instruccions que trobareu a l'apartat "Inici del daemon sendmail".
4. Processeu l'antiga cua de correu escrivint:
   ```
   /usr/sbin/sendmail -oQ/var/spool/omqueue -q
   ```

   El senyalador **-oQ** especifica un directori de cua alternatiu. El senyalador **-q** especifica que s'ha d'executar cada treball de la cua. Per aconseguir un informe sobre el progrés de l'operació, utilitzeu el senyalador **-v**.

   Nota: Aquesta operació pot trigar una estona.
5. Elimineu els fitxer de registre i el directori temporal quan la cua estigui buida escrivint:
   ```
   rm /var/spool/omqueue/*
   rmdir /var/spool/omqueue
   ```

Inici del daemon sendmail

Existeixen dues ordres que inicien el daemon **sendmail**.

Per iniciar el daemon **sendmail**, escriviu una de les ordres següents:

```
startsrc -s sendmail -a "-bd -q15"
```

```
/usr/lib/sendmail -bd -q15
```

Si el daemon **sendmail** ja es troba actiu quan escriviu una d'aquestes ordres, apareixerà el missatge següent a la pantalla:

```
The sendmail subsystem is already active. Multiple instances are not supported.
```

Si el daemon **sendmail** encara no està actiu, veureu un missatge que indica que el daemon **sendmail** s'ha iniciat.

Aturada del daemon sendmail

Per aturar el daemon **sendmail**, executeu l'ordre **stopsrc -s sendmail**.

Si el daemon **sendmail** no s'ha iniciat amb l'ordre **startsrc**:

- Busqueu l'ID de procés **sendmail**.
- Escriviu l'ordre **kill** *sendmail_pid* (on *sendmail_pid* és l'ID de procés del procés **sendmail**).

Registre de al correu

L'ordre **sendmail** enregistra l'activitat del sistema de correu mitjançant el daemon **syslogd**.

S'ha de configurar i executar el daemon **syslogd** per poder dur a terme l'enregistrament del correu. Concretament, el fitxer `/etc/syslog.conf` hauria de tenir la següent línia descomentada:

```
mail.debug          /var/spool/mqueue/log
```

Si no la té així, amb el l'editor que preferiu canvieu-la i assegureu-vos que el nom de camí d'accés sigui correcte. Si canvieu el fitxer `/etc/syslog.conf` mentre s'està executant el daemon **syslogd**, renoveu el daemon **syslogd** escrivint l'ordre següent a la línia d'ordres:

```
refresh -s syslogd
```

Si no existeix el fitxer `/var/spool/mqueue/log`, heu de crear-lo escrivint l'ordre següent:

```
touch /var/spool/mqueue/log
```

Els missatges del fitxer de registre apareixen amb el format següent:

Cada línia de l'enregistrament del sistema consta d'una indicació de l'hora, del nom de la màquina que l'ha generada (per iniciar la sessió des de diverses màquines a través de la xarxa d'àrea local), de la paraula `sendmail:` i d'un missatge. La majoria de missatges són una seqüència de parelles *nom=valor*.

Les dues línies més comunes que s'enregistren quan es processa un missatge són la línia **receipt** i la línia **delivery attempt**. La línia **receipt** enregistra la recepció d'un missatge; n'hi haurà una per missatge. Alguns camps es poden ometre. Són els següents:

Element	Descripció
`des de`	Especifica l'adreça del remitent del missatge.
`grandària`	Especifica la grandària del missatge en octets.
`classe`	Indica la classe (prioritat numèrica) del missatge.
`pri`	Especifica la prioritat inicial del missatge (utilitzat per fer una classificació de la cua).
`nrcpts`	Indica el nombre de destinataris d'aquest missatge (després de detectar-ne els àlies i de reenviar-lo).
`proto`	Especifica el protocol utilitzat per rebre el missatge, per exemple ESMTP o Programa de còpia UNIX a UNIX (UUCP).
`relay`	Especifica la màquina on s'ha rebut.

La línia **delivery attempt** s'enregistra cada vegada que es produeix un intent de lliurament (per tant, n'hi poden haver unes quantes per cada missatge si se'n difereix el lliurament o si hi ha múltiples destinataris). Aquests camps són:

Element	Descripció
per	Conté una llista separada per comes dels destinataris per aquesta aplicació de correu.
ctladdr	Especifica l'*usuari de control*, és a dir, el nom de l'usuari de qui es fan servir les credencial per al lliurament.
retard	Especifica el retard total entre el temps en que s'ha rebut el missatge i el temps en que es va lliurar.
retardx	Especifica la quantitat de temps que cal perquè es faci efectiu el lliurament.
aplicació de correu	Especifica el nom de l'aplicació de correu que es fa servir per fer un lliurament a aquest destinatari.
retransmissió	Especifica el nom de l'amfitrió que ha acceptat (o rebutjat) realment aquest destinatari.
estat	Especifica l'estat del lliurament.

Com que es pot enregistrar tota aquesta gran quantitat d'informació, el fitxer de registre s'ordena com una successió de nivells. Començant pel nivell 1, el nivell inferior, només s'enregistren situacions molt poc usuals. Al nivell superior, s'enregistren fins i tot les incidències més insignificants. Com a conveni, els nivells d'enregistrament fins el 10 es fan servir per la informació més útil. Els nivells d'enregistrament que hi ha per sobre del 64 es reserven per temes de depuració. Els nivells de l'11 al 64 es reserven per informació explicativa.

El tipus d'activitats que l'ordre **sendmail** posa al fitxer de registre s'especifiquen mitjançant l'opció **L** al fitxer `/etc/mail/sendmail.cf`.

Gestió d'enregistraments

Com que constantment s'afegeix informació al final de l'enregistrament, el fitxer pot esdevenir molt gran. A més, les condicions d'error poden provocar entrades imprevistes a la cua del correu. Per tal d'evitar que la cua del correu i el fitxer de registre creixin massa, executeu aquesta seqüència de l'intèrpret d'ordres `/usr/lib/smdemon.cleanu`.

Aquesta seqüència fa que l'ordre **sendmail** processi la cua i conservi quatre còpies d'antiguitat progressiva dels fitxers de registre, anomenades `log.0`, `log.1`, `log.2` i `log.3`. Cada vegada que s'executa l'script mou:

- El `log.2` al `log.3`
- El `log.1` al `log.2`
- El `log.0` al `log.1`
- El `log` al `log.0`

Si s'executa aquesta seqüència es permet que l'inici de sessió es faci amb un fitxer nou. Executeu aquesta seqüència ja sigui manualment o a un interval especificat amb el daemon **cron**.

Registres de trànsit

Utilitzeu el senyalador **-X** de l'ordre **sendmail** per establir l'enregistrament del trànsit.

Moltes implementacions del **Simple Mail Transfer Protocols (SMTP)** no implementen completament el protocol. Per exemple, alguns **SMTP** basats en ordinadors personals no comprenen les línies de continuació dels codis de resposta. Poden ser molt difícils de traçar. Si teniu sospites d'un problema així, podeu establir l'enregistrament del trànsit mitjançant el senyalador **-X**. Per exemple:

```
/usr/sbin/sendmail -X /tmp/traffic -bd
```

Aquesta ordre enregistra tot el trànsit del fitxer `/tmp/traffic`.

Com que aquesta ordre enregistra moltes dades molt de pressa, no s'hauria d'utilitzar mai durant operacions normals. Després d'executar l'ordre, forceu la implementació **errant** per enviar un missatge al vostre amfitrió. Tot el trànsit de missatges d'entrada i sortida de **sendmail**, inclòs el trànsit **SMTP** d'entrada, s'enregistrarà en aquest fitxer.

Mitjançant **sendmail**, podeu enregistrar un buidatge dels fitxers oberts i la memòria cau de connexió enviant-li un senyal **SIGUSR1**. Els resultats s'enregistraran amb la prioritat **LOG_DEBUG**.

Registres d'estadístiques de l'aplicació de correu

L'ordre **sendmail** fa un seguiment del volum de correu que gestiona cadascun dels programes d'aplicació de correu que operen interactivament amb ella.

Aquestes aplicacions de correu es defineixen al fitxer `/etc/mail/sendmail.cf`.

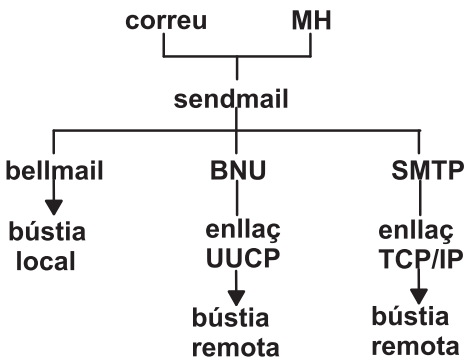


Figura 3. Aplicacions de correu (mailers) que utilitza l'ordre sendmail

Aquesta il•lustració és un tipus de gràfic organitzatiu en sentit vertical amb el correu i l'MH a dalt de tot. D'ell en pengen el bellmail, els BNU i l'SMTP. Per sota del nivell anterior hi ha el respectiu enllaç a la bústia local, l'enllaç UUCP i l'enllaç TCP/IP. Per sota de l'enllaç UUCP hi ha la bústia remota i per sota de l'enllaç TCP/IP hi ha la bústia remota.

Per iniciar l'acumulació de les estadístiques de l'aplicació de correu, creeu el fitxer `/etc/mail/statistics` escrivint el següent:

```
touch /etc/mail/statistics
```

Si l'ordre **sendmail** detecta errors quan intenta enregistrar informació d'estadístiques, l'ordre gravarà un missatge mitjançant la subrutina **syslog**. Aquests errors no afecten altres operacions de l'ordre **sendmail**.

L'ordre **sendmail** actualitza la informació del fitxer cada vegada que processa correu. La grandària del fitxer no creix però els nombres del fitxer sí. Representen el volum del correu des que vau crear o restablir el fitxer `/etc/mail/statistics`.

Visualització de la informació de l'aplicació de correu

Les estadístiques que es conserven al fitxer `/etc/mail/statistics` estan en format de base de dades i no es poden llegir com a fitxer de text.

Per tal de visualitzar les estadístiques de l'aplicació de correu, escriviu el següent en un indicador d'ordres_

```
/usr/sbin/mailstats
```

Així es llegeix la informació del fitxer `/etc/mail/statistics`, es formata i es grava a la sortida estàndard. Per obtenir informació sobre la sortida de l'ordre **/usr/sbin/mailstats**, llegiu- ne la descripció a la publicació *Commands Reference, Volume 3*.

L'API del filtre de correu Mail

L'API del filtre de correu (també coneguda com *Milter*) permet que programes d'altres empreses puguin accedir als missatges de correu a mesura que es van processant per tal de filtrar-ne la metainformació i el contingut.

Requisits del filtre sendmail

Com que els filtres utilitzen fils, els filtres han de tenir una seguretat contra els fils. Podeu configurar els filtres per tal de garantir-ne la compatibilitat amb els fils.

Mols sistemes operatius proporcionen suport pels fils POSIX a les biblioteques C estàndard. El senyalador compilador per enllaçar amb el suport a fils serà diferent en funció del compilador i de l'enllaçador que es faci servir. Si no sabeu del cert quin senyalador local s'utilitza, comproveu el directori `Makefile` al subdirectori de muntatge `obj.*/libmilter` corresponent.

Nota: Com que els filtres utilitzen fils, podria ser necessari alterar els límits del procés al vostre filtre. Per exemple, potser que vulgueu utilitzar setrlimit per augmentar el nombre de descriptors de fitxer oberts si el vostre filtre ha d'estar ocupat. Contràriament, el correu es podrà rebutjar.

Configuracions del filtre sendmail

Utilitzeu aquestes indicacions per especificar els filtres que vulgueu quan es configuri **sendmail**.

Especifiqueu filtres que utilitzin la lletra clau X (d'eXtern). A l'exemple següent s'especifiquen tres filtres.

```
Xfiltre1, S=local:/var/run/f1.sock, F=R
Xfilter2, S=inet6:999@localhost, F=T, T=C:10m;S:1s;R:1s;E:5m
Xfilter3, S=inet:3333@localhost
```

Podeu especificar filtres al fitxer .mc utilitzant la sintaxi següent:

```
INPUT_MAIL_FILTER(`filtre1', `S=local:/var/run/f1.sock, F=R')
INPUT_MAIL_FILTER(`filtre2', `S=inet6:999@localhost, F=T, T=C:10m;S:1s;R:1s;E:5m')
INPUT_MAIL_FILTER(`filtre3', `S=inet:3333@localhost')
```

en què el filtre(*número*) és el nom del vostre filtre. La primera línia de la sintaxi especifica que el filtre es connecta a un sòcol del domini UNIX del directori `/var/run`. La segona línia especifica que el filtre utilitza un sòcol IPv6 al port 999 de l'amfitrió local. La tercera línia especifica que el filtre utilitza un sòcol IPv4 al port 3333 de l'amfitrió local.

L'`F=` indica quin senyalador s'aplica:

Element	Descripció
R	Rebutja la connexió si el filtre no està disponible.
T	Finalitza temporalment la connexió si el filtre no està disponible.

Si no s'especifica cap senyalador, el missatge passarà a **sendmail** com si no hi hagués filtre.

Si s'especifica un valor per `T=`, podreu utilitzar els filtres per tal d'alterar temporalment els temps d'espera per defecte que utilitza **sendmail**. L'equació de la `T=` utilitza els camps següents:

Element	Descripció
C	El temps d'espera per connectar-se a un filtre (si és 0, utilitza el temps d'espera del sistema).
S	El temps d'espera per enviar informació de l'MTA a un filtre.
R	El temps d'espera per llegir les respostes del filtre.
E	El temps d'espera total entre enviar aviso de final de missatge al filtre i esperar la justificació de recepció final.

Tal com s'indica a l'exemple anterior, els separadors entre cada temps d'espera és el signe del punt i coma (**;**) i el separador entre cada equació és una coma (**,**).

Els valors per defecte dels temps d'espera són els següents:

```
T=C:0m;S:10s;R:10s;E:5m
```

en què `s` són els segons i `m` són els minuts.

L'opció **InputMailFilters** determina quins filtres es fan servir i en quina seqüència.

Nota: Si no s'especifica l'opció **InputMailFilters**, no es farà servir cap filtre.
L'opció **InputMailFilters** s'estableix automàticament segons l'ordre de les ordre INPUT_MAIL_FILTER al fitxer `.mc`. Podeu restablir aquest valor establint un valor per confINPUT_MAIL_FILTERS al fitxer `.mc`. Per exemple, si l'opció **InputMailFilters** s'ha establert com s'indica a continuació:

```
InputMailFilters=filtre1, filtre2, filtre3
```

es cridarà als tres filtres en el mateix ordre en què s'han especificat.

Si s'utilitza MAIL_FILTER() per comptes de INPUT_MAIL_FILTER() al vostre fitxer `.mc`, podeu definir un filtre sense afegir-lo a la llista dels filtres d'entrada.

Funcions de control de la biblioteca

El filtre sendmail crida les funcions de control de la biblioteca per establir el paràmetre **libmilter** abans de passar el control a **libmilter**. Els paràmetres **libmilter** s'estableixen cridant la funció **smfi_main** . El filtre també crida la funció **smfi_register** per registrar específicament les seves crides de retorn. Cada funció retorna el valor MI_SUCCESS o bé MI_FAILURE per indicar l'estat de l'operació. Aquestes funcions no es comuniquen amb l'agent de transferència de correu (MTA), sinó amb l'estat de la biblioteca, que es comunica amb l'MTA dins de la funció **smfi_main** .

Taula 1. Funcions de control de la biblioteca

Element	descripció
smfi_opensocket	**La funció smfi_opensocket crea el sòcol de la interfície.**
smfi_register	La funció **smfi_register** registra un filtre.
smfi_setconn	La funció **smfi_setconn** especifica el sòcol que s'utilitzarà.
smfi_settimeout	La funció **smfi_settimeout** estableix el temps d'espera.
smfi_setbacklog	La funció **smfi_setbacklog** defineix la mida de cua **listen (2)** d'entrada.
smfi_setdbg	La funció **smfi_setdbg** estableix el nivell de depuració (rastreig) de la biblioteca **milter**.
smfi_stop	La funció **smfi_stop** provoca una aturada ordenada .
smfi_main	La funció **smfi_main** passa el control a **libmilter**.

Funció smfi_opensocket:
Finalitat

La funció **smfi_opensocket** intenta crear agents de transferència de correu (MTA) de sòcol de la interfície que s'utilitzen per connectar-se al filtre.

Sintaxi

```
#include <libmilter/mfapi.h>
int smfi_opensocket(
bool rmsocket
);
```

Descripció

La funció **smfi_opensocket** es crida només des de la línia principal del programa després de cridar la funció **smfi_setconn** i la **smfi_register**, però abans de cridar la funció **smfi_main**. La funció **smfi_opensocket** crea el sòcol especificat prèviament cridant la funció **smfi_setconn** la qual és la interfície entre els MTA i el filtre. La funció **smfi_opensocket** permet que l'aplicació que es crida creï el sòcol. Si la funció **smfi_opensocket** no es crida, la funció **smfi_main** cridarà la funció implícitament.

Arguments

Taula 2. Arguments

Element	Descripció
rmsocket	Un indicador indica si la biblioteca ha d'intentar eliminar qualsevol sòcol de dominiUNIX abans d'intentar crear-ne un de nou.

Valors de retorn

La funció **smfi_opensocket** retorna el valor MI_FAILURE en els casos següents. Si no, la funció retorna MI_SUCCESS.

- El sòcol d'interfície no s'ha pogut crear.
- El valor *rmsocket* és cert, o no s'ha pogut examinar el sòcol o el sòcol existent no s'ha pogut eliminar.
- La funció **smfi_setconn** o la funció **smfi_register** no s'han cridat.

Informació relacionada

"Funció smfi_register"

"Funció smfi_setconn Function" a la pàgina 61

Funció smfi_register:
Finalitat

La funció **smfi_register** registra un conjunt de funcions de crida de retorn del filtre sendmail.

Sintaxi

```
#include <libmilter/mfapi.h>
int smfi_register(
smfiDesc descr)
);
```

Descripció

La funció **smfi_register** crea un filtre sendmail utilitzant la informació facilitada en l'argument **smfiDesc**. La funció **smfi_register** s'ha de cridar abans de la funció **smfi_main**.

Nota: No es permeten les crides múltiples correctes a la funció **smfi_register** dins d'un únic procés. Només es pot registrar correctament un sol filtre sendmail. No obstant, tingueu en compte que la biblioteca no pot comprovar si s'obeeix la restricció.

El camp xxfi_flags ha de contenir els bits, els zeros o qualsevol dels valors següents que descriuen les accions que pot realitzar el filtre sendmail.

Taula 3. Valors

Element	Descripció
SMFIF_ADDHDRS	La funció **smfi_addheader** afegeix capçaleres.
SMFIF_CHGHDRS	La funció **smfi_chgheader** modifica o suprimeix les capçaleres.
SMFIF_CHGBODY	La funció **smfi_replacebody** substitueix el cos durant el filtratge. El filtre té un impacte significatiu en el rendiment si altres filtres realitzen un filtratge de cos després d'aquest filtre.
SMFIF_ADDRCPT	La funció **smfi_addrcpt** afegeix destinataris al missatge.
SMFIF_ADDRCPT_PAR	La funció **smfi_addrcpt_par** afegeix destinataris, també s'hi inclouen els arguments de protocol simple de transferència de correu ampliat (ESMTP).

Taula 3. Valors (continuació)

Element	Descripció
SMFIF_DELRCPT	La funció **smfi_delrcpt** elimina destinataris del missatge.
SMFIF_QUARANTINE	La funció **smfi_quarantine** `posa en quarantena un missatge.
SMFIF_CHGFROM	La funció **smfi_chgfrom** modifica l'adreça del remitent (Mail From).
SMFIF_SETSYMLIST	La funció **smfi_setsymlist** envia un conjunt de símbols (macros) que són necessaris.

Arguments

Taula 4. Arguments

Element	Descripció

descr	Un filtre descriptor del tipus `smfiDesc` descriu les funcions del filtre. L'estructura té els membres següents:
	`struct smfiDesc`
	`{`
	`  char  *xxfi_name; /* filter name */`
	`  int  xxfi_version; /* version code`
	`-- do not change */`
	`  unsigned long xxfi_flags; /* flags */`
	
	`  /* connection info filter */`
	`  sfsistat (*xxfi_connect)(SMFICTX *,`
	`char`
	`*, _SOCK_ADDR *);`
	`  /* SMTP HELO command filter */`
	`  sfsistat (*xxfi_helo)(SMFICTX *,`
	`char *);`
	`  /* envelope sender filter */`
	`  sfsistat (*xxfi_envfrom)(SMFICTX *,`
	`char **);`
	`  /* envelope recipient filter */`
	`  sfsistat (*xxfi_envrcpt)(SMFICTX *,`
	`char **);`
	`  /* header filter */`
	`  sfsistat (*xxfi_header)(SMFICTX *,`
	`char *,`
	` char *);`
	`  /* end of header */`
	`  sfsistat (*xxfi_eoh)(SMFICTX *);`
	`  /* body block */`
	`  sfsistat (*xxfi_body)(SMFICTX *,`
	`unsigned char`
	`*, size_t);`
	`  /* end of message */`
	`  sfsistat (*xxfi_eom)(SMFICTX *);`
	`  /* message aborted */`
	`  sfsistat (*xxfi_abort)(SMFICTX *);`
	`  /* connection cleanup */`
	`  sfsistat (*xxfi_close)(SMFICTX *);`
	
	`  /* any unrecognized or unimplemented`
	`command filter */`
	`  sfsistat (*xxfi_unknown)(SMFICTX`
	`*, const char *);`
	
	`  /* SMTP DATA command filter */`
	`  sfsistat (*xxfi_data)(SMFICTX *);`
	
	`  /* negotiation callback */`
	`  sfsistat (*xxfi_negotiate)(SMFICTX *,`
	`    unsigned long, unsigned long,`
	`unsigned long,`
	` unsigned long,`
	`    unsigned long *, unsigned long *,`
	`unsigned long *,`
	`unsigned long *`
	`);`
	`};`
	
	Un valor NULL per a qualsevol funció de crida de retorn indica que el filtre no processa el tipus determinat d'informació i retorna **SMFIS_CONTINUE**.

headerf	El nom de capçalera és una sèrie acabada amb un valor nul que no és NULL.
headerv	El valor de capçalera que s'afegirà pot ser una sèrie acabada amb un valor nul que no és NULL o una sèrie buida.

Valors de retorn

La funció **smfi_register** retorna el valor MI_FAILURE en els casos següents. Si no, la funció retorna MI_SUCCESS.

- L'assignació de memòria ha fallat.
- Versió incompatible o valor d'indicador il•legal.

Informació relacionada

"Funció smfi_addheader" a la pàgina 71

"Funció smfi_chgheader" a la pàgina 73

"Funció smfi_replacebody" a la pàgina 79

"Funció smfi_addrcpt" a la pàgina 77

"Funció smfi_addrcpt_par" a la pàgina 77

"Funció smfi_delrcpt" a la pàgina 78

"Funció smfi_quarantine" a la pàgina 81

"Funció smfi_chgfrom" a la pàgina 76

"Funció smfi_setsymlist" a la pàgina 96

Funció smfi_setconn Function:
Finalitat

La funció **smfi_setconn** estableix el sòcol a través del qual aquest filtre es pot comunicar amb l'ordre **sendmail**.

Sintaxi

```
#include <libmilter/mfapi.h>
int smfi_setconn(
char *oconn;
);
```

Descripció

La funció **smfi_setconn** s'ha de cridar abans de cridar la funció **smfi_main**.

Els filtres no es poden executar com a arrel en comunicar-se sobre UNIX o sòcols de domini local.

Els permisos per a UNIX o per a sòcols locals han d'establir-se per a `0600` (permís de lectura o d'escriptura només per a propietari o per a grup de sòcols) o `0660` (permís de lectura o d'escriptura per a propietari de sòcols i per a grup). Aquests permisos són útils si s'utilitza l'opció **sendmail RunAsUser**.

Els permisos per a UNIX o un sòcol de domini local es determinen mitjançant **umask** que ha d'estar establert com a `007` or `077`. Per a sistemes operatius com Solaris que no utilitzen permisos del sòcol, poseu-lo en un directori protegit.

Arguments

Taula 5. Arguments

Element	Descripció

oconn	L'adreça del sòcol de comunicació desitjat. L'adreça ha de ser una sèrie acabada amb valor NULL en format **proto:address** format:
	`* {unix|local}:/path`
	`/to/file -- A named pipe.`
	`* inet:port`
	`@{hostname|ip-address} -- An IPV4 socket.`
	`* inet6:port`
	`@{hostname|ip-address} -- An IPV6 socket.`

Valors de retorn

La funció **smfi_setconn** no falla si és una adreça no vàlida. Tot i així, la funció **smfi_setconn** falla a l'hora d'establir el sòcol si no hi ha memòria. L'error només es detecta en la funció **smfi_main**.

Informació relacionada

"Funció smfi_main" a la pàgina 64

Funció smfi_settimeout:
Finalitat

La funció **smfi_settimeout** estableix el valor de temps d'espera E/S dels filtres.

Sintaxi

```
#include <libmilter/mfapi.h>
int smfi_settimeout((
int otimeout
);
```

Descripció

La funció **smfi_settimeout** es crida només des de la funció **smfi_main**. La funció **smfi_settimeout** estableix la durada (en segons) perquè el paràmetre **libmilter** esperi una comunicació de l'agent de transferència de correu (MTA) (lectura o escriptura) abans del temps d'espera.

Nota: Si la funció **smfi_settimeout** no es crida, la durada del temps d'espera per defecte són 7210 segons.

Arguments

Taula 6. Arguments

Element	Descripció
otimeout	La durada en segons perquè el paràmetre **libmilter** esperi un MTA abans del temps d'espera. El valor *otimeout* ha de ser superior a zero. Si el valor *otimeout* és zero, el paràmetre **libmilter** no espera un MTA.

Valors de retorn

La funció **smfi_settimeout** sempre retorna el valor MI_SUCCESS.

Informació relacionada

smfi_main

Funció smfi_setbacklog:
Finalitat

La funció **smfi_setbacklog** estableix el valor d'endarreriment **listen(2)** del filtre.

Sintaxi

```
#include <libmilter/mfapi.h>
int smfi_setbacklog(
int obacklog
);
```

Descripció

La funció **smfi_setbacklog** es crida només abans de cridar la funció **smfi_main**. La funció **smfi_setbacklog** estableix l'endarreriment del sòcol d'entrada que utilitza el valor d'endarreriment **listen(2)**. Si la funció **smfi_setbacklog** no es crida, s'utilitzarà el sistema operatiu per defecte.

Arguments

Taula 7. Arguments

Element	Descripció
obacklog	Nombre de connexions d'entrada permeses a la cua de recepció.

Valors de retorn

La funció **smfi_setbacklog** retorna el valor MI_FAILURE si l'argument *obacklog* està establert com a inferior o és igual al valor null.

Informació relacionada

"Funció smfi_main" a la pàgina 64

Funció smfi_setdbg:
Finalitat

La funció **smfi_setdbg** estableix el nivell de depuració (rastreig) de la biblioteca **milter**.

Sintaxi

```
#include <libmilter/mfapi.h>
int smfi_setdbg(
  int level;
);
```

Descripció

La funció **smfi_setdbg** estableix un nivell nou de depuració intern de la biblioteca **milter**, perquè es pugui fer seguiment dels detalls del codi. Si el nivell és zero, es desactiva la depuració. Com més alt sigui el nivell (més positiu), més detallada serà la depuració. El valor actual, més alt i útil és sis.

Arguments

Taula 8. Arguments

Element	Descripció
nivell	El nivell de depuració nou.

Valors de retorn

La funció **smfi_setdbg** retorna el valor MI_SUCCESS per defecte.

Funció smfi_stop:
Finalitat

La funció **smfi_stop** desactiva el **milter**. No s'accepten connexions després d'aquesta crida.

Sintaxi

```
#include <libmilter/mfapi.h>
int smfi_stop(void);
);
```

Descripció

La funció **smfi_stop** es crida des de la funció de crida de retorn o des de les rutines de gestió d'errors en qualsevol moment. La rutina **smfi_stop** no permet connexions noves. Tot i així, la funció no espera que les connexions existents(fils) es finalitzin. Aquesta funció fa que la funció **smfi_main** retorni al programa de crida, el qual pot sortir o reprendre el sistema.

Arguments

Taula 9. Arguments

Element	Descripció
void	Aquest argument no agafa cap valor.

Valors de retorn

La funció **smfi_stop** retorna el valor SMFI_CONTINUE en els casos següents:

- Una rutina interna provoca que la biblioteca **milter** s'aturi.
- Un rutina provoca que la biblioteca **milter** s'aturi.
- El procés que s'ha iniciat, no es pot aturar.

Exemple

```
int ret;
SMFICTX *ctx;
...
ret = smfi_addheader(ctx, "Content-Type",
"multipart/mixed;\n\tboundary=\"foobar\"");
```

Informació relacionada

Funcions de crida de retorn

Funció smfi_main:
Finalitat

La funció **smfi_main** passa el control al bucle d'esdeveniments **libmilter**.

Sintaxi

```
#include <libmilter/mfapi.h>
int smfi_main(
);
```

Descripció

La funció **smfi_main** es crida un cop s'ha completat l'inicialització del filtre.

Valors de retorn

La funció **smfi_main** retorna el valor MI_FAILURE si la connexió no s'ha pogut establir. Si no, la funció retorna MI_SUCCESS.

S'ha produït un error per diversos motius, i aquests motius es registren. Per exemple, passar una adreça no vàlida dins de la funció **smfi_setconn** fa que la funció falli.

Informació relacionada

"Funció smfi_setconn Function" a la pàgina 61

Funcions de l'accés de dades

Les funcions de l'accés de dades es criden dins de les funcions de crida de retorn que hi ha definides als filtres, per accedir a la informació sobre la connexió o al missatge actual .

Taula 10. Funcions de l'accés de dades

Element	Descripció
smfi_getsymal	La funció **smfi_getsymal** retorna el valor d'un símbol.
smfi_getpriv	La funció **smfi_getpriv** capta el punter de dades privades.
smfi_setpriv	La funció **smfi_setpriv** estableix el punter de dades privades.
smfi_setreply	La funció **smfi_setreply** estableix un codi de resposta específica que s'utilitzarà.
smfi_setmlreply	La funció **smfi_setmlreply** estableix la resposta específica de diverses línies que s'utilitzarà.

Funció smfi_getsymval:
Finalitat

La funció **smfi_getsymval** capta el valor d'una macro **sendmail** .

Sintaxi

```
#include <libmilter/mfapi.h>
char* smfi_getsymval(
SMFICTX *ctx,
char *headerf,
char *symname
);
```

Descripció

La funció **smfi_getsymval** es crida des de qualsevol de les funcions **xxfi_* callback** per afegir una capçalera al missatge. La definició de macro depèn de la funció que es crida.

Per defecte, són vàlides les macros següents:

Taula 11. Descripció

Element	Descripció
xxfi_connect	**daemon_name, if_name, if_addr, j, _**
xxfi_hello	**tls_version, cipher, cipher_bits, cert_subject, cert_issuer**
xxfi_envfrom	**i, auth_type, auth_authen, auth_ssf, auth_author, mail_mailer, mail_host, mail_addr**
xxfi_envrcpt	**rcpt_mailer, rcpt_host, rcpt_addr**
xxfi_data	Cap
xxfi_eoh	Cap
xxfi_eom	**msg_id**

Totes les macros segueixen actives des que es reben i fins el final de la connexió per a les funcions **xxfi_connect**, **xxfi_hello**.

Totes les macros segueixen actives fins el final del missatge per a la funció **xxfi_envfrom**, i la funció **xxfi_eom**.

Totes les macros segueixen actives per a cada destinatari de la funció **xxfi_envrcpt**.

La llista de macros es pot canviar a través de les opcions **confMILTER_MACROS_*** de **sendmail.mc**. L'àmbit d'aquestes macros es determina quan s'estableixen mitjançant l'ordre **sendmail**. Per a descripcions de valors de macros, vegeu *Guia de funcionament i d'instal•lació de sendmail*.

Arguments

Taula 12. Arguments

Element	Descripció
ctx	L'estructura de context opaca es manté en el paràmetre **libmilter**.
symname	El nom d'una macro **sendmail**. Les macros de lletra única poden estar, de forma opcional, entre claus ("{" i "}"), els noms de macro més llargs han d'estar entre claus, com en un fitxer **sendmail.cf**.

Valors de retorn

La funció **smfi_getsymval** retorna el valor de la macro com una sèrie acabada amb valor nul. En cas contrari, si la macro no està definida, la funció **smfi_getsymval** retorna el valor NULL.

Informació relacionada

"Funció de crida de retorn xxfi_connect" a la pàgina 83

"Funció de crida de retorn xxfi_helo" a la pàgina 84

"Funció de crida de retorn xxfi_envfrom" a la pàgina 85

"Funció de crida de retorn xxfi_envrcpt" a la pàgina 86

"Funció de crida de retorn xxfi_data" a la pàgina 87

"Funció de crida de retorn xxfi_eoh" a la pàgina 89

"Funció de crida de retorn xxfi_eom" a la pàgina 90

La funció smfi_getpriv:
Finalitat

La funció **smfi_getpriv** capta el punter de dades específiques de connexió per a aquesta connexió.

Sintaxi

```
#include <libmilter/mfapi.h>
void* smfi_getpriv(
SMFICTX *ctx
);
```

Descripció

La funció **smfi_getpriv** es pot cridar en qualsevol de les funcions **xxfi_* callback**.

Arguments

Taula 13. Arguments

Element	Descripció
ctx	L'estructura de context opaca es manté en el paràmetre **libmilter**.

Valors de retorn

La funció **smfi_getpriv** que s'emmagatzema retorna el punter de dades privades emmagatzemat a través d'una crida abans la funció **smfi_setpriv**. Si no, la funció **smfi_setpriv** retorna un valor NULL si el valor no està establert.

Informació relacionada

"Funció smfi_setpriv"

Funció smfi_setpriv:
Finalitat

La funció **smfi_setpriv** estableix el punter de dades privades per a aquesta connexió.

Sintaxi

```
#include <libmilter/mfapi.h>
int smfi_setpriv
SMFICTX *ctx,
void *privatedata
();
```

Descripció

La funció **smfi_setpriv** es crida des de qualsevol de les funcions **xxfi_* callback** per establir el punter de dades privades per a *ctx*.

Nota: Hi ha un punter de dades privades per connexió, les crides múltiples a la funció **smfi_setpriv** amb diversos valors provoquen que els valors anteriors es perdin. Abans que un filtre finalitzi, ha d'alliberar les dades privades i establir el punter amb un valor nul.

Arguments

Taula 14. Arguments

Element	Descripció
ctx	L'estructura de context opaca es manté en el paràmetre **libmilter**.
privatedata	Els punts de l'argument per a les dades privades. Aquest valor es retorna mitjançant crides següents a la funció **smfi_getpriv** utilitzant *ctx*.

Valors de retorn

La funció **smfi_setpriv** retorna el valor MI_FAILURE si *ctx* és un context no vàlid. Si no, la funció retorna MI_SUCCESS.

Informació relacionada

"Funció smfi_setpriv" a la pàgina 67

Funció smfi_setreply:
Finalitat

La funció **smfi_setreply** estableix el codi de resposta a l'error del protocol simple de transferència de correu (SMTP) i només accepta els codis de resposta 4XX i 5XX.

Sintaxi

```
#include <libmilter/mfapi.h>
int smfi_setreply
SFICTX *ctx,
char *rcode,
char *xcode,
char *message
);
```

Descripció

La funció **smfi_setreply** es crida des de qualsevol de les funcions **xxfi_ callback** excepte la **xxfi_connect**. La funció **smfi_setreply** estableix el codi de resposta d'error d'SMTP per a la connexió. Aquest codi s'utilitza per a respostes d'error subsegüents que han sorgit a causa d'accions realitzades per aquest filtre.

No es comprova si aquests valors passats a la funció **smfi_setreply** compleixen els estàndards.

L'argument *message* només ha de contenir caràcters imprimibles. Els altres caràcters poden provocar un comportament no definit. Per exemple, els caràcters com CR o LF provoquen que la crida falli, i els caràcters únics '%' provoquen que s'ignori el text.

Nota: Si es necessita una sèrie '%' al paràmetre, utilitzeu '%%' com a printf(3).

Per obtenir més detalls sobre els codis de resposta i què signifiquen, vegeu RFC 821 o 2821 i RFC 1893 o 2034.

Si l'argument *rcode* està establert com a 4XX però s'utilitza el valor SMFI_REJECT per al missatge, no s'utilitzarà la resposta personalitzada.

Si l'argument *rcode* està establert com a 5XX però s'utilitza el valor SMFI_TEMPFAIL per al missatge, no s'utilitzarà la resposta personalitzada.

Nota: En els dos casos anteriors, es retorna un error al paràmetre **milter**. El paràmetre **Libmilter** ignora el codi de resposta anterior.

Si el paràmetre **milter** retorna el valor SMFI_TEMPFAIL i estableix el codi de resposta 421, el servidor SMTP finalitza la sessió SMTP amb un codi d'error 421.

Arguments

Taula 15. Arguments

Element	Descripció
ctx	L'estructura de context opaca es manté en el paràmetre **libmilter**.
rcode	El codi de resposta SMTP de tres dígits(RFC 821 or 2821) és una sèrie acabada amb valor nul. *rcode* no pot ser un valor NULL, i ha de ser un codi de resposta 4XX o 5XX vàlid.
xcode	El codi de resposta ampliat (RFC 1893 o 2034). Si *xcode* és un valor NULL, no s'utilitzarà el codi ampliat. Si no, *xcode* ha d'ajustar-se a RFC 1893 o 2034.
message	La part del text de la resposta SMTP. Si el missatge és NULL, s'utilitzarà un missatge buit.

Valors de retorn

La funció **smfi_setreply** retorna el valor MI_FAILURE en els casos següents. Si no, la funció retorna MI_SUCCESS.

- L'argument *rcode* o *xcode* no és vàlid.
- S'ha produït un error d'assignació de memòria.

Informació relacionada

"Funció de crida de retorn xxfi_connect" a la pàgina 83

Funció smfi_setmlreply:
Finalitat

La funció **smfi_setmlreply** estableix el codi de resposta d'error del Simple Mail Transfer Protocol (SMTP) amb una resposta de diverses línies. La funció **smfi_setmlreply** només accepta respostes 4XX i 5XX .

Sintaxi

```
#include <libmilter/mfapi.h>
int smfi_setmlreply(
SMFICTX *ctx,
char *rcode,
char *xcode,
...
);
```

Descripció

La funció **smfi_setmlreply** es crida des de qualsevol de les funcions **xxfi_callback**, excepte la funció **xxfi_connect** . La funció **smfi_setmlreply** proporciona el codi de resposta d'error SMTP per a les connexions mencionades a sota de *xcode*. La llista d'arguments ha d'acabar amb nul. Aquest codi s'utilitza per a respostes d'error subsegüents que han sorgit a causa d'accions realitzades per aquest filtre.

Dels valors passats a la funció **smfi_setmlreply** no se'n comprova el compliment d'estàndards.

El paràmetre `missatge` ha de contenir només caràcters imprimibles, els altres caràcters poden produir un comportament no definit. Per exemple, els caràcters com CR o LF poden provocar que la crida doni error, els caràcters únics '%' fan que s'ignori el text.

Nota: Si es necessita una sèrie '%' en el paràmetre `missatge`, utilitzeu la sèrie '%%' de manera similar a com s'utilitza la sèrie **printf(3)**.

Per obtenir els codis de resposta i els seus significats, vegeu RFC 821 o 2821 i RFC 1893 o 2034.

Si el *rcode* està establert com a `4XX` , però el valor SMFI_REJECT s'utilitza per al missatge, no s'utilitzarà la resposta personalitzada.

Si el *rcode* està establert com a `5XX`, però el valor SMFI_TEMPFAIL s'utilitza per al missatge, no s'utilitzarà la resposta personalitzada.

Nota: En els dos casos anteriors, s'ha retornat un error al paràmetre **milter** , i el paràmetre **Libmilter** ignorarà aquest error.

Si el paràmetre **milter** retorna el valor SMFI_TEMPFAIL i estableix el codi de resposta `421`, el servidor SMTP finalitza la sessió SMTP amb el codi d'error `421`.

Arguments

Taula 16. Arguments

Element	Descripció
ctx	L'estructura de context opaca es manté en el paràmetre **libmilter**.
rcode	El codi de resposta SMTP de tres dígits (RFC 821 o 2821), com una sèrie acabada amb un valor nul. L'argument *rcode* no pot ser NULL, i ha de ser un codi de resposta vàlid `4XX` o `5XX`.
xcode	El codi de resposta ampliat (RFC 1893 o 2034). Si *xcode* és NULL, no s'utilitzarà un codi ampliat. Altrament, *xcode* ha d'ajustar-se a RFC 1893 o 2034
...	La resta d'arguments són línies úniques de text, fins a 32 arguments, que s'utilitzen com a part del text de la resposta SMTP.La llista ha d'acabar amb un valor nul.

Valors de retorn

La funció **smfi_setmlreply** retorna el valor MI_FAILURE en els casos següents. Si no, la funció retorna MI_SUCCESS.

- L'argument *rcode* o *xcode* no és vàlid.
- S'ha produït un error d'assignació de memòria.
- La línia de text conté un retorn de carro o salt de línia.
- La longitud de qualsevol línia de text és superior a `MAXREPLYLEN(980)`.
- Les respostes de text superen les 32 línies.

Exemple

```
ret = smfi_setmlreply(ctx, "550", "5.7.0",
"Accés de generador de correu brossa rebutjat",
"Vegeu la nostra política a:",
 "http://www.example.com/spampolicy.html",
NULL);
```

L'exemple anterior dóna el resultat següent :

```
Accés de generador de correu brossa rebutjat 550-5.7.0
Vegeu la nostra política 550-5.7.0 a:
550 5.7.0 http://www.example.com/spampolicy.html
```

Informació relacionada

"Funció de crida de retorn xxfi_connect" a la pàgina 83

Funcions de modificació de missatges

Les funcions de modificació de missatges canvien el contingut i els atributs del missatge. Les funcions es criden només mitjançant la funció **xxfi_eom**. Les funcions de modificació de missatges poden invocar comunicació addicional amb l'agent de transferència de correu (MTA). Aquestes funcions retornen el valor MI_SUCCESS o MI_FAILURE per indicar l'estat de l'operació.

Nota: Les dades del missatge (remitents, destinataris, capçaleres, i fragments del cos) que es passen a les funcions de modificació de missatges en el paràmetre es copien i no cal que es guardin (la memòria assignada es pot alliberar).

Per cridar una funció de modificació de missatges, el filtre ha d'establir l'indicador adequat en la descripció que es passa a la funció **smfi_register** . Si l'indicador no està establert, MTA considerarà la crida a la funció com un error error de filtre i finalitzarà la connexió.

Nota: L'estat retornat per la funció indica si el filtre del missatge s'ha enviat correctament a l'MTA. L'estat no indica si l'MTA ha realitzat l'operació sol•licitada. Per exemple, la funció **smfi_header**, quan es crida amb un nom de capçalera il•legal, retorna l'indicador MI_SUCCESS encara que posteriorment l'MTA pugui rebutjar que s'afegeixi la capçalera il•legal.

Taula 17. Funcions de modificació

Element	Descripció	funció
smfi_addheader	La funció **smfi_addheader** afegeix una capçalera al missatge.	**SMFIF_ADDHDRS**
smfi_chgheader	La funció **smfi_chgheader** modifica o suprimeix una capçalera.	**SMFIF_CHGHDRS**
smfi_insheader	La funció **smfi_insheader** insereix una capçalera al missatge.	**SMFIF_ADDHDRS**
smfi_chgfrom	La funció **smfi_chgfrom** modifica l'adreça del remitent del sobre.	**SMFIF_CHGFROM**
smfi_addrcpt	La funció **smfi_addrcpt** afegeix un destinatari al sobre.	**SMFIF_ADDRCPT**
smfi_addrcpt_par	La funció **smfi_addrcpt_par** afegeix un destinatari, el paràmetre del protocol simple de transferència de correu ampliat (ESMTP) al sobre inclòs.	**SMFIF_ADDRCPT_PAR**
smfi_delrcpt	La funció **smfi_delrcpt** suprimeix un destinatari del sobre.	**SMFIF_DELRCPT**
smfi_replacebody	La funció **smfi_replacebody** substitueix el cos del missatge.	**SMFIF_CHGBODY**

Funció smfi_addheader:
Finalitat

La funció **smfi_addheader** afegeix una capçalera al missatge actual.

Sintaxi

```
#include <libmilter/mfapi.h>
int smfi_addheader(
SMFICTX *ctx,
char *headerf,
char *headerv
);
```

Descripció

La funció **smfi_addheader** es crida des de la funció **xxfi_eom** per afegir una capçalera al missatge.

La funció **smfi_addheader** no modifica les capçaleres de missatge existents.

Per modificar el valor actual d'una capçalera, utilitzeu la funció **smfi_chgheader** .

Un filtre que crida la funció **smfi_addheader** ha d'establir l'indicador **SMFIF_ADDHDRS** en l'argument `smfiDesc_str`. Després, el filtre passa el valor a la funció **smfi_register**.

La funció **smfi_addheader** requereix que s'especifiqui l'ordre de filtre. Podeu visualitzar les modificacions de la capçalera utilitzant els filtres creats anteriorment.

No s'ha comprovat el compliment d'estàndards del nom o del valor de la capçalera. Tot i així, cada línia de la capçalera ha de tenir menys de 998 caràcters. Si necessiteu una capçalera més llarga, utilitzeu una capçalera de més d'una línia. Si heu de crear una capçalera de més d'una línia, inseriu un salt de pàgina (`ASCII 0x0a`, o `\n` en el llenguatge de programació C) seguit d'un caràcter d'espai en blanc com ara un espai (`ASCII 0x20`) o un tabulador (`ASCII 0x09`, o `\t` en el llenguatge de programació C). El salt de pàgina no pot anar precedit d'un retorn de carro (`ASCII 0x0d`). L'agent de transferència de correu (MTA) l'afegeix automàticament. La responsabilitat dels escriptors de filtres és assegurar-se que no s'infringeixi cap estàndard.

L'MTA afegeix un espai inicial a un valor de capçalera afegit llevat que s'estableixi l'indicador **SMFIP_HDR_LEADSPC** , i en aquest cas, el paràmetre **milter** ha d'incloure qualsevol espai inicial desitjat.

Arguments

Taula 18. Arguments

Element	Descripció
ctx	L'estructura de context opaca es manté en el paràmetre **libmilter**.
headerf	El nom de capçalera és una sèrie acabada amb un valor nul que no és NULL.
headerv	El valor de capçalera que s'afegirà pot ser una sèrie acabada amb un valor nul, no NULL o una sèrie buida.

Valors de retorn

La funció **smfi_addheader** retorna el valor MI_FAILURE en els casos següents. Si no, la funció retorna MI_SUCCESS.

- L'argument *headerf* o *headerv* és NULL.
- Afegir capçaleres en l'estat de connexió actual no és vàlid.
- L'assignació de memòria ha fallat.
- S'ha produït un error de xarxa.
- L'indicador **SMFIF_ADDHDRS** no estava establert quan s'ha cridat la funció **smfi_register**.

Exemple

```
int ret;
SMFICTX *ctx;
...
ret = smfi_addheader(ctx, "Content-Type",
"multipart/mixed;\n\tboundary=\"foobar\"");
```

Informació relacionada

"Funció de crida de retorn xxfi_eom" a la pàgina 90

"Funció smfi_chgheader"

"Funció smfi_register" a la pàgina 58

Funció smfi_chgheader:
Finalitat

La funció **smfi_chgheader** modifica o suprimeix una capçalera de missatge.

Sintaxi

```
#include <libmilter/mfapi.h>
int smfi_chgheader(
SMFICTX *ctx,
char *headerf,
mi_int32 hdridx,
char *headerv
);
```

Descripció

La funció **smfi_chgheader** es crida des de la funció **xxfi_eom** per modificar un valor de capçalera per al missatge actual.

La funció **smfi_chgheader** es pot utilitzar per afegir capçaleres noves. Tot i així, és més eficaç i segur utilitzar la funció **smfi_addheader** .

Un filtre que crida la funció **smfi_chgheader** ha d'establir l'indicador **SMFIF_CHGHDRS** en l'argument `smfiDesc_str`. Després, el filtre passa el valor a la funció **smfi_register**.

La funció **smfi_chgheader** requereix que s'especifiqui l'ordre de filtre. Podeu visualitzar les modificacions de la capçalera utilitzant els filtres creats anteriorment.

No s'ha comprovat el compliment d'estàndards del nom o del valor de la capçalera. Tot i així, cada línia de la capçalera ha de tenir menys de 998 caràcters. Si necessiteu una capçalera més llarga, utilitzeu una capçalera de més d'una línia. Si heu de crear una capçalera de més d'una línia, inseriu un salt de pàgina (`ASCII 0x0a`, o `\n` en el llenguatge de programació C) seguit d'un caràcter d'espai en blanc com ara un espai (`ASCII 0x20`) o un tabulador (`ASCII 0x09`, o `\t` en el llenguatge de programació C). El salt de pàgina no pot anar precedit d'un retorn de carro (`ASCII 0x0d`), el Mail Transfer Agent (MTA) l'afegeix automàticament. La responsabilitat dels escriptors de filtres és assegurar-se que no s'infringeixi cap estàndard.

L'MTA afegeix un espai inicial a un valor de capçalera afegit llevat que s'estableixi l'indicador **SMFIP_HDR_LEADSPC** , i en aquest cas, el paràmetre **milter** ha d'incloure l'espai inicial desitjat.

Arguments

Taula 19. Arguments

Element	Descripció
ctx	L'estructura de context opaca es manté en el paràmetre **libmilter**.
headerf	El nom de capçalera és una sèrie acabada amb un valor nul que no és NULL.
hdridx	El valor d'índex de capçalera (basat en u). Un valor *hdridx* d'u modifica la primera aparició d'una capçalera anomenada *headerf*. Si *hdridx* supera el nombre de vegades que apareix *headerf*, s'afegeix una còpia nova de *headerf*.
headerv	El valor de capçalera que s'afegirà pot ser una sèrie acabada amb un valor nul no NULL o una sèrie buida.

Valors de retorn

La funció **smfi_chgheader** retorna el valor MI_FAILURE en els casos següents. Si no, la funció retorna MI_SUCCESS.

- L'argument *headerf* és NULL.
- Modificar capçaleres en l'estat de connexió actual no és vàlid.
- L'assignació de memòria ha fallat.
- S'ha produït un error de xarxa.
- L'indicador **SMFIF_CHGHDRS** no estava establert quan s'ha cridat la funció **smfi_register**.

Exemple

```
int ret;
SMFICTX *ctx;
...

ret = smfi_chgheader(ctx, "Content-Type", 1,
"multipart/mixed;\n\tboundary=\"foobar\"");
```

Informació relacionada

"Funció de crida de retorn xxfi_eom" a la pàgina 90

"Funció smfi_addheader" a la pàgina 71

Funció smfi_insheader:

Finalitat

La funció **smfi_insheader** afegeix una capçalera al missatge actual.

Sintaxi

```
#include <libmilter/mfapi.h>
int smfi_insheader(
SMFICTX ,
int hdridx,
char *headerf,
char *headerv
);
```

Descripció

La funció **smfi_insheader** es crida des de la funció **xxfi_eom** per afegir una capçalera al missatge actual.

La funció **smfi_insheader** no modifica les capçaleres existents d'un missatge.

Per canviar el valor actual d'una capçalera, utilitzeu la funció **smfi_chgheader**.

Un filtre que crida la funció **smfi_insheader** ha d'establir l'indicador **SMFIF_ADDHDRS** en l'argument `smfiDesc_str` que es passa en la funció **smfi_register**.

La funció **smfi_insheader** requereix que s'especifiqui l'ordre de filtre. Podeu visualitzar les modificacions de la capçalera utilitzant els filtres creats anteriorment.

Un filtre rep capçaleres que s'envien mitjançant el client del protocol simple de transferència de correu (SMTP) i també les capçaleres modificades pels filtres anteriors. Les capçaleres inserides per l'ordre **sendmail** i les inserides per si mateixes no es reben. La posició per inserir la capçalera depèn de les capçaleres que hi ha al missatge d'entrada i també de les capçaleres configurades per afegir amb l'ordre **sendmail**.

Per exemple, l'ordre **sendmail** sempre afegeix un **Received: header** al principi de la capçalera. En establir el valor *hdridx* com a `0`, la capçalera s'insereix abans del paràmetre **Received: header**. Tot i així, quedaran corromputs quan rebin la capçalera afegida, però no la **Received: header**, cosa que farà difícil inserir una capçalera en una posició fixa.

Si el valor *hdridx* és superior al nombre de capçaleres del missatge, la capçalera s'afegeix.

No s'ha comprovat el compliment d'estàndards del nom o del valor de la capçalera. Tot i així, cada línia de la capçalera ha de tenir menys de 998 caràcters. Si necessiteu una capçalera més llarga, utilitzeu una capçalera de més d'una línia. Si heu de crear una capçalera de més d'una línia, inseriu un salt de pàgina (`ASCII 0x0a`, o `\n` en el llenguatge de programació C) seguit d'un caràcter d'espai en blanc com ara un espai (`ASCII 0x20`) o un tabulador (`ASCII 0x09`, o `\t` en el llenguatge de programació C). El salt de pàgina no pot anar precedit d'un retorn de carro (`ASCII 0x0d`). L'agent de transferència de correu (MTA)afegeix automàticament el retorn de carro. La responsabilitat dels escriptors de filtres és assegurar-se que no s'infringeixi cap estàndard.

L'MTA afegeix un espai inicial a un valor de capçalera inserit llevat que s'estableixi l'indicador **SMFIP_HDR_LEADSPC**, en aquest cas, el paràmetre **`milter`** ha d'incloure qualsevol espai inicial desitjat.

Arguments

Taula 20. Arguments

Element	Descripció
ctx	L'estructura de context opaca es manté en el paràmetre **`libmilter`**.
headerf	El nom de capçalera és una sèrie acabada amb un valor nul que no és NULL.
headerv	El valor de capçalera que s'afegirà pot ser una sèrie acabada amb un valor nul no NULL o una sèrie buida.

Valors de retorn

La funció **smfi_insheader** retorna el valor MI_FAILURE en els casos següents, en cas contrari, la funció retorna MI_SUCCESS.

- L'argument *headerf* o *headerv* és NULL.
- Afegir capçaleres en l'estat de connexió actual no és vàlid.
- L'assignació de memòria ha fallat.
- S'ha produït un error de xarxa.
- L'indicador **SMFIF_ADDHDRS** no estava establert quan s'ha cridat la funció **smfi_register**.

Exemple

```
int ret;
SMFICTX *ctx;
...
ret = smfi_insheader( ctx, 0, "First", "See me?");;
```

Informació relacionada

"Funció de crida de retorn xxfi_eom" a la pàgina 90

"Funció smfi_register" a la pàgina 58

"Funció smfi_chgheader" a la pàgina 73

Funció smfi_chgfrom:

Finalitat

La funció **smfi_chgfrom** modifica el remitent del missatge (MAIL From) per al missatge actual.

Sintaxi

```
#include <libmilter/mfapi.h>
int smfi_chgfrom(
SMFICTX *ctx,
const char *mail,
char *args
);
```

Descripció

La funció **smfi_chgfrom** es crida des de la funció **xxfi_eom** per modificar el remitent del missatge i el MAIL From del missatge actual.

Un filtre que crida la funció **smfi_chgfrom** ha d'establir l'indicador **SMFIF_CHGFROM** en l'argument `smfiDesc_str`. Després, el filtre passa el valor a la funció **smfi_register**.

Tots els arguments de protocol simple de transferència de correu ampliat (ESMTP) es poden establir a través de la crida. Però establir valors per alguns dels arguments com `SIZE` i `BODY` crea problemes. Per tant, heu d'anar en compte a l'hora d'establir els arguments. No hi ha comentaris de l'agent de transferència de correu (MTA) al paràmetre **milter** sobre si la crida és correcta o no.

Arguments

Taula 21. Arguments

Element	Descripció
ctx	L'estructura de context opaca es manté en el paràmetre **libmilter**.
correu	L'adreça del nou remitent.
args	Els arguments del protocol simple de transferència de correu ampliat (ESMTP).

Valors de retorn

La funció **smfi_chgfrom** retorna el valor MI_FAILURE en els casos següents. Si no, la funció retorna MI_SUCCESS.

- L'argument *correu* és NULL.
- Canviar el remitent en l'estat de connexió actual no és vàlid.

- S'ha produït un error de xarxa.
- L'indicador **SMFIF_CHGFROM** no estava establert quan s'ha cridat la funció **smfi_register**.

Informació relacionada

"Funció de crida de retorn xxfi_eom" a la pàgina 90

"Funció smfi_register" a la pàgina 58

Funció smfi_addrcpt:
Finalitat

La funció **smfi_addrcpt** afegeix un destinatari per al missatge actual .

Sintaxi

```
#include <libmilter/mfapi.h>
int smfi_addrcpt(
SMFICTX *ctx
char *rcpt
);
```

Descripció

La funció **smfi_addrcpt** es crida només des de la funció **xxfi_eom** per afegir un destinatari al sobre del missatge.

Nota: El filtre que crida la funció **smfi_addrcpt** ha d'establir l'indicador **SMFIF_ADDRCPT** en l'estructura **smfiDesc_str** que es passa a la funció **smfi_register**.

Arguments

Taula 22. Arguments

Element	Descripció
ctx	L'estructura de context opaca es manté en el paràmetre **libmilter**.
rcpt	L'adreça del nou destinatari.

Valors de retorn

La funció **smfi_addrcpt** retorna el valor MI_FAILURE en els casos següents. Si no, la funció retorna MI_SUCCESS.

- L'argument *rcpt* és NULL.
- Afegir destinataris a la connexió actual no és vàlid.
- S'ha produït un error de xarxa.
- L'indicador **SMFIF_ADDRCPT** no estava establert quan s'ha cridat la funció **smfi_register**.

Informació relacionada

"Funció de crida de retorn xxfi_eom" a la pàgina 90

"Funció smfi_register" a la pàgina 58

Funció smfi_addrcpt_par:

Finalitat

La funció **smfi_addrcpt_par** afegeix un destinatari per al missatge actual i inclou arguments de protocol simple de transferència de correu ampliat (ESMTP).

Sintaxi

```
#include <libmilter/mfapi.h>
int smfi_addrcpt_par(
SMFICTX *ctx,
char *rcpt,
char *args
);
```

Descripció

La funció **smfi_addrcpt_par** es crida des de la funció **xxfi_eom** per afegir un destinatari al sobre del missatge.

Arguments

Taula 23. Arguments

Element	Descripció
ctx	L'estructura de context opaca es manté en el paràmetre **libmilter**.
rcpt	L'adreça del nou destinatari.
args	Els paràmetres d'ESMTP del nou destinatari.

Valors de retorn

La funció **smfi_addrcpt** retorna el valor MI_FAILURE en els casos següents. Si no, la funció retorna MI_SUCCESS.

- L'argument *rcpt* és NULL.
- Afegir destinataris a la connexió actual no és vàlid.
- S'ha produït un error de xarxa.
- L'indicador **SMFIF_ADDRCPT_PAR** no estava establert quan s'ha cridat la funció **smfi_register** .

Informació relacionada

"Funció smfi_addrcpt" a la pàgina 77

"Funció smfi_register" a la pàgina 58

Funció smfi_delrcpt:

Finalitat

La funció **smfi_delrcpt** suprimeix el destinatari del sobre per al missatge actual.

Sintaxi

```
#include <libmilter/mfapi.h>
int smfi_delrcpt(
 SMFICTX *ctx;
  char *rcpt;
);
```

Descripció

La funció **smfi_delrcpt** es crida des de la funció de crida de retorn **xxfi_eom** per eliminar el nom del destinatari del sobre de missatges actual.

Nota: Les adreces que s'han d'eliminar han de coincidir exactament.Per exemple, una adreça i la seva forma ampliada no coincideixen.

Arguments

Taula 24. Arguments

Element	Descripció
ctx	L'estructura de context opaca es manté en el paràmetre **libmilter**.
rcpt	L'adreça de destinatari que s'eliminarà, una sèrie acabada en valor nul i no NULL

Valors de retorn

La funció **smfi_delrcpt** retorna el valor MI_FAILURE en els casos següents. Si no, la funció retorna MI_SUCCESS.

- L'argument *rcpt* és NULL.
- Suprimir els destinataris en l'estat de connexió actual no és vàlid.
- S'ha produït un error de xarxa.
- L'indicador SMFIF_DELRCPT no estava establert quan s'ha cridat la funció **smfi_register**.

Informació relacionada

smfi_register

xxfi_eom

Funció smfi_replacebody:
Finalitat

La funció **smfi_replacebody** substitueix el cos del missatge.

Sintaxi

```
#include <libmilter/mfapi.h>
int smfi_replacebody(
  SMFICTX *ctx,
  unsigned char *bodyp,
 int bodylen
);
```

Descripció

La funció **smfi_replacebody** substitueix el cos del missatge actual. Si la funció es crida més d'una vegada, les crides següents fan que s'adjuntin dades al nou cos. Es pot cridar la funció més d'una vegada.

Com que el cos del missatge és massa gran, establir l'indicador SMFIF_CHGBODY podria afectar de forma significativa el rendiment del filtre.

Si un filtre estableix l'indicador SMFIF_CHGBODY però no crida la funció **smfi_replacebody**, el cos original seguirà sense canviar-se.

L'ordre de filtre és important per la funció **smfi_replacebody**. Els continguts nous del cos es creen mitjançant filtres antics en els fitxers de filtre nous.

Arguments

Taula 25. Arguments

Element	Descripció
ctx	L'estructura de context opaca es manté en el paràmetre **libmilter**.
bodyp	Un punter en l'inici de les dades del cos nou que no té per què acabar amb un valor nul. Si el *bodyp* és NULL, es tractarà com si tingués longitud == 0. Les dades del cos han d'estar en format CR o LF.
bodylen	El nombre bits apuntats per *bodyp*.

Valors de retorn

La funció **smfi_replacebody** retorna el valor MI_FAILURE en els casos següents. Si no, la funció retorna MI_SUCCESS.

- *bodyp* == NULL i *bodylen* > 0
- Canviar el cos en l'estat de connexió actual no és vàlid.
- S'ha produït un error de xarxa.
- L'indicador SMFIF_CHGBODY no estava establert quan s'ha cridat la funció **smfi_register**.

Informació relacionada

smfi_register

Funció de gestió de missatges

Les funcions de gestió de missatges donen instruccions especials sobre com gestionarel paràmetre **milter** o l'agent de transferència de correu (MTA), sense alterar el contingut ni l'estat del missatge. Les Funcions de gestió de missatges només es poden cridar en la funció **xxfi_eom**. La funció **xxfi_eom** pot invocar comunicació addicional amb l'MTA y retornatant el valor MI_SUCCESS com MI_FAILURE per indicar l'estat de l'operació.

Nota: L'estat retornat per la funció indica si el filtre del missatge s'ha enviat correctament a l'MTA. L'estat no indica si l'MTA ha realitzat l'operació sol•licitada.

Taula 26. Funció de gestió de missatges

Element	Descripció
smfi_progress	La funció **smfi_progress** informa sobre el progrés de l'operació.
smfi_quarantine	La funció **smfi_quarantine** posa en quarantena un missatge.

La funció smfi_progress:
Finalitat

La funció **smfi_progress** informa sobre el progrés de l'operació.

Sintaxi

```
#include <libmilter/mfapi.h>
int smfi_progress(
 SMFICTX *ctx;
);
```

Descripció

La funció **smfi_progress** es crida des de la funció de retorn **xxfi_eom** per notificar a l'agent de transferència de correu (MTA) que el filtre encara funciona en un missatge. Aquesta funció fa que l'MTA reiniciï els temps d'espera.

Arguments

Taula 27. Arguments

Element	Descripció
ctx	L'estructura de context opaca es manté en el paràmetre **libmilter**.

Valors de retorn

La funció **smfi_progress** retorna el valor MI_FAILURE si hi ha un error de xarxa. Si no, la funció retorna MI_SUCCESS.

Informació relacionada

xxfi_eom

Funció smfi_quarantine: Finalitat

La funció **smfi_quarantine** posa el missatge en quarantena.

Sintaxi

```
#include <libmilter/mfapi.h>
int smfi_quarantine(
 SMFICTX *ctx;
  char *reason;
);
```

Descripció

La funció **smfi_quarantine** es crida des de la funció de crida de retorn **xxfi_eom** per posar en quarantena un missatge utilitzant un motiu determinat.

Arguments

Taula 28. Arguments

Element	Descripció
ctx	L'estructura de context opaca es manté en el paràmetre **libmilter**.
motiu	El motiu de la quarantena, una sèrie acabada amb un valor nul, no NULL, i no buit.

Valors de retorn

La funció **smfi_quarantine** retorna el valor MI_FAILURE en els casos següents. Si no, la funció retorna MI_SUCCESS.

- El *motiu* és NULL o buit.
- S'ha produït un error de xarxa.
- L'indicador SMFIF_QUARANTINE no estava establert quan s'ha cridat la funció **smfi_register**.

Informació relacionada

smfi_register

xxfi_eom

Funcions de crida de retorn

El filtre sendmail ha d'implementar una o divereses funcions de crida de retorn, que es registraran mitjançant la funció **smfi_register**.

Taula 29. Funcions de crida de retorn

Element	Descripció
xxfi_connect	La funció **xxfi_connect** es crida una vegada en l'inici de cada connexió SMTP. La funció retorna el valor SMFIS_CONTINUE.
xxfi_hello	La funció **xxfi_hello** es crida sempre que el client envia una ordre HELO/EHLO.
xxfi_envfrom	La funció **xxfi_envfrom** es crida al principi d'un missatge.
xxfi_envrcpt	La funció **xxfi_envrcpt** es crida per a cada destinatari.
xxfi_data	La funció **xxfi_data** gestiona l'ordre DATA.
xxfi_unknown	La funció **xxfi_unknown** gestiona ordres de Simple Mail Transfer Protocol (SMTP).
xxfi_header	La funció **xxfi_header** gestiona la capçalera del missatge.
xxfi_eoh	La funció **xxfi_eoh** gestiona les capçaleres del missatge.
xxfi_body	La funció **xxfi_body** gestiona un fragment del cos del missatge.
xxfi_eom	La funció **xxfi_eom** gestiona el final del missatge.
xxfi_abort	La funció **xxfi_abort** gestiona els missatges que s'han avortat.
xxfi_close	La funció **xxfi_close** es crida per finalitzar la connexió actual.
xxfi_negotiate	La funció **xxfi_negotiate** es crida a l'inici de la connexió SMTP.

Les funcions de crida de retorn han de retornar un valor adequat. Si les funcions de crida de retorn retornen qualsevol altre valor que no sigui el que hi ha definit, es produeix un error i l'ordre **sendmail** finalitza la connexió amb el filtre.

El paràmetre **Milter** fa diferència entre rutines **orientades a la connexió** , de **destinatari-** i de **missatge**:

- Les funcions de crida de retorn **orientades al destinatari** afecta el processament d'un únic destinatari del missatge.
- Les funcions de crida de retorn **orientades al missatge** afecten a un únic missatge.
- Les funcions de crida de retorn **orientades a la connexió** afecten a tota una connexió (durant la qual es poden poden enviar missatges múltiples a diversos conjunts de destinataris).
- La funció **xxfi_envrcpt** està orientada al destinatari. Les funcions **xxfi_conect**, **xxfi_hello** i **xxfi_close** estan orientades a la connexió. Totes les altres funcions de crida de retorn estan orientades al missatge.

Taula 30. Funcions de crida de retorn

Element	Descripció
SMFIS_CONTINUE	Continueu processant la connexió actual, el missatge o el destinatari.
SMFIS_REJECT	• Per a una rutina **orientada a la connexió**, rebutgeu aquesta connexió; crideu **xxfi_close**. • Per a una rutina **orientada al missatge** (excepte per a la funció **xxfi_eom**, o **xxfi_abort**), rebutgeu aquest missatge. • Per a una rutina **orientada al destinatari**, rebutgeu el destinatari actual (però continueu processant el missatge actual).
SMFIS_DISCARD	• Per a una rutina **orientada al missatge** o **al destinatari** , accepteu aquest missatge, però descarteu-lo. • SMFIS_DISCARD no ha de retornar-se mitjançant una rutina **orientada a la connexió** .
SMFIS_ACCEPT	• Per a una rutina **orientada a la connexió**, accepteu aquesta connexió sense cap procés de filtratge addicional; crideu la funció **xxfi_close**. • Per a una rutina **orientada al missatge o al destinatari** , accepteu aquest missatge sense cap procés de filtratge addicional.
SMFIS_TEMPFAIL	Retorna un error temporal, això significa que l'ordre de simple mail transfer protocol (SMTP) retorna el codi d'estat `4xx`. • Per a una rutina **orientada al missatge** (excepte per a la funció **xxfi_envfrom**), aquest missatge dóna error. • Per a una rutina **orientada a la connexió** , aquesta connexió dóna error; cridi la funció **xxfi_close** . • Per a una rutina **orientada al destinatari** , només dóna error el destinatari actual ; continueu processant el missatge.
SMFIS_SKIP	En aquesta transacció, us podeu saltar les crides de retorn posteriors que siguin del mateix tipus. Actualment, aquest valor de retorn només està permès a la funció **xxfi_body** . El valor de retorn es pot utilitzar si un paràmetre **milter** ha rebut prou fragments del cos per prendre una decisió. Però si el valor de retorn encara vol invocar les funcions de modificació del missatge, només es poden cridar des de la funció **xxfi_eom**. **Nota:** El paràmetre **milter** ha de negociar aquest comportament amb l'agent de transferència de correu (MTA). El paràmetre **milter** comprova si l'acció de protocol SMFIP_SKIP està disponible. Si ho està, el paràmetre **milter** ha de sol•licitar-la.
SMFIS_NOREPLY	• No envieu una resposta a l'MTA. El paràmetre **milter** ha de negociar aquest comportament amb l'MTA. El paràmetre **milter** ha de comprovar si l'acció de protocol adequada SMFIP_NR_* està disponible. Si l'acció de protocol SMFIP_NR_* està disponible, el paràmetre **milter** ha de sol•licitar-la. • Si establiu l'acció de protocol SMFIP_NR_* per a una crida de retorn, aquesta sempre ha de respondre amb SMFIS_NOREPLY. Utilitzar un altre codi de resposta suposa una violació de l'interfície de programació d'aplicació (API). Si en alguns casos la vostra crida de retorn retorna un altre valor (a causa d'una reducció de recursos), no heu d'establir SMFIP_NR_* , sinó que heu d'utilitzar SMFIS_CONTINUE com a codi de retorn per defecte. Com a alternativa, podeu intentar retardar el fet d'informar sobre el problema a una crida de retorn posterior per a la qual SMFIP_NR_* no està establert.

Funció de crida de retorn xxfi_connect:

Finalitat

La funció de crida de retorn **xxfi_connect** proporciona informació sobre la connexió.

Sintaxi

```
#include <libmilter/mfapi.h>
sfsistat (*xxfi_connect)(
        SMFICTX    *ctx,
        char       *hostname,
        _SOCK_ADDR *hostaddr);
```

Descripció

La funció de crida de retorn **xxfi_connect** es crida un cop a l'inici de cada connexió de protocol simple de transferència de correu (SMTP) i retorna l'indicador `SMFIS_CONTINUE`.

Nota: Si un filtre anterior rebutja la connexió en la rutina de la funció de crida de retorn **xxfi_connect**, la funció de crida de retorn **xxfi_connect** del filtre no es cridarà.

Arguments

Taula 31. Arguments

Element	Descripció
ctx	L'estructura de context opaca es manté a **libmilter**.
nom_amfitrió	El nom del sistema principal del remitent del missatge, tal com determina una cerca inversa a l'adreça del sistema principal. Si la cerca inversa falla o si cap de les adreces IP del nom del sistema principal resolt coincideix amb l'adreça IP original, el nom de sistema principal podria contenir l'adreça IP del remitent del missatge, que es tancarà entre delimitadors (per exemple,`[a.b.c.d]'). Si la connexió de protocol simple de transferència de correu (SMTP) es realitza mitjançant stdin, el valor és localhost.
hostaddr	L'adreça del sistema principal, tal com es determina mitjançant la crida de retorn **getpeername(2)** call en el sòcol de l'SMTP. El valor és NULL si el tipus no s'admet en la versió actual o si la connexió SMTP es realitza mitjançant **stdin**.

Funció de crida de retorn xxfi_helo:
Finalitat

La funció de crida de retorn **xxfi_helo** gestiona l'ordre **HELO or EHLO**.

Sintaxi

```
#include <libmilter/mfapi.h>
sfsistat (*xxfi_helo)(
  SMFICTX *ctx,
 char *helohost
);
```

Descripció

La funció de crida de retorn **xxfi_hello** es crida sempre que el client envia una ordre **HELO or EHLO** i retorna l'indicador SMFIS_CONTINUE. Per tant, la crida de retorn es pot cridar diverses vegades o fins i tot no cridar-la. Es poden imposar restriccions mitjançant l'agent de transferència de correu (MTA).

Arguments

Taula 32. Arguments

Element	Descripció
ctx	L'estructura de context opaca es manté en el paràmetre **libmilter**.
helohost	El valor passat a l'ordre **HELO or EHLO** hauria de ser el nom del domini del sistema principal emissor

Funció de crida de retorn xxfi_envfrom: Finalitat

La funció de crida de retorn **xxfi_envfrom** gestiona l'ordre **MAIL** (remitent del sobre).

Sintaxi

```
#include <libmilter/mfapi.h>
sfsistat (*xxfi_envfrom)(
  SMFICTX *ctx,
 char **argv
);
```

Descripció

La funció de crida de retorn **xxfi_envfrom** es crida quan el client utilitza l'ordre **DATA** i retorna l'indicador SMFIS_CONTINUE.

Nota: Per obtenir més informació sobre les respostes d'ESMTP, vegeu RFC 1869.

Arguments

Taula 33. Arguments

Element	Descripció
ctx	L'estructura de context opaca es manté en el paràmetre **libmilter**.
argv	Els arguments de l'ordre SMTP acabats amb valor nul; està garantit que `argv[0]` sigui l'adreça del remitent. Els arguments posteriors són els arguments del protocol simple de transferència de correu ampliat (ESMTP).

Valors de retorn

Taula 34. Valors de retorn

Element	Descripció
SMFIS_TEMPFAIL	El remitent i el missatge es rebutgen amb un error temporal, més endavant es pot especificar un remitent nou (i un missatge nou)i la funció de crida de retorn **xxfi_abort** no es crida.
SMFIS_REJECT	El remitent i el missatge es rebutgen; es pot especificar un remitent i missatge nou i la funció de crida de retorn **xxfi_abort** no es crida.
SMFIS_DISCARD	El missatge s'accepta i es descarta, i la funció de crida de retorn **xxfi_abort** no es crida.
SMFIS_ACCEPT	El missatge s'accepta i la funció de crida de retorn **xxfi_abort** no es crida.

Informació relacionada

xxfi_abort

Funció de crida de retorn xxfi_envrcpt: Finalitat

La funció de crida de retorn **xxfi_envrcpt** gestiona l'ordre **RCPT**.

Sintaxi

```
#include <libmilter/mfapi.h>
sfsistat (*xxfi_envrcpt)(
  SMFICTX *ctx,
 char **argv
);
```

Descripció

La funció de crida de retorn **xxfi_envrcpt** es crida un cop per destinatari, i una o més vegades per missatge immediatament després de la funció de crida de retorn **xxfi_envfrom** i retorna l'indicador SMFIS_CONTINUE.

Nota: Per obtenir més informació sobre les respostes protocol simple de transferència de correu ampliat (ESMTP), vegeu RFC 1869.

Arguments

Taula 35. Arguments

Element	Descripció
ctx	L'estructura de context opaca es manté en el paràmetre **libmilter**.
argv	Els arguments de l'ordre SMTP acabats amb valor nul; està garantit que `argv[0]` sigui l'adreça del destinatari. Els arguments posteriors són els arguments del protocol simple de transferència de correu ampliat (ESMTP).

Valors de retorn

Taula 36. Valors de retorn

Element	Descripció
SMFIS_TEMPFAIL	El destinatari ha fallat temporalment, podeu enviar missatges a més destinataris i no es crida la funció de crida de retorn **xxfi_abort**.
SMFIS_REJECT	El destinatari es rebutja; es poden enviar missatges a més destinataris i es crida la funció de crida de retorn **xxfi_abort**.
SMFIS_DISCARD	El missatge s'accepta o es descarta, i es crida la funció de crida de retorn **xxfi_abort**.
SMFIS_ACCEPT	El destinatari s'accepta i no es crida la funció de crida de retorn **xxfi_abort**.

Informació relacionada

xxfi_envfrom

xxfi_abort

Funció de crida de retorn xxfi_data:
Finalitat

La funció de crida de retorn **xxfi_data** gestiona l'ordre **DATA**.

Sintaxi

```
#include <libmilter/mfapi.h>
sfsistat (*xxfi_data)(
 SMFICTX *ctx
);
```

Descripció

La funció de crida de retorn **xxfi_data** es crida quan el client utilitza l'ordre **DATA** i retorna l'indicador SMFIS_CONTINUE.

Nota: Per obtenir més informació sobre les respostes d'ESMTP, vegeu RFC 1869.

Arguments

Taula 37. Arguments

Element	Descripció
ctx	L'estructura de context opaca es manté en el paràmetre **libmilter**.

Valors de retorn

Taula 38. Valors de retorn

Element	Descripció
SMFIS_TEMPFAIL	El missatge es rebutja amb un error temporal.
SMFIS_REJECT	El missatge es rebutja.
SMFIS_DISCARD	El missatge s'accepta i es descarta.
SMFIS_ACCEPT	El missatge s'accepta.

Funció de crida de retorn xxfi_unknown:
Finalitat

La funció de crida de retorn **xxfi_unknown** gestiona les ordres desconegudes i no implementades del protocol simple de transferència de correu (SMTP).

Sintaxi

```
#include <libmilter/mfapi.h>
sfsistat (*xxfi_unknown)(
  SMFICTX *ctx,
  const char *arg
);
```

Descripció

La funció de crida de retorn **xxfi_unknown** es crida quan el client utilitza una ordre SMTP desconeguda o no implementada per l'agent de transferència de correu (MTA) i retorna l'indicador SMFIS_CONTINUE.

Nota: El servidor sempre rebutja l'ordre SMTP. Només és possible retornar un codi d'error diferent.

Arguments

Taula 39. Arguments

Element	Descripció
ctx	L'estructura de context opaca es manté en el paràmetre **libmilter**.
arg	L'ordre SMTP, amb tots els arguments inclosos.

Valors de retorn

Taula 40. Valors de retorn

Element	Descripció
SMFIS_TEMPFAIL	L'ordre es rebutja amb un error temporal.
SMFIS_REJECT	L'ordre es rebutja.

Funció de crida de retorn xxfi_header: Finalitat

La funció de crida de retorn **xxfi_header** gestiona la capçalera del missatge.

Sintaxi

```
#include <libmilter/mfapi.h>
sfsistat (*xxfi_header)(
  SMFICTX *ctx,
  char *headerf,
 char *headerv
);
```

Descripció

La funció de crida de retorn **xxfi_header** es crida un cop per a cada capçalera de missatge i retorna l'indicador SMFIS_CONTINUE.

Nota:

- Començant amb sendmail 8.14, els espais després dels dos punts en un camp de capçalera es reserven si se sol•liciten utilitzant l'indicador SMFIP_HDR_LEADSPC. Per exemple, la capçalera següent:

  ```
  From: sender <f@example.com>
  To:  user <t@example.com>
  Subject: no
  ```

  s'enviaria a un paràmetre milter de la manera següent:

  ```
  "From", " sender <f@example.com>"
  "To", "  user <t@example.com>"
  "Subject", "no"
  ```

  mentre que anteriorment (o sense l'indicador SMFIP_HDR_LEADSPC) era de la manera següent:

  ```
  "From", "sender <f@example.com>"
  "To", "user <t@example.com>"
  "Subject", "no"
  ```

- El filtre antic realitza canvis o addicions a la capçalera dels filtres nous.
- Per obtenir més informació sobre el format de capçalera, vegeu RFC 822 i RFC 2822.

Arguments

Taula 41. Arguments

Element	Descripció
ctx	L'estructura de context opaca es manté en el paràmetre **libmilter**.
headerf	El nom del camp de capçalera.
headerv	El valor del camp de capçalera. El contingut de la capçalera pot incloure un espai en blanc plegat, o sigui, diverses línies amb l'espai en blanc següent on les línies estan separades per LF (ni CR o LF). S'elimina el terminador de línia de cua (CR o LF).

Informació relacionada:

RFC 2822

RFC 822

Funció de crida de retorn xxfi_eoh:
Finalitat

La funció de crida de retorn **xxfi_eoh** gestiona el final de les capçaleres de missatge.

Sintaxi

```
#include <libmilter/mfapi.h>
sfsistat (*xxfi_eoh)(
 SMFICTX *ctx
);
```

Descripció

La funció de crida de retorn **xxfi_eoh** es crida un cop s'han enviat i processat totes les capçaleres i retorna l'indicador SMFIS_CONTINUE.

Arguments

Taula 42. Arguments

Element	Descripció
ctx	L'estructura de context opaca es manté en el paràmetre **libmilter**.

Funció de crida de retorn xxfi_body:
Finalitat

La funció de crida de retorn **xxfi_body** gestiona una part del cos del missatge.

Sintaxi

```
#include <libmilter/mfapi.h>
sfsistat (*xxfi_body)(
  SMFICTX *ctx,
  unsigned char *bodyp,
 size_t len
);
```

Descripció

La funció de crida de retorn **xxfi_body** no es crida o es crida diverses vegades entre la funció de crida de retorn **xxfi_eoh** i **xxfi_eom** i retorna l'indicador SMFIS_CONTINUE.

Nota:

- Els punts **bodyp** per a una seqüència de bytes. No és una sèrie C (una seqüència de caràcters que acaba amb '\0'). Per tant, no utilitzeu les funcions de sèrie C normals com **strlen(3)** en aquest bloc de bytes. La seqüència de bytes pot contenir caràcters '\0' dins del bloc. Per tant, encara que s'afegeixi un '\0' a la cua, les funcions de sèrie C podrien fallar i no funcionar com s'espera.
- Com que els cossos del missatge poden ser llargs, definir la funció de crida de retorn **xxfi_body** pot afectar de forma significativa el rendiment del filtre.
- Els finals de línia es representen com a rebuts des de l'SMTP (normalment CR/LF).
- Els filtres antics fan canvis de cos als filtres nous.
- Els cossos del missatge es poden enviar en diversos fragments cridant la funció de crida de retorn **xxfi_body** per fragment.
- Aquesta funció retorna l'indicador SMFIS_SKIP si un paràmetre milter ha rebut prou fragments de cos per prendre una decisió, però vol invocar les funcions de modificació del missatge que només es poden cridar des de la funció de crida de retorn**xxfi_eom**.
- El paràmetre milter ha de negociar aquest comportament amb l'agent de transferència de correu (MTA), o sigui, ha de comprovar si l'indicador de l'acció de protocol SMFIP_SKIP està disponible, i si ho està, el paràmetre **milter** l'ha de sol•licitar.

Arguments

Taula 43. Arguments

Element	Descripció
ctx	L'estructura de context opaca es manté en el paràmetre **libmilter**.
bodyp	El punter en l'inici d'aquest bloc de dades del cos. *bodyp* no és vàlid fora d'aquesta crida a la funció de crida de retorn**xxfi_body**.
len	La quantitat de dades apuntades per *bodyp*.

Informació relacionada

xxfi_eoh

xxfi_eom

Funció de crida de retorn xxfi_eom:
Finalitat

La funció de crida de retorn **xxfi_eom** gestiona el final del missatge.

Sintaxi

```
#include <libmilter/mfapi.h>
sfsistat (*xxfi_eom)(
 SMFICTX *ctx
);
```

Descripció

La funció de crida de retorn **xxfi_eom** es crida un cop després de totes les crides a la funció de crida de retorn **xxfi_body** per a un missatge determinat i retorna l'indicador SMFIS_CONTINUE.

Nota: Es necessita un filtre per realitzar totes les modificacions a les capçaleres, al cos i al sobre del missatge en la funció de crida de retorn **xxfi_eom**. Les modificacions es realitzen amb les rutines **smfi_***.

Arguments

Taula 44. Arguments

Element	Descripció
ctx	L'estructura de context opaca es manté en el paràmetre **libmilter**.

Informació relacionada

xxfi_body

Funció de crida de retorn xxfi_abort: Finalitat

La funció de crida de retorn **xxfi_abort** gestiona els missatges actuals que s'han avortat.

Sintaxi

```
#include <libmilter/mfapi.h>
sfsistat (*xxfi_abort)(
 SMFICTX *ctx
);
```

Descripció

La funció de crida de retorn **xxfi_abort** es crida en qualsevol moment durant el processament del missatges (entre algunes rutines orientades a missatges i la funció de crida de retorn **xxfi_eom**) i retorna l'indicador SMFIS_CONTINUE.

Nota:

- La funció de crida de retorn **xxfi_abort** ha de reclamar qualsevol recurs assignat a una base per missatge, i ha de ser tolerant a l'hora de ser cridada entre qualsevol de les crides de retorn orientades al missatge.
- Les crides a les funcions de crida de retorn **xxfi_abort** i **xxfi_eom** s'exclouen mútuament.
- La funció de crida de retorn **xxfi_abort** no és responsable de reclamar dades específiques de connexió perquè la funció de crida de retorn **xxfi_close** sempre es crida quan ha finalitzat una connexió.
- Com que el missatge actual ja s'està avortant, s'ignora el valor de retorn.
- La funció de crida de retorn **xxfi_abort** només es crida si el missatge s'avorta fora del control del filtre i el filtre no ha completat el processament orientat al missatge. Per exemple, si un filtre ja ha retornat l'indicador SMFIS_ACCEPT, SMFIS_REJECT, o SMFIS_DISCARD des de la rutina orientada a missatges. La funció de crida de retorn **xxfi_abort** no es cridarà encara que el missatge s'avorti posteriorment fora del control.

Arguments

Taula 45. Arguments

Element	Descripció
ctx	L'estructura de context opaca es manté a **libmilter**.

Informació relacionada

xxfi_close

xxfi_eom

Funció de crida de retorn xxfi_close: Finalitat

La funció de crida de retorn **xxfi_close** finalitza la connexió actual.

Sintaxi

```
#include <libmilter/mfapi.h>
sfsistat (*xxfi_close)(
 SMFICTX *ctx
);
```

Descripció

La funció de crida de retorn **xxfi_close** sempre es crida un cop al final de cada connexió i retorna l'indicador SMFIS_CONTINUE.

La funció de crida de retorn **xxfi_close** es pot cridar fora de seqüència, o sigui, fins i tot abans que es cridi la crida de funció de retorn **xxfi_connect**. Un cop l'agent de transferència de correu (MTA) estableixi connexió amb el filtre, si l'MTA decideix descartar el trànsit d'aquesta connexió (per exemple, mitjançant un resultat access_db), no es passaran dades al filtre des de l'MTA fins que el client es tanqui. En aquest moment, es crida la funció de crida de retorn **xxfi_close**. Per tant, pot ser l'única crida de retorn que s'hagi utilitzat per a una connexió determinada, i hauríeu d'anticipar aquesta possibilitat quan controleu manualment el codi de funció de la crida de retorn **xxfi_close**. En concret, és incorrecte donar per fet que el punter del context privat serà un valor diferent a NULL en aquesta crida de retorn.

La funció de crida de retorn **xxfi_close** es crida en tancat encara que la transacció de correu prèvia s'avortés.

La funció de crida de retorn **xxfi_close** és responsable d'alliberar qualsevol recurs assignat a una base per connexió.

Com que la connexió ja s'està finalitzant, el valor de retorn s'ignora actualment.

Arguments

Taula 46. Arguments

Element	Descripció
ctx	L'estructura de context opaca es manté en el paràmetre **libmilter**.

Informació relacionada

xxfi_connect

Funció de crida de retorn xxfi_negotiate: Finalitat

La funció de crida de retorn **xxfi_negotiate** gestiona la negociació.

Sintaxi

```
#include <libmilter/mfapi.h>
#include <libmilter/mfdef.h>
sfsistat (*xxfi_negotiate)(
        SMFICTX    "Funció de crida de retorn xxfi_negotiate",
  unsigned long f0,
  unsigned long f1,
  unsigned long f2,
```

```
unsigned long f3,
unsigned long *pf0,
unsigned long *pf1,
unsigned long *pf2,
unsigned long  *pf3);
```

Descripció

La funció de crida de retorn **xxfi_negotiate** es crida a l'inici de cada connexió del protocol simple de transferència de correu (SMTP) i retorna l'indicador `SMFIS_ALL_OPTS`.

Amb aquesta funció un paràmetre **milter** podria determinar dinàmicament i sol•licitar operacions i accions durant l'engegada. En les versions anteriors, les accions (`f0`) estaven fixades en els camps dels indicadors de l'estructura **smfiDesc** i els passos de protocol (`f1`) es derivaven implícitament comprovant si la crida de retorn estava definida. A causa de les extensions de la nova versió de **milter**, aquesta selecció estàtica no funcionarà si un paràmetre **milter** requereix noves accions que no estiguin disponibles quan es parli a un agent de transferència de correu (MTA) més antic.Per tant, en la negociació una crida de retorn pot determinar quines operacions estan disponibles i seleccionar dinàmicament les funcions de crida de retorn que necessita i que s'ofereixen. Si algunes operacions no estan disponibles, el paràmetre **milter** pot tornar a un mode més antic o aturar la sessió i demanar a l'usuari que actualitzi.

Passos de protocol
`(f1, *pf1)`

:

- SMFIP_RCPT_REJ: Si establiu aquesta part, el paràmetre **milter** pot sol•licitar que l'MTA també enviï ordres RCPT que s'hagin rebutjat perquè l'usuari és desconegut (o per motius similars), però no les funcions que s'han rebutjat perquè contenien errors sintàctics. Si un **milter** sol•licita aquest pas de protocol, ha de comprovar la macro **{rcpt_mailer}:** si s'estableix com a error, l'MTA pot rebutjar el destinatari. Normalment, les macros **{rcpt_host}** i **{rcpt_addr}** poden contenir un codi d'estat ampliat i, en aquest cas, un text d'error.
- SMFIP_SKIP indica que l'MTA entén el codi de retorn SMFIS_SKIP.
- SMFIP_NR_* indica que l'MTA entén el codi de retorn SMFIS_NOREPLY. Hi ha indicadors per a diversos passos de protocol:
  - SMFIP_NR_CONN: “Funció de crida de retorn xxfi_connect” a la pàgina 83
  - SMFIP_NR_HELO: “Funció de crida de retorn xxfi_helo” a la pàgina 84
  - SMFIP_NR_MAIL: “Funció de crida de retorn xxfi_envfrom” a la pàgina 85
  - SMFIP_NR_RCPT: “Funció de crida de retorn xxfi_envrcpt” a la pàgina 86
  - SMFIP_NR_DATA: “Funció de crida de retorn xxfi_data” a la pàgina 87
  - SMFIP_NR_UNKN: “Funció de crida de retorn xxfi_unknown” a la pàgina 87
  - SMFIP_NR_EOH: “Funció de crida de retorn xxfi_eoh” a la pàgina 89
  - SMFIP_NR_BODY: “Funció de crida de retorn xxfi_body” a la pàgina 89
  - SMFIP_NR_HDR: “Funció de crida de retorn xxfi_header” a la pàgina 88
- L'indicador SMFIP_HDR_LEADSPC indica que l'MTA pot enviar valors de capçalera amb l'espai inicial intacte. Si se sol•licita aquest pas de protocol, l'MTA no afegirà un espai en blanc inicial a les capçaleres quan s'afegeixin, insereixin o canviïn.
- Es poden donar instruccions a l'MTA perquè no enviï informació sobre diverses etapes d'SMTP, aquestes instruccions es donen amb indicadors que comencen per: SMFIP_NO*.
  - SMFIP_NOCONNECT: “Funció de crida de retorn xxfi_connect” a la pàgina 83
  - SMFIP_NOHELO: “Funció de crida de retorn xxfi_header” a la pàgina 88
  - SMFIP_NOMAIL: “Funció de crida de retorn xxfi_envfrom” a la pàgina 85
  - SMFIP_NORCPT: “Funció de crida de retorn xxfi_envrcpt” a la pàgina 86

– SMFIP_NOBODY: “Funció de crida de retorn xxfi_body” a la pàgina 89
– SMFIP_NOHDRS: “Funció de crida de retorn xxfi_header” a la pàgina 88
– SMFIP_NOEOH: “Funció de crida de retorn xxfi_eoh” a la pàgina 89
– SMFIP_NOUNKNOWN: “Funció de crida de retorn xxfi_unknown” a la pàgina 87
– SMFIP_NODATA: “Funció de crida de retorn xxfi_data” a la pàgina 87

Per a cadascuna d'aquestes **xxfi_* callbacks** que un paràmetre `milter` no utilitza, s'hauria d'establir l'indicador corresponent a
`*pf1.`

Les accions disponibles
`(f0, *pf0)`

estan descrites a **(xxfi_flags)**.

Si un `milter` retorna l'indicador SMFIS_CONTINUE, el `milter` estableix les accions desitjades i els passos del protocol mitjançant els paràmetres (de sortida) `pf0` i `pf1` (que es corresponen amb f0 i f1, respectivament). Els paràmetres (de sortida) `pf2` i `pf3` haurien d'establir-se com a 0 per ser compatibles amb versions futures.

Arguments

Taula 47. Arguments

Element	Descripció
`ctx`	L'estructura de context opaca es manté en el paràmetre **`libmilter`**.
`f0`	Les accions ofertes per l'MTA.
`f1`	Els passos de protocol ofertes per l'MTA.
`f2`	Per a futures extensions.
`f3`	Per a futures extensions.
`pf0`	Les accions que ha sol•licitat **`milter`**
`pf1`	Els passos de protocol sol•licitats per **`milter`**.
`pf2`	Per a futures extensions.
`pf3`	Per a futures extensions.

Valors de retorn

Taula 48. Valors de retorn

Element	Descripció
`SMFIS_ALL_OPTS`	Si un **`milter`** només vol inspeccionar els passos de protocol disponibles i les accions, pot retornar l'indicador SMFIS_ALL_OPTS i l'MTA durà a terme tots els passos de protocol i accions disponibles a **`milter`**. En aquest cas, no s'haurien d'assignar valors als paràmetres de sortida `pf0` -`pf3` ja que s'ignoraran.
`SMFIS_REJECT`	L'engegada **`milter`** falla i no es tornarà a contactar (per a la connexió actual).
`SMFIS_CONTINUE`	Continueu processant. En aquest cas, el paràmetre **`milter`** ha d'establir tots els paràmetres de sortida `pf0` - `pf3`. Vegeu l'explicació següent per saber com s'han d'establir els paràmetres de sortida.

Funcions diverses i constants

Les funcions diverses i constants capten la informació de la versió dels paràmetres **`libmilter`**.

Taula 49. Funcions constants

Element	Descripció
smfi_version	La funció **smfi_version** capta la informació de la versió del paràmetre **libmilter** (temps d'execució).
smfi_setsymlist	La **smfi_setsymlist** estableix la llista de macros que el paràmetre **libmilter** desitja rebre des de l'agent de transferència de correu (MTA) per a una etapa de protocol.

Taula 50. Funcions constants

Element	Descripció
SMFI_VERSION	La **SMFI_VERSION** obté la versió de temps d'execució del paràmetre **libmilter**.

Funció smfi_version: Finalitat

La funció **smfi_version** proporciona la informació de la versió de **libmilter** (temps d'execució).

Sintaxi

```
#include <libmilter/mfapi.h>
int smfi_version(
 Enter sense signe *pmajor,
 Enter sense signe*pminor,
 Enter sense signe *ppl,
);
```

Descripció

La funció de crida de retorn **smfi_version** es pot cridar en qualsevol moment.

La versió de temps de compilació de la biblioteca **libmilter** està disponible en la macro SMFI_VERSION. Per extreure la versió major i menor així com també el nivell de pedaç actual d'aquesta macro, es poden utilitzar les macros SM_LM_VRS_MAJOR(v), SM_LM_VRS_MINOR(v), i SM_LM_VRS_PLVL(v). Un paràmetre **milter** pot comprovar la macro SMFI_VERSION per determinar quines funcions utilitzarà (en el temps de compilació mitjançant les sentències del preprocessador C). En utilitzar aquesta macro i la funció **smfi_version**, un paràmetre **milter** pot determinar en el temps d'execució si s'ha enllaçat (dinàmicament) a la versió de **libmilter** esperada. Aquesta funció ha de comparar només la versió major i menor, no el nivell de pedaç, o sigui, la biblioteca **libmilter** serà compatible encara que hi hagi nivells de pedaç diferents.

Arguments

Taula 51. Arguments

Element	Descripció
pmajor	Un punter per a una variable int no firmada per emmagatzemar el número de versió del nivell de pedaç.
pminor	Un punter per a una variable int no firmada per emmagatzemar un número de versió menor.
ppl	Un punter per a una variable int no firmada per emmagatzemar el número de nivell de pedaç.

Valors de retorn

La funció **smfi_version** retorna el valor MI_SUCCESS.

Funció smfi_setsymlist:
Finalitat

La funció **smfi_setsymlist** estableix la llista de macros que el paràmetre **milter** vol rebre des de l'agent de transferència de correu (MTA) per a una etapa de protocol.

Sintaxi

```
#include <libmilter/mfapi.h>
int smfi_setsymlist(
        SMFICTX    *ctx,
  int        stage,
 char     *macros
);
```

Descripció

La funció de crida de retorn **smfi_setsymlist** ha de cridar-se durant la funció **xxfi_negotiate**, i aquesta funció es pot utilitzar per alterar temporalment la llista de macros que el paràmetre **milter** vol rebre des de l'agent de transferència de correu (MTA).

Nota: Hi ha un límit intern de nombre de macros que es poden establir (actualment 5). Tot i així, aquest límit no l'aplica el paràmetre **milter**, sinó només l'MTA;si es produeix una possible infracció d'aquesta restricció, no es comunicarà al paràmetre **milter**.

Arguments

Taula 52. Arguments

Element	Descripció
ctx	L'estructura de context opaca es manté en el paràmetre **libmilter**.
stage	L'etapa de protocol durant la qual s'ha d'utilitzar la llista de macros. Vegeu el fitxer `include/libmilter/mfapi.h` per veure els valors legals, i busqueu les macros C amb el prefix SMFIM_. Les etapes de protocol disponibles són com a mínim la connexió inicial, HELO o EHLO, MAIL, RCPT, DATA, el final de capçalera i final d'un missatge.
macros	La llista de macros (separades per un espai). Per exemple: "**{rcpt_mailer} {rcpt_host}**".

Valors de retorn

La funció **smfi_setsymlist** retorna el valor MI_FAILURE en els casos següents. Si no, la funció retorna MI_SUCCESS.

- No hi ha prou memòria lliure per fer una còpia de la llista de macros.
- Les *macros* tenen un valor NULL o estan buides.
- La *stage* no és una etapa de protocol vàlida.
- La llista de macros per a una etapa que s'ha establert anteriorment.

Informació relacionada

xxfi_negotiate

Senyaladors de depuració per sendmail

Existeix un gran nombre de senyaladors de depuració creats a l'ordre **sendmail**.

Cada senyalador de depuració té un nombre i un nivell. Els nivells superior imprimeixen més informació. La convenció és que els nivells més grans que 9 imprimeixen tanta informació que només s'utilitzen per depurar una part de codi particular. Els senyaladors de depuració s'estableixen mitjançant el senyalador **-d** tal com es mostra a l'exemple següent:

```
debug-flag:     -d debug-list
debug-list:     debug-flag[.debug-flag]*
debug-flag:     debug-range[.debug-level]
debug-range:    integer|integer-integer
debug-level:    integer

-d12            Set flag 12 to level 1
-d12.3          Set flag 12 to level 3
-d3-17          Set flags 3 through 17 to level 1
-d3-17.4        Set flags 3 through 17 to level 4
```

Els senyaladors disponibles són:

Element	Descripció
-d0	Depuració general.
-d1	Mostrar informació d'enviament.
-d2	Finalitzar amb *finis*( ).
-d3	Imprimir la mitjana de càrrega.
-d4	Espai en disc suficient.
-d5	Mostrar incidències.
-d6	Mostrar correu amb errors.
-d7	Nom del fitxer de cua.
-d8	Resolució de noms DNS.
-d9	Realitzar un seguiment de les consultes RFC1413.
-d9.1	Crea el nom canònic del nom d'amfitrió.
-d10	Mostrar lliurament de destinatari.
-d11	Realitzar seguiment del lliurament.
-d12	Mostrar mapatge de l'amfitrió relatiu.
-d13	Mostrar lliurament.
-d14	Mostrar comes de camp de capçalera.
-d15	Mostrar activitat de sol•licitud d'obtenció de xarxa.
-d16	Connexions de sortida.
-d17	LListar amfitrions MX.

Nota: existeixen quasi 200 senyaladors de depuració definits a **sendmail**.

Protocol d'accés a missatges i protocol d'oficina de correus

L'AIX proporciona dues implementacions de servidors de protocols de correu basats en Internet per accedir de forma remota la correu.

- **Protocol d'oficina de correus** (**POP** o **POP3DS**)
- **Protocol d'accés a missatges d'Internet** (**IMAP** o **IMAPDS**)

Cada tipus de servidor emmagatzema i proporciona accés a missatges electrònics. Utilitzant aquests protocols d'accés al correu en un servidor s'elimina la necessitat que, per rebre correu, un ordinador hagi d'estar sempre engegat i en funcionament.

El servidor **POP** o **POP3DS** proporciona un sistema de correu fora de línia, mitjançant el qual un client que faci servir el programari de client **POP** o **POP3DS** pot accedir de forma remota a un servidor de correu per recuperar missatges de correu. El client pot baixar els missatges de correu i suprimir-los immediatament del servidor o baixar els missatges i deixar-los residents al servidor **POP** o **POP3DS**.

Després de baixar el correu a la màquina client, tot el processament de correu es fa de forma local a la màquina client. El servidor **POP** permet accedir a una bústia d'un usuari d'un client cada vegada. La versió **POP3DS** utilitza les biblioteques OpenSSL, que requereixen certificats de seguretat.

El servidor **IMAP** o **IMAPDS** proporciona un superconjunt de funcions **POP** però té una interfície diferent. El servidor **IMAP** o **IMAPDS** proporciona un servei fora de línia, així com un servei en línia i un servei desconnectat. El protocol s'ha dissenyat per permetre la manipulació de bústies remotes com si estiguessin en local. Per exemple, els client poden fer cerques i marcar missatges amb senyaladors d'estat com ara **suprimit** o **contestat**. A més, els missatges es poden quedar a la base de dades del servidor fins que no s'eliminin de forma explícita. El servidor **IMAP** també permet un accés interactiu simultani a les bústies d'usuaris per múltiples clients. La versió **IMAPDS** utilitza les biblioteques OpenSSL, que requereixen certificats de seguretat.

Cada tipus de servidor es fa servir només per accedir al correu. Aquests servidors es basen en el **Simple Mail Transfer Protocol (SMTP)** per enviar correu.

Cada protocol és un protocol obert, basat en les normatives que es descriuen als RFC. Els servidors **IMAP** es basen en els RFC 2060 i 2061, i els servidors **POP** es basen en l'RFC 1939. Tots dos tipus estan connectats mitjançant els sòcols TCP. El servidor **IMAP** rep missatges al port 143, i el servidor **IMAPDS** rep missatges al port 993. El servidor **POP** rep missatges al port 110 i el servidor **POP3DS** rep missatges al port 995. Tots els servidors els gestiona el daemon **inetd**.

Requisit: Per utilitzar les versions d'OpenSSL, heu de tenir instal•lat l'OpenSSL. L'OpenSSL està disponible al CD *AIX Toolbox for Linux Applications*.

Configuració dels servidors IMAP i POP

Utilitzeu aquest procediment per configurar els servidors **IMAP** i **POP**.

Per tal de dur a terme aquesta tasca, heu de disposar d'autorització root.

1. Descomenteu les entrades de configuració **imapd** o **imapds** i **pop3d** o **pop3ds** del fitxer `/etc/inetd.conf`. A continuació hi trobareu exemples de les entrades de configuració:

```
#imap2  stream  tcp     nowait  root    /usr/sbin/imapd imapd
#pop3   stream  tcp     nowait  root    /usr/sbin/pop3d pop3d
#imaps  stream  tcp     nowait  root    /usr/sbin/imapds imapds
#pop3s   stream  tcp     nowait  root   /usr/sbin/pop3ds pop3ds
```

2. Consulteu els fitxers de configuració per al servidor **imapds** al fitxer `/etc/imapd.cf` i per al servidor **pop3ds** al fitxer `/etc/pop3d.cf`. Per defecte, els protocols de seguretat de menys nivell Secure Sockets Layer versió 2 (SSLv2) i SSLv3 estan habilitats per als servidors **imapds** i **pop3ds**. Tanmateix, podeu inhabilitar SSLv2 i SSLv3 actualitzant els fitxers de configuració tal com es mostra als exemples següents. També podeu habilitar o inhabilitar qualsevol tipus de xifrat especificant la cadena `SSL_CIPHER_LIST` al fitxer de configuració. Aquesta opció sobreescriu la cadena de xifrats per defecte que està definida internament a les aplicacions.

   Fitxer de configuració per al servidor imapds (`/etc/imapd.cf`):

```
#============================================================
#
# Fitxer de configuració d'IMAP d'exemple
#
#============================================================
#============================================================
# Descomenteu la línia de sota per inhabilitar SSL v2 per al servidor d'imap.
#
#   Disable SSL V2  --->  SSL_OP_NO_SSLv2         YES
#   Allow SSL V2    --->  SSL_OP_NO_SSLv2         NO
#
#
#SSL_OP_NO_SSLv2         YES  <-------------- descomenteu aquesta línia per inhabilitar el sslv2
#============================================================
# Descomenteu la línia de sota per inhabilitar SSL v3 per al servidor d'imap.
```

```
#
#   Disable SSL V3  --->  SSL_OP_NO_SSLv3         YES
#   Allow SSL V3    --->  SSL_OP_NO_SSLv3         NO
#
#
#SSL_OP_NO_SSLv3         YES  <-------------- descomenteu aquesta línia per inhabilitar el sslv3
#=====================================================================
# Descomenteu la línia de sota per utilitzar la llista de xifrats proporcionada per l'usuari
# per al servidor d'imap. La lògica de l'analitzador espera les cadenes de xifrat entre cometes " ".
#
#
#SSL_CIPHER_LIST "ALL:!LOW" <--- Descomenteu aquesta línia per tenir cadenes de
# xifrat (habilitades o inhabilitades) personalitzades
#=====================================================================
```

Fitxer de configuració per al servidor pop3ds (/etc/pop3d.cf):

```
#=====================================================================
#
# Fitxer de configuració de POP3 d'exemple
#
#=====================================================================
#=====================================================================
# Descomenteu la línia de sota per inhabilitar SSL v2 per al servidor pop3d.
#
#   Disable SSL V2  --->  SSL_OP_NO_SSLv2         YES
#   Allow SSL V2    --->  SSL_OP_NO_SSLv2         NO
#
#
#SSL_OP_NO_SSLv2         YES  <----------- descomenteu aquesta línia per inhabilitar el sslv2
#=====================================================================
# Descomenteu la línia de sota per inhabilitar SSL v3 per al servidor pop3d.
#
#   Disable SSL V3  --->  SSL_OP_NO_SSLv3         YES
#   Allow SSL V3    --->  SSL_OP_NO_SSLv3         NO
#
#
#SSL_OP_NO_SSLv3         YES  <----------- descomenteu aquesta línia per inhabilitar el sslv3
#=====================================================================
# Descomenteu la línia de sota per utilitzar la llista de xifrats proporcionada per l'usuari
# per al servidor pop3d. La lògica de l'analitzador espera les cadenes de xifrat entre cometes " ".
#
#
#SSL_CIPHER_LIST "ALL:!LOW" <---- Descomenteu aquesta línia per tenir cadenes de
# xifrat (habilitades o inhabilitades) personalitzades
#=====================================================================
```

3. Renoveu el daemon **inetd** executant l'ordre següent:

   ```
   refresh -s inetd
   ```

Execució de proves de configuració:

Dueu a terme unes quantes proves per tal de verificar si els servidors estan a punt per funcionar.

1. Primer, verifiqueu si els servidors estan a l'espera en els seus ports. Per fer-ho, escriviu les ordres següents en un indicador d'ordres i feu clic a Intro després de cada ordre:

   ```
   netstat -a | grep imap
   netstat -a | grep pop
   ```

   A continuació es mostra la sortida de les ordres **netstat**:

   ```
   tcp     0       0     *.imap2         *.*        LISTEN
   tcp     0       0     *.imaps         *.*        LISTEN
   tcp     0       0     *.pop3          *.*        LISTEN
   tcp     0       0     *.pop3s         *.*        LISTEN
   ```

2. Si no rebeu una sortida similar, torneu a comprovar les entrades al fitxer `/etc/inetd.conf` i, a continuació, torneu a executar l'ordre **refresh -s inetd**.

3. Per provar la configuració del servidor imapd, utilitzeu Telnet per accedir al servidor imap2, el port 143 (per IMAPDS, el port Telnet és 993). Quan establiu connexió utilitzant Telnet, obtindreu una pregunta de l'imapd. Aleshores podeu indicar les ordres de la versió 4 de l'IMAP segons es defineix a l'RFC 1730. Per executar una ordre, escriviu un punt (.), seguit d'un espai, després el testimoni, el nom de l'ordre i els paràmetres que calguin. El testimoni es fa servir per tal de posar en seqüències el nom de l'ordre. Per exemple:

   ```
   . testimoni nom de l'ordre paràmetres
   ```

   Es fa eco de les paraules clau quan accediu mitjançant Telnet al servidor imapd.

   A l'exemple Telnet següent, heu de proporcionar la vostra paraula clau i *id_paraula clau* s'indica a l'ordre **login**.

   Consell: Pels IMAPDS, l'ordre i la sortida varia una mica.

   ```
   telnet e-xbelize 143
   Trying...
   Connected to e-xbelize.austin.ibm.com.
   Escape character is '^]'.
   * OK e-xbelize.austin.ibm.com IMAP4 server ready
   . 1 login id id_password
   . OK
   . 2 examine /usr/spool/mail/root
   * FLAGS (\Answered \Flagged \Draft \Deleted \Seen)
   * OK [PERMANENTFLAGS (\Answered \Flagged \Draft \Deleted \Seen \*)]
   * 0 EXISTS
   * 0 RECENT
   * OK [UIDVALIDITY 823888143]
   . OK [READ-ONLY] Examine completed
   . 3 logout
   * BYE Server terminating connection
   . OK Logout completed
   Connection closed.
   ```

4. Per provar la configuració del servidor pop3d, utilitzeu Telnet per accedir al port del POP3, 110 (per POP3DS, el port Telnet és 995). Quan establiu connexió utilitzant Telnet, obtindreu una pregunta del pop3d. Podeu indicar ordres POP que estiguin definides a l'RFC 1725. Per executar una ordre, escriviu un punt (.), seguit d'un espai i, a continuació, el nom de l'ordre. Per exemple:

   ```
   . Nom de l'ordre
   ```

   Es fa eco de les paraules clau quan accediu mitjançant Telnet al servidor pop3d.

   A l'exemple Telnet següent, heu de proporcionar la vostra paraula clau i *id_paraula clau* s'indica a l'ordre **pass**.

   Consell: Pels POP3DS, l'ordre i la sortida varia una mica.

   ```
   telnet e-xbelize 110
   Trying...
   Connected to e-xbelize.austin.ibm.com.
   Escape character is '^]'.
   +OK e-xbelize.austin.ibm.com POP3 server ready
   user id
   +OK Name is a valid mailbox
   pass id_password
   +OK Maildrop locked and ready
   list
   +OK scan listing follows
   .
   stat
   +OK 0 0
   quit
   +OK
   Connection closed.
   ```

Inici de sessió amb el recurs SYSLOG

El programari del servidor **IMAP** (i **IMAPDS**) i **POP** (i **POP3DS**) envia missatges d'enregistrament al recurs **SYSLOG**.

1. Per configurar el sistema per l'inici de sessió d'**IMAP** i **POP** a través del recurs **SYSLOG**, haureu de ser usuari root. Editeu el fitxer `/etc/syslog.conf` i afegiu una entrada per ***.debug** de la manera següent:

   ```
   *.debug /usr/adm/imapd.log
   ```

2. El fitxer `usr/adm/imapd.log` ha d'existir abans que el daemon **syslogd** llegeixi el fitxer de configuració `/etc/syslog.conf`. Per crear aquest fitxer, escriviu el següent a l'indicador de la línia d'ordres i feu clic a Intro:

   ```
   touch /usr/adm/imapd.log
   ```

3. Renoveu el daemon **syslogd** per tornar a llegir el seu fitxer de configuració. Escriviu el següent a la sol•licitud de la línia d'ordres i feu clic a Intro:

   ```
   refresh -s syslogd
   ```

Ordres de gestió de correu

En aquest apartat es resumeixen les ordres de gestió del correu.

Element	Descripció
bugfiler	Emmagatzema informes d'error en directoris de correu específics.
comsat	Avisa els usuaris que tenen correu d'entrada (daemon).
mailq	Imprimeix el contingut de la cua del correu.
mailstats	Mostra la informació d'estadístiques sobre el trànsit de correu.
newaliases	Crea una còpia nova de la base de dades d'àlies a partir del fitxer `/etc/mail/aliases`.
rmail	Gestiona el correu remot rebut mitjançant l'ordre **uucp** dels BTU (Programes d'utilitat bàsics de la xarxa).
sendbug	Envia per correu un informa d'errors del sistema a una adreça específica.
sendmail	Encamina el correu perquè es lliuri de forma local o a la xarxa.
smdemon.cleanu	Neteja la cua **sendmail** fent-ne un manteniment periòdic.

Fitxers i directoris de correu

Els fitxers i els directoris de correu es poden ordenar per funcions.

Element	Descripció
`/usr/share/lib/Mail.rc`	Estableix els valors per defecte del sistema local per tots els usuaris del programa de correu. Podeu modificar un fitxer de text per establir les característiques per defecte de l'ordre **mail**.
`$HOME/.mailrc`	Permet que l'usuari canviï els valors per defecte del sistema local pel recurs de correu.
`$HOME/mbox`	Emmagatzema el correu processat d'un usuari en concret.
`/usr/bin/Mail`, `/usr/bin/mail` o `/usr/bin/mailx`	Especifica tres noms enllaçats al mateix programa. El programa de correu és *una* de les interfícies al sistema de correu.
`/var/spool/mail`	Especifica el directori del dipòsit de correu per defecte. Tot el correu es lliura, per defecte, al fitxer `/var/spool/mail/UserName`.
`/usr/bin/bellmail`	Du a terme el lliurament de correu local.
`/usr/bin/rmail`	Du a terme la interfície de correu remota pels BNU.
`/var/spool/mqueue`	Conté el fitxer de registre i fitxers temporal associats als missatges de la cua de correu.

Element	Descripció
/usr/sbin/sendmail	L'ordre **sendmail**.
/usr/ucb/mailq	Enllaça a /usr/sbin/sendmail. Si s'utilitza mailq equival a utilitzar l'ordre /usr/sbin/sendmail -bp.
/usr/ucb/newaliases	Enllaça al fitxer /usr/sbin/sendmail. Si s'utilitza newaliases equival a utilitzar l'ordre /usr/sbin/sendmail -bi.
/etc/netsvc.conf	Especifica la sol•licitud de determinats serveis de resolució de noms.
/usr/sbin/mailstats	Dona format i imprimeix les estadístiques de **sendmail** tal com les troba al fitxer /etc/sendmail.st, si n'hi ha. El fitxer /etc/sendmail.st és el valor per defecte però podeu especificar un fitxer alternatiu.
/etc/mail/aliases	Descriu una versió de text del fitxer d'àlies per l'ordre **sendmail**. Podeu editar aquest fitxer per crear, modificar o suprimir àlies del sistema.
/etc/aliasesDB	Descriu un directori que conté els fitxers de base de dades d'àlies, DB.dir i DB.pag, que es creen a partir del fitxer /etc/mail/aliases quan s'executa l'ordre **sendmail -bi**.
/etc/mail/sendmail.cf	Conté la informació de configuració **sendmail** en format de text. Editeu el fitxer per canviar aquesta informació.
/usr/lib/smdemon.cleanu	Especifica un fitxer d'intèrpret d'ordres que executa la cua de correu i que conserva els fitxers de registre **sendmail** al directori /var/spool/mqueue.
/etc/mail/statistics	Recopila estadístiques sobre el trànsit de correu. Aquest fitxer no creix. Utilitzeu l'ordre /usr/sbin/mailstats per visualitzar el contingut del fitxer. Suprimiu aquest fitxer si no voleu recopilar aquest tipus d'informació.
/var/spool/mqueue	Descriu un directori que conté els fitxers temporals associats a cada missatge de la cua. El directori pot contenir el fitxer de registre.
/var/spool/cron/crontabs	Descriu un directori que conté fitxers que llegeix el daemon **cron** per tal de determinar quin treball ha d'iniciar. El fitxer root conté una línia per iniciar seqüència de l'intèrpret d'ordres smdemon.cleanu.

Ordres IMAP i POP

Les ordres de correu **imapd** i **pop3d** es fan servir per l'IMAP i el POP.

Element	Descripció
/usr/sbin/**imapd**	El procés del servidor del protocol d'accés a missatges d'Internet (IMAP).
/usr/sbin/**pop3d**	El procés del servidor del protocol d'oficina de correus versió 3 (POP3).

Transmission Control Protocol/Internet Protocol

Quan els sistemes es comuniquen amb altres sistemes, hi ha algunes normes o *protocols* que els permeten transmetre i rebre dades de manera ordenada. Un dels conjunts de protocols més utilitzats arreu del món és el **Transmission Control Protocol/Internet Protocol (TCP/IP)**. (Gran part d'Europa, però, utilitza el protocol **X.25**). Algunes de les funcions comunes per utilitzar el **TCP/IP** són el correu electrònic, la transferència de fitxers sistema a sistema i l'inici de sessió remota.

L'ordre d'usuari **mail**, les ordres d'usuari de l'MH (Message Handling) i l'ordre de servidor **sendmail** poden utilitzar el **TCP/IP** per enviar i rebre correu entre sistemes, i els BNU (Basic Networking Utilities) poden utilitzar el **TCP/IP** per enviar i rebre fitxers i ordres entre sistemes.

El **TCP/IP** és un conjunt de protocols que especifiquen estàndards de comunicació entre sistemes i convencions detallades per encaminar i interconnectar xarxes. S'utilitza de manera extensiva a Internet i, per tant, permet que institucions de recerca, universitats, el govern i la indústria es puguin comunicar entre ells.

El **TCP/IP** permet la comunicació entre un nombre determinat de sistemes (anomenats amfitrions) connectats a una xarxa. Cada xarxa es pot connectar a una altra xarxa per comunicar-se amb els amfitrions d'aquesta xarxa. Tot i que hi ha molts tipus de tecnologies de xarxa, molts dels quals funcionen amb commutació de paquets i transport en modalitat contínua, el **TCP/IP** ofereix un avantatge superior: la independència del maquinari.

Com que els protocols d'Internet defineixen la unitat de transmissió i especifiquen la manera d'enviar-la, el **TCP/IP** pot amagar els detalls del maquinari de la xarxa, cosa que permet que molts tipus de tecnologies de xarxa es connectin i intercanviïn informació. Les adreces d'Internet permeten que qualsevol màquina de la xarxa es comuniqui amb una altra màquina de la xarxa. El **TCP/IP** també proporciona estàndards per a molts dels serveis de comunicacions que són necessaris per als usuaris.

El **TCP/IP** proporciona recursos que fan que el sistema informàtic esdevingui un amfitrió d'Internet, el qual es pot connectar a una xarxa i pot comunicar-se amb altres amfitrions d'Internet. El **TCP/IP** incorpora ordres i recursos que permeten:

- Transferir fitxers entre sistemes
- Iniciar la sessió en sistemes remots
- Executar ordres en sistemes remots
- Imprimir fitxers en sistemes remots
- Enviar correu electrònic a usuaris remots
- Mantenir converses interactives amb usuaris remots
- Gestionar una xarxa

> **Nota:** El **TCP/IP** proporciona una possibilitat de gestió bàsica de xarxes. L'**SNMP (Simple Network Management Protocol)** proporciona més ordres i funcions de gestió de xarxa.

Terminologia TCP/IP

Seria útil que us familiaritzéssiu amb els següents termes d'Internet tal i com s'utilitzen en relació al TCP/IP.

Element	Descripció
client	Sistema o procés que accedeix a les dades, serveis o recursos d'un altre sistema o procés de la xarxa.
amfitrió	Sistema que està connectat a una xarxa d'Internet i que pot comunicar-se amb altres amfitrions Internet. L'*amfitrió local* d'un usuari concret és el sistema en què està treballant l'usuari. Un *amfitrió extern* és qualsevol altre nom d'amfitrió de la xarxa. Des del punt de vista de les xarxes de comunicacions, els amfitrions són tant l'origen com la destinació dels paquets. Un amfitrió pot ser un client, un servidor o tots dos. En una xarxa d'Internet, un amfitrió s'identifica pel seu nom i adreça d'Internet.
xarxa	Combinació de dos amfitrions o més i els enllaços de connexió que els uneixen. Una *xarxa física* és el maquinari que constitueix la xarxa. Una *xarxa lògica* és l'organització abstracta que s'estén per totes o per una part d'una o més xarxes físiques. La xarxa Internet és un exemple de xarxa lògica. El programa d'interfície gestiona la conversió d'operacions de xarxa lògiques en operacions de xarxa físiques.
paquet	Bloc d'informació i dades de control per a una transacció entre un amfitrió i la seva xarxa. Els paquets són el mitjà d'intercanvi que utilitzen els processos per enviar i rebre dades a través de les xarxes Internet. Un paquet s'envia d'un *origen* a una *destinació*.
port	Punt de connexió lògic d'un procés. Les dades es transmeten entre processos a través de ports (o *sòcols*). Cada port proporciona cues per enviar dades i rebre'n. En una xarxa de programa d'interfície, cada port té un *número de port* d'Internet basat en la manera com s'utilitza. Un port concret s'identifica amb una *adreça de sòcol* d'Internet, que és la combinació d'un amfitrió d'Internet i un número de port.
procés	Programa que s'està executant. Un programa és l'element actiu d'un sistema. Els terminals, els fitxers i altres dispositius d'E/S es comuniquen entre ells mateixos a través de processos. Per tant, la comunicació en xarxa és una *comunicació entre processos*.
protocol	Conjunt de regles per gestionar la comunicació a nivell físic o lògic. Els protocols utilitzen sovint altres protocols per proporcionar serveis. Per exemple, un *protocol de nivell-connexió* utilitza un *protocol de nivell-transport* per transportar els paquets que mantenen una connexió entre dos amfitrions.
servidor	Sistema o procés que proporciona dades, serveis o recursos als quals poden accedir altres sistemes o processos de la xarxa.

Planificació de la vostra xarxa TCP/IP

Com que el **TCP/IP** és una eina de treball en xarxa molt flexible, podeu personalitzar-la perquè s'ajusti a les necessitats específiques de la vostra organització. Tingueu en compte els aspectes principals d'aquest tema en la planificació de la vostra xarxa. Els detalls d'aquests aspectes es tracten en altres temes. Aquesta llista només pretén fer-vos una introducció a aquests aspectes.

1. Decidiu quin tipus de maquinari de xarxa voleu emprar: Token-Ring, Ethernet Versió 2, IEEE 802.3, Interfície de dades distribuïdes per fibra (FDDI), Canal òptic de sèrie (SOC), o Protocol d'interfície de línia sèrie (SLIP).
2. Planifiqueu els disseny físic de la xarxa. Tingueu en consideració quines funcions servirà cada màquina d'amfitrió. Per exemple, heu de decidir quina màquina o màquines funcionaran com a passarel•les abans de cablejar la xarxa.
3. Decidiu si per a les vostres necessitats s'ajustarà millor una organització de xarxa *plana* o de xarxa *jeràrquica*.

   Si la vostra xarxa és bastant petita, en un sol lloc, i consta d'una xarxa física, aleshores una xarxa plana segurament satisfarà les vostres necessitats. Si la vostra xarxa és molt gran o complexa amb múltiples xarxes físiques, és possible que una xarxa jeràrquica us representi una organització de xarxa més eficaç.
4. Si la vostra xarxa ha d'estar connectada a altres xarxes, cal que planifiqueu com s'instal•laran i es configuraran les passarel•les. El que cal tenir en compte és:
   a. Decidir quina màquina o màquines funcionaran com a passarel•les.
   b. Decidir si necessiteu utilitzar un encaminament dinàmic o estàtic, o bé una combinació de tots dos. Si trieu un encaminament dinàmic, decidiu quins daemons d'encaminament utilitzarà cada passarel•la en funció dels tipus de protocols de comunicacions als quals necessiteu donar suport.
5. Preneu una decisió sobre un esquema d'adreçament.

   Si la vostra xarxa no formarà part de cap internetwork més gran, trieu l'esquema d'adreçament que millor s'adapti a les vostres necessitats. Si voleu que la vostra xarxa estigui connectada a una internetwork més gran com ara Internet, caldrà que obtingueu un conjunt oficial d'adreces del vostre proveïdor de serveis d' Internet (ISP).
6. Decidiu si cal que el vostre sistema estigui dividit en subxarxes. En cas afirmatiu, decidiu com assignareu les màscares de subxarxa.
7. Preneu una decisió sobre un esquema de denominació. Cada màquina de la xarxa necessita el seu propi nom d'amfitrió exclusiu.
8. Decidiu si la vostra xarxa necessita un servidor de noms per a la traducció de noms o si serà suficient l'ús del fitxer `/etc/hosts`.

   Si trieu l'ús de servidors de noms, penseu el tipus de servidor de noms que necessiteu i quants en necessiteu per servir la vostra xarxa de forma eficaç.
9. Decidiu els tipus de serveis que voleu que proporcioni la vostra xarxa als usuaris remots; per exemple, serveis de correu, serveis d'impressió, compartir fitxers, inici de sessió remota, execució d'ordres remota, entre d'altres.

Instal•lació del TCP/IP

En aquest apartat es descriu la instal•lació de **TCP/IP (Transmission Control Protocol/Internet Protocol)**.

Per obtenir informació sobre la instal•lació de **TCP/IP (Transmission Control Protocol/Internet Protocol)**, consulteu el manual Installation and Migration.

Configuració del TCP/IP

Un cop tingueu instal•lat el programari **TCP/IP** al sistema, podeu començar a configurar-lo.

Moltes tasques de configuració del **TCP/IP** es poden realitzar de més d'una manera:

- Mitjançant la System Management Interface Tool (SMIT)
- Amb l'edició d'un format de fitxer
- Mitjançant l'execució d'una ordre a l'indicador d'intèrpret d'ordres.

Per exemple, la seqüència de l'intèrpret d'ordres `rc.net` du a terme la configuració d'amfitrió mínima requerida per al **TCP/IP** durant el procés d'engegada del sistema (el programa gestor de configuracions

executa la seqüència `rc.net` durant la segona fase d'engegada). Mitjançant la SMIT per realitzar la configuració de l'amfitrió, el fitxer `rc.net` es configura automàticament.

Alternativament, podeu configurar el fitxer `/etc/rc.bsdnet` mitjançant un editor de textos estàndard. Amb aquest mètode, podeu especificar les ordres de configuració de l'UNIX **TCP/IP** tradicionals com ara **ifconfig**, **hostname** i **route**. Si utiliteu el mètode d'edició de fitxers, heu d'entrar al camí d'accés ràpid `smit configtcp` i, a continuació, seleccionar **BSD Style rc Configuration**. Consulteu la Llista de referències de programació del TCP/IP a l'*Communications Programming Concepts* per obtenir informació sobre els fitxers **TCP/IP** i els formats dels fitxers.

Hi ha unes quantes tasques, com ara la configuració d'un servidor de noms, que no es poden dur a terme mitjançant la SMIT.

Configuració d'amfitrions

Cada màquina d'amfitrió de la xarxa s'ha de configurar per tal que funcioni segons les necessitats dels usuaris finals i de la xarxa en general.

Per a cada amfitrió de la xarxa, heu de configurar la interfície de xarxa, establir l'adreça d'Internet i també el nom de l'amfitrió. Així mateix, heu de configurar encaminaments estàtics cap a les passarel•les o altres amfitrions, especificar que els daemons s'iniciïn per defecte i configurar el fitxer `/etc/hosts` per a la resolució de noms (o bé configurar l'amfitrió per utilitzar un servidor de noms per a la resolució de noms).

L'amfitrió com a configuració de servidor

Si la màquina d'amfitrió fa la funció específica de passarel•la, servidor de fitxers o servidor de noms, cal que dueu a terme les tasques de configuració necessàries un cop s'hagi completat la configuració bàsica.

Per exemple, si la xarxa està organitzada jeràrquicament i voleu utilitzar el protocol **Nom de domini** per resoldre els noms en adreces d'Internet, cal que configureu com a mínim un servidor de noms per proporcionar aquesta funció a la xarxa.

Recordeu que un amfitrió de servidor no ha de ser una màquina d'ús exclusiu, sinó que també es pot utilitzar per altres tasques. Si la funció de servidor de noms a la xarxa és reduïda, també es pot utilitzar la màquina com a estació de treball o com a servidor de fitxers de la xarxa.

Nota: Si el vostre sistema té instal•lat el NIS, aquests serveis també poden proporcionar resolució de noms.

Configuració de la passarel•la

Si la vostra xarxa s'ha de comunicar amb altres xarxes, cal que configureu un amfitrió de passarel•la com a mínim.

Heu de decidir a quins protocols de comunicacions voleu donar suport i, aleshores, utilitzar el daemon d'encaminament (el daemon **routed** o **gated**) que dóna suport a aquests protocols.

Configuració i ordres de gestió del TCP/IP

Podeu utilitzar diverses ordres per configurar i gestionar una xarxa **TCP/IP**. Es descriuen en aquesta taula.

Element	Descripció
arp	Visualitza o transforma l'adreça d'Internet en taules de conversió d'adreces de maquinari que utilitza el Protocol de **resolució d'adreces**.
cercausuaris	Torna informació sobre els usuaris en un amfitrió especificat.
amfitrió	Mostra l'adreça d'Internet d'un amfitrió especificat o el nom d'amfitrió d'una adreça d'Internet especificada.
nom_amfitrió	Mostra o estableix el nom i l'adreça d'Internet de l'amfitrió local.
ifconfig	Configura les interfícies de xarxa i les seves característiques.
netstat	Mostra les adreces externes i locals, les taules d'encaminament, les estadístiques de maquinari i un resum dels paquets transferits.
no	Estableix o mostra les opcions de kernel de la xarxa corrent.
ping	Determina si un amfitrió és assolible.
encaminament	Us permet manipular les taules d'encaminament de manera manual.
ruptime	Mostra la informació d'estat als amfitrions que estan connectats a xarxes físiques locals i estan executant el servidor **rwhod**.
rwho	Mostra la informació d'estat per als usuaris d'amfitrions que estan connectats a xarxes físiques locals i estan executant el servidor **rwhod**.
setclock	Llegeix el servei horari de xarxa i estableix l'hora i la data de l'amfitrió local en conseqüència.
timedc	Retorna informació sobre el daemon **timed**.
trpt	Informa sobre la traça de protocols en sòcols TCP.
whois	Proporciona el servei de directori de noms d'Internet.

Configuració d'una xarxa TCP/IP

Utilitzeu aquest procediment com a guia per configurar la vostra xarxa. Assegureu-vos que heu llegit i entès el material adequat.

Abans d'iniciar aquest procediment, assegurar-vos que es compleixen els prerequisits següents:

1. El maquinari de xarxa està instal•lat i cablejat. Per obtenir més informació sobre la instal•lació i el cablatge del maquinari, consulteu l'apartat "Targetes adaptadores de xarxa d'àrea local TCP/IP" a la pàgina 160.
2. El programari del **TCP/IP** està instal•lat. Per obtenir més informació sobre la instal•lació del programari del TCP/IP, consulteu *Installation and migration*.

Després d'iniciar la vostra xarxa i que s'executi correctament, és possible que us resulti útil consultar aquesta llista de control per motius de depuració.

Per configurar la vostra xarxa **TCP/IP**, utilitzeu els passos següents:

1. Llegiu l'apartat "Protocols TCP/IP" a la pàgina 121 per veure l'organització bàsica del **TCP/IP**. Cal que entengueu:
   - la naturalesa de capes del **TCP/IP** (és a dir, diferents protocols resideixen en diferents capes)
   - com és el flux de dades a través de les capes
2. Configureu mínimament cada màquina d'amfitrió de la xarxa. Això significa afegir un adaptador de xarxa, assignar una adreça IP i assignar un nom d'amfitrió a cada amfitrió, així com definir un camí per defecte cap a la xarxa. Per obtenir informació de fons sobre aquestes tasques, consulteu els apartats "Interfícies de xarxa del TCP/IP" a la pàgina 163, "Adreçament TCP/IP" a la pàgina 169 i "Denominació d'amfitrions a la vostra xarxa" a la pàgina 177.

   Nota: Cada màquina de la xarxa necessita aquesta configuració bàsica ja sigui un amfitrió d'usuari final, un servidor de fitxers, una passarel•la, o un servidor de noms.
3. Configureu i inicieu el daemon **inetd** a cada màquina d'amfitrió de la xarxa. Llegiu l'apartat "Daemons TCP/IP" a la pàgina 353 i, a continuació, seguiu les instruccions de l'apartat "Configuració del daemon inetd" a la pàgina 354.

4. Configureu cada màquina d'amfitrió per realitzar traducció de noms locals o per utilitzar un servidor de noms. Si esteu configurant una xarxa jeràrquica de noms de domini, configureu com a mínim un amfitrió perquè funcioni com un servidor de noms. Llegiu i seguiu les instruccions de l'apartat "Traducció de noms" a la pàgina 180.
5. Si la vostra xarxa s'ha de comunicar amb xarxes remotes, configureu com a mínim un amfitrió perquè funcioni com una passarel•la. La passarel•la pot utilitzar camins estàtics o un daemon d'encaminament per realitzar l'encaminament internetwork. Llegiu i seguiu les instruccions de l'apartat "Encaminament TCP/IP" a la pàgina 355.
6. Decidiu quins serveis utilitzarà cada màquina d'amfitrió de la xarxa. Per defecte, tots els serveis estan disponibles. Seguiu les instruccions de l'apartat "Serveis de xarxa de client" a la pàgina 355 si voleu fer que un servei determinat no estigui disponible.
7. Decidiu quins amfitrions de la xarxa seran servidors i quins serveis proporcionarà un servidor determinat. Seguiu les instruccions de l'apartat "Serveis de xarxa del servidor" a la pàgina 355 per iniciar els daemons de servidor que voleu executar.
8. Configureu els servidors d'impressió remots que necessitareu. Per obtenir més informació, consulteu l'apartat Printing administration de la publicació *Printers and printing*.
9. **Opcional:** si ho desitgeu, configureu un amfitrió per utilitzar-lo com el servidor horari mestre de la xarxa. Per obtenir més informació, consulteu el daemon **timed** a la publicació *Commands Reference, Volume 5*.

Autentificació i rcmds de seguretat

Aquestes ordres s'han millorat per oferir mètodes d'autentificació diferents dels que s'utilitzen avui en dia.

Les rcmds de seguretat són **rlogin**, **rcp**, **rsh**, **telnet**, i **ftp**. Per defecte, aquestes ordres utilitzen el mètode d'autentificació *estàndard d'AIX*. Els dos mètodes addicionals són Kerberos V.5 i Kerberos V.4.

Quan s'utilitza el mètode d'autentificació Kerberos V.5, el client obté un certificat Kerberos V.5 del servidor de seguretat DCE o del servidor Native Kerberos. El certificat és una part de les credencials del DCE o del Native actuals de l'usuari encriptades per al servidor **TCP/IP** amb el qual es volen connectar. El daemon del servidor **TCP/IP** desencripta el certificat. D'aquesta manera, el servidor **TCP/IP** pot identificar l'usuari per complet. Si es permet l'accés del principal DCE o Native descrit al certificat al compte de l'usuari del sistema operatiu, es duu a terme la connexió.

> **Nota:** A partir de la versió 2.2 del DCE, el servidor de seguretat DCE pot retornar certificats Kerberos V.5. Les rcmds de seguretat de l'AIX utilitzen la biblioteca Kerberos V.5 i la biblioteca GSSAPI de NAS (Network Authentication Service), versió 1.3.

A més d'autentificar el client, Kerberos V.5 envia les credencials de l'usuari actual al servidor **TCP/IP**. Si les credencials poden ser reenviades, el client les envia al servidor com a Kerberos TGT (Ticket Granting Ticket). Pel que fa al servidor **TCP/IP**, si algú es comunica amb un servidor de seguretat DCE, el daemon actualitza el TGT amb totes les credencials de DCE amb l'ordre **k5dcecreds**.

L'ordre **ftp** utilitza un mètode d'autentificació diferent de les altres ordres. Utilitza el mecanisme de seguretat GSSAPI per passar l'autentificació entre l'ordre **ftp** i el daemon **ftpd**. Mitjançant les subordres **clear**/**safe**/**private**, el client **ftp** dóna suport a l'encriptació de dades.

Entre els clients i els servidors del sistema operatiu, l'**ftp** s'ha millorat perquè es puguin efectuar transferències de diversos octets per a connexions de dades encriptades. Els estàndards només defineixen transferències d'un sol octet per a connexions de dades encriptades. Quan s'està connectat a màquines de tercers i utilitza l'encriptació de dades, l'**ftp** segueix el límit de transferència d'un sol octet.

Nota: Les ordres de seguretat rcmds **rlogin**, **rsh** i **telnet**, juntament amb els mètode d'autentificació **klogin** and **kshell** del Kerberos V.5, permeten tres intents abans que la connexió a l'amfitrió remot es tanqui.

Configuració del sistema de les rcmds de seguretat

Per a totes les rcmds de seguretat, hi ha un mecanisme de configuració de nivell de sistema per determinar quins mètodes d'autentificació es permeten al sistema. La configuració controla tant les connexions de sortida com d'entrada.

La configuració de l'autentificació consta d'una biblioteca, `libauthm.a`, i de dues ordres, **lsauthent** i **chauthent**, que ofereixen accés de línia d'ordres a les dues rutines de la biblioteca: **get_auth_methods** i **set_auth_methods**.

El sistema dóna suport a tres mètodes diferents d'autentificació: Kerberos V.5, Kerberos V.4 i *EstàndardAIX*. El mètode d'autentificació defineix el mètode que s'utilitza per autentificar un usuari a la xarxa.

- Kerberos V.5 és el mètode més freqüent i constitueix la base del DCE (Distributed Computing Environment). El sistema operatiu amplia els certificats d'entrada Kerberos V.5 a credencials DCE completes o fa servir el Native Kerberos.
- Kerberos V.4 només és utilitzat per dues rcmds de seguretat: **rsh** i **rcp**. Es facilita per donar suport a la compatibilitat amb versions anteriors en sistemes SP i només serà funcional en un. Un certificat Kerberos V.4 no s'actualitza amb les credencials DCE.
- El terme mètode d'autentificació *estàndard AIX* mencionat abans es refereix al mètode d'autentificació que utilitza l'AIX.

Quan es configura més d'un mètode d'autentificació, es produeix una implementació de reserva. Si amb el primer mètode no s'aconsegueix establir una connexió, el client intenta autentificar-se mitjançant el següent mètode d'autentificació configurat.

Els mètodes d'autentificació es poden configurar en qualsevol ordre. L'única excepció és que l'*AIX estàndard* ha de ser el darrer mètode d'autentificació que es configuri, ja que no presenta cap opció de reserva. Si l'*AIX estàndard* no és un mètode d'autentificació configurat, l'autentificació de la paraula clau no s'intenta i es rebutja qualsevol intent de connexió que utilitzi aquest mètode.

Es pot configurar el sistema sense cap mètode d'autentificació. En aquest cas, el sistema rebutja totes les connexions des d'un terminal i cap a un terminal que utilitzi rcmds de seguretat. A més, com que només es dóna suport a Kerberos V.4 amb les ordres **rsh** i **rcp**, un sistema que estigui configurat per utilitzar només Kerberos V.4 no permetrà les connexions que utilitzin **telnet**, **ftp** o **rlogin**.

Informació relacionada:

subrutina get_auth_method

subrutina set_auth_method

ordre lsauthent

ordre chauthent

Validació d'usuari de Kerberos V.5 per a les rcmds de seguretat

Quan s'utilitza el mètode d'autentificació Kerberos V.5, el client **TCP/IP** obté un certificat de servei encriptat per al servidor **TCP/IP**. Quan el servidor desencripta el certificat, té un mètode segur per identificar l'usuari (pel principal DCE o Native).

Tot i així, encara ha de determinar si el principal DCE o Native té accés al compte local. El mapatge del principal DCE o Native amb el compte del sistema operatiu local es gestiona a través d'una biblioteca compartida, `libvaliduser.a`, que té una sola subrutina **kvalid_user**. Si es prefereix un mètode de mapatge diferent, l'administrador del sistema ha de proporcionar una alternativa a la biblioteca `libvaliduser.a`.

Configuració del DCE per a les rcmds segures

Per utilitzar les rcmds de seguretat, han d'existir dos principals DCE per a cada interfície de xarxa a la qual es poden connectar.

Són les següents:

```
host/nom_complet_interfície
ftp/nom_complet_interfície
```

en què *nom_complet_interfície* és el nom d'interfície i el nom de domini per al *Nom_amfitrió.Nom_domini* primari.

Configuració nadiua de les rcmds segures

Per utilitzar les rcmds de seguretat, han d'existir dos principals per a cada interfície de xarxa a la qual es poden connectar.

Són les següents:

```
host/nom_complet_interfície@nom_real
ftp/nom_interfície_complet@nom_domini
```

en què *nom_interfície_complet* és el nom d'interfície i el nom de domini per al `nom_amfitrió.nom_domini` primari. *Nom_domini* és el nom del domini de Native Kerberos V.

Personalització del TCP/IP

Per personalitzar el **TCP/IP**, creeu un fitxer `.netrc`.

El fitxer `.netrc` especifica informació d'inici de sessió automàtic per a les ordres **ftp** i **rexec**. També podeu escriure noves macros **ftp**, que es defineixen al fitxer `$HOME/.netrc`. Per personalitzar les seqüències o funcions clau, creeu i editeu el fitxer `$HOME/.3270keys`. A més, el fitxer `.k5login` especifica quins principals DCE de quines cel•les tenen permès l'accés al compte de l'usuari.

Creació del fitxer .netrc

Els següents passos descriuen la manera de crear i editar el fitxer `$HOME/.netrc`:

1. Heu de tenir una còpia del fitxer `/usr/samples/tcpip/netrc`.
2. Cal que l'ordre **securetcpip** no s'estigui executant al vostre sistema.

Per crear el fitxer `.netrc`:

1. Copieu el fitxer `/usr/samples/tcpip/netrc` al vostre directori `$HOME` escrivint l'ordre següent:
   ```
   cp /usr/samples/tcpip/netrc $HOME
   ```
2. Editeu el fitxer `$HOME/netrc` per subministrar les variables *nom_amfitrió*, *nom_inici_sessió* i *paraula_clau* adequades. Per exemple:
   ```
   màquina amfitrió1.austin.century.com inici_de_sessió
   fred paraula clau rosella
   ```
3. Per establir els permisos per al fitxer `$HOME/netrc` a 600 utilitzant l'ordre **chmod** a l'indicador de línia d'ordres ($), escriviu:
   ```
   chmod 600 $HOME/.netrc
   ```
4. Canvieu el nom del fitxer `$HOME/netrc` pel de `$HOME/.netrc`. El punt inicial (.) fa que el fitxer quedi ocult.
   ```
   mv $HOME/netrc $HOME/.netrc
   ```

El fitxer `$HOME/.netrc` pot contenir moltes definicions d'inici de sessió i fins a 16 macros per cada definició d'inici de sessió.

Escriptura de macros ftp

En aquests passos es descriu com crear una macro **ftp**.

Cal que hàgiu creat el fitxer `$HOME/.netrc`.

Per escriure una macro **ftp**:

1. Editeu el fitxer `$HOME/.netrc` per incloure les següents instruccions:

   ```
   macdef init
   put schedule
   ```

   Assegureu-vos que inseriu una línia en blanc al final de la macro **ftp**. La línia en blanc interromp la macro **ftp**. A l'exemple anterior, la subordre **macdef** defineix la macro de subordre `init`. La línia següent és l'ordre que la macro especifica, en aquest cas `put` *`horari`*, on *horari* és el nom d'un fitxer.
2. Després d'haver creat la macro **ftp**, escriviu a l'indicador de la línia d'ordres:

   ```
   ftp
   nom_amfitrió
   ```

   En què *nom_amfitrió* és el nom de l'amfitrió al qual us esteu connectant. L'ordre **ftp** explora el fitxer `$HOME/.netrc` per obtenir una definició d'inici de sessió coincident amb el nom del vostre amfitrió i utilitza aquesta definició d'inici de sessió per iniciar la vostra sessió.
3. Després d'haver iniciat la sessió, escriviu a l'indicador de la línia d'ordres:

   ```
   ftp init
   ```

   En aquest exemple, l'**ftp** explora la macro anomenada `init` i executa l'ordre o les ordres que la macro especifica.

   Una macro **ftp** s'associa amb l'entrada d'inici de sessió immediatament anterior. Les macros **ftp** no són globals per al fitxer `$HOME/.netrc`. La macro `init` s'executa automàticament en iniciar la sessió. Es poden executar altres macros des de l'indicador **ftp** (`ftp>`) escrivint el següent:

   ```
   $getit
   ```

   En aquest exemple, $ executa la macro **ftp getit**.

Canvi d'assignació d'un conjunt de tecles

En personalitzar el **TCP/IP**, podeu utilitzar aquest procediment per canviar les seqüències i les funcions de les tecles.

1. Cal que conegueu el funcionament de l'editor **vi**.
2. Cal que tingueu l'editor vi al vostre sistema.

Els següents passos descriuen la manera de crear i editar el fitxer `$HOME/.3270keys`:

1. Copieu el fitxer `/etc/3270.keys` al directori `$HOME` i canvieu-li el nom pel de `.3270keys` mitjançant l'ordre següent:

   ```
   cp /etc/3270.keys $HOME/.3270keys
   ```
2. Canvieu les sentències de vincle del fitxer `$HOME/.3270keys` per canviar l'assignació d'un conjunt de tecles.
   a. Inicieu l'editor vi en un fitxer nou i especifiqueu la modalitat d'inserció.
   b. Premeu la seqüència de tecles Control-V i, tot seguit, la tecla que voleu mapar. Això fa que aparegui un valor per a la tecla premuda.
   c. Situeu el valor mostrat a la línia adequada de la columna `Sequence` del fitxer `$HOME/.3270keys`.

   Per exemple, després d'haver invocat l'editor vi i especificat la modalitat d'inserció, feu clic a Control-V i, tot seguit, Alt-Insert. Això fa aparèixer `[[141q`. El primer `[` és substituït per `\e` a la columna `Sequence` per tal que la línia configurada tingui un aspecte com el següent:

   ```
   3270 Function  Sequence   Key
   bind   pa1           "\e[141q"  #a_insert
   ```

Fitxer .k5login:

El fitxer `.k5login` s'utilitza quan s'empra l'autentificació Kerberos V.5 per a les rcmds de seguretat. Aquest fitxer especifica els principals DCE en què es permet l'accés de les cel•les al compte de l'usuari.

El fitxer és a `$HOME/.k5login`. Cal que sigui propietat de l'usuari i que el propietari tingui permís de lectura sobre aquest fitxer. El valor mínim de permís per a aquest fitxer és 400.

El fitxer `.k5login` conté una llista de les parelles de principal DCE/cel•la a què es permet l'accés al compte. Les parelles de principal/cel•la es mantenen amb un format de Kerberos (diferent del format DCE). Per exemple, si el fitxer conté

```
UsuariA@Cel•la1
```

aleshores el principal DCE `UsuariA` a la cel•la DCE `Cel•la1` pot accedir al compte.

Si el principal DCE és igual que el nom de compte de l'usuari i si no hi ha cap fitxer `$HOME/.k5login` per al compte de l'usuari, el principal DCE obté accés al compte (si l'autentificació Kerberos V.5 està configurada).

Per obtenir més informació sobre l'autentificació Kerberos V.5, consulteu l'apartat "Autentificació i rcmds de seguretat" a la pàgina 107.

Mètodes de comunicació amb altres sistemes i usuaris

Hi ha diversos mètodes de comunicació amb altres sistemes i usuaris. En aquest apartat en comentem dos. El primer mètode consisteix a connectar un amfitrió local a un amfitrió remot. El segon mètode consisteix a mantenir una conversa amb un usuari remot.

Connexions de l'amfitrió local a un amfitrió remot

Aquestes ordres de connexió de l'amfitrió **TCP/IP** són per executar ordres i inicis de sessió remota.

Hi ha diverses raons per les quals és probable que necessiteu accedir a un sistema que no sigui el vostre. Per exemple, és possible que l'administrador del sistema necessiti tornar a assignar els permisos a un fitxer important en què heu estat treballant o pot ser que necessiteu accedir a un fitxer personal des de l'estació de treball d'algú altre. Fins i tot podeu connectar el vostre sistema a l'estació de sistema d'algú altre. Les funcions d'inici de sessió remota, com ara les ordres **rlogin**, **rexec** i **telnet**, permeten que l'amfitrió local rendeixi com un amfitrió de terminals d'entrada/sortida. Les pulsacions de tecles s'envien a l'amfitrió remot i els resultats apareixen al monitor local. Quan sortiu de la sessió remota, totes les funcions tornen al vostre amfitrió local.

El **TCP/IP** conté les següents ordres per a inicis de sessió remota i l'execució d'ordres:

Element	Descripció
rexec	L'ordre **rexec** facilita l'execució d'ordres de manera interactiva en amfitrions diferents si inicieu la sessió en un amfitrió remot amb l'ordre **rlogin**. El gestor del sistema inhabilita aquesta ordre si la xarxa necessita mesures de seguretat extraordinàries. Quan executeu l'ordre **rexec**, el vostre amfitrió local cerca al fitxer `$HOME/.netrc` de l'amfitrió remot el nom d'usuari i una paraula clau de l'amfitrió local. Si es troben l'ordre que heu demanat que s'executi a l'amfitrió local s'executarà aleshores. Si no, se us demanarà que faciliteu un nom d'inici de sessió i una paraula clau abans que la sol•licitud es pugui complir.

Element	Descripció
rlogin	L'ordre **rlogin** permet iniciar la sessió en amfitrions externs semblants. A diferència de **telnet**, que es pot utilitzar amb amfitrions remots diferents, l' ordre**rlogin** es pot utilitzar només en amfitrions UNIX. El gestor del sistema inhabilita aquesta ordre si la xarxa necessita mesures de seguretat extraordinàries. L'ordre **rlogin** és semblant a l'ordre **telnet** en el sentit que totes dues permeten que un amfitrió local es connecti a un amfitrió remot. L'única diferència és que l'ordre **rlogin** no és una ordre fiable i es pot inhabilitar si el sistema necessita més seguretat. L'ordre **rlogin** no és una ordre fiable perquè tant el fitxer `$HOME/.rhosts`, propietat de l'usuari local, com el fitxer `/etc/hosts.equiv`, propietat del vostre administrador del sistema, guarden un llistat dels amfitrions remots que tenen accés a l'amfitrió local. Per tant, si deixeu el terminal encès, qualsevol usuari sense autorització podria accedir als noms i a les paraules clau que hi ha en aquests fitxers o, el que seria pitjor, malmetre d'alguna manera un amfitrió remot. Per anar bé, els usuaris remots haurien d'escriure una paraula clau després d'executar l'ordre **rlogin**, tot i que és molt senzill evitar aquesta opció. Si ni el fitxer `$HOME/.rhosts` ni el fitxer `/etc/hosts.equiv` no contenen el nom d'un amfitrió remot que està intentant iniciar la sessió, l'amfitrió local sol•licita una paraula clau. El fitxer de paraules clau remotes es comprova primer per verificar la paraula clau especificada; l'indicador d'inici de sessió torna a aparèixer si la paraula clau no és correcta. Prement la tilde i el punt (~.) a l'indicador d'inici de sessió es finalitza l'intent d'inici de sessió remota. També podeu configurar l'ordre **rlogin** per utilitzar el Kerberos V.5 per autentificar l'usuari. Aquesta opció permet identificar l'usuari sense utilitzar cap fitxer `$HOME/.rhosts` ni passar la paraula clau per la xarxa. Per obtenir més informació sobre aquest ús de l'ordre **rlogin**, consulteu l'apartat “Autentificació i rcmds de seguretat” a la pàgina 107.
rsh i **remsh**	Les ordres **rsh** i **remsh** permeten executar ordres en amfitrions externs semblants. Totes les entrades necessàries les ha de dur a terme l'amfitrió remot. El gestor del sistema inhabilita les ordres **rsh** i **remsh** si la xarxa necessita mesures de seguretat extraordinàries. L'ordre **rsh** es pot utilitzar de dues maneres: • Per executar una sola ordre en un amfitrió remot quan s'ha especificat un nom d'ordre • Per executar l'ordre **rlogin** quan no s'ha especificat cap nom d'ordre Quan s'executa l'ordre **rsh**, l'amfitrió local cerca al fitxer `/etc/hosts.equiv` de l'amfitrió remot el permís per iniciar la sessió. Si el resultat no és satisfactori, la cerca s'efectua al fitxer `$HOME/.rhosts`. Tots dos fitxers són llistes d'amfitrions remots que tenen permís d'inici de sessió. Els usuaris remots haurien d'escriure una paraula clau després d'executar l'ordre **rsh**. També és possible eliminar la necessitat d'executar l'ordre **rlogin**. L'ordre **rsh** permet l'execució d'ordres en un amfitrió remot, però no facilita cap mitjà per evitar el requisit de paraula clau. Si és necessària una paraula clau per accedir a un amfitrió remot, aleshores també caldrà una paraula clau per utilitzar l'ordre **rsh** perquè totes dues ordres accedeixen als fitxers `$HOME/.rhosts` i `/etc/hosts.equiv`. També podeu configurar l'ordre **rsh** per utilitzar el Kerberos V.5 per autentificar l'usuari. Aquesta opció permet identificar l'usuari sense utilitzar cap fitxer `$HOME/.rhosts` ni passar la paraula clau per la xarxa. Per obtenir més informació sobre aquest ús de l'ordre **rsh**, consulteu l'apartat “Autentificació i rcmds de seguretat” a la pàgina 107.

Element	Descripció
telnet, **tn** i **tn3270**	L'ordre **telnet** és un programa d'emulació de terminal que implementa el protocol TELNET i permet iniciar la sessió en amfitrions externs semblants o no. Utilitza el protocol TCP/IP per comunicar amb altres amfitrions de la xarxa. **Nota:** A efectes pràctics, amb el terme **telnet** ens referirem d'ara endavant a les ordres **telnet**, **tn** i **tn3270**. L'ordre **telnet** és mètode amb el qual un usuari pot iniciar la sessió en un amfitrió remot. La característica més important de l'ordre **telnet** és que és una ordre *fiable*. Per contra, l'ordre **rlogin**, que també permet l'inici de sessió remota, no es considera una ordre fiable. És probable que un sistema necessiti mesures de seguretat extraordinàries per evitar que usuaris sense autorització obtinguin accés als fitxers i robin dades importants, suprimeixin fitxers o introdueixin virus o cucs al sistema. Les funcions de seguretat del TCP/IP estan dissenyades per evitar aquests incidents. Un usuari que desitgi iniciar la sessió en un amfitrió remot amb l'ordre **telnet** ha de proporcionar el nom d'usuari i la paraula clau d'un usuari autoritzat per a aquest sistema. Això és semblant al procediment utilitzat per iniciar la sessió en un amfitrió local. Un cop s'ha efectuat satisfactòriament l'inici de sessió, el terminal de l'usuari funciona com si estigués connectat directament a l'amfitrió. L'ordre **telnet** dóna suport a una opció anomenada *negociació de terminal*. Si l'amfitrió remot dóna suport a la negociació de terminal, l'ordre **telnet** envia el tipus de terminal local a l'amfitrió remot. Si l'amfitrió remot no accepta el tipus de terminal local, l'ordre **telnet** intenta emular un terminal 3270 i un terminal DEC VT100. Si especifiqueu un terminal per emular, l'ordre **telnet** no negocia el tipus de terminal. Si els amfitrions local i remot no es posen d'acord sobre un tipus de terminal, l'amfitrió local estableix **none** per defecte. L'ordre **telnet** dóna suport a aquests tipus de terminals 3270: 3277-1, 3278-1, 3278-2, 3278-3, 3278-4 i 3278-5. Si utilitzeu l'ordre **telnet** en modalitat 3270 amb una pantalla en color, els colors i camps es visualitzen per defecte com els d'una pantalla 3279. Podeu seleccionar altres colors editant un dels fitxers de mapatge de teclat de la llista precedents de tipus de terminals. Un cop la sessió de **telnet** ha finalitzat, la pantalla es restableix en els colors que s'utilitzaven abans que comencés la sessió. També podeu configurar l'ordre **telnet** per utilitzar el Kerberos V.5 per autentificar l'usuari. Aquesta opció permet identificar l'usuari sense utilitzar cap fitxer `$HOME/.rhosts` ni passar la paraula clau per la xarxa. Per obtenir més informació sobre aquest ús de l'ordre **telnet**, consulteu l'apartat "Autentificació i rcmds de seguretat" a la pàgina 107.

Nota: Les ordres **rsh** i **rexec** es poden utilitzar per executar ordres en un amfitrió remot, però cap de les dues és una ordre fiable, per la qual cosa és possible que no compleixin tots els nivells de seguretat configurats al vostre sistema. Com a resultat, aquestes ordres poden quedar inhabilitades si el sistema requereix mesures de seguretat extraordinàries.

Inicis de sessió a amfitrions remots

Per iniciar sessió a un amfitrió remot podeu utilitzar l'ordre **telnet**.

Per fer-ho, heu de tenir un ID d'usuari i una contrasenya vàlids per accedir a l'amfitrió remot.

Per iniciar sessió a un amfitrió remot (`host1` en aquest exemple), escriviu:

```
telnet host1
```

A la pantalla apareixerà informació semblant a la següent:

```
Trying . . .
Connected to host1
Escape character is '^T'.

AIX telnet (host1)

AIX Operating System
Versió 7.1
(/dev/pts0)
login:_
```

Després d'iniciar la sessió, podeu executar ordres. Per sortir de la sessió amb el sistema i tancar la connexió, premeu la seqüència de tecles Ctrl-D.

Si no podeu iniciar la sessió, premeu la seqüència de tecles Ctrl-T per cancel•lar la connexió.

Conversa amb un usuari remot

Utilitzeu l'ordre **talk** per mantenir una conversa en temps real amb un altre usuari situat en un amfitrió remot.

1. El dimoni **talkd** ha d'estar actiu a l'amfitrió local i al remot.
2. L'usuari de l'amfitrió remot ha d'haver iniciat la sessió.

L'ordre **talk** necessita una adreça vàlida per vincular-s'hi. El nom de l'amfitrió del terminal remot ha d'estar vinculat a una interfície de xarxa operativa que altres ordres de xarxa puguin fer servir, com ara l'ordre t**ping**. Si la màquina no té una interfície de xarxa que sigui un terminal independent, ha de vincular el seu nom d'amfitrió a l'adreça de bucle de retorn (127.0.0.1) per tal que l'ordre **talk** funcioni.

Per mitjà del correu electrònic, podeu enviar missatges de text a altres usuaris d'una xarxa local i rebre correu. Si un ordinador està ben configurat i coneixeu l'adreça electrònica adient, podeu enviar missatges de correu electrònic a qualsevol part del món a una persona ubicada en un sistema remot.

El **TCP/IP** conté les següents ordres per la comunicació remota:

Element	Descripció
mail	Envia i rep documents i cartes electrònics
talk	Permet establir una conversa interactiva amb un usuari en un amfitrió remot

1. Per parlar amb l'usuari remot `dale@host2` que ha iniciat sessió en amfitrió remot, `jane@host1` escriu:
   ```
   talk dale@host2
   ```
   Un missatge semblant al següent es mostrarà a la pantalla de `dale@host2`:
   ```
   Message from TalkDaemon@host1 at 15:16...
   talk: connection requested by jane@host1.
   talk: respond with: talk jane@host1
   ```
   Aquest missatge informa `dale@host2` que `jane@host1` està intentant conversar amb ella.
2. Per acceptar la invitació, `dale@host2` escriu:
   ```
   talk jane@host1
   ```
   Els usuaris `dale@host2` i `jane@host1` ja poden ara mantenir una conversa interactiva.
3. Per finalitzar una conversa en qualsevol moment, qualsevol dels dos usuaris pot prémer la seqüència de tecles Ctrl-C. Això els torna a l'indicador de la línia d'ordres.

Transferències de fitxers

Encara que és possible enviar fitxers relativament curts mitjançant el correu electrònic, hi ha maneres més eficaces de transferir fitxers grans.

Els programes de correu electrònic estan dissenyats normalment per transmetre quantitats de text relativament petites: per tant, calen altres mitjans per transferir de manera eficaç fitxers grans. Les ordres **ftp**, **rcp** i **tftp** compten amb el **TCP/IP** per establir connexions directes de l'amfitrió local a un amfitrió remot. Els Basic Network Utilities (BNU) també poden utilitzar el **TCP/IP** per proporcionar connexions directes amb amfitrions externs.

Transferències de fitxers mitjançant les ordres ftp i rcp

Utilitzeu l'ordre **ftp** per copiar un fitxer des d'un amfitrió remot. L'ordre **ftp** no protegeix atributs de fitxers ni copia subdirectoris. Si una d'aquestes condicions és necessària, utilitzeu l'ordre **rcp**.

Element	Descripció
ftp	Utilitza el**File Transfer Protocol (FTP)** per transferir fitxers entre amfitrions que utilitzen diferents sistemes de fitxers i representacions de caràcters, com ara EBCDIC i ASCII. Proporciona mesures de seguretat en enviar paraules clau a l'amfitrió remot i també permet l'inici de sessió automàtic, transferències de fitxers i el final de la sessió.
rcp	Copia un o més fitxers entre l'amfitrió local i l'amfitrió remot, entre dos amfitrions remots separats o entre fitxers del mateix amfitrió remot. Aquesta ordre és semblant a l'ordre **cp** tret del fet que només funciona amb operacions de fitxers remotes. Si calen mesures de seguretat extraordinàries per a la xarxa, el gestor del sistema inhabilita aquesta ordre.

Abans d'intentar transferir el fitxer mitjançant les ordres **ftp** and **rcp**, assegureu-vos que es compleixen les condicions següents:

1. Cal tenir permís d'inici de sessió remota especificat al fitxer `$HOME/.netrc` de l'amfitrió remot si s'ha d'utilitzar la funció d'inici de sessió automàtic. Si no, cal que conegueu un nom i una paraula clau d'inici de sessió per a l'amfitrió remot. Per obtenir més informació sobre el fitxer `.netrc`, consulteu l'apartat "Creació del fitxer .netrc" a la pàgina 109.

   Per altra part, el sistema es pot configurar perquè utilitzi l'autentificació Kerberos V.5. Es fa servir en comptes dels fitxers `.netrc` o `$HOME/.rhosts`. Consulteu l'apartat "Autentificació i rcmds de seguretat" a la pàgina 107.
2. Si desitgeu copiar un fitxer des d'un amfitrió remot, cal que tingueu un permís de lectura per a aquest fitxer.

   Nota: Els permisos de lectura i d'escriptura per a fitxers i directoris d'un amfitrió remot es determinen amb el nom d'inici de sessió utilitzat.
3. Si desitgeu copiar un fitxer de l'amfitrió local a un amfitrió remot, cal que tingueu un permís d'escriptura per al directori que ha de contenir el fitxer copiat. A més a més, si el directori de l'amfitrió remot conté un fitxer amb el mateix nom que el fitxer que voleu copiar-hi, cal que disposeu d'un permís d'escriptura per afegir el fitxer a l'amfitrió remot.

Iniciar sessió en un amfitrió remot directament:

Quan s'utilitza el **TCP/IP** per transferir fitxers, podeu emprar aquest procediment per iniciar la sessió en un amfitrió remot directament.

1. Utilitzeu l'ordre **cd** per desplaçar-vos al directori que conté el fitxer que voleu enviar (enviament d'un fitxer) o al directori en què voleu que el fitxer transferit resideixi (recepció d'un fitxer).
2. Inicieu la sessió en un amfitrió remot directament escrivint:

   `ftp` *`nom_amfitrió`*

   Si disposeu de permís d'inici de sessió automàtic, es mostrarà a l'amfitrió local una informació semblant a la següent:

   ```
   Connectat a canopus.austin.century.com.
   220 canopus.austin.century.com FTP server
   (Version 4.1 Sat Nov 23 12:52:09 CST 1995) preparat.
   331 Es necessita la paraula clau per a pep.
   230 L'usuari pep ha iniciat la sessió.
   ftp>
   ```

   Si no, a l'amfitrió local apareixerà una informació semblant a la següent:

   ```
   Connectat a canopus.austin.century.com.
   220 canopus.austin.century.com FTP server
   (Version 4.1 Sat Nov 23 12:52:09 CST 1995) preparat.
   Nom (canopus:eric): pep
   331 Es necessita la paraula clau per a pep.
   Paraula clau:
   230 L'usuari pep ha iniciat la sessió.
   ftp>
   ```
3. Escriviu el nom i la paraula clau d'inici de sessió quan el sistema us ho sol•liciti.

Ja esteu preparats per copiar un fitxer entre dos amfitrions.

Iniciar sessió en un amfitrió remot indirectament:

Quan utilitzeu el **TCP/IP** per transferir fitxers, podeu emprar aquest procediment per iniciar la sessió en un amfitrió remot indirectament.

1. Utilitzeu l'ordre **cd** per desplaçar-vos al directori que conté el fitxer que voleu enviar (enviament d'un fitxer) o al directori en què voleu que el fitxer transferit resideixi (recepció d'un fitxer).
2. Inicieu la sessió en un amfitrió remot indirectament escrivint:

   ```
   ftp
   ```
3. Quan aparegui l'indicador `ftp>`, escriviu:

   open *Nom_amfitrió*

   Si disposeu de permís d'inici de sessió automàtic, es mostrarà a l'amfitrió local una informació semblant a la següent:

   ```
   Connectat a canopus.austin.century.com.
   220 canopus.austin.century.com FTP server
   (Version 4.1 Sat Nov 23 12:52:09 CST 1995) preparat.
   331 Es necessita la paraula clau per a pep.
   230 L'usuari pep ha iniciat la sessió.
   ftp>
   ```

   Si no, a l'amfitrió local apareixerà una informació semblant a la següent:

   ```
   Connectat a canopus.austin.century.com.
   220 canopus.austin.century.com FTP server
   (Version 4.1 Sat Nov 23 12:52:09 CST 1995) preparat.
   Nom (canopus:eric): pep
   331 Es necessita la paraula clau per a pep.
   Paraula clau:
   230 L'usuari pep ha iniciat la sessió.
   ftp>
   ```
4. Escriviu el vostre nom i paraula clau quan el sistema us ho sol•liciti.

Còpia d'un fitxer des d'un amfitrió remot a un amfitrió local:

Utilitzeu l'ordre **ftp** per copiar un fitxer des d'un amfitrió remot a un amfitrió local.

Per copiar un fitxer d'un amfitrió remot a un amfitrió local mitjançant l'ordre **ftp**, primer heu d'iniciar la sessió al sistema remot de manera directa o indirecta. Per obtenir més informació, vegeu Inici de sessió directe a un amfitrió remot o Inici de sessió indirecte a un amfitrió remot.

Nota: L'ordre **ftp** utilitza el tipus de transferència per defecte ASCII per copiar els fitxers.

Per copiar un fitxer d'un amfitrió remot a un amfitrió local:

1. Executeu la subordre **dir** per saber si el fitxer que voleu copiar és al directori actual. (La subordre **dir** per a l'ordre **ftp** funciona igual que l'ordre **ls -l**.) Si el fitxer no hi és, utilitzeu la subordre **cd** per anar al directori adequat.
2. Per copiar el fitxer local mitjançant una imatge binària, escriviu:

   ```
   binary
   ```
3. Per copiar un fitxer a l'amfitrió, escriviu:

   `get` *Nom_Fitxer*

   El fitxer es copia al directori des del qual heu executat l'ordre **ftp**.
4. Per finalitzar la sessió, premeu la seqüència de tecles Ctrl-D o escriviu `quit`.

Còpia d'un fitxer d'un amfitrió local a un amfitrió remot:

Utilitzeu l'ordre **ftp** per copiar un fitxer des d'un amfitrió local a un amfitrió remot.

Per copiar un fitxer d'un amfitrió local a un amfitrió remot mitjançant l'ordre **ftp**, primer heu d'iniciar la sessió al sistema remot de manera directa o indirecta. Per obtenir més informació, vegeu Inici de sessió directe a un amfitrió remot o Inici de sessió indirecte a un amfitrió remot.

Nota: L'ordre **ftp** utilitza el tipus de transferència per defecte ASCII per copiar els fitxers.

Per copiar un fitxer d'un amfitrió local a un amfitrió remot:

1. Si voleu copiar el fitxer en un directori que no sigui el directori `$HOME`, utilitzeu la subordre **cd** per anar al directori que vulgueu.
2. Per copiar el fitxer local mitjançant una imatge binària, escriviu:
   ```
   binary
   ```
3. Per copiar un fitxer a l'amfitrió remot, escriviu:
   ```
   put Nom_Fitxer
   ```
4. Per finalitzar la sessió, premeu la seqüència de tecles Ctrl-D o escriviu `quit`.

Transferències de fitxers mitjançant les ordres tftp i utftp

Utilitzeu les ordres **tftp** i **utftp** del **Trivial File Transfer Protocol** (**TFTP**) per transferir fitxers a amfitrions i des d'aquests.

Com que el **TFTP** és un protocol de transferència de fitxer únic, les ordres **tftp** i **utftp** no proporcionen totes les funcions de l'ordre **ftp**. Si calen mesures de seguretat extraordinàries per a la xarxa, el gestor del sistema pot inhabilitar aquesta ordre.

Nota: l'ordre **tftp** no està disponible quan l'amfitrió està funcionant amb un nivell de seguretat alt.

Abans d'intentar transferir un fitxer mitjançant les ordres **tftp** i **utftp**, assegureu-vos que es compleixen les condicions següents:

1. Si desitgeu copiar un fitxer *des d'un* amfitrió remot, cal que tingueu permís de *lectura* per al directori que conté el fitxer en qüestió.
2. Si desitgeu copiar un fitxer *en* un amfitrió remot, cal que tingueu permís d'*escriptura* per al directori en el qual s'ha d'ubicar el fitxer.

Còpia d'un fitxer des d'un amfitrió remot:

Quan utilitzeu el **TCP/IP** per copiar fitxers, podeu emprar aquest procediment per copiar fitxers des d'un amfitrió remot.

1. Per establir una connexió amb un amfitrió remot, escriviu:
   ```
   tftp amfitrió_1
   ```
   En aquest exemple, `amfitrió1` és el nom de l'amfitrió al qual us voleu connectar.

   Apareix l'indicador `tftp>`.
2. Per determinar si s'ha establert una connexió, escriviu:
   ```
   status
   ```
   Apareix un missatge semblant al següent:
   ```
   Connectat a amfitrió1
   Mode: netascii Verbós: desactivat Traçat: desactivat
   Interval-Remxt: 5 segons, Temps màxim d'espera: 25 segons
   tftp>
   ```
3. Escriviu la subordre **get**, el nom del fitxer que voleu transferir i el nom que voleu assignar al fitxer del sistema remot:

```
get /home/alice/update update
```

El directori /home/alice de l'amfitrió remot ha de tenir establert el permís de lectura per a altres usuaris. En aquest exemple, el fitxer /home/alice/update es transfereix des de l'amfitrió1 al fitxer update del directori actual del sistema local.

4. Per finalitzar la sessió, escriviu:

```
quit
```

o feu clic a la seqüència de tecles Control-D.

Còpia d'un fitxer a un amfitrió remot:

Quan utilitzeu el **TCP/IP** per copiar fitxers, podeu emprar aquest procediment per copiar un fitxer a un amfitrió remot.

1. Per establir una connexió amb un amfitrió remot, escriviu:

```
tftp amfitrió_1
```

En aquest exemple, amfitrió1 és el nom de l'amfitrió al qual us voleu connectar.

Apareix l'indicador tftp>.

2. Per determinar si s'ha establert una connexió, escriviu:

```
status
```

Apareix un missatge semblant al següent:

```
Connectat a amfitrió1
Mode: netascii Verbós: desactivat Traçat: desactivat
Interval-Remxt: 5 segons, Temps màxim d'espera: 25 segons
tftp>
```

3. Escriviu la subordre **put**, el nom del fitxer que voleu transferir des de l'amfitrió local i el camí d'accés i el nom del fitxer de l'amfitrió local:

```
put mfitxer /home/alice/tfitxer
```

El directori /home/alice de l'amfitrió remot ha de tenir establert el permís d'escriptura per a altres. El fitxer mfitxer, ubicat al directori de treball actual de l'usuari, es transfereix al amfitrió1. Cal especificar el nom del camí d'accés si no és que se n'ha establert un per defecte. El fitxer mfitxer apareix a l'amfitrió remot com a tfitxer.

4. Per finalitzar la sessió, escriviu:

```
quit
```

o utilitzeu la seqüència de tecles Control-D.

Impressió de fitxers en un sistema remot

Si teniu connectada una impressora local al vostre amfitrió, els procediments següents es referiran a la impressió en una impressora remota. Si no teniu cap impressora local, els procediments següents es referiran a la impressió en una impressora remota no establerta com a impressora per defecte.

1. Cal que el nom del vostre amfitrió aparegui al fitxer /etc/hosts.lpd de l'amfitrió remot.

Nota: El sistema de col•locació en cua no dóna suport a noms d'amfitrions multioctets.

Per implementar canvis al fitxer /etc/hosts.lpd sense reiniciar el sistema, utilitzeu l'ordre **refresh** del Controlador de recursos del sistema (SRC).

2. Cal que pugueu determinar el nom de la cua i el nom de la impressora remota del fitxer local /usr/lib/lpd/qconfig.

Podeu utilitzar tant l'ordre **enq** com la SMIT (System Management Interface Tool) per completar aquesta tasca.

Nota: En aquest apartat s'explica la manera com imprimir en un amfitrió remot al nivell més senzill possible. Per obtenir més informació i idees sobre la impressió remota, consulteu l'ordre **enq**.

Col•locar un treball d'impressió en una cua d'impressió remota

Quan utilitzeu el **TCP/IP** per imprimir fitxers, podeu emprar aquest procediment per col•locar un treball en una cua d'impressió remota.

Per col•locar un treball a una cua d'impressió remota, el nom del vostre amfitrió ha d'estar inclòs al fitxer `/etc/hosts.lpd` de l'amfitrió remot (el sistema de cua no admet els noms d'amfitrionse multioctet). Per implementar canvis al fitxer `/etc/hosts.lpd` sense reiniciar el sistema, utilitzeu l'ordre **refresh** del Controlador de recursos del sistema (SRC). A més, cal que pugueu determinar el nom de la cua i el nom de la impressora remota del fitxer local `/usr/lib/lpd/qconfig`.

1. Trobeu el nom de cua i el nom de dispositiu remot adequats. El nom de cua normalment comença amb les lletres `rp` seguides d'un numeral o d'un grup de numerals. El nom de la impressora remota normalment comença amb les lletres `drp` seguides d'un numeral o d'un grup de numerals.
2. Escriviu l'ordre següent:

   `enq -P` *`nom_cua:nom_impressora nom_fitxer`*

   en què *nom_cua* és el nom de la cua (com ara `rp1`) i *nom_impressora* és el nom de la impressora (com ara `drp1`) tal i com consta al fitxer `/usr/lib/lpd/qconfig`. No us descuideu els dos punts (`:`) entre *nom_cua* i *nom_impressora*. *nom_fitxer* és el nom del fitxer que voleu imprimir.

A continuació es mostren alguns exemples del funcionament de l'ordre **enq**:

- Per imprimir el fitxer `memo` a la impressora per defecte, escriviu:

  ```
  enq memo
  ```

- Per imprimir el fitxer `prog.c` amb els números de pàgina, escriviu:

  ```
  pr prog.c | enq
  ```

  L'ordre **pr** afegeix una capçalera a la part superior de cada pàgina que inclou la data de la darrera modificació del fitxer, el nom del fitxer i el número de pàgina. L'ordre **enq** imprimeix el fitxer.

- Per imprimir el fitxer `informe` a la següent impressora disponible configurada per a la cua `fred`, escriviu:

  ```
  enq -P fred informe
  ```

- Per imprimir tots els fitxers que comencen per `sam` a la següent impressora disponible configurada per a la cua `fred`, escriviu:

  ```
  enq -P fred sam*
  ```

  Tots els fitxers que comencin amb el prefix `sam` s'inclouran al mateix treball d'impressió. Les ordres d'estat normals només mostren el títol del treball d'impressió, que en aquest cas és el nom del primer fitxer de la cua a no ser que s'especifiqui un valor diferent amb el senyalador **-T**. Per veure una llista dels noms de tots els fitxers del treball d'impressió, feu servir l'estat llarg de l'ordre **enq -A -L**.

Col•locar en cua un treball mitjançant la SMIT

Quan utilitzeu el **TCP/IP** per posar a la cua fitxers, podeu emprar l'ordre **smit**.

1. Per posar un treball en cua amb la SMIT, escriviu l'ordre següent:

   ```
   smit
   ```

2. Seleccioneu el menú **Programa de control de cua** i inicieu un treball d'impressió.
3. Seleccioneu l'opció **Fitxer per imprimir** i escriviu el nom del fitxer que voleu imprimir.
4. Seleccioneu l'opció **Cua d'impressió** i seleccioneu el nom de la impressora remota on voleu imprimir.

Ara esteu preparat per imprimir en una impressora remota.

Impressió de fitxers des d'un sistema remot

És probable que de vegades us calgui imprimir un fitxer que es troba en un amfitrió remot. La ubicació de la sortida impresa depèn de quines impressores remotes estiguin disponibles per a l'amfitrió remot.

1. Cal que pugueu iniciar la sessió al sistema remot mitjançant l'ordre **rlogin** o **telnet**.
2. Cal que tingueu permís de lectura per al fitxer remot que voleu imprimir a la impressora local.

Nota: aquest procediment explica com imprimir en un amfitrió remot al nivell més senzill possible. Per obtenir més informació i idees sobre la impressió remota, consulteu l'ordre **enq**.

Per imprimir des d'un sistema remot:

1. Inicieu la sessió en el sistema remot mitjançant l'ordre **rlogin** o **telnet**.
2. Trobeu el nom de cua i el nom de dispositiu remot adequats. El nom de cua normalment comença amb les lletres `rp` seguides d'un numeral o d'un grup de numerals. El nom de la impressora remota normalment comença amb les lletres `drp` seguides d'un numeral o d'un grup de numerals.
3. Escriviu l'ordre següent:

   ```
   enq -P nom_cua:nom_impressora nom_fitxer
   ```

   en què *nom_cua* és el nom de la cua (com ara `rp1`) i *nom_impressora* és el nom de la impressora (com ara `drp1`) tal i com consta al fitxer `/usr/lib/lpd/qconfig`. No us descuideu els : (dos punts) entre *nom_cua* i *nom_impressora*. *Nom_fitxer* és el nom del fitxer que voleu imprimir.
4. Tanqueu la connexió amb l'amfitrió remot prement la seqüència de tecles Control-D o escrivint `quit`.

Visualització de la informació d'estat

Podeu utilitzar les ordres del **TCP/IP** per determinar l'estat d'una xarxa, visualitzar informació sobre un usuari i resoldre la informació d'amfitrió necessària per comunicar-se amb un altre amfitrió o usuari.

Ordres d'estat TCP/IP

El **TCP/IP** conté ordres d'estat per determinar l'estat dels amfitrions remot i local i de les seves xarxes.

Element	Descripció
finger o **f**	Mostra informació sobre els usuaris actuals d'un amfitrió especificat. Aquesta informació pot incloure el nom d'inici de sessió de l'usuari, nom complet, i el nom del terminal, així com la data i l'hora de l'inici de sessió.
amfitrió	Resol un nom d'amfitrió en una adreça d'Internet o una adreça d'Internet en un nom d'amfitrió.
ping	Ajuda a determinar l'estat d'una xarxa o amfitrió. S'utilitza més habitualment per verificar que una xarxa o amfitrió estigui funcionant en aquest moment.
rwho	Mostra quins usuaris inicien la sessió en amfitrions d'una xarxa local. Aquesta ordre mostra el nom d'usuari, el nom d'amfitrió i la data i l'hora de l'inici de sessió de tothom que sigui a la xarxa local.
whois	Identifica a qui pertany l'ID d'usuari o el sobrenom. Aquesta ordre només es pot utilitzar si la xarxa local està connectada a Internet.

Visualització d'informació sobre tots els usuaris que han iniciat la sessió en un amfitrió

Utilitzeu aquest procediment per visualitzar informació sobre *tots* els usuaris que han iniciat sessió a un amfitrió remot.

Per visualitzar informació sobre tots els usuaris que han iniciat sessió en un amfitrió remot:

1. Inicieu sessió a l'amfitrió remot amb el qual voleu comunicar-vos.
2. Per veure informació sobre tots els usuaris que han iniciat la sessió a l'amfitrió `alcatraz`, escriviu:

   ```
   finger @alcatraz
   ```

   Apareixerà informació semblant a la següent:

```
brown    console  Mar 15 13:19
smith    pts0     Mar 15 13:01
jones    tty0    Mar 15 13:01
```

L'usuari `puig` ha iniciat la sessió a la consola; l'usuari `prat`, des de la línia d'un pseudoterminal pts0, i l'usuari `pujol`, des d'un terminal tty0. L'administrador del sistema pot configurar el sistema per tal que l'ordre **finger** funcioni de manera diferent. Si teniu qualsevol problema a l'hora d'utilitzar l'ordre **finger**, poseu-vos en contacte amb l'administrador del sistema.

Visualització d'informació sobre un usuari que ha iniciat sessió a un amfitrió

Utilitzeu aquest procediment per visualitzar informació sobre un usuari *concret* que ha iniciat sessió a un amfitrió remot.

Per visualitzar informació sobre un usuari que ha iniciat sessió en un amfitrió remot:

1. Inicieu sessió a l'amfitrió remot amb el qual voleu comunicar-vos.
2. Per visualitzar informació sobre l'usuari `brown` a l'amfitrió `alcatraz`, escriviu:

   ```
   finger brown@alcatraz
   ```

   Apareixerà informació semblant a la següent:

   ```
   Login name:  brown
   Directory:  /home/brown     Shell:  /home/bin/xinit -L -n Startup
   On since May 8 07:13:49 on console
   No Plan.
   ```

L'administrador del sistema pot configurar el sistema per tal que l'ordre **finger** funcioni de manera diferent. Si teniu qualsevol problema a l'hora d'utilitzar l'ordre **finger**, poseu-vos en contacte amb l'administrador del sistema.

Protocols TCP/IP

Els protocols són conjunts de normes per als procediments i formats de missatges que permeten a les màquines i programes d'aplicació intercanviar informació. Cal que cada màquina implicada en la comunicació segueixi aquestes normes perquè l'amfitrió receptor pugui entendre el missatge. El *conjunt* de protocols TCP/IP es pot comprendre en termes de capes (o nivells).

Aquesta figura mostra les capes del protocol **TCP/IP**. Des de la part superior són: capa d'aplicació, capa de transport, capa de xarxa, capa d'interfície de xarxa i maquinari.

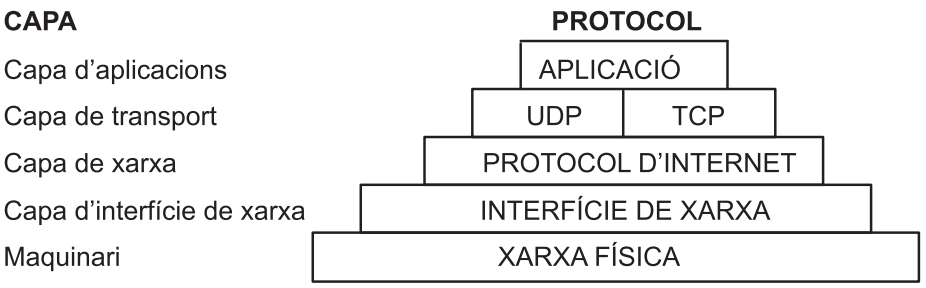


Figura 4. Conjunt de protocols TCP/IP

El TCP/IP defineix amb compte com es mou la informació des de l'emissor fins al receptor. Primer, els programes d'aplicació envien missatges o corrents de dades a un dels protocols de capa de transport d'Internet, ja sigui l'**User Datagram Protocol** (**UDP**) o bé el **Transmission Control Protocol** (**TCP**). Aquests protocols reben les dades de l'aplicació, la divideixen en parts més petites anomenades *paquets*, afegeixen una adreça de destinació i, a continuació, passen els paquets a la següent capa de protocol, la capa de xarxa d'Internet.

La capa de xarxa d'Internet inclou el paquet en un datagrama **IP** (**Internet Protocol**), el posa a la capçalera i la cua del datagrama, decideix a on enviar el datagrama (sigui directament a una destinació o bé a una passarel•la), i passa el datagrama a la capa d'interfície de xarxa.

La capa d'interfície de xarxa accepta els datagrames **IP** i els transmet com a *trames* a un maquinari de xarxa específic, com ara xarxes Ethernet o Token-Ring.

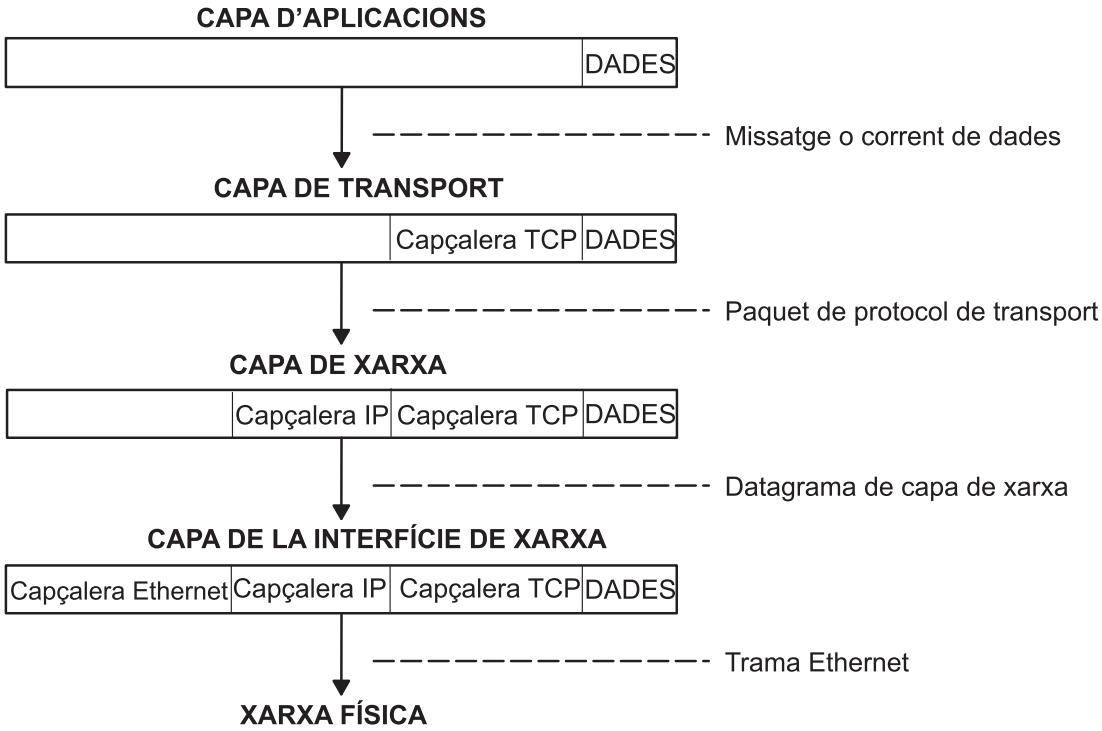


Figura 5. Moviment de la informació des de l'aplicació de l'emissor fins a l'amfitrió del receptor

Aquesta figura mostra el flux descendent de la informació per les capes del protocol TCP/IP des de l'emissor fins a l'amfitrió.

Les trames rebudes per un amfitrió van per les capes del protocol a l'inversa. Cada capa fragmenta la informació de capçalera corresponent, fins que les dades tornen a la capa d'aplicació.

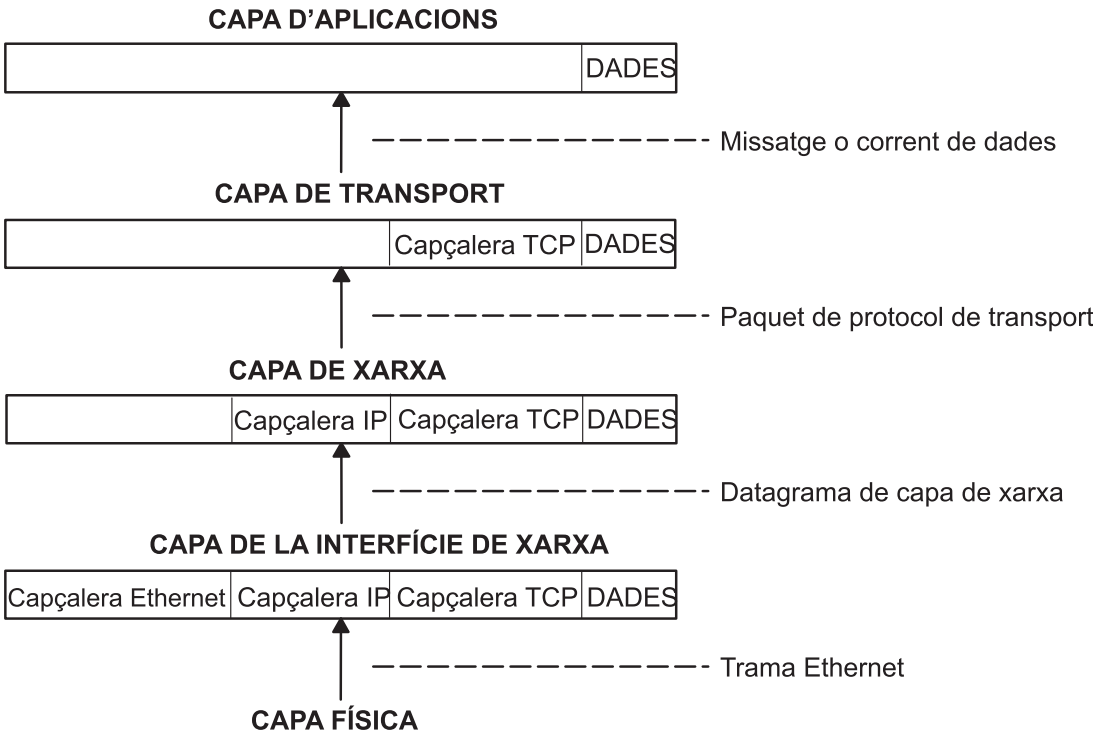
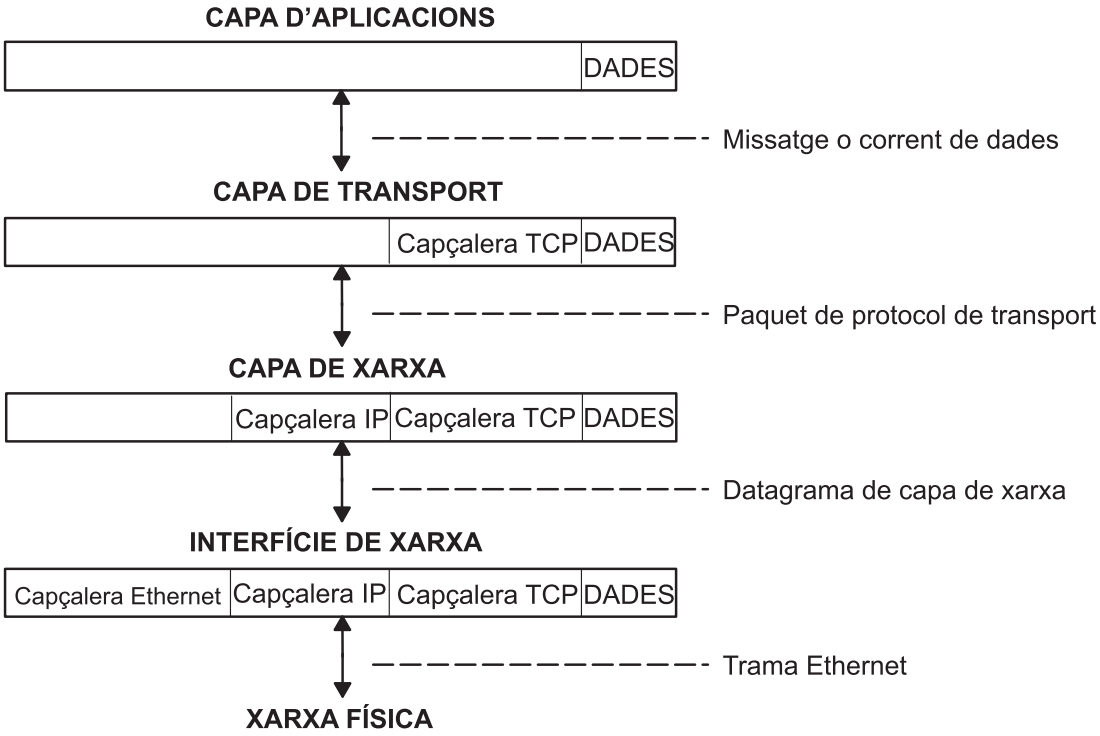


Figura 6. Moviment de la informació des de l'amfitrió fins a l'aplicació

Aquesta figura mostra el flux ascendent de la informació per les capes del protocol **TCP/IP** des de l'amfitrió fins a l'emissor.

La capa d'interfície de xarxa (en aquest cas, un adaptador Ethernet) rep les trames. La capa d'interfície de xarxa fragmenta la capçalera Ethernet i envia el datagrama cap a la capa de xarxa. A la capa de xarxa, el protocol d'Internet fragmenta la capçalera IP i envia el paquet a la capa de transport. A la capa de transport, el **TCP** (en aquest cas) fragmenta la capçalera **TCP** i envia les dades a la capa d'aplicació.

Els amfitrions d'una xarxa envien i reben informació simultàniament. Figura 7 a la pàgina 124 representa de forma més acurada un amfitrió en comunicació.



Nota: Les capçaleres s'afegeixen o s'eliminen a cada capa de protocol quan un amfitrió transmet o rep les dades.

Figura 7. Transmissions i recepcions de dades d'amfitrió

Aquesta figura mostra els fluxos de dades en ambdós sentits a través de les capes **TCP/IP**.

Protocol d'Internet (IP) versió 6

El **Protocol d'Internet** (**IP**) Versió 6 (**IPv6** o IP*ng*) és la propera generació de l'**IP** i s'ha dissenyat perquè sigui un pas evolutiu a partir de l'**IP** Versió 4 (**IPv4**).

Tot i que l'**IPv4** ha permès el desenvolupament d'un Internet global, no és capaç d'aportar gaire cosa més en un futur a causa de dos factors fonamentals: espai d'adreces limitat i complexitat d'encaminament. Les adreces de 32 bits de l'**IPv4** no proporcionen prou flexibilitat per a l'encaminament global d'Internet. El desplegament de CIDR (Classless InterDomain Routing) ha ampliat el temps de vida de l'encaminament de l'**IPv4** en un nombre d'anys, però haurà de continuar l'esforç per millorar la gestió de l'encaminament. Fins i tot si l'encaminament de l'**IPv4** es pogués ajustar a l'alça, a la llarga Internet esgotarà els números de xarxa.

La IETF (Internet Engineering Task Force) va reconèixer que l'**IPv4** no seria capaç de donar suport al creixement fenomenal d'Internet, i per tant es va crear el grup de treball de l'IP*ng*. De les propostes fetes, es va triar el **SIPP** (**Simple Internet Protocol Plus**) com un pas evolutiu en el desenvolupament de l'IP. Se li va canviar el nom per IP*ng*, i l'RFC1883 es va finalitzar el desembre de 1995.

L'IPv6 amplia el nombre màxim d'adreces d'Internet per gestionar la població d'usuaris d'Internet en constant creixement. Com a canvi evolutiu a partir de l'**IPv4**, l'**IPv6** té l'avantatge de permetre la coexistència d'allò nou i allò antic en la mateixa xarxa. Aquesta coexistència habilitar una migració ordenada des de l'**IPv4** (adreçament de 32 bits) a l'**IPv6** (adreçament de 128 bits) en una xarxa operativa.

La intenció d'aquesta descripció general és oferir al lector una descripció general del protocol IP*ng*. Per obtenir informació detallada, consulteu els RFC 2460, 2373, 2465, 1886, 2461, 2462 i 2553.

Security proporciona informació de seguretat sobre el paquet ofimàtic de protocols **TCP/IP**, inclòs l'**IPv6**. Per veure els detalls de la Seguretat IP, versions 4 i 6, consulteu Internet Protocol security.

Encaminament i adreçament ampliats de l'IPv6:

L'**IPv6** augmenta la grandària de les adreces **IP** de 32 bits a 128 bits, per la qual cosa dóna suport a més nivells de jerarquia d'adreçament, a un nombre molt més gran de nodes d'adreçament, i a una autoconfiguració de les adreces més senzilla.

L'**IPv6** té tres tipus d'adreces:

Element	Descripció
difusió individual	Un paquet enviat a una adreça de difusió individual es lliura a la interfície identificada per aquesta adreça. Una adreça de difusió individual té un àmbit determinat: local d'enllaç, local de lloc o global. També hi ha dos adreces de difusió individual especials: • ::/128 (adreça no especificada) • ::1/128 (adreça de bucle de retorn)
difusió múltiple	Un paquet enviat a una adreça de multidifusió es lliura a totes les interfícies identificades per aquesta adreça. Una adreça de multidifusió s'identifica pel prefix ff::/8. Com amb les adreces de difusió individual, les adreces de multidifusió tenen un àmbit similar: local de node, local d'enllaç, local de lloc i local d'organització.
servei	Una adreça de servei és una adreça que té un únic emissor, múltiples receptors i només un emissor de resposta (normalment el "més proper", d'acord amb el mesurament de distància dels protocols d'encaminament). Per exemple, diversos servidors web pendents d'una adreça de servei. Quan s'envia una sol•licitud a l'adreça de servei, només respon un dels servidor. Una adreça de servei és indistingible d'una adreça de difusió individual. Una adreça de difusió individual passa a ser una adreça de servei quan hi ha més d'una interfície configurada amb aquesta adreça.

Nota: A l'**IPv6** no hi ha adreces de difusió. La seva funció s'ha substituït per l'adreça de multidifusió.

Autoconfiguració de l'IPv6:

Els mecanismes primaris disponibles que habiliten que un node s'engegui i es comuniqui amb altres nodes en una xarxa **IPv4** estan protegits pel sistema, **BOOTP**, i **DHCP**.

L'**IPv6** introdueix el concepte d'*àmbit* a les adreces **IP**, una de les quals és local d'enllaç. Això permet que un amfitrió construeixi una adreça vàlida a partir del prefix local d'enllaç predefinit i el seu identificador local. Aquest identificador local normalment es deriva de l'adreça de control d'accés al medi (MAC) de la interfície que s'ha de configurar. Mitjançant aquesta adreça, el node es pot comunicar amb altres amfitrions de la mateixa subxarxa i, per a una subxarxa totalment aïllada, és possible que no necessiti cap altra configuració d'adreces.

Adreces amb significat de l'IPv6:

Amb l'**IPv4**, l'únic significat generalment identificable de les adreces són la difusió (normalment tot uns o tot zeros) i les classes (per exemple, una classe D és difusió múltiple). Amb l'**IPv6**, es pot examinar ràpidament el prefix per determinar l'*àmbit* (per exemple, local d'enllaç), difusió múltiple versus difusió individual, i un mecanisme d'assignació (basat en el proveïdor o en la geografia).

També es pot carregar de forma explícita la informació d'encaminament als bits superiors de les adreces, però això encara no s'ha finalitzat per part de la IETF (en les adreces basades en el proveïdor, la informació d'encaminament es troba present de forma implícita en l'adreça).

Detecció d'adreces duplicades de l'IPv6:

Quan s'inicialitza o es reinicialitza una interfície, aquesta utilitza l'autoconfiguració per associar provisionalment una adreça local d'enllaç amb aquesta interfície (l'adreça encara no s'assigna a la interfície en el sentit tradicional). En aquest punt, la interfície uneix els grups de difusió múltiple de tots els nodes i dels nodes sol•licitats, i els envia un missatge de descobriment de veïnatge. Mitjançant l'adreça de multidifusió, el node pot determinar si aquella adreça local d'enllaç en particular ja s'ha assignat anteriorment i triar una adreça alternativa.

Així s'elimina la possibilitat d'assignar per accident la mateixa adreça a dues interfícies diferents dins el mateix enllaç. (Encara continua sent possible crear adreces d'àmbit global duplicades per a nodes que no es troben al mateix enllaç.)

Descobriment de veïnatge/autoconfiguració d'adreces sense estat:

El **Protocol de descobriment de veïnatge** (**NDP**) de l'**IPv6** l'utilitzen els nodes (amfitrions i encaminadors) per determinar les adreces de capa d'enllaç dels veïns que se sap que resideixen en enllaços connectats i per mantenir taules d'encaminament per destinació per a les connexions actives. L'**IPv6** defineix un mecanisme d'autoconfiguració d'adreces tant amb estat com sense estat. L'*autoconfiguració sense estat* requereix que no hi hagi configuració manual dels amfitrions; una configuració dels encaminadors mínima, si n'hi ha; i que no hi hagi cap servidor addicional.

Els amfitrions també utilitzen l'**NDP** per trobar encaminadors adjacents disposats a reenviar paquets de part seva i detectar adreces canviades de capa d'enllaç. L'**NDP** utilitza l'**Internet Control Message Protocol** (**ICMP**) Versió 6 amb els seus propis tipus de missatges únics. En termes generals, el Protocol de descobriment de veïnatge de l'**IPv6** correspon a una combinació del **Protocol de resolució d'adreces** (**ARP**) de l'**IPv4**, el Descobriment d'encaminaments ICMP (RDISC), i el Readreçament **ICMP** (ICMPv4), però amb moltes millores sobre aquests protocols de l'**IPv4**.

El mecanisme sense estat permet a un amfitrió generar la seva pròpia adreça mitjançant una combinació de la informació disponible localment i la informació anunciada pels encaminadors. Els encaminadors mostraran els prefixos que identifiquen les subxarxes associades amb un enllaç, mentre que els amfitrions generen un testimoni d'interfície que identifica de forma exclusiva una interfície d'una subxarxa. Una adreça es forma amb la combinació de tots dos. En absència d'encaminadors, un amfitrió només pot generar adreces locals d'enllaç. No obstant això, les adreces locals d'enllaç són suficients per permetre la comunicació entre els nodes connectats al mateix enllaç.

Simplificació de l'encaminament:

Per simplificar els aspectes de l'encaminament, les adreces de l'**IPv6** es consideren en dues parts: un prefix i un ID. Pot semblar el mateix que l'anàlisi d'adreces xarxa-amfitrió de l'**IPv4**, però té dos avantatges.

Element	Descripció
sense classe	No hi ha un nombre fix de bits per al prefix ni l'ID, cosa que permet una reducció de la pèrdua a causa de la sobreassignació.
imbricació	Es pot emprar un nombre arbitrari de divisions considerant nombres diferents de bits com el prefix.

Cas 1

128 bits
adreça de node

Cas 2

Element	Descripció
n bits	128-*n* bits
Prefix de subxarxa	ID d'interfície

Cas 3:

Element	Descripció	
n bits	80-*n* bits	48 bits
Prefix de subscriptor	ID de subxarxa	ID d'interfície

Cas 4:

Element	Descripció		
s bits	*n* bits	*m* bits	128-*s*-*n*-*m* bits
Prefix de subscripció	ID d'àrea	ID de subxarxa	ID d'interfície

Generalment, l'IPv4 no pot anar més enllà del Cas 3, fins i tot amb la màscara de subxarxa de longitud variable (VLSM és un mitjà per assignar recursos d'adreçament **IP** a subxarxes d'acord amb llur necessitat individual en comptes de seguint una regla de xarxa general). Es tracta més aviat d'un tema de longitud més curta d'adreça que de la definició de prefixos de longitud variable, però, tanmateix, val la pena esmentar-ho.

Simplificació del format de capçalera:

L'**IPv6** simplifica la capçalera de l'**IP** eliminant per complet alguns dels camps que es trobaven a la capçalera de l'**IPv4**, o bé traslladant-los a una capçalera d'extensió. Defineix un format més flexible per a la informació opcional (les capçaleres d'extensió).

Concretament, tingueu en compte l'absència de:
- longitud de la capçalera (la longitud és constant)
- identificació
- senyaladors
- desplaçament de fragments (traslladats a les capçaleres d'extensió de fragmentació)
- suma de comprovació de la capçalera (el protocol de la capa superior o la capçalera d'extensió de seguretat gestiona la integritat de les dades).

Taula 53. Capçalera de l'IPv4

Element	Descripció	Descripció	Descripció	Descripció
Versió	IHL	Tipus de servei	Longitud total	
Identificació	Identificació	Identificació	Senyaladors	Desplaçament de fragments
Temps de vida	Temps de vida	Protocol	Suma de comprovació de la capçalera	Suma de comprovació de la capçalera
Adreça d'origen	Adreça d'origen	Adreça d'origen	Adreça d'origen	Adreça d'origen
Adreça de destinació	Adreça de destinació	Adreça de destinació	Adreça de destinació	Adreça de destinació
Opcions	Opcions	Opcions	Opcions	Rebliment

Taula 54. Capçalera de l'IPv6

Element	Descripció	Descripció	Descripció	Descripció
Versió	Prio		Etiqueta de flux	
Longitud de càrrega	Longitud de càrrega	Longitud de càrrega	Capçalera següent	Límit de salts
Adreça d'origen	Adreça d'origen	Adreça d'origen	Adreça d'origen	Adreça d'origen
Adreça de destinació	Adreça de destinació	Adreça de destinació	Adreça de destinació	Adreça de destinació

L'IP*ng* inclou un mecanisme d'opcions millorades sobre l'**IPv4**. Les opcions de l'**IPv6** se situen en capçaleres d'extensió separades que es localitzen entre la capçalera de l'**IPv6** i la capçalera de la capa de transport d'un paquet. La majoria de les capçaleres d'extensió no s'examinen ni es processen per part de cap encaminador en un camí d'accés de lliurament de paquets fins que no arriba a la seva destinació final. Aquest mecanisme facilita una millora important en el rendiment de l'encaminador per a paquets que contenen opcions. A l'**IPv4** la presència d'opcions requereix que l'encaminador les examini totes.

Una altra millora és que, a diferència de les opcions de l'**IPv4**, les capçalera d'extensió de l'**IPv6** poden tenir una longitud arbitrària i que la quantitat total d'opcions d'un paquet no està limitada a 40 octets. Aquesta característica, a més de la manera en què es processa, permet que les opcions de l'**IPv6** s'utilitzin per a funcions que no eren pràctiques a l'**IPv4**, com ara les opcions d'encapsulació de seguretat i autenticació de l'**IPv6**.

Per millorar el rendiment quan es gestionen capçaleres d'opcions subsegüents i el protocol de transport següent, les opcions de l'IPv6 sempre tenen una longitud d'un enter múltiple de vuit octets per mantenir aquesta alineació per a les capçaleres subsegüents.

Amb l'ús de capçaleres d'extensió en comptes d'un especificador de protocol i camps d'opcions, les extensions de nova definició es poden integrar amb més facilitat.

Les especificacions actuals defineixen les capçaleres d'extensió de les maneres següents:

- Opcions de salt a salt que s'apliquen a cada salt (encaminador) del camí d'accés
- Capçalera d'encaminament per a l'encaminament d'origen lliure/estricte (poc utilitzat)
- Un fragment defineix el paquet com un fragment i conté informació sobre el fragment (els encaminadors de l'**IPv6** no fragmenten)
- Autenticació (vegeu informació sobre la seguretat del **TCP/IP** a *Security*)
- Encriptació (vegeu informació sobre la seguretat del **TCP/IP** a *Security*)
- Opcions de destinació per al node de destinació (ignorat pels encaminadors).

Control millorat de qualitat de servei/trànsit:

Mentre que la qualitat de servei es pot controlar mitjançant un protocol de control com ara **RSVP**, l'**IPv6** proporciona una definició de prioritats explícita per a paquets mitjançant el camp de prioritat de la capçalera **IP**.

Un node pot establir aquest valor per indicar la prioritat relativa d'un paquet o conjunt de paquets determinat, que després pot utilitzar el node, un o més encaminadors o la destinació per realitzar seleccions referents al paquet (és a dir, eliminar-lo o no).

L'**IPv6** especifica dos tipus de prioritats, les del trànsit de congestió controlada o les del trànsit de congestió no controlada. Entre els dos tipus no hi ha implícita cap sol•licitud relativa.

El *trànsit de congestió controlada* es defineix com a trànsit que respon a la congestió mitjançant alguna classe de "retrocés" o altres algorismes de limitació. Les prioritats del trànsit de congestió controlada són:

Element	Descripció
0	trànsit no caracteritzat
1	trànsit d'"emplenament" (per exemple, notícies de xarxa)
2	transferència de dades no atesa (per exemple, correu)
3	(reservat)
4	transferència de volums atesa (per exemple, **FTP**)
5	(reservat)
6	trànsit interactiu (per exemple, Telnet)
7	trànsit de control (per exemple, protocols d'encaminament)

El *trànsit de congestió no controlada* es defineix com a trànsit que respon a la congestió eliminant paquets (o simplement no reenviant-los), com ara vídeo, àudio o altres tipus de trànsit en temps real. Els nivells explícits no es defineixen amb exemples, però la sol•licitud és similar a la del trànsit de congestió controlada:

- El valor més baix que l'origen desitja més tenir descartat s'hauria d'utilitzar per al trànsit.
- El valor més alt que l'origen desitja menys tenir descartat s'hauria d'utilitzar per al trànsit.

Aquest control de prioritats només és aplicable al trànsit d'una determinada adreça d'origen. El trànsit de control d'una adreça no representa de forma explícita una prioritat major que la transferència de volums atesa d'una altra adreça.

Etiquetatge de fluxos:

Fora de la prioritització bàsica del trànsit, l'**IPv6** defineix un mecanisme per especificar un flux particular de paquets. En termes de l'**IPv6**, un *flux* es defineix com una seqüència de paquets enviats des d'un determinat origen fins a una destinació concreta (difusió individual o difusió múltiple) per a la qual l'origen vol una gestió especial per part dels encaminadors intermediaris.

Aquesta identificació de fluxos es pot utilitzar per al control de prioritats, però també per a un nombre de controls diferents.

L'etiqueta del flux es tria de forma aleatòria i no identifica cap característica del trànsit que no sigui el flux al qual pertany. Això significa que un encaminador no pot determinar que un paquet és d'un tipus determinat si examina l'etiqueta del flux. No obstant això, sí pot determinar que forma part de la mateixa seqüència de paquets que l'últim paquet que contenia aquella etiqueta.

Nota: Fins que l'**IPv6** no sigui d'ús general, l'etiqueta de flux és principalment experimental. Els usos i controls que impliquen etiquetes de flux encara no s'han definit ni estanditzat.

Transmissió a través d'un túnel de l'IPv6:

La transmissió a través d'un túnel proporciona una forma d'utilitzar una infraestructura d'encaminament existent de l'**IPv4** per portar el trànsit de l'**IPv6**.

La clau per a una transició de l'**IPv6** satisfactòria és la compatibilitat amb la base instal•lada existent dels amfitrions i encaminadors de l'**IPv4**. Mantenir la compatibilitat amb l'**IPv4** durant el desplegament de l'**IPv6** perfecciona la tasca de transició d'Internet a l'**IPv6**. Mentre es desplega la infraestructura de l'**IPv6**, la infraestructura d'encaminament existent de l'**IPv4** pot romandre operativa i es pot utilitzar per portar el trànsit de l'**IPv6**.

Els amfitrions i encaminadors de l'**IPv6** o l'**IPv4** poden transmetre a través d'un túnel els datagrames de l'**IPv6** per les regions de la topologia d'encaminament de l'**IPv4** encapsulant-los en paquets de l'**IPv4**. La transmissió a través d'un túnel es pot utilitzar de diferents maneres:

Element	Descripció
D'encaminador a encaminador	Els encaminadors de l'**IPv6** o l'**IPv4** interconnectats per una infraestructura de l'**IPv4** poden transmetre's entre ells a través d'un túnel paquets de l'**IPv6**. En aquest cas, el túnel estén un segment del camí d'accés d'extrem a extrem que pren el paquet de l'**IPv6**.
D'amfitrió a encaminador	Els amfitrions de l'**IPv6** o l'**IPv4** poden transmetre a través d'un túnel paquets de l'**IPv6** a un encaminador intermediari de l'**IPv6** o l'**IPv4** al qual es pot accedir a través d'una infraestructura de l'**IPv4**. Aquest tipus de túnel estén el primer segment del camí d'accés d'extrem a extrem del paquet.
D'amfitrió a amfitrió	Els amfitrions de l'**IPv6** o l'**IPv4** que estan interconnectats per una infraestructura de l'**IPv4** poden transmetre's entre ells a través d'un túnel paquets de l'**IPv6**. En aquest cas, el túnel estén tot el camí d'accés d'extrem a extrem que pren el paquet.
D'encaminador a amfitrió	Els encaminadors de l'**IPv6/IPv4** poden transmetre a través d'un túnel paquets de l'**IPv6** a l'amfitrió de l'**IPv6** o l'**IPv4** de llur destinació final. Aquest túnel estén només l'últim segment del camí d'accés d'extrem a extrem.

Les tècniques de transmissió a través d'un túnel normalment es classifiquen d'acord amb el mecanisme pel qual el node d'encapsulament determina l'adreça del node al final del túnel. Als mètodes d'encaminador a encaminador o d'amfitrió a encaminador, el paquet de l'**IPv6** es transmet a través d'un túnel a un encaminador. Als mètodes d'amfitrió a amfitrió o d'encaminador a amfitrió, el paquet de l'**IPv6** es transmet a través d'un túnel fins a la seva destinació final.

El node d'entrada del túnel (el node d'encapsulament) crea una capçalera d'encapsulament de l'**IPv4** i transmet el paquet encapsulat. El node de sortida del túnel (el node de desencapsulament) rep el paquet encapsulat, elimina la capçalera de l'**IPv4**, actualitza la capçalera de l'**IPv6**, i processa el paquet de l'**IPv6** rebut. No obstant això, el node d'encapsulament necessita mantenir una informació d'estat flexible per a cada túnel, com ara la unitat de transmissió màxima (MTU) del túnel, per processar els paquets de l'**IPv6** reenviats al túnel.

A l'**IPv6** hi ha dos tipus de túnels:

túnels automàtics
: Els túnels automàtics es configuren mitjançant la informació d'adreces de l'**IPv4** intercalada en una adreça de l'**IPv6**. L'adreça de l'**IPv6** de l'amfitrió de destinació inclou informació sobre a quina adreça de l'**IPv4** s'hauria de transmetre el paquet a través d'un túnel.

túnels configurats
: Els túnels configurats s'han de configurar manualment. Aquests túnels s'utilitzen quan s'empren adreces de l'**IPv6** que no tenen intercalada cap informació de l'**IPv4**. S'han d'especificar les adreces de l'**IPv6** i l'**IPv4** dels punts finals del túnel.

Per obtenir informació sobre la configuració dels túnels automàtics i configurats, consulteu l'apartat “Configuració de la tunelització a IPv6” a la pàgina 138.

Suport local d'enllaç i local de lloc d'inicis múltiples de l'IPv6:

Un amfitrió pot tenir definida més d'una interfície. Un amfitrió amb dos o més interfícies actives s'anomena d'inicis múltiples. Cada interfície té associada una adreça local d'enllaç.

Les adreces locals d'enllaç són suficients per permetre la comunicació entre els nodes connectats al mateix enllaç.

Un amfitrió d'inicis múltiples té associades dues o més adreces locals d'enllaç. La implementació de l'**IPv6** de l'AIX té 4 opcions per gestionar com es realitza la resolució d'adreces de la capa d'enllaç als amfitrions d'inicis múltiples. L'opció 1 és el valor per defecte.

Element	Descripció
Opció 0	No es realitza cap acció d'inicis múltiples. Les transmissions es faran en la primera interfície local d'enllaç. Quan el **Protocol de descobriment de veïnatge** (**NDP**) ha de realitzar la resolució d'adreces, difon de forma múltiple un missatge de sol•licitud de veïnatge a cada interfície amb una adreça local d'enllaç definida. L'NDP posa en cua el paquet de dades fins que es rep el primer missatge d'anunci de veïnatge. Aleshores el paquet de dades s'envia a aquest enllaç.
Opció 1	Quan l'**NDP** ha de realitzar la resolució d'adreces, és a dir, quan envia un paquet de dades a una destinació i la informació de la capa d'enllaç del següent salt no es troba a la memòria cau de veïnatge, difon de forma múltiple un missatge de sol•licitud de veïnatge a cada interfície amb una adreça local d'enllaç definida. Aleshores, l'**NDP** posa en cua el paquet de dades fins que rep la informació de la capa d'enllaç. Després, l'**NDP** espera fins que es rep una resposta per a cada interfície. Això garanteix que els paquets de dades s'enviïn en les interfícies de sortida adequades. Si l'**NDP** no ha esperat, sinó que ha respost al primer anunci de veïnatge rebut, és possible que un paquet de dades s'enviï a un enllaç no associat amb l'adreça d'origen del paquet. Com que l'**NDP** ha d'esperar, es produeix un retard en l'enviament del primer paquet. No obstant això, el retard es produeix de qualsevol manera a l'espera de la primera resposta.
Opció 2	L'operació d'inicis múltiples està permesa, però la distribució d'un paquet de dades està limitada a la interfície especificada per main_if6. Quan l'**NDP** ha de realitzar la resolució d'adreces, difon de forma múltiple un missatge de sol•licitud de veïnatge a cada interfície amb una adreça local d'enllaç definida. Aleshores, espera un missatge d'anunci de veïnatge de part de la interfície especificada per main_if6 (vegeu l'ordre **no**). Quan es rep una resposta d'aquesta interfície, el paquet de dades s'envia a aquest enllaç.
Opció 3	L'operació d'inicis múltiples està permesa, però la distribució d'un paquet de dades està limitada a la interfície especificada per main_if6 i les adreces locals de lloc només s'encaminen per a la interfície especificada per main_site6 (vegeu l'ordre **no**). L'NDP opera igual que a l'Opció 2. En les aplicacions que encaminen paquets de dades mitjançant adreces locals de lloc en un amfitrió d'inicis múltiples, només s'utilitza l'adreça local de lloc especificada per main_site6.

Actualització a l'IPv6 amb l'IPv4 configurat:

Aquest escenari us guiarà a través d'una actualització manual de l'**IPv4** a l'**IPv6**.

La xarxa emprada en aquest exemple està formada per un encaminador i dues subxarxes. A cada subxarxa hi ha dos amfitrions: l'encaminador i un altre amfitrió. Haureu d'actualitzar cada màquina d'aquesta xarxa a l'**IPv6**. En acabar aquest escenari, l'encaminador anunciarà el prefix `3ffe:0:0:aaaa::/64` a la interfície de xarxa `en0` i el prefix `3ffe:0:0:bbbb::/64` a la interfície de xarxa `en1`. Primer de tot haureu de configurar les màquines per tal que admetin temporalment l'**IPv6** amb l'objectiu de provar-les. A continuació, configurareu les màquines per tal que estiguin preparades per a l'**IPv6** quan s'engeguin.

Si executeu el sistema operatiu AIX i no teniu l'**IPv4** configurat, consulteu l'apartat "Actualització a l'IPv6 amb l'IPv4 no configurat." a la pàgina 133.

Informació que cal tenir en compte

- La informació d'aquest cas s'ha provat amb versions específiques de l'AIX. Els resultats obtinguts poden variar força segons la versió i el nivell de l'AIX.

Pas 1: Configuració dels amfitrions per a l'IPv6

En els amfitrions d'ambdues subxarxes, realitzeu les accions següents:

1. Escriviu l'ordre següent per assegurar-vos que l'**IPv4** estigui configurat:

   ```
   netstat -ni
   ```

   Els resultats haurien de ser semblants als següents:

   ```
   Name  Mtu   Network     Address            Ipkts Ierrs    Opkts Oerrs  Coll
   en0   1500  link#2      0.6.29.4.55.ec      279393     0     2510     0     0
   en0   1500  9.3.230.64  9.3.230.117         279393     0     2510     0     0
   lo0   16896 link#1                            913     0      919     0     0
   lo0   16896 127         127.0.0.1              913     0      919     0     0
   lo0   16896 ::1                               913     0      919     0     0
   ```

2. Amb l'autoritat root, escriviu l'ordre següent per configurar els valors de l'**IPv6**:

   ```
   autoconf6
   ```

3. Torneu a executar aquesta ordre:

   ```
   netstat -ni
   ```

   Els resultats haurien de ser semblants als següents:

   ```
   Name  Mtu   Network     Address            Ipkts Ierrs    Opkts Oerrs  Coll
   en0   1500  link#2      0.6.29.4.55.ec      279679     0     2658     0     0
   en0   1500  9.3.230.64  9.3.230.117         279679     0     2658     0     0
   en0   1500  fe80::206:29ff:fe04:55ec        279679     0     2658     0     0
   sit0  1480  link#3      9.3.230.117              0     0        0     0     0
   sit0  1480  ::9.3.230.117                        0     0        0     0     0
   lo0   16896 link#1                            2343     0     2350     0     0
   lo0   16896 127         127.0.0.1             2343     0     2350     0     0
   lo0   16896 ::1                               2343     0     2350     0     0
   ```

4. Escriviu l'ordre següent per iniciar el dimoni **ndpd-host**:

   ```
   startsrc -s ndpd-host
   ```

Pas 2: Configuració de l'encaminador per a l'IPv6

1. Escriviu l'ordre següent per assegurar-vos que l'**IPv4** estigui configurat:

   ```
   netstat -ni
   ```

2. Escriviu l'ordre següent amb autoritat root:

   ```
   autoconf6
   ```

3. Escriviu les ordres següents per configurar manualment adreces globals a les interfícies de l'encaminador que pertanyen a cadascuna de les dues subxarxes:

   ```
   # ifconfig en0 inet6 3ffe:0:0:aaaa::/64 eui64 alias
   # ifconfig en1 inet6 3ffe:0:0:bbbb::/64 eui64 alias
   ```

   Haureu d'executar aquestes ordres per a cada subxarxa a la qual enviï paquets l'encaminador.

4. Per activar el reenviament d'IPv6, escriviu el següent:

   ```
   no -o ip6forwarding=1
   ```

5. Per iniciar el dimoni **ndpd-router**, escriviu el següent:

   ```
   startsrc -s ndpd-router
   ```

   El dimoni **ndpd-router** anunciarà els prefixos corresponents a les adreces globals que heu configurat a l'encaminador. En aquest cas, el dimoni ndpd-router anunciarà el prefix `3ffe:0:0:aaaa::/64` a `en0` i el prefix `3ffe:0:0:bbbb::/64` a `en1`

Pas 3. Configuració de l'IPv6 que s'ha de configurar als amfitrions en engegar

L'**IPv6** que acabeu de configurar se suprimirà quan reinicieu la màquina. Per habilitar la funcionalitat de l'amfitrió de l'**IPv6** cada vegada que reinicieu, realitzeu el següent:

1. Obriu el fitxer /etc/rc.tcpip amb l'editor de textos que vulgueu.
2. Elimineu els símbols de comentari de les següents línies d'aquest fitxer:

   ```
   # Start up autoconf6 process
   start /usr/sbin/autoconf6 ""

   # Start up ndpd-host daemon
   start /usr/sbin/ndpd-host "$src_running"
   ```

3. Afegiu el senyalador **-A** a start /usr/sbin/autoconf6 "":

   ```
   start /usr/sbin/autoconf6 "" -A
   ```

Quan reinicieu, s'establirà la configuració de l'**IPv6**. Repetiu aquest procés per a cada amfitrió.

Pas 4: Configuració de l'IPv6 que s'ha de configurar a l'encaminador en engegar

L'**IPv6** que acabeu de configurar se suprimirà quan reinicieu. Per habilitar la funcionalitat de l'encaminador de l'**IPv6** cada vegada que reinicieu, realitzeu el següent:

1. Obriu el fitxer /etc/rc.tcpip amb l'editor de textos que vulgueu.
2. Elimineu el símbol de comentari de la línia següent d'aquest fitxer:

   ```
   # Start up autoconf6 process
   start /usr/sbin/autoconf6 ""
   ```

3. Afegiu les línies següents immediatament després de la línia de la qual heu eliminat els símbols de comentari al pas anterior:

   ```
   # Configure global addresses for router
   ifconfig en0 inet6 3ffe:0:0:aaaa::/64 eui64 alias
   ifconfig en1 inet6 3ffe:0:0:bbbb::/64 eui64 alias
   ```

   En aquest escenari, la nostra xarxa només té dues subxarxes, en0 i en1. Haureu d'afegir una línia a aquest fitxer per a cada subxarxa a la qual enviï paquets l'encaminador.
4. Elimineu el símbol de comentari de la línia següent del fitxer:

   ```
   # Start up ndpd-router daemon
   start /usr/sbin/ndpd- router "$src_running"
   ```

Quan reinicieu, l'**IPv6** s'iniciarà automàticament.

Actualització a l'IPv6 amb l'IPv4 no configurat.:

Aquest escenari mostra com es configuren els amfitrions i un encaminador per a l'**IPv6** sense que l'**IPv4** estigui configurat.

La xarxa emprada en aquest exemple està formada per un encaminador i dues subxarxes. A cada subxarxa hi ha dos amfitrions: l'encaminador i un altre amfitrió. En acabar aquest escenari, l'encaminador anunciarà el prefix 3ffe:0:0:aaaa::/64 a la interfície de xarxa en0 i el prefix 3ffe:0:0:bbbb::/64 a la interfície de xarxa en1. Primer de tot haureu de configurar les màquines per tal que admetin temporalment l'**IPv6** amb l'objectiu de provar-les. A continuació, configurareu les màquines per tal que estiguin preparades per a l'IPv6 quan s'engeguin.

En aquest escenari es pressuposa que el catàleg de fitxers bos.net.tcp.client està instal•lat.

Per actualitzar a l'**IPv6** amb l'**IPv4** ja configurat, consulteu “Actualització a l'IPv6 amb l'IPv4 configurat” a la pàgina 131.

Informació que cal tenir en compte

- La informació d'aquest cas s'ha provat amb versions específiques de l'AIX. Els resultats obtinguts poden variar força segons la versió i el nivell de l'AIX.

Pas 1: Configuració dels amfitrions per a l'IPv6

1. Escriviu l'ordre següent amb autoritat root a cada amfitrió de la subxarxa:

   ```
   autoconf6 -A
   ```

   S'activaran totes les interfícies preparades per a l'**IPv6** del sistema.

   Nota: Per activar un subconjunt de les interfícies, utilitzeu el senyalador **-i**. Per exemple, `autoconf6 -i en0 en1` activarà les interfícies `en0` i `en1`.

2. Escriviu l'ordre següent per visualitzar les interfícies:

   ```
   netstat -ni
   ```

   Els resultats haurien de ser semblants als següents:

   ```
   Name  Mtu   Network     Address            Ipkts Ierrs    Opkts Oerrs  Coll
   en0   1500  link#3      0.4.ac.17.b4.11        7     0       17     0     0
   en0   1500  fe80::204:acff:fe17:b411            7     0       17     0     0
   lo0   16896 link#1                           436     0      481     0     0
   lo0   16896 127         127.0.0.1            436     0      481     0     0
   lo0   16896 ::1                             436     0      481     0     0
   ```

3. Escriviu l'ordre següent per iniciar el dimoni **ndpd-host**:

   ```
   startsrc -s ndpd-host
   ```

Pas 2: Configuració de l'encaminador per a l'IPv6

1. Escriviu l'ordre següent amb autoritat root a l'amfitrió de l'encaminador:

   ```
   autoconf6 -A
   ```

   S'activaran totes les interfícies preparades per a l'**IPv6** del sistema.

   Nota: Per activar un subconjunt de les interfícies, utilitzeu el senyalador `-i`. Per exemple, `autoconf6 -i en0 en1` activarà les interfícies `en0` i `en1`.
   Els resultats haurien de ser semblants als següents:

   ```
   Name  Mtu   Network     Address            Ipkts Ierrs    Opkts Oerrs  Coll
   en1   1500  link#2      0.6.29.dc.15.45        0     0        7     0     0
   en1   1500  fe80::206:29ff:fedc:1545            0     0        7     0     0
   en0   1500  link#3      0.4.ac.17.b4.11        7     0       17     0     0
   en0   1500  fe80::204:acff:fe17:b411            7     0       17     0     0
   lo0   16896 link#1                           436     0      481     0     0
   lo0   16896 127         127.0.0.1            436     0      481     0     0
   lo0   16896 ::1                             436     0      481     0     0
   ```

2. Escriviu les ordres següents per configurar manualment adreces globals a les interfícies de l'encaminador que pertanyen a cadascuna de les dues subxarxes:

   ```
   # ifconfig en0 inet6 3ffe:0:0:aaaa::/64 eui64 alias
   # ifconfig en1 inet6 3ffe:0:0:bbbb::/64 eui64 alias
   ```

   Nota: Haureu d'executar aquestes ordres per a cada subxarxa a la qual enviï paquets l'encaminador.

3. Per activar el reenviament d'**IPv6**, escriviu el següent:

   ```
   no -o ip6forwarding=1
   ```

4. Per iniciar el dimoni **ndpd-router**, escriviu el següent:

   ```
   startsrc -s ndpd-router
   ```

   El dimoni **ndpd-router** anunciarà els prefixos corresponents a les adreces globals que heu configurat a l'encaminador. En aquest cas, el dimoni ndpd-router anunciarà el prefix `3ffe:0:0:aaaa::/64` a `en0` i el prefix `3ffe:0:0:bbbb::/64` a `en1`.

5. Premeu Intro per continuar.

6. Premeu Intro una altra vegada per confirmar la vostra decisió i començar la instal•lació del paquet de programari.

Pas 3. Configuració de l'IPv6 que s'ha de configurar als amfitrions en engegar

Després de realitzar el Pas 1 per a cada amfitrió, l'**IPv6** se suprimirà quan reinicieu la màquina. Per habilitar la funcionalitat de l'amfitrió de l'**IPv6** cada vegada que reinicieu, realitzeu el següent:

1. Obriu el fitxer `/etc/rc.tcpip` amb l'editor de textos que vulgueu.
2. Elimineu els símbols de comentari de les següents línies d'aquest fitxer:

   ```
   # Start up autoconf6 process
   start /usr/sbin/autoconf6 ""

   # Start up ndpd-host daemon
   start /usr/sbin/ndpd-host "$src_running"
   ```

3. Afegiu el senyalador **-A** a `start /usr/sbin/autoconf6 ""`:

   ```
   start /usr/sbin/autoconf6 "" -A
   ```

4. Repetiu aquest procés per a cada amfitrió.

Quan reinicieu, l'**IPv6** s'iniciarà automàticament.

Pas 4: Configuració de l'IPv6 que s'ha de configurar a l'encaminador en engegar

Després de realitzar el Pas 2 per a cada encaminador, l'**IPv6** se suprimirà quan reinicieu. Per habilitar la funcionalitat de l'encaminador de l'**IPv6** cada vegada que reinicieu, realitzeu el següent:

1. Obriu el fitxer `/etc/rc.tcpip` amb l'editor de textos que vulgueu.
2. Elimineu el símbol de comentari de la línia següent d'aquest fitxer:

   ```
   # Start up autoconf6 process
   start /usr/sbin/autoconf6 ""
   ```

3. Afegiu el senyalador **-A** a la línia:

   ```
   start /usr/sbin/autoconf6 "" -A
   ```

4. Afegiu les línies següents immediatament després de la línia de la qual heu eliminat els símbols de comentari al pas anterior:

   ```
   # Configure global addresses for router
   ifconfig en0 inet6 3ffe:0:0:aaaa::/64 eui64 alias
   ifconfig en1 inet6 3ffe:0:0:bbbb::/64 eui64 alias
   ```

   En aquest escenari, la nostra xarxa només té dues subxarxes, `en0` i `en1`. Haureu d'afegir una línia a aquest fitxer per a cada subxarxa a la qual enviï paquets l'encaminador.

5. Elimineu el símbol de comentari de la línia següent al fitxer:

   ```
   # Start up ndpd-router daemon
   start /usr/sbin/ndpd-router "$src_running"
   ```

6. Executeu l'ordre següent per habilitar el reenviament IP durant l'engegada:

   ```
   no -r -o ip6forwarding=1
   ```

Quan reinicieu, l'**IPv6** s'iniciarà automàticament.

Configuració estàtica del temps d'execució:

Aquest cas pràctic us guiarà a través de la configuració del temps d'execució d'un node amb la utilització de camins i IP estàtiques.

La xarxa que s'ha emprat en aquest exemple consisteix en un amfitrió i un encaminador. En acabar el cas pràctic, l'amfitrió tindrà configurat una interfície d'IPv6. Primer de tot haureu de configurar les màquines per tal que admetin temporalment l'IPv6 amb l'objectiu de provar-les. A continuació, configurareu les màquines per tal que estiguin preparades per a l'IPv6 quan s'engeguin.

Informació que cal tenir en compte

- La informació d'aquest cas s'ha provat amb versions específiques d'AIX. El resultat obtinguts poden variar força segons la versió i el nivell de l'AIX.
- L'exemple assumeix que **2001:1:2::/48** és l'Aggregate Global Unicast Address per la interfície d'IPv6 assignada per l'Internet Assigned Numbers Authority (IANA) al proveïdor. **2001:1:2:3:4::/64** és la subxarxa que utilitza els bits 49 - 64 assignats per l'administrador de la xarxa.
- Heu de consultar l'RFC 3587 per entendre el Global Unicast Address Format d'IPv6.

Informació relacionada:

Ordres de la configuració del temps d'execució

Ordre autoconf6

Pas 1. Configurar els amfitrions per a l'IPv6:

Seguiu aquest procediment per configurar els amfitrions per a l'IPv6.

1. Amb autorització root, configureu els paràmetres de l'IPv6 mitjançant l'ordre següent:
   ```
   # autoconf6
   ```
2. Torneu a executar aquesta ordre:
   ```
   # netstat -ni
   ```
   Els resultats haurien de ser semblants a la sortida següent:
   ```
   Name  Mtu   Network     Address            Ipkts Ierrs    Opkts Oerrs  Coll
   en0   1500  link#2      0.6.29.4.55.ec      279679     0     2658     0     0
   en0   1500  9.3.230.64  9.3.230.117         279679     0     2658     0     0
   en0   1500  fe80::206:29ff:fe04:55ec        279679     0     2658     0     0
   sit0  1480  link#3      9.3.230.117              0     0        0     0     0
   sit0  1480  ::9.3.230.117                        0     0        0     0     0
   lo0   16896 link#1                           2343     0     2350     0     0
   lo0   16896 127         127.0.0.1            2343     0     2350     0     0
   lo0   16896 ::1                             2343     0     2350     0     0
   ```
3. Utilitzeu l'ordre **chdev** per afegir l'adreça IPv6 a l'interfície de l'amfitrió. Per exemple, es prenen els 64 bits d'ordre de la IP local d'enllaç generades per **autoconf6** a l'interfície **en0**.
   ```
   # chdev -l en0 -a netaddr6='2001:2:3:4:206:29ff:fe04:55ec' -a prefixlen=64
   ```
4. Suprimiu qualsevol prefix de camí d'enllaç existent per al prefix següent:
   ```
   # route delete -inet6 2001:2:3:4::/64
   ```
5. Configureu el prefix de d'encaminament estàtic a l'amfitrió per afegir accessibilitat a l'encaminador, en què **fe80::206:29ff:fe04:66e** és l'encaminador o la passarel•la que té connectivitat a l'encaminador.
   ```
   # route add -inet6 -net 2001:2:3:4::/64 fe80::206:29ff:fe04:66e -static
   ```

   Nota: Si es necessita un canvi per al camí per defecte, assegureu-vos que l'**autoconf6** s'executa amb l'opció **-R**, que evita l'addició o sobreescriptura qualsevol camí per defecte del node. A continuació, repetiu els passos 3-5.

Pas 2. Configuració de l'encaminador per a IPv6:

Seguiu aquest procediment per configurar l'encaminador per a IPv6.

1. Comproveu que els paràmetres de l'IPv4 estan configurats mitjançant l'ordre següent:
   ```
   # netstat -ni
   ```
2. Amb autorització root, escriviu l'ordre següent:
   ```
   # autoconf6
   ```
3. Per activar el reenviament d'IPv6, escriviu l'ordre següent:
   ```
   # no -o ip6forwarding=1
   ```
4. Configureu l'IP global a l'interfície de l'encaminador mitjançant l'ordre següent:
   ```
   # chdev -l en0 -a netaddr6='2001:4:5:6:207:30ff:fe05:66ec' -a prefixlen=64
   ```

5. Configureu manualment rutes de l'encaminador per habilitar l'enviament de paquets de manera eficaç. Per exemple, si **fe80:: 3ca6:70ff:fe00:3004/64** és la passarel•la per al prefix **2001:2:3:4::/64**, afegiu un prefix de ruta com s'indica a continuació:

   ```
   # route add –inet6 –net 2001:2:3:4::/64 fe80::3ca6:70ff:fe00:3004 –static
   ```

Pas 3. Configuració de l'IPv6 perquè es configuri als amfitrions a cada reinici:

Els paràmetres dels amfitrions d'IPv6 que s'han configurat al **Pas 1. Configuració dels amfitrions d'IPv6** es suprimiran quan reinicieu la màquina. Per habilitar la funcionalitat dels amfitrions d'IPv6 cada vegada que reinicieu la màquina, seguiu aquest procediment.

1. Obriu el fitxer **/etc/rc.tcpip** a un editor de text.
2. Elimineu el símbol de comentari de la línia següent al fitxer **/etc/rc.tcpip**:

   ```
   # Start up autoconf6 process
   start /usr/sbin/autoconf6 ""
   ```

   Nota: Si la línia anterior no és al fitxer **/etc/rc.tcpip**, afegiu-la.
3. Afegiu el senyalador **-A** a **start /usr/sbin/autoconf6 ""**.

   ```
   start /usr/sbin/autoconf6 "" –A
   ```
4. Afegiu la línia següent al fitxer **/etc/rc.tcpip** després de la línia que heu eliminat (o afegit):

   ```
   chdev –l en0 –a netaddr6='2001:2:3:4:206:29ff:fe04:55ec' –a prefixlen=64
   ```
5. Elimineu qualsevol prefix de ruta existent prèviament mitjançant l'ordre següent:

   ```
   chdev -l inet0 –a delrout6='–net, 2001:2:3:4::/64'
   ```
6. Configureu una ruta mitjançant l'ordre següent:

   ```
   chdev -l inet0 –a rout6='–net, 2001:2:3:4::/64 ,fe80::206:29ff:fe04:66e,–static'
   ```

Quan reinicieu la màquina, la configuració IPv6 estarà establerta.

Nota: Haureu de repetir aquest procediment per cada amfitrió.

Pas 4. Configuració de l'IPv6 perquè es configuri a l'encaminador a cada reinici:

Els paràmetres de l'encaminador configurats a **Pas 2. Configuració de l'encaminador per a IPv6** s'eliminen quan reiniceu la màquina. Per habilitar la funcionalitat de l'encaminador d'IPv6 cada vegada que reinicieu la màquina, seguiu aquest procediment.

1. Obriu el fitxer **/etc/rc.tcpip** a un editor de text.
2. Elimineu el símbol de comentari de la línia següent al fitxer **/etc/rc.tcpip**:

   ```
   # Start up autoconf6 process
   start /usr/sbin/autoconf6 ""
   ```

   Nota: Si la línia anterior no és al fitxer **/etc/rc.tcpip**, afegiu-la.
3. Afegiu el senyalador **-A** a **start /usr/sbin/autoconf6 ""**.

   ```
   start /usr/sbin/autoconf6 "" –A
   ```
4. Afegiu les línies següents després de la línia que heu eliminat (o afegit) al pas 2 per configurar l'IP global a l'encaminador i per configurar el prefix de la ruta.

   ```
   chdev –l en0 –a netaddr6='2001:4:5:6:207:30ff:fe05:66ec' –a prefixlen=64
   chdev -l inet0 –a rout6='–net,2001:2:3:4::/64,fe80::3ca6:70ff:fe00:3004,–static'
   ```

   En aquest cas, la xarxa només té una subxarxa **en0**. Haureu d'afegir una línia a aquest fitxer per a cada subxarxa a la qual l'encaminador enviï paquets.

Quan reinicieu la màquina, l'IPv6 s'iniciarà automàticament.

Nota: Quan utilitzeu configuracions estàtiques de manera simultània amb **ndpd-host**, assegureu-vos que s'exploren diferents senyaladors a **ndpd-host** per retenir camins i IP estàtiques, si cal.

Configuració de la tunelització a IPv6:

Per configurar la tunelització d'IPv6 podeu utilitzar qualsevol dels dos mètodes següents. El primer mètode configura un túnel automàtic, mentre que el segon configura un túnel que ja està configurat.

Informació que cal tenir en compte

- La informació d'aquest cas s'ha provat amb versions específiques de l'AIX. Els resultats obtinguts poden variar força segons la versió i el nivell de l'AIX.

Configuració de la tunelització automàtica a IPv6

En aquest escenari, l'ordre **autoconf6** s'utilitzarà per configurar IPv6 i establir un túnel automàtic a través de la interfície principal, `en2`. A continuació, l'ordre **autoconf6** s'utilitzarà per configurar un túnel a través de la interfície secundària, `en0`.

A continuació es mostra el resultat de l'ordre **netstat -ni**, que visualitza la configuració actual de la xarxa del sistema:

```
en0   1500  link#2      Adreça MAC aquí          0     0       33     0     0
en0   1500  1.1         1.1.1.3                  0     0       33     0     0
en2   1500  link#3      Adreça MAC aquí      79428     0      409     0     0
en2   1500  10.1        10.1.1.1             79428     0      409     0     0
```

- Per habilitar IPv6 i un túnel automàtic, escriviu aquesta ordre:

  ```
  autoconf6
  ```

  L'execució ara de l'ordre **netstat -ni** mostra els resultats següents:

  ```
  # netstat -in
  en0   1500  link#2      Adreça MAC aquí          0     0       33     0     0
  en0   1500  1.1         1.1.1.3                  0     0       33     0     0
  en0   1500  fe80::204:acff:fe49:4910              0     0       33     0     0
  en2   1500  link#3      Adreça MAC aquí      79428     0      409     0     0
  en2   1500  10.1        10.1.1.1             79428     0      409     0     0
  en2   1500  fe80::220:35ff:fe12:3ae8
  sit0  1480  link#7      10.1.1.1                 0     0        0     0     0
  sit0  1480  ::10.1.1.1
  ```

  Si `en2` (adreça IP 10.1.1.1) és la interfície principal, l'adreça ::10.1.1.1 està ara disponible per a la tunelització automàtica a través de la interfície `en2`.

- Per habilitar un túnel automàtic a través de la interfície `en0`, escriviu l'ordre següent:

  ```
  autoconf6 -s -i en0
  ```

  L'execució ara de l'ordre **netstat -ni** mostra els resultats següents:

  ```
  # netstat -in
  en0   1500  link#2      Adreça MAC aquí          0     0       33     0     0
  en0   1500  1.1         1.1.1.3                  0     0       33     0     0
  en0   1500  fe80::204:acff:fe49:4910              0     0       33     0     0
  en2   1500  link#3      Adreça MAC aquí      79428     0      409     0     0
  en2   1500  10.1        10.1.1.1             79428     0      409     0     0
  en2   1500  fe80::220:35ff:fe12:3ae8
  sit0  1480  link#7      1.1.1.3                  0     0        3     0     0
  sit0  1480  ::10.1.1.1                           0     0        3     0     0
  sit0  1480  ::1.1.1.3                            0     0        3     0     0
  ```

  Aquesta acció fa que que una adreça IPv6 compatible amb IPv4 s'afegeixi a la interfície SIT existent, `sit0`. La tunelització també està habilitada ara per a la interfície `en0` mitjançant l'adreça ::1.1.1.3. La mateixa interfície, `sit0`, s'utilitzarà per a ambdós túnels.

Nota: Els túnels automàtics se suprimeixen quan el sistema es reinicia. Per tal que el túnel automàtic estigui present durant l'inici, afegiu els arguments necessaris a l'ordre **autoconf6** dins del fitxer `/etc/rc.tcpip`.

Configuració de túnels configurats

En aquest escenari s'utilitza l'SMIT per configurar un túnel que ja està configurat. Aquest túnel estarà disponible quan el sistema es reinicii perquè s'emmagatzemarà a l'ODM. Es configurarà un túnel entre els sistemes `alpha` i `beta`. L'adreça IPv4 del sistema `alpha` és 10.1.1.1, i l'adreça IPv4 del sistema `beta` és 10.1.1.2.

Per configurar túnels configurats, seguiu aquests passos:

1. Per configurar un túnel entre `alpha` i `beta`, escriviu l'ordre següent als dos sistemes:
   ```
   smit ctinet6
   ```
2. Seleccioneu **Afegir IPV6 a una interfície de túnel IPV4** a tots dos sistemes.
   ```
   autoconf6
   ```
3. En aquest escenari, hem especificat de la següent manera els valors al sistema `alpha`, en funció de les adreces IPv4:
   ```
   * ADREÇA D'ORIGEN IPV4 (decimal amb punts)           [10.1.1.1]
   * ADREÇA DE DESTINACIÓ IPV4 (decimal amb punts)      [10.1.1.2]
     ADREÇA D'ORIGEN IPV6 (separada per dos punts)      []
     ADREÇA DE DESTINACIÓ IPV6 (separada per dos punts) []
   ```
   Al sistema `beta`, s'han introduït els valors següents:
   ```
   * ADREÇA D'ORIGEN IPV4 (decimal amb punts)           [10.1.1.2]
   * ADREÇA DE DESTINACIÓ IPV4 (decimal amb punts)      [10.1.1.1]
     ADREÇA D'ORIGEN IPV6 (separada per dos punts)      []
     ADREÇA DE DESTINACIÓ IPV6 (separada per dos punts) []
   ```
4. Per visualitzar les interfícies configurades, escriviu l'ordre següent:
   ```
   ifconfig cti<X>
   ```
   en què *X* és el número de la interfície. En aquest escenari, s'han tornat els valors següents. Al sistema `alpha`:
   ```
   cti0: flags=8080051<UP,POINTOPOINT,RUNNING,MULTICAST>
           inet6 fe80::a01:101/128 --> fe80::a01:102
   ```
   Al sistema `beta`:
   ```
   cti0: flags=8080051 <UP,POINTOPOINT,RUNNING,MULTICAST>
           inet6 fe80::a01:102/128 --> fe80::a01:101
   ```

L'SMIT crea automàticament les adreces IPv6 per a tots dos extrems del túnel utilitzant aquest mètodes:

- Els 32 bits inferiors contenen l'adreça IPv4
- Els 96 bits superiors contenen el prefix `fe80::/96`

Si voleu, podeu omplir adreces IPv6 específiques.

Rastreig de paquets

La traça de paquets és el procés pel qual es pot verificar el camí d'accés d'un paquet a través de les capes fins a la seva destinació.

L'ordre **iptrace** realitza la traça de paquets a nivell d'interficie de xarxa. L'ordre **ipreport** emet la sortida a la traça del paquet en format hexadecimal i ASCII. L'ordre **trpt** realitza la traça de paquets a nivell de protocol de transport per **TCP**. La sortida de l'ordre **trpt** és més detallada i inclou informació sobre l'hora, l'estat de **TCP** i la seqüència dels paquets.

Capçaleres de paquet d'interfície de la xarxa

A la capa de l'interfície de xarxa, les capçaleres de paquet s'adjunten a les dades de sortida.

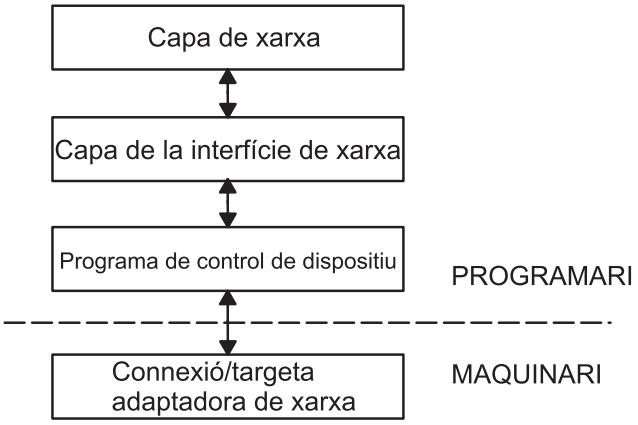


Figura 8. Flux de paquets a través de l'estructura de l'interfície de xarxa

Aquesta il•lustració mostra el flux de dades bidireccional a través de capes de l'estructura de l'interfície de xarxa. Des de la part superior (programari), són la capa de xarxa, la capa d'interfície de xarxa, el programa de control de dispositiu i la connexió o targeta d'adaptador de xarxa (maquinari).

A continuació, els paquets s'envien a través de l'adaptador de xarxa a la xarxa adient. Els paquets poden passar per moltes passarel•les abans d'arribar a les seves destinacions. A la xarxa de destinació, les capçaleres es fragmenten a partir dels paquets i les dades s'envien a l'amfitrió adequat.

La secció següent conté informació de capçalera de paquets d'algunes de les interfícies de xarxa més comunes.

Capçaleres de marc d'adaptadors Ethernet:

Una capçalera de marc del **protocol d'Internet** (**IP**) o del **protocol de resolució d'adreces** (**ARP**) per l'adaptador d'Ethernet està formada per aquests tres camps.

Taula 55. Capçalera de marc d'adaptadors Ethernet

Camp	Longitud	Definició
DA	6 octets	Adreça de destinació.
SA	6 octets	Adreça d'origen. Si el bit 0 d'aquest camp s'ha establert en 1, indica que hi ha informació d'encaminament (RI).
Tipus	2 octets	Especifica si el paquet és **IP** o **ARP**. Els valors numèrics del tipus es llisten a continuació.

Números del camp Tipus:

Element	Descripció
IP	0800
ARP	0806

Capçaleres de trama Token-Ring:

Hi ha cinc camps que comprenen la capçalera de control d'accés al medi (MAC) per a l'adaptador Token-Ring.

Taula 56. Capçalera MAC Token-Ring

Camp	Longitud	Definició
AC	1 octet	Control d'accés. El valor d'aquest camp x`00' dóna la prioritat de capçalera 0.
FC	1 octet	Control de camp. El valor d'aquest camp x`40' especifica la trama de control d'enllaços lògics.
DA	6 octets	Adreça de destinació.
SA	6 octets	Adreça d'origen. Si el bit 0 d'aquest camp s'estableix en 1, indica que la informació d'encaminament (RI) està present.
RI	18 octets	Informació d'encaminament. Els camps vàlids es tracten més avall.

La capçalera MAC consta de dos camps d'informació d'encaminament de dos octets cadascun: control d'encaminament (RC) i números de segment. Es pot utilitzar un màxim de vuit números de segment per especificar els destinataris d'una difusió limitada. La informació RC es troba als octets 0 i 1 del camp RI. Els valors dels dos primers bits del camp RC tenen els significats següents:

Element	Descripció
bit (0) = 0	Utilitzar el camí de no difusió especificat al camp RI.
bit (0) = 1	Crear el camp RI i difondre a tots els anells.
bit (1) = 0	Difondre a través de tots els ponts.
bit (1) = 1	Difondre a través de ponts limitats.

La capçalera de control d'enllaços lògics (LLC) està composta per cinc camps, tal com s'indica a la taula de capçalera LLC següent.

Taula 57. Capçalera LLC del 802.3

Camp	Longitud	Definició
DSAP	1 octet	Punt d'accés de servei de destinació. El valor d'aquest camp és x`aa'.
SSAP	1 octet	Punt d'accés de servei d'origen. El valor d'aquest camp és x`aa'.
CONTROL	1 octet	Determina les ordres i respostes LLC. Els tres valors possibles per a aquest camp es tracten més avall.
PROT_ID	3 octets	ID de protocol. Aquest camp està reservat. Té un valor x`0'.
TYPE	2 octets	Especifica si el paquet és **IP** o **ARP**.

Valors del camps de control:

Els camps de control Token-Ring inclouen una trama d'informació sense número, una trama d'identificació d'intercanvi i una trama de prova. A continuació es descriuen els seus valors.

Element	Descripció
x`03'	Trama d'informació sense número (UI). És la forma normal, o sense seqüència, de transmetre les dades d'adaptador Token-Ring a través de la xarxa. El **TCP/IP** fa seqüències de les dades.
x`AF'	Trama d'identificació d'intercanvi (XID). Aquesta trama comunica les característiques de l'amfitrió emissor.
x`E3'	Trama de prova. Aquesta trama dóna suport a les proves del camí d'accés de transmissió, fent eco de tornada de les dades rebudes.

Capçaleres de marc de 802.3:

La capçalera MAC per l'adaptador 802.3 està formada per dos camps, tal com mostra la taula de capçaleres MAC.

Taula 58. Capçalera MAC de 802.3

Camp	Longitud	Definició
DA	6 octets	Adreça de destinació.
SA	6 octets	Adreça d'origen. Si el bit 0 d'aquest camp s'ha establert en 1, indica que hi ha informació d'encaminament (RI).

La capçalera LLC del 802.3 és la mateixa que la de la capçalera MAC de Token-Ring.

Protocols de nivell de xarxa d'Internet

Els protocols de nivell de xarxa d'Internet gestionen la comunicació entre màquines.

En altres paraules, aquesta capa implementa l'encaminament **TCP/IP**. Aquests protocols accepten sol•licituds per enviar paquets (junt amb l'adreça de xarxa de la màquina de destinació) des de la capa de transport, converteixen els paquets al format de datagrama i els envien a la capa d'interfície de xarxa per continuar el seu processament.

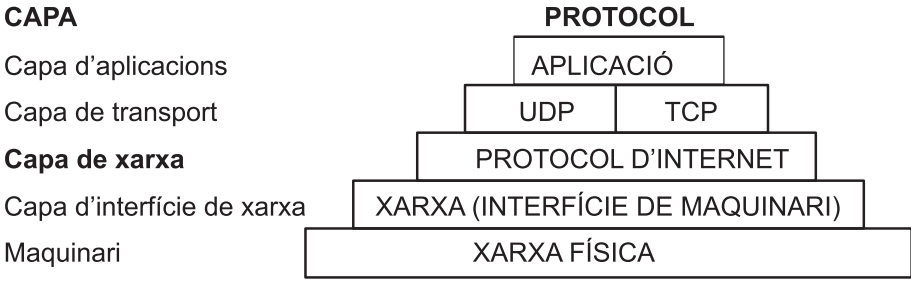


Figura 9. La capa de xarxa del paquet ofimàtic de protocols TCP/IP

Aquesta il•lustració mostra les diferents capes del paquet ofimàtic de protocols **TCP/IP**. Des de la part superior, la capa d'aplicacions consta de l'aplicació. La capa de transport conté **UDP** i **TCP**. La capa de xarxa conté l'interfície (maquinari) de xarxa. I finalment, la capa de maquinari conté la xarxa física.

TCP/IP proporciona els protocols que són necessaris per complir amb RFC 1100, els *protocols oficials d'Internet* i altres protocols que normalment utilitzen els amfitrions a la comunitat d'Internet.

Nota: La utilització de números de xarxa, versió, sòcol, servei i protocol d'Internet a **TCP/IP** també compleix amb els*números assignats* RFC 1010.

Protocol de resolució d'adreces:

El protocol de primer nivell de xarxa és el **protocol de resolució de xarxes** (**ARP**). **ARP** converteix de forma dinàmica adreces d'Internet en adreces de maquinari exclusives en xarxes d'àrea local.

Per il•lustrar com funciona una **ARP**, considereu dos nodes, X i Y. Si el node X es vol comunicar amb Y, i X i Y es troben a diferents LAN, X i Y es comunicaran a través de *ponts*, *encaminadors* o *passarel•les*, mitjançant adreces IP. Dins d'una LAN, els nodes es comuniquen mitjançant adreces de maquinari de baix nivell.

Els nodes del mateix segment de la mateixa LAN utilitzen **ARP** per determinar l'adreça de maquinari de la resta de nodes. En primer lloc, el node X envia una sol•licitud de protocol **ARP** per l'adreça de hardware del node Y. La sol•licitud **ARP** conté les adreces de maquinari i **IP** de X i l'adreça **IP** de Y. Si Y rep la sol•licitud **ARP**, col•loca una entrada per X a la seva memòria cau **ARP** (la qual s'utilitza per mapar ràpidament des de l'adreça IP fins a l'adreça de maquinari). A continuació, respon directament a X amb una resposta de **ARP** que conté les adreces de maquinari i **IP** de Y. Quan el node X rep la resposta **ARP** de Y, col•loca una entrada per Y a la seva memòria cau de **ARP**.

Un cop que existeix una entrada de memòria cau **ARP** a X per Y, el node X pot enviar paquets directament a Y sense tornar a fer ús del protocol **ARP** (tret que s'elimini l'entrada de memòria cau **ARP** per Y. En tal cas, es tornarà a fer servir **ARP** per contactar amb Y).

A diferència de la majoria dels protocols, els paquets **ARP** no tenen capçaleres de format fixe. Enlloc d'això, el missatge es dissenya per tal que sigui útil amb una varietat de tecnologies de xarxa, com:

- Adaptador LAN d'Ethernet (suporta protocols Ethernet i 802.3)
- Adaptador de xarxa Token-ring
- Adaptador de xarxa d'interfície de dades distribuïdes per fibra

De tota manera, ARP no converteix adreces pel **protocol d'interfície de línia sèrie** (**SLIP**) o el **convertidor de canal òptic de sèrie** (**SOC**), donat que són connexions de punt a punt.

El kernel manté les taules de conversió i el protocol **ARP** no es troba directament disponible als usuaris o aplicacions. Quan una aplicació envia un paquet d'Internet a un dels programes de control d'interfície, el programa de control sol•licita la correlació d'adreces adient. Si la correlació no es troba a la taula, s'envia un paquet de difusió general **ARP** a través del programa de control d'interfície de sol•licitud als amfitrions de la xarxa d'àrea local.

Les entrades de la taula de correlació **ARP** s'eliminen després de 20 minuts. Les entrades incompletes s'eliminen després de 3 minuts. Per realitzar una entrada permanent a les taules de correlació **ARP**, utilitzeu l'ordre **arp** amb el paràmetre *pub*:

```
arp -s 802.3 host2 0:dd:0:a:8s:0 pub
```

Quan un amfitrió qualsevol dóna suport a **ARP**, rep un paquet de sol•licitud **ARP**, l'amfitrió anota les adreces de maquinari i d'**IP** del sistema que realitza la sol•licitud i actualitza la seva taula de correlació, si és necessari. Si l'adreça **IP** d'amfitrió que es rep no coincideix amb l'adreça sol•licitada, l'amfitrió rebutja el paquet de sol•licitud. Si l'adreça **IP** no coincideix, l'amfitrió que rep la sol•licitud envia un paquet de resposta al sistema que realitza la sol•licitud. El sistema que realitza la sol•licitud emmagatzema la nova correlació i l'utilitza per transmetre qualsevol altre paquet d'Internet pendent.

Protocol d'Internet Control Message:

El protocol de segon nivell de xarxa és el protocol **Internet Control Message Protocol** (**ICMP**). **ICMP** és una part necessària de cada implementació **IP**. **ICMP** gestiona els missatges d'error i de control per **IP**.

Aquest protocol permet a les passarel•les i amfitrions enviar informes de problemes a la màquina que envia un paquet. **ICMP** fa el següent:

- Prova si una destinació està activa i és accessible.
- Informa sobre problemes de paràmetre amb la capçalera de datagrames.
- Realitza la sincronització de rellotge i els càlculs de temps de transmissió.

- Obté submàscares de xarxa i adreces d'Internet.

Nota: **ICMP** utilitza el suport bàsic d'**IP** com si fos un protocol de nivell superior. De tota manera, **ICMP** és, en realitat, una part integral d'**IP** i ha de ser implementat per cadascun dels mòduls **IP**.

ICMP proporciona comentaris sobre problemes a l'entorn de comunicació però no garanteix la fiabilitat d'**IP**. És a dir, **ICMP** no garanteix que un paquet **IP** s'entregui de forma fiable o que es retorni un missatge **ICMP** a l'amfitrió d'origen quan no s'entregui un paquet **IP** o quan s'hagi entregat de forma incorrecta.

Els missatges **ICMP** es poden enviar en qualsevol de les situacions següents:
- Quan un paquet no pot arribar a la seva destinació.
- Quan un amfitrió de passarel•la no té la capacitat de col•locar al buffer per reenviar un paquet.
- Quan una passarel•la pot dirigir un amfitrió per a què enviï tràfic per una ruta més curta.

TCP/IP envia i rep diferents tipus de missatge ICMP (consulteu "Tipus de missatges de protocol d'Internet Control Message Protocol"). **ICMP** està intercalat al kernel i no es proporciona cap interfície de programació d'aplicació a aquest protocol.

Tipus de missatges de protocol d'Internet Control Message Protocol:

ICMP envia i rep aquest tipus de missatges.

Element	Descripció
Sol•licitud eco	Enviada per amfitrions i passarel•les per provar si una destinació està activa i accessible.
Sol•licitud d'informació	Enviada per amfitrions i passarel•les per obtenir una adreça d'Internet per a una xarxa a la qual es troben adjunts. Aquest tipus de missatge s'envia amb la part de xarxa de l'adreça de destinació **IP** establerta al valor 0.
Sol•licitud d'indicació de l'hora	Enviada per sol•licitar que la màquina de destinació retorni el seu valor actual de l'hora del dia.
Sol•licitud de màscara d'adreça	Enviada per l'amfitrió per conèixer la seva màscara de subxarxa. L'amfitrió pot enviar-la a una passarel•la, si coneix l'adreça de la passarel•la o enviar un missatge de difusió.
Destinació inaccessible	Enviada quan una passarel•la no pot proporcionar un datagrama **IP**.
Satisfacció d'origen	Enviada per una màquina de descart quan els datagrames arriben massa ràpid per a què els processi una passarel•la o un amfitrió, per tal de sol•licitar que l'origen original redueixi la velocitat de enviament de datagrames.
Missatge de redirecció	S'envia quan una passarel•la detecta que un amfitrió està utilitzant una ruta que no es òptima.
Resposta d'eco	Enviada per qualsevol màquina que rep una sol•licitud d'eco com a resposta a la màquina que ha enviat la sol•licitud.
Resposta d'informació	Enviada per passarel•les en resposta a sol•licituds per adreces de xarxa, amb les camps d'origen i de destinació del datagrama **IP** especificats.
Resposta d'indicació de l'hora	Enviada amb el valor actual de l'hora del dia.
Resposta de màscara d'adreça	Enviada a màquines que sol•liciten màscares de subxarxa.
Problema de paràmetre	Enviat quan un amfitrió o una passarel•la troben un problema amb la capçalera del datagrama.
Temps excedit	Enviat quan es dóna qualsevol de les situacions següents: • Cada datagrama **IP** conté un comptador de duració (comptador de salts), que es redueix mitjançant cada passarel•la. • Una passarel•la rebutja un datagrama perquè el seu comptador de salts ha arribat al valor 0.
Indicació de l'hora d'Internet	S'utilitza per enregistrar les indicacions de l'hora a través de la ruta.

Protocol d'Internet:

El tercer protocol de nivell de xarxa és el **protocol d'Internet** (**IP**), que proporciona el lliurament de paquets sense connexió de forma inestable.

IP no té connexió perquè tracta cada paquet d'informació per separat. És inestable perquè no garanteix el lliurament, és a dir, que no requereix reconeixements de l'amfitrió que els envia, que els rep ni d'amfitrions indeterminats.

IP proporciona l'interfície pels protocols de nivell d'interfície de xarxa. Les connexions físiques de l'informació de transferència de xarxa en un marc amb capçalera i dades. La capçalera conté l'adreça d'origen i l'adreça de destinació. **IP** utilitza un datagrama d'Internet que conté informació semblant al marc físic. El datagrama també té una capçalera que conté adreces del protocol d'Internet sobre l'origen i la destinació de les dades.

IP defineix el format de totes les dades enviades per Internet.

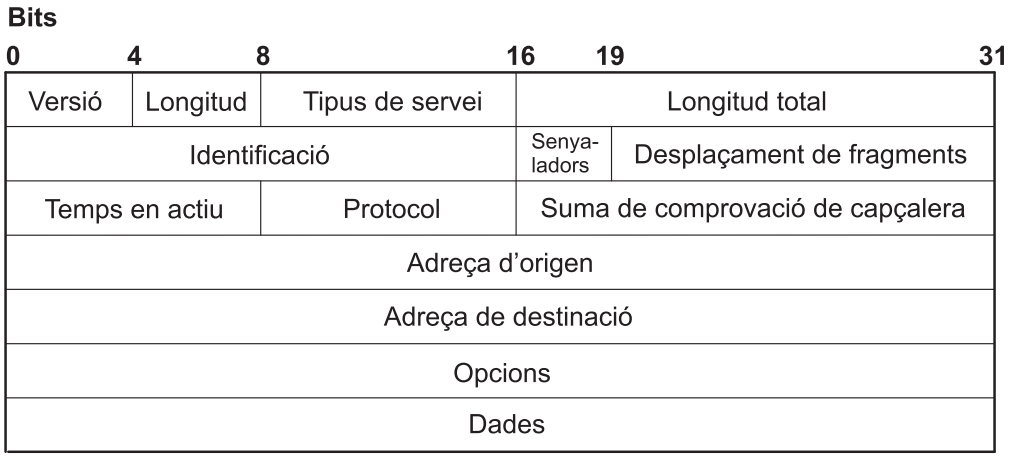


Figura 10. Capçalera de paquet de protocol d'Internet

Aquesta il•lustració mostra els primers 32 bits d'una capçalera de paquet IP típica. A la taula següent, es llisten les diferents entitats.

Definicions de camp de capçalera IP

Element	Descripció
Versió	Especifica la versió **IP** utilitzada. La versió actual del protocol **IP** és 4.
Longitud	Especifica la longitud de capçalera del datagrama, mesurada en paraules de 32 bits.
Tipus de servei	Conté cinc subcamps que especifiquen el tipus de prioritat, retard, rendiment i fiabilitat desitjats pel paquet en qüestió. (Internet no garanteix aquesta sol•licitud.) Els valors per defecte d'aquests cinc subcamps són prioritat de rutina, retard normal, rendiment normal i fiabilitat normal. Aquest camp normalment no s'utilitza normalment per Internet. Aquesta implementació d'**IP** compleix amb els requisits de l'especificació **IP**, RFC 791, *protocol d'Internet*.
Longitud total	Especifica la longitud del datagrama, incloses la capçalera i les dades mesurades en octets. Es proporciona la fragmentació de paquets en passarel•les amb destinacions de reacoblament. La longitud total del paquet **IP** es pot configurar d'interfície a interfície amb l'ordre **ifconfig** o el camí d'accés ràpid de la SMIT, `smit chinet`. Utilitzeu la SMIT per establir els valors de forma permanent a la base de dades de configuració. Utilitzeu l'ordre **ifconfig** per establir o canviar els valors al sistema que s'estigui executant.
Identificació	Conté un únic enter que identifica el datagrama.

Element	Descripció
Senyaladors	Controla la fragmentació de datagrames, junt amb el camp Identificació. Els senyaladors de fragment especifiquen si el datagrama es pot fragmentar i si el fragment actual és l'últim.
Desplaçament de fragment	Especifica el desplaçament d'aquest fragment al datagrama original mesurat en unitats de 8 octets.
Temps en actiu	Especifica el temps que un datagrama pot estar a Internet. Això fa que els datagrames sense ruta es quedin a Internet de forma permanent. El temps per defecte que un diagrama pot estar actiu és de 255 segons.
Protocol	Especifica el tipus de protocol de nivell superior.
Suma de comprovació de capçalera	Indica un número calculat per garantir l'integritat dels valors de capçalera.
Adreça d'origen	Especifica l'adreça d'Internet de l'amfitrió emissor.
Adreça de destinació	Especifica l'adreça d'Internet de l'amfitrió receptor.
Opcions	Proporciona la realització de proves i la depuració de la xarxa. Aquest camp no és necessari per a cada datagrama. **Final de la llista d'opcions** Indica el final de la llista d'opcions. S'utilitza al final de l'opció final, no al final de cada opció individual. Aquesta opció només s'ha d'utilitzar si el final de les opcions no coincideix amb el final de la capçalera **IP**. El final de la llista d'opcions s'utilitza si les opcions excedeixen la longitud del datagrama. **Cap operació** Proporciona l'alineació entre altres opcions; per exemple, per alinear l'inici d'una opció següent en un límit de 32 bits. **Origen flexible i ruta d'enregistrament** Proporciona un mode per a què l'origen d'un datagrama d'Internet proporcioni informació d'encaminament utilitzada per les passarel•les a l'hora de reenviar el datagrama a una destinació i a l'hora d'enregistrar l'informació de ruta. Això és la ruta d'origen *flexible*: l'**IP** de passarel•la o d'amfitrió pot utilitzar qualsevol ruta de qualsevol número de passarel•les intermèdies per arribar a la següent adreça de la ruta. **Origen estricte i ruta d'enregistrament** Proporciona un mode per a què l'origen d'un datagrama d'Internet proporcioni informació d'encaminament utilitzada per les passarel•les a l'hora de reenviar el datagrama a una destinació i a l'hora d'enregistrar l'informació de ruta. Això es una ruta d'origen *estricte*: Per arribar a la passarel•la o a l'amfitrió següent especificat a la ruta, cal enviar l'**IP** de la passarel•la o de l'amfitrió ha d'enviar el datagrama directament a l'adreça següent de la ruta d'origen i només a la xarxa directament connectada, la qual s'indica a l'adreça següent. **Ruta d'enregistrament** Proporciona un mode d'enregistrar la ruta d'un datagrama d'Internet. **Identificador de corrent** Proporciona un mode amb el qual l'identificador de corrent pot dur-se a terme a través de xarxes que no suporten el concepte de corrent. **Indicació de l'hora d'Internet** Proporciona un enregistrament de les indicacions de l'hora a través de la ruta.

Els paquets de sortida automàticament tenen una capçalera **IP** prefixada. La capçalera **IP** dels paquets d'entrada s'elimina abans d'enviar-se al protocols de nivell superior. El protocol **IP** proporciona l'adreçament universal d'amfitrions a la xarxa d'Internet.

Protocols de nivell de transport d'Internet

Els protocols de nivell de transport **TCP/IP** permeten als programes d'aplicació comunicar-se amb altres programes d'aplicació.

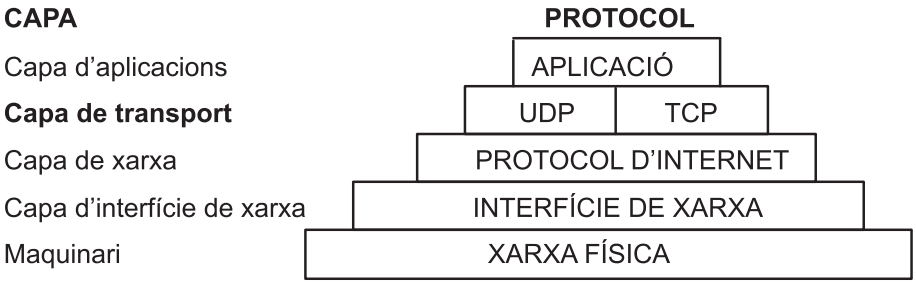


Figura 11. Capa de transport del paquet ofimàtic de protocols TCP/IP.

Aquesta il•lustració mostra les diferents capes del paquet ofimàtic de protocols **TCP/IP**. Des de la part superior, la capa d'aplicacions consta de l'aplicació. La capa de transport conté **UDP** i **TCP**. La capa de xarxa conté l'interfície (maquinari) de xarxa. I finalment, la capa de maquinari conté la xarxa física.

Els protocols **User Datagram Protocol** (**UDP**) i **TCP** són els protocols de nivell de transport bàsics per realitzar connexions entre amfitrions d'Internet. Ambdós **TCP** i **UDP** permeten als programes enviar i rebre missatges d'altres aplicacions en altres amfitrions. Quan una aplicació envia una sol•licitud a la capa de transport per enviar un missatge, **UDP** i **TCP** divideixen l'informació en paquets, afegeixen una capçalera de paquet que inclou l'adreça de destinació i envien l'informació a la capa de xarxa per continuar el seu processament. Tant **TCP** com **UDP** utilitzen ports de protocol a l'amfitrió per identificar la destinació específica del missatge.

Els protocols i les aplicacions de nivell superior utilitzen **UDP** per realitzar connexions de diagrama i **TCP** per realitzar connexions de corrent. L'interfície de sòcols de sistema operatiu implementa aquests protocols.

User Datagram Protocol:

De vegades, una aplicació d'una xarxa ha d'enviar missatges a una aplicació o un procés específics d'una altra xarxa. El protocol **UDP** proporciona al diagrama un mitja de comunicació entre aplicacions i amfitrions d'Internet.

Donat que els emissors no coneixen els processos que estan actius en un moment determinat, **UDP** utilitza els ports de protocol de destinació (o punts de destinació abstractes dins d'una màquina), identificats per enters positius, per enviar missatges a una o vàries destinacions d'un amfitrió. Els ports de protocol reben i retenen missatges en cues fins que les aplicacions de la xarxa receptora els poden recuperar.

Donat que **UDP** utilitza l'**IP** subjacent per enviar els seus datagrames, **UDP** proporciona el mateix lliurament de missatges sense connexió que en forma d'**IP**. No ofereix cap garantia del lliurament de datagrames ni de la protecció de duplicació. Tanmateix, **UDP** permet a l'emissor especificar els números de port d'origen i de destinació del missatge i calcula una suma de comprovació per les dades i la capçalera. Aquestes dues funcions permeten enviar i rebre aplicacions per garantir el lliurament correcte d'un missatge.

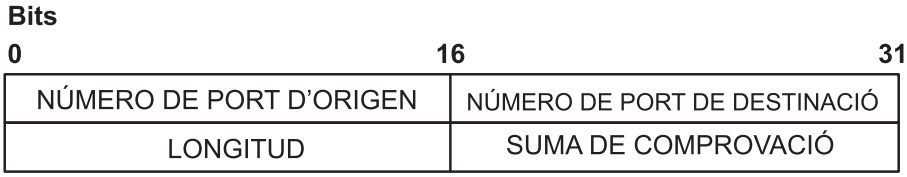


Figura 12. Capçalera de paquet del User Datagram Protocol (UDP)

Aquesta il•lustració mostra els primers 32 bits de la capçalera de paquet **UDP**. Els primers 16 bits contenen el número de port d'origen i la longitud. Els segons 16 bits contenen el número de port de destinació i la suma de comprovació.

Les aplicacions que requereixen el lliurament fiable de datagrames han d'implementar les seves comprovacions de fiabilitat quan utilitzin **UDP**. Les aplicacions que requereixen el lliurament fiable de corrents de dades han d'utilitzar **TCP**.

Definicions de cap de capçalera UDP

Element	Descripció
Número de port d'origen	Adreça del port de protocol que envia l'informació.
Número de port de destinació	Adreça del port de protocol que rep l'informació.
Longitud	Longitud en octets del datagrama **UDP**.
Suma de comprovació	Proporciona una comprovació del datagrama **UDP** mitjançant el mateix algorisme que l'**IP**.

L'interfície de programació d'aplicacions (API) d'**UDP** és un conjunt de subrutines de biblioteca proporcionat per l'interfície de sòcols.

Reliable Datagram Sockets sobre InfiniBand i RoCE:

El Reliable Datagram Sockets (RDS) és un protocol sense connexió i orientat al registre que proporciona un servei ordenat i sense duplicitats sobre InfiniBand i RDMA sobre Ethernet Convergit (RoCE). L'RDS mostra el subconjunt de l'User Datagram Protocol (UDP) de l'API del sòcol.

L'RDS és part del domini **AF_BYPASS**, el qual s'utilitza per protocols que eviten la pila TCP/IP del kernel.

L'AIX proporciona dos versions de l'RDS: l'RDSv2 i l'RDSv3. L'RDSv3 és l'última versió i inclou suport per al Remote Direct Memory Access (RDMA). RDSv3 en AIX 7.2 i posteriors admeten RDMA sobre adaptadors Ethernet convergits (RoCE) basat en Open Fabrics Enterprise Distribution (OFED).

Creació d'un sòcol RDS: Per crear un sòcol RDS, invoqueu la crida del sistema **socket()** mitjançant l'addició de les línies següents a l'aplicació del programa:

```
#include <sys/bypass.h>
include <net/rds_rdma.h>           /* for RDSv3 only */
sock = socket (AF_BYPASS, SOCK_SEQPACKET,BYPASSPROTO_RDS);
```

Si el protocol **BYPASSPROTO_RDS** és l'únic reliable datagram protocol que s'admet a la família **AF_BYPASS**, podeu cridar també la crida del sistema **socket()** de la manera següent:

```
sock = socket (AF_BYPASS, SOCK_SEQPACKET,0);
```

Crides del sistema

L'RDS també suporta les crides del sistema següents:
- blind()
- close()
- getsockopt()
- recvform()
- recvmsg()
- sendmsg()
- sendto()
- setsockopt()

A més, l'RDSv3 també admet les crides del sistema següents:
- connect()
- read()
- recv()
- send()
- write()

Nota: Encara que els sòcols del RDS són sense connexió, l'RDSv3 admet la crida del sistema **connect()**. No obstant això, en aquest cas, **connect()** no crea una connexió a nivell de sòcol entre dos punts finals d'RDS. Senzillament associa un punt final de destinació per defecte amb el sòcol. Per aquesta raó, no s'admeten les crides del sistema **listen()**, **accept()** i **shutdown()** per als sòcols RDS.

La utilitat rdsctrl per l'RDSv2: Empreu la utilitat **rdsctrl** (`/usr/sbin/rdsctrl`) per canviar els ajustables i els diagnòstics de les estadístiques de l'RDS. Per a l'RDSv2, es pot emprar la utilitat després que l'RDS s'hagi carregat (**bypassctrl load rds**). Per obtenir més informació sobre aquesta utilitat, executeu l'ordre rdsctrl sense arguments.

Estadístiques

Per visualitzar diverses estadístiques de l'RDS, executeu l'ordre `# rdsctrl stats`.

Per restablir les estadístiques, executeu l'ordre `# rdsctrl stats reset`.

Ajustament dels paràmetres

Els paràmetres RDS següents poden ajustar-se després que l'RDS s'hagi carregat i abans que s'hagi executat:

rds_sendspace
Especifica la marca de límit superior de la memòria intermèdia d'enviament per flux. Cada sòcol fluxos diversos. El valor per defecte és de 524288 bytes (512 KB). El valor es defineix mitjançant l'ordre següent`# rdsctrl set rds_sendspace= <valor en bytes>`.

rds_recvspace
Especifica la marca de límit superior per flux de la memòria intermèdia de recepció per sòcol. Per a cada flux addicional d'aquest sòcol, la marca de **recepció límit superior** s'augmenta en aquest valor. El valor per defecte és de 524288 bytes (512 KB). El valor es defineix mitjançant l'ordre següent`# rdsctrl set rds_recvspace= <valor en bytes>`.

Nota: Per augmentar el rendiment de la reproducció de modalitat contínua, els valors dels paràmetres **rds_sendspace** i **rds_recvspace** han de quadruplicar, com a mínim, el valor de la mida

més gran de l'RDS **sendmsg()**. L'RDS envia un ACK per cada conjunt de quatre missatges rebuts. Si el **rds_recvspace** no es quatre vegades més gran que la mida del missatge, la mitjana de rendiment és molt baixa.

rds_mclustsize
Especifica la mida de la memòria individual del clúster, el qual també és la mida del fragment del missatge. La mida per defecte és de 16384 bytes (16 KB). El valor, sempre múltiple de 4096, es defineix mitjançant l'ordre següent: `# rdsctrl set rds_mclustsize= <múltiple de 4096, en bytes>`.

Atenció: El valor **rds_mclustsize** ha de ser el mateix en tots els sistemes (nodes) del clúster. El fet de canviar aquest valor tendrà implicacions en el rendiment.

El valors actuals pels paràmetres anteriors es poden recuperar mitjançant l'ordre `# rdsctrl get <paràmetre>`.

Per obtenir la llista dels ajustables i els valors, executeu l'ordre `# rdsctrl gettot`.

La utilitat rdsctrl per l'RDSv3: Per l'RDSv3, l'ordre **rdsctrl** admeten opcions. A continuació es llisten les opcions:

Element	Descripció
help [<*nom d'ajustable*>**]**	L'opció **help** mostra un missatge descriptiu de l'ajustable RDSv3 específic. Si no s'especifica cap ajustable, aquesta opció mostra la llista de tots els ajustables que RDSv3 admet amb la seva descripció.
set [-p] {<*nom d'ajustable*> **=** <*valor*>**}**	L'opció **set** defineix el valor de l'ajustable RDSv3 específic. Verifica que l'usuari té els privilegis necessaris per prevenir que els usuaris no autoritzats canviïn els ajustables RDS. També valida l'interval pels nous valors ajustables. El senyalador **-p** fa que la tasca sigui permanent després de cada reinici.
get [<*nom d'ajustable*>**]**	L'opció **get** obté el valor actual del ajustable consultat. Quan no s'especifica el camp de nom en aquesta ordre, es retornarà el valor actual de totes les RDS ajustables.
default [-p] [<*tunable name*>**]**	L'opció **default** s'utilitza per restablir el valor per defecte d'un ajustable. Quan s'especifica el camp de nom, només es restablirà l'ajustable especificat. Si no s'especifica cap nom, aquesta ordre restablirà el valor per defecte de tots els ajustables. Aquesta opció també proporciona una manera de fer que el canvi sigui persistent després de cada reinici mitjançant el senyalador **-p**.
load [`ofed | aixib`]	L'opció **load** carrega l'extensió de kernel RDSv3 (si no s'ha carregada ja). L'argument `ofed` carrega l'extensió del kernel en verbs RDSv3 en OFED en mode RoCE. L'argument `aixib` carrega l'extensió del kernel in RDSv3 en mode InfiniBand. Especificar un argument per a l'opció **`load`** és opcional. L'opció **`load`** pren per defecte l'argument `aixib` quan no se n'especifica cap. Per defecte, l'utilitat **rdsctrl** carrega el dispositiu InfiniBand excepte si s'especifica el nou atribut (`ofed`) a la línia d'ordres.
unload	L'opció **unload** s'utilitza per descarregar l'extensió del kernel RDSv3.
ras [-p] <*mínima* **|** *normal* **|** *detall* **|** *màxima*>	L'opció **ras** defineix els paràmetres del rastreig RAS i de la comprovació d'errors de l'AIX per a l'RDSv3 al nivell especificat. De manera interna, aquesta ordre crida a les ordres **errctrl** i **ctctrl** de l'AIX. El senyalador **-p** fa que els paràmetres siguin persistents després de cada reinici.
ras extract	L'opció **ras extract** buida els continguts de les memòries intermèdies de seguiment dels errors i no errors de la RAS per a la sortida estàndard de l'RDS.
info [<*senyaladors*>**]**	L'opció **info** és un àlies de l'ordre **rds-info**.
ping [<*adreça IP v4*>**]**	L'opció **ping** és un àlies de l'ordre **rds-ping**.

Element	Descripció
conn *<restart | kill > <adreça IP d'origen> <adreça IP de destinació>*	L'opció **conn** reinicia la connexió RDS específica (subconnexió **restart**) o acaba permanentment amb la connexió RDS especifíca (subopció **kill**). La connexió RDS que s'ha de reiniciar o acabar s'especifica a través de les adreces IP dels nodes locals i remots de les connexions. El reinici d'una connexió fa que la connexió subjacent d'InfiniBand s'elimini i s'intenti establir connexió una altra vegada. Per contra, acabar una connexió (subopció kill) fa que la connexió subjacent d'InfiniBand s'elimini i es desassignen tots els recursos de la connexió RDS corresponent.
trace start *<trace file path> <dades màximes capturades per fragment RDS>*	L'opció **trace start** inicia una sessió de rastreig per capturar el trànsit de la xarxa per al protocol RDSv3. Els missatges RDSv3 es transmeten per fragments. Cada fragment d'RDS que es transmet o es rep es captura com a un paquet rastrejat a l'arxiu de rastreig especificat. Per a cada fragment d'RDS, es captura la càrrega fins a *<dades màximes capturades per fragment RDS>* bytes. Només els usuaris amb privilegis poden rastrejar el trànsit RDS i només hi pot haver una sessió de rastreig activa.
trace stop	L'opció **trace stop** acaba una sessió de rastreig que s'havia iniciat prèviament per l'ordre **trace start**. Tanca l'arxiu de rastreig que estava associat a la sessió de rastreig. Després d'aquesta ordre, es pot utilitzar l'ordre **trace report** per generar un informe de text del fitxer de rastreig.
trace report *<trace file path>*	L'opció **trace report** imprimeix un informe de text a la sortida estàndard d'un fitxer de rastreig d'un protocol RDS capturat anteriorment.
version	L'opció **version** imprimeix una versió del protocol RDS que està carregat actualment en el sistema.

Ajustables d'RDSv3: Per veure la llista d'ajustables que admet l'RDSv3, executeu l'ordre **rdsctrl help** sense arguments.

API de l'RDMA (només RDSv3): El model de programació per treballar en RDMA amb sòcols RDS està basat en el model de client/servidor. El client RDMA és la aplicació que inicia l'operació de lectura o escriptura de l'RDMA des d'un servidor RDMA específic. El servidor RDMA és la aplicació que processa la transferència de dades RDMA. Una operació de lectura RDMA és una transferència de dades des de l'espai d'adreces del client a l'espai d'adreça del servidor, mentre que una operació d'escriptura RDMA és una transferència de dades des de l'espai d'areces del servidor a l'espai d'adreces del client. En qualsevol cas, les dades es transfereixen directament a l'espai de la memòria de l'usuari en els dos costat, sense que s'hagi copiat a l'espai de la memòria kernel en cap costat.

Una aplicació client pot iniciar una operació de lectura o escriptura RDMA mitjançant l'enviament d'una sol•licitud a nivell d'aplicació, juntament amb una galeta RDMA, a una aplicació de servidor RDMA. La sol•licitud a nivell d'aplicació ha d'especificar si l'operació n'és una de lectura o d'escriptura així com l'adreça i la longitud de l'àrea de memòria del client que el servidor RDMA ha de llegir o escriure de manera remota.

Hi ha dos mètodes per enviar una sol•licitud RDMA des del client RDMA fins al servidor RDMA.

El primer mètode és enviar un missatge de control **RDS_CMSG_RDMA_MAP** (amb una estructura **rds_get_mr_args**) junt amb la sol•licitud RDMA a nivell d'aplicació mitjançant la crida del sistema **sendmsg()** en un sòcol RDS. El kernel d'AIX del client processa el missatge de control **RDS_CMSG_RDMA_MAP** i fa el mapatge de l'àrea específica de la memòria local (des de l'espai d'adreces de l'aplicació del client), per l'accés DMA, i genera una galeta RDMA. A continuació, la sol•licitud a nivell d'aplicació s'envia al servidor junt amb la galeta RDMA.

El segon mètode es conforma de dos passos. El primer és fer la crida del sistema **setsockopt()** amb l'opcío de sòcol **RDS_GET_MR** socket option, passant una estructura **rds_get_mr_args**. Aquesta crida mapeja l'àrea de la memòria local especifica per l'accés DMA i retorna una galeta RDMA. El segon pas és enviar un missatge de control **RDS_CMSG_RDMA_DEST** (que porti la galeta RDMA obtinguda del primer pas) junt amb la sol•licitud RDMA a nivell d'aplicació mitjançant la crida del sistema **sendmsg()**.

Es prefereix el primer mètode, el qual només necessita una crida del sistema, ja que el segon en necessita dues.

Quan el servidor d'aplicacions RDMA rep la sol•licitud de **lectura RDMA** a nivell d'aplicació del client, alhora també rep un missatge de control **RDS_CMSG_RDMA_DEST** que porta la galeta RDMA del client. A continuació, el servidor inicia l'operació de **lectura RDMA** mitjançant l'enviament de la resposta a nivell d'aplicació al client amb el missatge de control **RDS_CMSG_RDMA_ARGS** (amb una estructura **rds_rdma_args**). El kernel de l'AIX del servidor processa el missatge de control **RDS_CMSG_RDMA_ARGS** i mapeja l'àrea de memòria local específica (des de l'espai d'adreces del servidor d'aplicacions) per l'accés DMA, i comença físicament l'operació de lectura RDMA. L'operació de lectura RDMA es realitza per l'adaptador de servidor InfiniBand, el qual interactua amb l'adaptador de client InfiniBand, per dur a terme la transferència de dades directament de la memòria d'aplicacions del client a la memòria d'aplicacions del servidor, sense cap intervenció de maquinari. Després que l'operació de lectura RDMA s'hagi completat, l'adaptador de servidor envia una resposta a nivell d'aplicació al client. D'aquesta manera l'aplicació del client sap que l'operació de lectura RDMA s'ha completat.

Nota: El client sol•licita una operació RDMA mitjançant l'ús del missatge de control **RDS_CMSG_RDMA_MAP** en la qual està establert el senyalador **RDS_RDMA_USE_ONCE**. Per a aquesta sol•licitud, l'àrea de la memòria que s'assigna per el DMA a l'espai d'adreces del client, es desassigna automàticament per el DMA quan el client rep la resposta a nivell d'aplicació del servidor.

Encara que aquest mecanisme d'assinació o desassignació implícit de DMA faci més fàcil escriure a les aplicacions RDMA, els desenvolupadors han de tenir en compte que registrar memòria per a DMA a l'AIX és una operació costosa. Per tant, si s'ha d'accedir a la mateixa àrea de la memòria mitjançant l'ús de l'RDMA diverses veades, és més eficient fer el registre DMA només el primer cop. Per dur a terme aquesta activitat, l'aplicació del client necessita utilitzar un missatge de control **RDS_CMSG_RDMA_MAP** sense tenir establert el senyalador **RDS_RDMA_USE_ONCE** quan s'envii la sol•licitud RDMA al servidor. A continuació, l'aplicació del servidor RDMA pot iniciar les transferències RDMA subsegüents a la mateixa àrea de la memòria del client sense que el client necessiti enviar una altra sol•licitud al servidor. Al final, l'aplicació del client necessitaria desassignar explícitament la memòria DNA assignada mitjançant la crida del sistema **setsockopt()** amb l'opció de sòcol **RDS_FREE_MR**.

Les opcions de sòcol RDS específiques es detallen mitjançant l'**SOL_RDS** com a nivell de paràmetre per a les crides del sistema **setsockopt()** o **getsockopt()**

Protocol de control de transmissió:

TCP proporciona el lliurament de corrent fiable de dades entre els amfitrions d'Internet.

Igual que **UDP**, **TCP** utilitza el protocol d'Internet, el protocol subjacent, per transportar datagrames i dóna suport a les transmissions de bloc d'un corrent continu de datagrames entre ports de procés. A diferència de **UDP**, **TCP** proporciona un lliurament de missatges fiable. **TCP** garanteix que les dades no es malmeten, perden, dupliquen ni es lliuren en un moment no adient en un procés de rebuda. Aquesta garantia de fiabilitat de transport evita que els programadors d'aplicacions hagin de construir proteccions per les comunicacions al programari.

Característiques operatives de **TCP**:

Element	Descripció
Transferència de dades bàsiques	**TCP** pot transferir un corrent continu d'octets de 8 bits en cada direcció entre els seus usuaris mitjançant l'empaquetament d'alguns nombres d'octets en segments per transmetre'ls a través del sistema d'Internet. L'implementació **TCP** permet una grandària de segment de 1024 octets com a mínim. En general, **TCP** decideix quan es pot bloquejar i reenviar paquets segons convingui.
Fiabilitat	**TCP** ha de recuperar dades que es malmeten, perden, dupliquen o lliuren incorrectament per Internet. **TCP** aconsegueix aquesta fiabilitat assignant un número de seqüència a cada octet que transmet i sol•licitant un reconeixement positiu (ACK) del **TCP** receptor. Si no es rep l'ACK dins de l'interval del temps d'espera, es retransmeten les dades. El valor de temps d'espera de retransmissió **TCP** es determina de forma dinàmica per a cada connexió, segons el temps d'anada i tornada. Al receptor, s'utilitzen els números de seqüència per ordenar correctament els segments que es poden rebre de forma incorrecta i eliminar els duplicats. Els danys es gestionen afegint una suma de comprovació a cada segment transmès, comprovant-lo al receptor i rebutjant els segments malmesos.
Control de flux	**TCP** controla la quantitat de dades enviades mitjançant el retorn d'una finestra amb cada ACK per indicar una varietat de números de seqüència acceptables més enllà de l'últim segment rebut correctament. La finestra indica un número d'octets permès que l'emissor pot transmetre abans de rebre més permisos.
Multiplexatge	**TCP** permet que molts processos dins d'un sol amfitrió utilitzin recursos de comunicacions **TCP** a la vegada. **TCP** rep un conjunt d'adreces de ports dins de cada amfitrió. **TCP** combina el número de port amb l'adreça de xarxa i l'adreça d'amfitrió per identificar de forma exclusiva cada sòcol. Una parella de sòcols identifica de manera exclusiva cada connexió.
Connexions	**TCP** ha d'inicialitzar i mantenir determinada informació d'estat per a cada corrent de dades. La combinació d'aquesta informació, inclosos sòcols, números de seqüència i grandàries de finestra, s'anomena connexió. Cada connexió s'especifica de manera exclusiva mitjançant una parella de sòcols que identifiquen els seus dos costats.
Prioritat i seguretat	Els usuaris de **TCP** poden indicar la seguretat i la prioritat de les seves comunicacions. Els valors per defecte s'utilitzen quan aquestes característiques no són necessàries.

La figura **Capçalera de paquet TCP** mostra aquestes característiques.

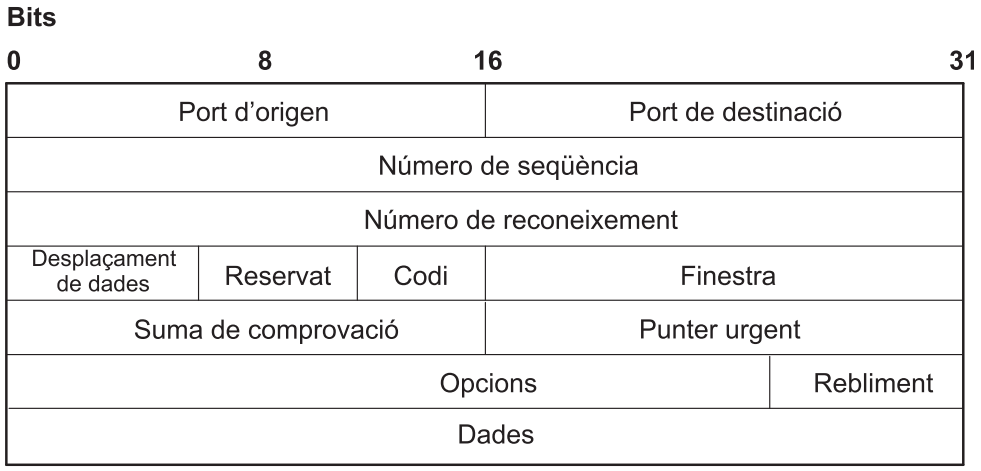


Figura 13. Capçalera de paquet de protocol de control de transmissió

Aquest il•lustració mostra el que conté la capçalera de paquet **TCP**. Les entitats individuals apareixen llistades en el text següent.

Definicions de camp de capçalera TCP:

A continuació, es presenten descripcions breus de cada camp de **protocol de control de transmissió** (**TCP**).

Element	Descripció
Port d'origen	Identifica el número de port del programa d'aplicació d'origen.
Port de destinació	Identifica el número de port d'un programa d'aplicació de destinació.
Número de seqüència	Especifica el número de seqüència del primer octet de dades en aquest segment.
Número de reconeixement	Identifica la posició de l'octet més elevat rebut.
Desplaçament de dades	Especifica el desplaçament de la part de dades del segment.
Reservat	Reservat per un ús futur.
Codi	Bits de control per identificar la finalitat del segment: **URG** El camp de punter urgent és vàlid. **ACK** El camp de reconeixement és vàlid. **PSH** El segment sol•licita un empilament. **RTS** Restableix la connexió. **SYN** Sincronitza els números de seqüència. **FIN** L'emissor ha arribat al final del corrent d'octets.
Finestra	Especifica la quantitat de dades que la destinació vol acceptar.
Suma de comprovació	Verifica l'integritat de la capçalera i les dades del segment.
Punter urgent	Indica que les dades s'han de lliurar el més ràpid possible. Aquest punter especifica la posició on finalitzen les dades urgents.
Opcions	**Final de la llista d'opcions** Indica el final de la llista d'opcions. S'utilitza a l'opció final, no al final de cada opció individual. Aquesta opció només s'ha d'utilitzar si el final de les opcions no coincideix amb el final de la capçalera **TCP**. **Cap operació** Indica els límits entre les opcions. Es pot utilitzar entre altres opcions, per exemple, per alinear el principi d'una opció posterior en un límit de paraula. No hi ha cap garantia que els emissors utilitzin aquesta opció, per tant, els receptors ha d'estar preparats per processar opcions encara que no comencin un límit de paraula. **Grandària màxima de segment** Indica la grandària de segment màxima que **TCP** pot rebre. Això només s'envia a la sol•licitud de connexió inicial.

L'interfície de programació d'aplicació de **TCP** consta d'un conjunt de subrutines de biblioteca proporcionades per l'interfície de sòcols.

Protocols de nivell d'aplicació d'Internet

TCP/IP implementa protocols d'Internet de nivell superior al nivell de programa d'aplicació.

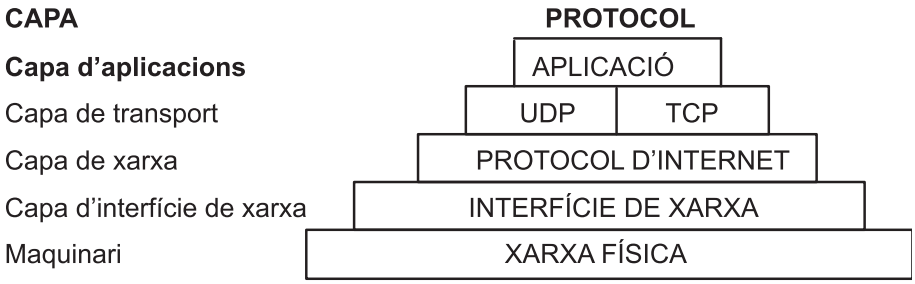


Figura 14. Capa d'aplicació del paquet ofimàtic de protocols TCP/IP

Aquesta il•lustració mostra les diferents capes del paquet ofimàtic de protocols **TCP/IP**. Des de la part superior, la capa d'aplicacions consta de l'aplicació. La capa de transport conté **UDP** i **TCP**. La capa de xarxa conté l'interfície (maquinari) de xarxa. I finalment, la capa de hardware conté la xarxa física.

Quan una aplicació ha d'enviar dades a una altra aplicació en un altre amfitrió, les aplicacions envien l'informació als protocols de nivell de transport per preparar l'informació i transmetre-la.

Els protocols de nivell d'aplicació d'Internet oficials inclouen:

- **Protocol de nom de domini**
- **Protocol de passarel•la exterior**
- **Protocol de transferència de fitxers**
- **Protocol de nom/Finger**
- **Protocol Telnet**
- **Trivial File Transfer Protocol**

TCP/IP implementa altres protocols de nivell superior que no són protocols d'Internet oficials però que s'utilitzen habitualment a la comunitat d'Internet al nivell del programa d'aplicacions. Aquests protocols inclouen:

- Distributed Computer Network (DCN) **Protocol de xarxa local**
- **Protocol d'execució d'ordres remot**
- **Protocol d'inici de sessió remot**
- **Protocol d'intèrpret d'ordres remot**
- **Protocol Wake On LAN**
- **Protocol d'encaminament**
- **Protocol de servidor horari**

TCP/IP no proporciona API a cap d'aquests protocols de nivell d'aplicació.

Protocol de nom de domini:

El **protocol de nom de domini** (**DOMAIN**) permet a un amfitrió d'un domini actuar com a *servidor de nom* per altres amfitrions dins del domini.

DOMAIN utilitza **UDP** o **TCP** com a protocol subjacent i permet a una xarxa local assignar noms d'amfitrió dins del se domini independentment d'altres dominis. Normalment, el protocol **DOMAIN** utilitza **UDP**. De tota manera, si es trunca la resposta **UDP**, es pot utilitzar **TCP**. El protocol **DOMAIN** de **TCP/IP** dóna suport a ambdós.

Al sistema de denominació jeràrquica **DOMAIN**, les rutines de solucionador local poden resoldre noms i adreces d'Internet mitjançant una base de dades de resolució de noms locals mantinguda pel daemon **named**. Si el nom sol•licitat per l'amfitrió no es troba a la base de dades local, la rutina de solucionador

realitza una consulta a un servidor de nom **DOMAIN** remot. En qualsevol cas, si l'informació de resolució de noms no es troba disponible, les rutines de solucionador intenten utilitzar el fitxer `/etc/hosts` per la resolució de noms.

Nota: **TCP/IP** configura rutines de solucionador locals pel protocol **DOMAIN** si existeix el fitxer `/etc/resolv.conf` local. Si aquest fitxer no existeix, el protocol **TCP/IP** configura les rutines de solucionador local per utilitzar la base de dades `/etc/hosts`.

El protocol **TCP/IP** implementa el protocol **DOMAIN** del daemon **named** i a les rutines de solucionador i no proporciona cap API per aquest protocol.

Protocol de passarel•la exterior:

El **protocol de passarel•la exterior** (**EGP**) és el mecanisme que permet a la passarel•la exterior d'un *sistema autònom* compartir informació d'encaminament amb passarel•les exteriors d'altres sistemes autònoms.

Sistemes autònoms:

Un sistema autònom és un grup de xarxes i passarel•les de les quals es fa càrrec una autorització administrativa.

Les passarel•les són *veïnatges interiors* si es troben al mateix sistema autònom i *veïnatge exterior* si es troben a sistemes autònoms diferents. Les passarel•les que intercanvien informació d'encaminament mitjançant **EGP** es coneixen com a *similars* o *veïnatge***EGP**. Les passarel•les de sistema autònom utilitzen **EGP** per proporcionar informació d'accés als seus veïnatges **EGP**.

EGP permet a una passarel•la exterior sol•licitar a una altra passarel•la exterior que estigui d'acord a intercanviar informació d'accés i realitza comprovacions continuament per garantir que els seus veïnatges **EGP** responen i ajuda als veïnatges **EGP** a intercanviar informació d'accés passant missatges d'actualització d'encaminament.

EGP limita les passarel•les exteriors permitint-los només mostrar les xarxes de destinació a les quals es pot arribar de forma completa dins del sistema autònom de la passarel•la. D'aquesta manera, una passarel•la exterior que utilitza **EGP** transmet informació als seus veïnatges **EGP** però no mostra informació d'accés sobre els seus veïnatges **EGP** fora del seu sistema autònom.

EGP no interpreta cap mètrica de distància que apareix en missatges d'actualització d'encaminament d'altres protocols. **EGP** utilitza el camp de distància per especificar si existeix un camí d'accés (un valor de 255 significa que la xarxa no és accessible). El valor no es pot utilitzar per calcular quina és, de les dues rutes, la més curta, tret que aquestes dues rutes es trobin dins d'un sol sistema autònom. Per tant, **EGP** no es pot fer servir com a algorisme d'encaminament. Com a resultat, només hi haurà un camí d'accés des de la passarel•la exterior a qualsevol xarxa.

En contrast amb el protocol **Routing Information Protocol** (**RIP**), el qual es pot utilitzar dins d'un sistema autònom de xarxes d'Internet que reconfiguren rutes de forma dinàmica, les rutes **EGP** es predeterminen al fitxer **/etc/gated.conf**. **EGP** suposa que **IP** és un protocol subjacent.

Tipus de missatge EGP:

Els tipus de missatge Exterior Gateway Protocol (EGP) es defineixen aquí.

Element	Descripció
Sol•licitud d'adquisició de veïnatge	Utilitzada per passarel•les exterior per sol•licitar convertir-se en veïnatge els uns dels altres.
Resposta d'adquisició de veïnatge	Utilitzada per passarel•les exteriors per acceptar la sol•licitud de convertir-se en veïnatge.
Rebuig d'adquisició de veïnatge	Utilitzat per passarel•les exteriors per denegar la sol•licitud de convertir-se en veïnatge. El missatge de rebuig inclou motius pel rebuig com, per exemple, `espai fora de taula`.
Cessament de veïnatge	Utilitzat per passarel•les exteriors per cessar la relació de veïnatge. El missatge de cessament inclou els motius pel cessament com, per exemple, la `desconnexió`.
Reconeixement de cessament de veïnatge	Utilitzat per passarel•les exteriors per reconèixer la sol•licitud de cessament per la relació de veïnatge.
Benvinguda de veïnatge	Utilitzada per passarel•les exteriors per determinar la connectivitat. Una passarel•la emet un missatge `Hello` i un altre missatge `I Heard You`.
I Heard You	Utilitzat per passarel•les exteriors per respondre al missatge `Hello`. El missatge `I Heard You` inclou l'accés de la passarel•la de resposta i, si la passarel•la no és accessible, es mostra un motiu de la falta d'accés com, per exemple, `You are unreachable because of problems with my network interface`.
Sondeig NR	Utilitzat per passarel•les exteriors per realitzar consultes a passarel•les de veïnatge sobre la seva capacitat per arribar a altres passarel•les.
Accessibilitat de xarxa	Utilitzada per passarel•les exteriors per respondre al missatge `NR Poll`. Per a cada passarel•la del missatge, el missatge `Network Reachability` conté informació sobre les adreces a les quals la passarel•la pot accedir a través del seu veïnatge.
Error EGP	Utilitzat per passarel•les exteriors per respondre a missatges EGP que contenen sumes de comprovació errònies o camps que contenen valors incorrectes.

TCP/IP implementa el protocol **EGP** a l'ordre del servidor **gated** i no proporciona cap API a aquest protocol.

Protocol de transferència de fitxers:

El **protocol de transferència de fitxers** (**FTP**) permet als amfitrions transferir dades entre amfitrions diferents, així com fitxers entre dos amfitrions externs de forma indirecta.

FTP proporciona per tasques com el llistat de directoris remots, la modificació del directori remot actual, la creació i l'eliminació de directoris remots i la transferència de múltiples fitxers en una sola sol•licitud. **FTP** manté la seguretat del transport passant les paraules clau d'usuari i compte a l'amfitrió extern. Encara que **FTP** s'hagi dissenyat principalment per ser utilitzat per aplicacions, també permet realitzar sessions interactives orientades a l'usuari.

FTP utilitza el lliurament de corrent fiable (**TCP/IP**) per enviar fitxers i utilitza una connexió Telnet per transferir ordres i respostes. **FTP** també comprèn diferents formats de fitxer bàsics, que inclouen NETASCII, IMAGE i Local 8.

TCP/IP implementa **FTP** a l'ordre de l'usuari **ftp** i l'ordre del servidor **ftpd** i no proporciona cap interfície de programació d'aplicació (API) per aquest protocol.

En crear usuaris i directoris ftp anònims, assegureu-vos que el directori d'inici del usuaris ftp i anònims (per exemple, `/u/ftp`) es troba al nivell d'arrel i no permet permisos d'escriptura (per exemple, `dr-xr-xr-x`). La seqüència `/usr/samples/tcpip/anon.ftp` es pot utilitzar per crear aquests comptes, fitxers i directoris.

Protocol Telnet:

El **protocol Telnet** (**TELNET**) proporciona un mètode estàndard per dispositius de terminal i processos orientats a terminal per l'interfície.

TELNET és utilitzat normalment per programes d'emulació de terminal que permeten iniciar sessió en un amfitrió remot. De tota manera, **TELNET** també es pot utilitzar per comunicació entre terminals i entre processos. **TELNET** també l'utilitzen altres protocols (per exemple, **FTP**) per establir un canal de control de protocol.

TCP/IP implementa **TELNET** a les ordres d'usuari **tn**, **telnet** o **tn3270**. El daemon **telnetd** no proporciona cap API per **TELNET**.

TCP/IP dóna suport a les opcions **TELNET** següents les quals negocien el client i el servidor:

Element	Descripció
BINARY TRANSMISSION (utilitzada a les sessions **tn3270**)	Transmet caràcters en forma de dades binàries.
SUPPRESS GO_AHEAD (El sistema operatiu suprimeix les opcions GO-AHEAD.)	Indica que quan s'estableix una connexió entre un emissor i un receptor de dades, l'emissor no ha de transmetre l'opció GO_AHEAD. Si no es vol utilitzar l'opció GO_AHEAD, les parts de la connexió probablement la suprimiran en ambdues direccions. Aquesta acció s'ha de dur a terme en ambdues direccions de forma independent.
TIMING MARK (Reconeguda però té una resposta negativa)	Garanteix que les dades transmeses anteriorment s'han processat completament.
EXTENDED OPTIONS LIST	Amplia la llista d'opcions **TELNET** en 256 opcions més. Sense aquesta opció, l'opció **TELNET** permet només 256 opcions.
ECHO (Ordre que pot ser modificada per l'usuari)	Transmet caràcters de dades eco ja retornats a l'emissor original.
TERM TYPE	Permet al servidor determinar el tipus de terminal connectat a un programa **TELNET** d'usuari.
SAK (Clau d'atenció de seguretat)	Estableix l'entorn necessari per establir comunicacions segures entre l'usuari i el sistema.
NAWS (Negociar sobre la grandària de la finestra)	Permet al client i al servidor negociar dinàmicament sobre la grandària de la finestra. Això és utilitzat per aplicacions que donen suport a la modificació de la grandària de la finestra.

Nota: **TELNET** ha de permetre la transmissió de caràcters de vuit bits quan no es troba en mode binari per implementar la pàgina de codis ISO 8859 Latin.

Trivial File Transfer Protocol:

El protocol **Trivial File Transfer Protocol** (**TFTP**) pot llegir i escriure fitxers des d'un amfitrió extern i cap a aquest.

Donat que **TFTP** utilitza el protocol **User Datagram Protocol** inestable per transportar fitxers, normalment resulta més ràpid que **FTP**. Igual que **FTP**, **TFTP** pot transferir fitxers com a caràcters NETASCII o com a dades binàries de 8 bits. A diferència de **FTP**, **TFTP** no es pot utilitzar per llistar ni canviar directoris en un amfitrió extern i no conté disposicions per seguretat com, per exemple, la protecció de paraula clau. A més, les dades només es poden escriure o recuperar en directoris públics.

TCP/IP implementa **TFTP** a les ordres d'usuari **tftp** i **utftp** de l'ordre del servidor **tftpd**. L'ordre **utftp** és una forma d'ordre **tftp** que s'utilitza en un conducte. **TCP/IP** no proporciona una API per a aquest protocol.

Per obtenir més informació, consulteu la descripció de l'ordre **tftp** o **utftp** i la descripció del daemon **tftpd** que apareixen a *Commands Reference, Volume 5*.

Protocol de nom/cercausuaris:

El **protocol de nom/Finger** (**FINGER**) és un protocol d'Internet de nivell d'aplicació que proporciona una interfície entre l'ordre **finger** i el daemon **fingerd**.

El daemon **fingerd** retorna informació sobre els usuaris actualment connectats a un amfitrió remot especificat. Si executeu l'ordre finger especificant un usuari en un amfitrió determinat, obtindreu informació específica sobre l'usuari en qüestió. El protocol **FINGER** ha d'estar present a l'amfitrió remot i a l'amfitrió de la sol•licitud. **FINGER** utilitza el **protocol de transmissió de control** ("Protocol de control de transmissió" a la pàgina 152) com a protocol subjacent.

Nota: TCP/IP no proporciona una API per a aquest protocol.

Per obtenir més informació, consulteu la descripció de l'ordre **finger** i la descripció del daemon **fingerd** que apareix a *Commands Reference, Volume 2*.

Protocol de xarxa local de Distributed Computer Network:

El daemon **gated** proporciona el protocol de xarxa local de **Distributed Computer Network (DCN)**.

El **protocol de xarxa local** (**HELLO**) és un protocol de passarel•la interior dissenyat per a utilitzar-se a sistemes autònoms. (Per obtenir més informació, consulteu "Sistemes autònoms" a la pàgina 156.) **HELLO** manté l'informació de connectivitat, enrutament i actualització. Permet a cada màquina de la xarxa determinar el camí d'accés més curt a una destinació basada en un retard temporal i, a continuació, actualitza de forma dinàmica l'informació d'encaminament a aquesta destinació.

Per obtenir més informació, consulteu la descripció del daemon **gated** que apareix a *Commands Reference, Volume 2*.

Protocol d'execució d'ordres remot:

L'ordre d'usuari **rexec** i el daemon **rexecd** proporcionen el protocol d'execució d'ordres remot que permet als usuaris executar ordres en un amfitrió remot compatible.

Per obtenir més informació, consulteu la descripció de l'ordre **rexec** i la descripció del daemon **rexecd** que apareix a *Commands Reference, Volume 4*.

Protocol d'inici de sessió remot:

L'ordre d'usuari **rlogin** i el daemon **rlogind** proporcionen el **protocol d'inici de sessió remot**, el qual permet als usuaris iniciar sessió en un amfitrió remot i utilitzar els seus terminals com si estiguessin directament connectats a l'amfitrió remot.

Per obtenir més informació, consulteu la descripció de l'ordre **rlogin** i la descripció del daemon **rlogind** que apareixen a *Commands Reference, Volume 4*.

Protocol d'intèrpret d'ordres remot:

L'ordre d'usuari **rsh** i el daemon **rshd** proporcionen el **protocol d'intèrpret d'ordres remot**, el qual permet als usuaris obrir un intèrpret d'ordres en un amfitrió extern compatible per l'execució d'ordres.

Per obtenir més informació, consulteu la descripció de l'ordre **rsh** i la descripció del daemon **rshd** que apareixen a *Commands Reference, Volume 4*.

Protocol Wake On LAN:

El protocol **Wake On LAN (WOL)** permet activar un o varis amfitrions que estan connectats a la xarxa en mode de suspensió enviant un paquet Magic a l'adreça o adreces especificades a la subxarxa especificada.

Per obtenir més informació sobre la utilització de **WOL**, consulteu la descripció de l'ordre **wol** que apareix a *Commands Reference, Volume 6*.

Protocol d'encaminament:

El **protocol d'encaminament** (**RIP**) i els daemons **routed** i **gated** que implementen, realitzen un seguiment de l'informació d'encaminament basant-se en salts de passarel•la i mantenen les entrades de taula d'encaminament de kernel.

Per obtenir més informació, consulteu els daemon **routed** i **gated**.

Protocol de servidor horari:

El daemon **timed** s'utilitza per sincronitzar un amfitrió amb l'hora d'altres amfitrions.

Es basa en el concepte client/servidor. Per obtenir més informació, consulteu la descripció de l'ordre **timedc** i la descripció del daemon **timed** que apareixen a *Commands Reference, Volume 5*.

Números assignats

Per raons de compatibilitat amb l'entorn de xarxa general, s'assignen números coneguts a les versions, les xarxes, els ports, els protocols i les opcions de protocol d'Internet. A més, també s'assignen noms coneguts a màquines, xarxes, sistemes operatius, protocols, serveis i terminals.

TCP/IP compleix amb els noms i números assignats a RFC 1010, *Números assignats*.

El **protocol d'Internet** (**IP**) defineix un camp de 4 bits a la capçalera **IP** que identifica la versió del protocol de xarxa d'Internet general que s'està utilitzant. En el cas del protocol **IP**, aquest número de versió en decimals és 4. Per obtenir informació detallada sobre els números i els noms assignats utilitzats per **TCP/IP**, consulteu els fitxers `/etc/protocols` i `/etc/services` inclosos amb **TCP/IP**. Per obtenir més informació detallada sobre els números i noms assignats, consulteu RFC 1010 i el fitxer `/etc/services`.

Targetes adaptadores de xarxa d'àrea local TCP/IP

La targeta adaptadora de xarxa és el maquinari connectat físicament al cablatge de xarxa. És responsable de la recepció i transmissió de dades a nivell físic.

El programa de control de dispositiu adaptador de xarxa controla la targeta adaptadora de xarxa.

Una màquina ha de tenir una targeta (o connexió) adaptadora de xarxa per a cada xarxa (no tipus de xarxa) a la qual es connecta. Per exemple, si un amfitrió es connecta a dues xarxes Token-Ring, ha de tenir dues targetes adaptadores de xarxa.

El **TCP/IP** utilitza les connexions i targetes adaptadores de xarxa següents:

- Standard Ethernet Versió 2
- IEEE 802.3
- Token-ring
- Adaptadors asíncrons i ports en sèrie nadius
- Interfície de dades distribuïdes per fibra (FDDI)
- Convertidor de canal òptic de sèrie (descrit a l'*Kernel Extensions and Device Support Programming Concepts*)

- Fibre Channel

L'Ethernet i les tecnologies de xarxa 802.3 utilitzen el mateix tipus d'adaptador.

Cada màquina proporciona un nombre limitat de ranures d'expansió, les quals es poden utilitzar si es vol per als adaptadors de comunicacions. A més a més, cada màquina dóna suport a un nombre limitat d'adaptadors de comunicacions d'un determinat tipus. Dins d'aquests límits (limitacions de programari), podeu instal•lar qualsevol combinació d'adaptadors a totes les ranures d'expansió de la màquina disponibles (limitacions de maquinari).

Només es pot configurar una interfície **Transmission Control Protocol/Internet Protocol (TCP/IP)** independentment del nombre de Convertidors de canal òptic de sèrie als quals el sistema dóna suport. El programa de control de dispositiu Òptic de sèrie utilitza ambdós convertidors de canal tot i que només es trobi configurada una interfície **TCP/IP** lògica.

Instal•lació d'un adaptador de xarxa

Utilitzeu aquest procediment per instal•lar un adaptador de xarxa.

Per instal•lar un adaptador de xarxa:

1. Atureu l'ordinador. Consulteu l'ordre **shutdown** per obtenir informació sobre com aturar un sistema.
2. Desconnecteu l'ordinador de la font d'alimentació.
3. Retireu la coberta de l'ordinador.
4. Busqueu una ranura lliure i inseriu-hi l'adaptador de xarxa. Assegureu-vos que l'adaptador encaixa correctament dins la ranura.
5. Torneu a col•locar la coberta de l'ordinador.
6. Reinicieu l'ordinador.

Configuració i gestió d'adaptadors

Per configurar i gestionar adaptadors token ring o Ethernet, utilitzeu les tasques de la taula següent:

Taula 59. Tasques de configuració i gestió d'adaptadors

Tasca	Camí d'accés ràpid de la SMIT	Ordre o fitxer
Configurar un adaptador	`smit chgtok` (token-ring) `smit chgenet` (Ethernet)	1. Determineu el nom de l'adaptador:[1] `lsdev -C -c adapter -t tokenring -H` o `lsdev -C -c adapter -t ethernet -H` 2. Restabliu la velocitat d'anell (token-ring) o el tipus de connector (Ethernet), si és necessari. Per exemple: `chdev -l tok0 -a ring_speed=16 -P` o `chdev -l ent0 -a bnc_select=dix -P`
Determinació d'una adreça de maquinari d'adaptador de xarxa	`smit chgtok` (token-ring) `smit chgenet` (Ethernet)	`lscfg -l tok0 -v` (token-ring)[2] `lscfg -l ent0 -v` (Ethernet)[2]

Establiment d'una adreça de maquinari alternativa	`smit chgtok` (token-ring) `smit chgenet` (Ethernet)	1. Definiu l'adreça de maquinari alternativa. Per exemple, per a token-ring:[2,3]
		`chdev -l tok0 -a alt_addr=0X10005A4F1B7F`
		Per a Ethernet:[2,3]
		`chdev -l ent0 -a alt_addr=0X10005A4F1B7F -p`
		2. Comenceu a utilitzar l'adreça alternativa, per a token-ring:[4]
		`chdev -l tok0 -a use_alt_addr=yes`
		Per a Ethernet:[4]
		`chdev -l ent0 -a use_alt_addr=yes`

Nota:

1. El nom d'un adaptador de xarxa pot canviar si el moveu d'una ranura a una altra o si l'elimineu del sistema. Si alguna vegada moveu l'adaptador, executeu l'ordre **diag -a** per actualitzar la base de dades de configuració.
2. Substituïu el nom d'adaptador per `tok0` i `ent0`.
3. Substituïu l'adreça de maquinari per `0X10005A4F1B7F`.
4. Després de realitzar aquest procediment, podríeu experimentar una interrupció de la comunicació amb altres amfitrions fins que aquest llancin la seva memòria cau d'ARP (protocol de resolució d'adreces) i obtinguin la nova adreça de maquinari d'aquest amfitrió.

Xarxes d'àrees locals virtuals

Les VLAN (xarxes d'àrees locals virtuals) poden considerar-se com a dominis de difusió lògics. Una VLAN divideix grups d'usuaris d'una xarxa física real en segments de xarxes lògiques.

Aquesta implementació dóna suport a l'estàndard de creació d'etiquetes de la VLAN IEEE 802.1Q amb la possibilitat de donar suport a múltiples ID de VLAN que s'executen en adaptadors Ethernet. Cada ID de VLAN està associat amb una interfície Ethernet diferent a les capes superiors (IP, etc.) i crea instàncies exclusives de l'adaptador Ethernet lògic, com per exemple `ent1`, `ent2` i així successivament.

El suport de la VLAN IEEE 802.1Q pot configurar-se sobre qualsevol adaptador Ethernet suportat. Els adaptadors s'han de connectar amb un commutador que doni suport a la VLAN IEEE 802.1Q.

Podeu configurar diversos dispositius lògics VLAN en un únic sistema. Cada dispositiu lògic VLAN constitueix una instància addicional de l'adaptador Ethernet. Aquests dispositius lògics poden utilitzar-se per configurar les mateixes interfícies IP d'Ethernet que les utilitzades amb els adaptadors Ethernet físics. Com a tal, l'opció de **no**, *ifsize* (valor per defecte 8), s'ha d'augmentar per incloure no tan sols les interfícies Ethernet per a cada adaptador, sinó també els dispositius lògics VLAN que es configuren. Consulteu la documentació de l'ordre **no**.

Cada VLAN pot tenir un valor MTU (unitat de transmissió màxima) diferent fins i tot si comparteix un únic adaptador Ethernet físic.

El suport de la VLAN es gestiona mitjançant la SMIT. Escriviu el camí d'accés ràpid `smit vlan` des de la línia d'ordres i efectueu la vostra selecció al menú principal de la VLAN. La ajuda en línia està disponible.

Després de configurar la VLAN, configureu la interfície IP; per exemple, `en1` per a Ethernet estàndard o `et1` per a IEEE 802.3, utilitzant la SMIT o bé les ordres.

L'AIX 5.3 i posteriors donen suport a l'Ethernet virtual utilitzant un commutador d'E/S virtual com a mètode per a dur a terme la comunicació de memòria interna entre particions d'un sistema POWER5. El commutador també dóna suport a la creació d'etiquetes IEEE 802.1Q, que permet als adaptadors Ethernet virtuals pertànyer a diferents VLAN del commutador. Els adaptadors Ethernet virtuals es creen i configuren en particions utilitzant la consola de gestió del maquinari (HMC). Un cop creada, la partició veurà l'adaptador Ethernet virtual a l'arbre de microprogramari obert quan escanegi per trobar dispositius. Un cop detectat, l'adaptador Ethernet virtual es configura i utilitza de la mateixa manera que un adaptador Ethernet físic. Per obtenir més informació, vegeu la documentació del maquinari del vostre sistema POWER5.

Nota:

1. Si intenteu configurar un valor d'ID de VLAN que ja s'està utilitzant per a l'adaptador especificat, la configuració no es realitza satisfactòriament i dóna el següent error:

```
Method error (/usr/lib/methods/chgvlan):
  0514-018 The values specified for the following attributes
           are not valid:
           id_etiqueta_vlan    ID Etiqueta VLAN
```

2. Si un usuari (per exemple, la interfície IP) actualment utilitza el dispositiu lògic VLAN, qualsevol intent d'eliminar el dispositiu lògic VLAN no serà satisfactori. Es visualitza un missatge semblant al següent:

   ```
   Method error (/usr/lib/methods/ucfgcommo):
           0514-062 Cannot perform the requested function because the
                    specified device is busy.
   ```

   Per eliminar el dispositiu VLAN lògic, primer desconnecteu l'usuari. Per exemple, si l'usuari és la interfície IP `en1`, podeu utilitzar la següent ordre:

   ```
   ifconfig en1 detach
   ```

   A continuació, elimineu la interfície de xarxa utilitzant els menús TCP/IP de la SMIT.

3. Si un usuari (per exemple, la interfície IP) actualment utilitza el dispositiu lògic VLAN, qualsevol intent de canviar la característica VLAN (ID d'etiqueta de VLAN o adaptador base) no serà satisfactori. Es visualitza un missatge semblant al següent:

   ```
   Method error (/usr/lib/methods/chgvlan):
           0514-062 Cannot perform the requested function because the
                    specified device is busy.
   ```

   Per canviar el dispositiu VLAN lògic, primer desconnecteu l'usuari. Per exemple, si l'usuari és la interfície IP `en1`, podeu utilitzar la següent ordre:

   ```
   ifconfig en1 detach
   ```

   A continuació, canvieu la VLAN i torneu a afegir la interfície de xarxa utilitzant els menús TCP/IP de la SMIT.

Resolució de problemes de la VLAN:

tcpdump i **trace** poden utilitzar-se per resoldre problemes de la VLAN.

A continuació s'indica l'ID d'enganxament de traça per a cada tipus de paquet de transmissió:

Element	Descripció
paquets de transmissió	3FD
paquets de recepció	3FE
altres incidències	3FF

L'ordre **entstat** dóna les estadístiques agregades de l'adaptador físic per al qual la VLAN està configurada. *No* proporciona les estadístiques individuals per aquest dispositiu lògic VLAN en concret.

Restriccions de la VLAN:

El buidatge remot no està suportat a través d'una VLAN. A més, els dispositius lògics VLAN no poden utilitzar-se per crear un Etherchannel de Cisco Systems.

Interfícies de xarxa del TCP/IP

La capa Interfície de xarxa del **TCP/IP** formata datagrames IP a la capa Xarxa en paquets que les tecnologies de xarxa específiques puguin comprendre i transmetre.

Una interfície de xarxa és un programari específic de xarxa que es comunica amb el programa de control de dispositiu específic de xarxa i la capa IP per tal de proporcionar a la capa IP una interfície coherent amb tots els adaptadors de xarxa que hi puguin haver.

La capa IP selecciona la interfície de xarxa adequada en funció de l'adreça de destinació del paquet que s'ha de transmetre. Cada interfície de xarxa té una adreça de xarxa. La capa Interfície de xarxa és responsable d'afegir o eliminar les capçaleres de protocol de capa d'enllaç necessàries per lliurar un missatge a la seva destinació. El programa de control de dispositiu **adaptador de xarxa** controla la targeta adaptadora de xarxa.

Tot i que no és necessari, s'acostuma a associar una interfície de xarxa amb un adaptador de xarxa. Per exemple, la interfície de bucle de retorn no té cap adaptador de xarxa associat. Una màquina ha de tenir una targeta adaptadora de xarxa per a cada xarxa (no tipus de xarxa) a la qual es connecta. No obstant això, una màquina requereix només una còpia del programari d'interfície de xarxa per a cada adaptador de xarxa que utilitza. Per exemple, si un amfitrió es connecta a dues xarxes Token-Ring, ha de tenir dues targetes adaptadores de xarxa. No obstant això, només és necessària una còpia del programari d'interfície de xarxa **Token-Ring** i una còpia del programa de control de dispositiu Token-Ring.

El **TCP/IP** dóna suport als tipus d'interfícies de xarxa:

- Ethernet estàndard Versió 2 (en)
- IEEE 802.3 (et)
- Token-Ring (tr)
- **SLIP (Serial Line Internet Protocol)**
- Bucle de retorn (lo)
- FDDI
- Òptica de sèrie (so)
- **Protocol punt a punt (PPP)**
- Adreça IP virtual (vi)

Les interfícies Ethernet, 802.3, i Token-Ring s'han d'utilitzar amb xarxes d'àrea local (LAN). La interfície **SLIP** s'ha d'utilitzar amb connexions en sèrie. La interfície de bucle de retorn la utilitza un amfitrió per enviar-se missatges a si mateix. La interfície Òptica de sèrie s'ha d'utilitzar amb xarxes punt a punt òptiques mitjançant el manejador de dispositiu d'enllaç òptic de sèrie. El **Protocol punt a punt** s'acostuma a utilitzar en les connexions amb altres ordinadors o xarxes a través d'un mòdem. La interfície Adreça IP virtual (que també s'anomena *interfície virtual*) no està associada amb cap adaptador de xarxa en particular. En un amfitrió es poden configurar diverses instàncies d'una interfície virtual. Quan es configuren interfícies virtuals, l'adreça de la primera interfície virtual passa a ser l'adreça d'origen, tret que una aplicació hagi triat una interfície diferent. Els processos que utilitzen una adreça IP virtual com la seva adreça d'origen poden enviar paquets a través de qualsevol interfície de xarxa que proporcioni el millor camí per a aquella destinació. Els paquets d'entrada destinats a una adreça IP virtual es lliuren al procés independentment de la interfície per la qual arriben.

Configuració automàtica de les interfícies de xarxa

Quan s'instal•la físicament un adaptador de xarxa nou al sistema, el sistema operatiu afegeix automàticament la interfície de xarxa corresponent per a l'adaptador en qüestió.

Per exemple, si instal•leu un adaptador token ring al vostre sistema, el sistema operatiu li assigna el nom `tok0` i afegeix una interfície de xarxa token ring anomenada `tr0`. Si instal•leu un adaptador Ethernet al vostre sistema, el sistema operatiu li assigna el nom `ent0` i afegeix tant una interfície Ethernet versió 2 com una interfície IEEE 802.3, anomenades respectivament `en0` i `et0`.

La majoria de vegades, es produeix una correspondència d'un a un entre els noms d'adaptadors i els noms de les interfícies de xarxa. Per exemple, l'adaptador token ring `tok0` correspon a la interfície `tr0`, l'adaptador tok1 correspon a la interfície `tr1`, etc. Igualment, l'adaptador Ethernet `ent0` correspon a la interfície `en0` (per la versió 2 d'Ethernet) i `et0` (per IEEE 802.3), i l'adaptador `ent1` correspon a la interfície `en1` (per la versió 2 d'Ethernet) i `et1` (per IEEE 802.3).

Nota: En circumstàncies normals, no cal suprimir o afegir una interfície de xarxa manualment. No obstant això, altres procediments de determinació d'un problema podrien requerir-ho. En aquest cas, utilitzeu el camí d'accés ràpid de la SMIT **smit inet**, per suprimir i tornar a afegir la interfície corresponent.

Valors de configuració TCP/IP per defecte

Cada vegada que s'engega el sistema, el sistema operatiu configura automàticament el programari de la interfície de la xarxa segons la informació de la base de dades de l'ODM. Inicialment, la interfície de la xarxa es configura amb els valors per defecte.

Per tal de comunicar-se a través d'una determinada interfície de xarxa, cal establir una adreça d'Internet. És l'únic atribut que heu d'establir. Tots els altres atributs necessaris poden utilitzar els valors per defecte. A continuació trobareu els valors per defecte de cada interfície de xarxa.

Valor Ethernet per defecte de TCP/IP:

Els atributs d'adaptador de xarxa Ethernet vàlids poden canviar els valors utilitzant el menú Selecció d'interfície de xarxa de la SMIT.

Atribut	Valor per defecte	Valors possibles
netaddr		
state	down	up, down, detach
arp	yes	yes, no
netmask		
broadcast		

Al menú Controladors d'interfície de xarxa de la SMIT es mostra el següent programa de control de dispositiu de xarxa Ethernet vàlid juntament amb els seus valors per defecte.

Atribut	Valor per defecte	Valors possibles
mtu	1500	De 60 a 1500

Valors de 802.3 per defecte de TCP/IP:

Els atributs d'adaptador de xarxa 802.3 vàlids poden canviar els valors utilitzant el menú Selecció d'interfície de xarxa de la SMIT.

Atribut	Valor per defecte	Valors possibles
netaddr		
state	down	up, down, detach
arp	yes	yes, no
netmask		
broadcast		

Al menú Controladors d'interfície de xarxa de la SMIT es mostra el següent programa de control de dispositiu de xarxa 802.3 vàlid juntament amb els seus valors per defecte.

Atribut	Valor per defecte	Valors possibles
mtu	1492	De 60 a 1492

Valor Token-Ring per defecte de TCP/IP:

Els atributs d'adaptador de xarxa token-ring vàlids poden canviar els valors utilitzant el menú Selecció d'interfície de xarxa de la SMIT.

Atribut	Valor per defecte	Valors possibles
netaddr		
netmask		
state	down	up, down, detach
arp	yes	yes, no
hwloop	no	yes, no
netmask		
broadcast		
allcast	no	yes, no

Al menú Controladors d'interfície de xarxa de la SMIT es mostra el següent programa de control de dispositiu de xarxa token ring vàlid juntament amb els seus valors per defecte.

Atribut	Valor per defecte	Valors possibles
mtu (4 Mbps)	1500	De 60 a 4056
mtu (16 Mbps)	1500	De 60 a 17960

Nota: Quan es treballa a través d'un pont, el valor per defecte de 1500 per MTU (unitat de transmissió màxima) s'hauria de canviar per un valor que fos el valor del camp d'informació màxima (I-frame màxima), que indica el pont en el camp de control d'encaminament, menys 8. Per exemple, si el valor I-frame màxima és 1500 al camp de control d'encaminament, la grandària MTU s'hauria d'establir a 1492. Això és només per interfícies de xarxa Token-Ring. Per obtenir més informació, consulteu l'apartat "Problemes del TCP/IP amb un pont Token-Ring/Token-Ring" a la pàgina 427.

Quan es fa servir l'adaptador Token-Ring d'IBM® 16/4 PowerPC (ISA), el valor MTU queda restringit a 2000.

Valor SLIP per defecte de TCP/IP:

Els atributs d'adaptador de xarxa SLIP vàlids poden canviar els valors utilitzant el menú Selecció d'interfície de xarxa de la SMIT.

Atribut	Valor per defecte	Valors possibles
netaddr		
dest		
state	up	up, down, detach
netmask		

Al menú Controladors d'interfície de xarxa de la SMIT es mostra el següent programa de control de dispositiu de xarxa SLIP vàlid juntament amb els seus valors per defecte.

Atribut	Valor per defecte	Valors possibles
mtu	1006	De 60 a 4096

Valors òptics sèrie per defecte de TCP/IP:

El convertidor de canals de xarxa òptic sèrie pot canviar els valors utilitzant el menú Selecció d'interfície de xarxa de la SMIT.

Atribut	Valor per defecte	Valors possibles
netaddr		
state	down	up, down, detach
netmask		

Al menú Controladors d'interfície de xarxa de la SMIT es mostra el següent manejador de controlador de xarxa òptic sèrie vàlid juntament amb els seus valors per defecte.

Atribut	Valor per defecte	Valors possibles
mtu	61428	De l'1 al 61428

Implicacions de les diverses interfície de la xarxa en la mateixa xarxa

Si hi ha diverses interfícies de xarxa connectades a una única xarxa, cada interfície ha de tenir una adreça IP exclusiva.

La funció Multipath Routing permet afegir camins a la taula d'encaminaments IP per a interfícies de múltiples camins d'accés de la mateixa subxarxa. D'aquesta manera s'aconsegueix que el trànsit de sortida s'alterni entre les interfície per comptes d'enviar-lo a través d'una sola interfície.

Gestió de la interfície de xarxa

Per gestionar les interfícies de xarxa, utilitzeu la xarxa WSM, FastPath (aplicació) o les tasques d'aquesta taula.

Taula 60. Gestió de les tasques de les interfícies de xarxa

Tasca	Camí d'accés ràpid de la SMIT	Ordre o fitxer
Llistar tots els dispositius de xarxa	`smit lsinet`	**lsdev -C -c if**
Configurar un dispositiu de xarxa	`smit chinet`	Consulteu l'ordre **ifconfig** i el fitxer `rc.net`.
Canviar la informació de la interfície de xarxa amb un `/usr` muntat remotament	`smit chdev`[1,2]	**chgif**[1,2]
Obtenció d'estadístiques per una interfície de xarxa		**netstat -v**

Nota:

1. El canvis d'un `/usr` muntat remotament només afecten la base de dades d'informació (ODM) fins que es torna a iniciar la xarxa o fins que es fa servir l'ordre **ifconfig** per fer que els canvis entrin en vigor immediatament.
2. Quan s'utilitza un `/usr` muntat remotament, aneu amb compte de no modificar la interfície que s'utilitza, perquè aquesta és la ubicació de les biblioteques, les ordres i el kernel.

Opcions de xarxa específiques de l'interfície

Les interfícies **TCP/IP** s'han de sintonitzar específicament per tal d'aconseguir un rendiment de xarxa òptim i d'alta velocitat (100 Mb o més). Aquest esforç és complicat ateses les múltiples interfícies de xarxa i que es pot utilitzar una combinació d'interfícies **TCP/IP** tradicionals i d'alta velocitat en un sol sistema.

En el sistema operatiu AIX, les opcions de xarxa específiques per a la interfície (ISNO) permeten que els administradors del sistema puguin ajustin cada interfície **TCP/IP** individualment per al millor rendiment.

Hi ha cinc paràmetres ISNO per a cada interfície a la que es dóna suport: **rfc1323**, **tcp_nodelay**, **tcp_sendspace**, **tcp_recvspace** i **tcp_mssdflt**. Una vegada establerts, els valors per aquests paràmetres alteren temporalment els paràmetres de tot el sistema del mateixos noms que s'havien establert amb l'ordre **no**. Quan no s'estableixen les opcions ISNO per una interfície en particular, s'utilitzen les opcions

de tot el sistema. Quan les opcions s'han establert mitjançant una aplicació per un sòcol en particular utilitzant la subrutina **setsockopt**, aquestes opcions alteraran temporalment les ISNO.

L'opció de xarxa **use_isno**, establerta amb l'ordre **no**, ha de tenir un valor d'1 perquè les ISNO entrin en vigor. El valor per defecte per **use_isno** és d'1.

Alguns adaptadors d'alta velocitat tenen paràmetres ISNO establerts per defecte a la base de dades de l'ODM.

Les interfícies Ethernet de gigabits, quan es configuren perquè utilitzin una MTU de 9000, utilitzen, per defecte, els següents valors ISNO:

Nom	Valor de l'AIX 4.3.3	Valor de l'AIX 4.3.3 (4330-08)	Valor de l'AIX 5.1 (i posterior)
tcp_sendspace	131072	262144	262144
tcp_recvspace	92160	131072	131072
rfc1323	1	1	1

Les interfícies Ethernet de gigabits, quan es configuren perquè utilitzin una MTU de 1500, utilitzen, per defecte, els següents valors ISNO:

Nom	Valor de l'AIX 4.3.3	Valor de l'AIX 4.3.3 (4330-08)	Valor de l'AIX 5.1 (i posterior)
tcp_sendspace	65536	131072	131072
tcp_recvspace	16384	65536	65536
rfc1323	0	no s'ha establert	no s'ha establert

Les interfícies FDDI, quan es configuren perquè utilitzin una MTU de 4352, utilitzen, per defecte, els següents valors ISNO:

Nom	Valor
tcp_sendspace	45046
tcp_recvspace	45046

Els paràmetres ISNO no es poden visualitzar o canviar utilitzant la SMIT. Es poden establir utilitzant l'ordre **chdev** o l'ordre **ifconfig**. L'ordre **ifconfig** canvia els valors només fins la propera vegada que es reengegui l'equip. L'ordre **chdev** canvia els valors de la base de dades de l'ODM de manera que s'utilitzaran les properes vegades que es reengegui l'equip. Les ordres **lsattr** o **ifconfig** es poden utilitzar per visualitzar els valors actuals.

Els exemples següents mostren ordres que es poden utilitzar primer per verificar el suport al sistema i a la interfície i, després per establir i verificar els nous valors.

1. Verifiqueu el suport al sistema en general i a la interfície utilitzant les ordres **no** i **lsattr**.
   - Assegureu-vos que s'hagi habilitat l'opció **use_isno** utilitzant una ordre similar a la següent:
     ```
     $ no -a | grep isno
               use_isno=1
     ```
   - Assegureu-vos que la interfície doni suport als cinc ISNO nous utilitzant l'ordre **lsattr -El**, tal com es mostra a continuació:
     ```
     $ lsattr -E -l en0 -H
               attribute   value  description
               rfc1323                     N/A
               tcp_nodelay                 N/A
               tcp_sendspace               N/A
               tcp_recvspace               N/A
               tcp_mssdflt                 N/A
     ```

2. Establiu els valors específics de la interfície utilitzant l'ordre **ifconfig** o **chdev**. L'ordre **ifconfig** estableix els valors temporalment, que és el que es recomana per dur a terme les comprovacions. L'ordre **chdev** altera l'ODM, per tant, els valors personalitzats continuaran essent vàlids després de reengegar el sistema.
   - Establiu **tcp_recvspace** i **tcp_sendspace** a 64 K i habiliteu **tcp_nodelay** utilitzant una d'aquestes alternatives:

     ```
     $ ifconfig en0 tcp_recvspace 65536 tcp_sendspace 65536 tcp_nodelay 1
     $ chdev -l en0 -a tcp_recvspace=65536 -a tcp_sendspace=65536 -a tcp_nodelay=1
     ```
   - Una altra possibilitat és que, suposant que l'ordre **no** informi d'un valor global de `rfc1323=1`, l'usuari root pot apagar l'**rfc1323** per totes les connexions per sobre d'en0 amb les ordres següents:

     ```
     $ ifconfig en0 rfc1323 0
     $ chdev -l en0 -a rfc1323=0
     ```
3. Verifiqueu els valors utilitzant l'ordre **ifconfig** o **lsattr**, tal com es mostra a l'exemple següent:

   ```
   $ ifconfig en0 <UP,BROADCAST,NOTRAILERS,RUNNING,SIMPLEX,MULTICAST,GROUPRT,64BIT>
             en0: flags=e080863
                 inet 9.19.161.100 netmask 0xffffff00 broadcast 9.19.161.255
                 tcp_sendspace 65536 tcp_recvspace 65536 tcp_nodelay 1 rfc1323 0
   $ lsattr -El en0
             rfc1323         0           N/A               True
             tcp_nodelay     1           N/A               True
             tcp_sendspace   65536       N/A               True
             tcp_recvspace   65536       N/A               True
             tcp_mssdflt                 N/A               True
   ```

Adreçament TCP/IP

El**TCP/IP** inclou un esquema d'adreçament d'Internet que permet als usuaris i a les aplicacions identificar una xarxa o un amfitrió específics amb els quals comunicar-se.

Una adreça d'Internet funciona com una adreça postal, ja que permet que les dades s'encaminin cap a la destinació seleccionada. El **TCP/IP** proporciona estàndards per assignar adreces a xarxes, subxarxes, amfitrions i sòcols, així com per utilitzar adreces especials per a les difusions i els bucles de retorn locals.

Les adreces d'Internet estan integrades per una adreça de xarxa o bé una adreça de l'amfitrió (o local). Aquesta adreça amb dues parts permet que l'emissor especifiqui tant la xarxa com un amfitrió específic de la xarxa. A cada xarxa s'assigna una adreça de xarxa oficial i exclusiva quan es connecta a altres xarxes d'Internet. Tanmateix, si una xarxa local no s'ha de connectar a altres xarxes d'Internet, se li pot assignar qualsevol adreça de xarxa que sigui adequada per fer-ne un ús local.

L'esquema d'adreçament d'Internet consisteix en adreces d'Internet Protocol (IP) i dos casos especials d'adreces IP: les adreces de difusió i les de bucle de retorn.

Adreces d'Internet

El protocol d'Internet (IP) utilitza un camp d'adreces de 32 bits format per dues parts.

Els 32 bits es divideixen en quatre *octets*, com a l'exemple següent:

```
01111101   00001101   01001001   00001111
```

Aquests números binaris es converteixen en:

```
125              13              73              15
```

Les dues parts d'una adreça d'Internet són la part d'adreça de xarxa i la part d'adreça d'amfitrió. Això permet que un amfitrió remot pugui especificar tant la xarxa remota com l'amfitrió de la xarxa remota a l'hora d'enviar informació. Per conveni, un número d'amfitrió de 0 s'utilitza per fer referència a la pròpia xarxa.

TCP/IP dóna suport a tres classes d'adreces d'Internet: Classe A, Classe B i Classe C. Les diferents classes d'adreces d'Internet es designen per la forma en que estan assignats els 32 bits de l'adreça. La classe d'adreça concreta que té assignada una xarxa depèn de la grandària de la xarxa.

Adreces de Classe A:

Una adreça de Classe A està formada per una adreça de xarxa de 8 bits i una adreça local o d'amfitrió de 24 bits.

El primer bit de l'adreça de xarxa serveix per indicar la classe de xarxa, deixant 7 bits per l'adreça de xarxa real. Com que el número més alt que 7 bits poden representar en binari és 128, hi ha 128 adreces de xarxa possibles de Classe A. De les 128 adreces de xarxa possibles, dues estan reservades per casos especials: l'adreça de xarxa 127 està reservada per a adreces de bucle de retorn local i una adreça de xarxa que tot són uns indica una adreça de difusió.

Hi ha 126 adreces de xarxa possibles de Classe A i 16.777.216 adreces d'amfitrió local. En una adreça de Classe A, el bit d'ordre més alt està establert en 0.

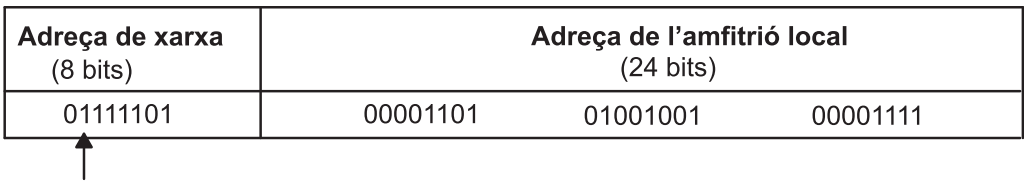


Figura 15. Adreça de Classe A

Aquesta il•lustració mostra una estructura típica d'adreça de Classe A. Els primers 8 bits contenen l'adreça de xarxa (que sempre comença amb un zero). Els 24 bits restants contenen l'adreça d'amfitrió local.

El primer octet d'una adreça de Classe A està a l'interval de l'1 al 126.

Adreces de Classe B:

Una adreça de Classe B està formada per una adreça de xarxa de 16 bits i una adreça local o d'amfitrió de 16 bits.

Els dos primers bits de l'adreça de xarxa serveixen per indicar la classe de xarxa, deixant 14 bits per l'adreça de xarxa real. Hi ha 16.384 adreces de xarxa possibles i 65.536 adreces d'amfitrió local. En una adreça de Classe B, els bits d'ordre més alts estan establerts en 1 i 0.

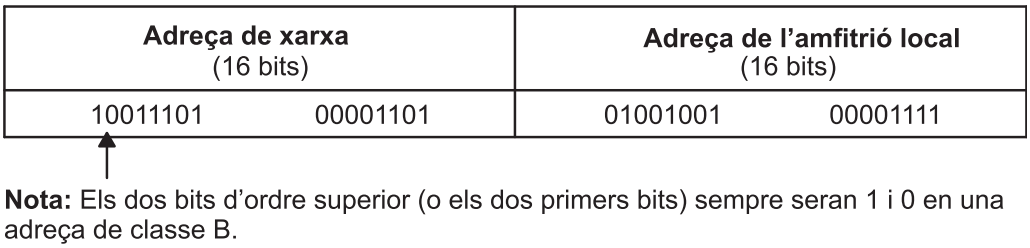


Figura 16. Adreça de Classe B

Aquesta il•lustració mostra una estructura típica d'adreça de Classe B. Els primers 16 bits contenen l'adreça de xarxa. Els dos bits d'ordre més alts sempre seran un ú i un zero. Els 16 bits restants contenen l'adreça d'amfitrió local.

El primer octet d'una adreça de Classe A està a l'interval del 128 al 191.

Adreces de Classe C:

Una adreça de Classe C està formada per una adreça de xarxa de 24 bits i una adreça d'amfitrió local de 8 bits.

Els primers tres bits de l'adreça de xarxa indiquen la classe de xarxa, deixant 21 bits per l'adreça de xarxa real. Per tant, hi ha 2.097.152 adreces de xarxa possibles i 256 adreces d'amfitrió local possibles. En una adreça de classe C, els bits d'ordre més alts estan establerts en 1-1-0.

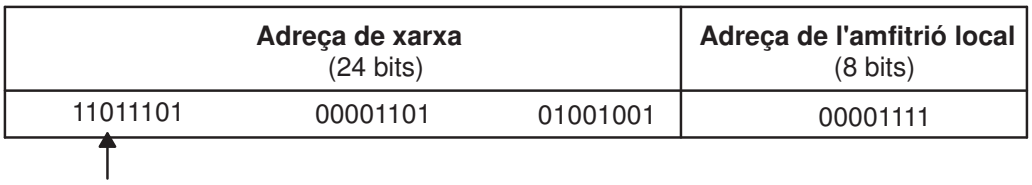


Figura 17. Adreça de Classe C

Aquesta figura mostra una estructura típica d'adreça de Classe C. Els primers 24 bits contenen l'adreça de xarxa (els tres bits d'ordre més alt sempre seran 1-1-0). Els 8 bits restants contenen l'adreça d'amfitrió local.

És a dir, el primer octet d'una adreça de Classe C està dins l'interval del 192 al 223.

A l'hora de decidir quina classe d'adreça de xarxa cal utilitzar, heu de considerar quants amfitrions hi haurà a la xarxa i quantes subxarxes hi haurà a l'organització. Si l'organització és petita i la xarxa tindrà menys de 256 amfitrions, una adreça de Classe C probablement serà suficient. Si l'organització és gran, una adreça de Classe B o de Classe A podria ser més convenient.

Nota: Les adreces de Classe D (1-1-1-0 en els bits d'ordre més alts) proporcionen adreces de multidifusió i estan suportades per UDP/IP en aquest sistema operatiu.

Les màquines llegeixen adreces en codi binari. La notació convencional per a adreces d'amfitrió d'Internet és la *decimal amb punt*, que divideix l'adreça de 32 bits en quatre camps de 8 bits. El següent valor binari:

```
0001010   00000010   00000000   00110100
```

pot expressar-se com:

`010.002.000.052` ó `10.2.0.52`

on el valor de cada camp s'especifica com un número decimal i els camps estan separats per punts.

Nota: L'ordre **hostent** reconeix les següents adreces: .08, .008, .09 i .009. Les adreces amb zeros inicials s'interpreten com a octal, i els numerals de l'octal no poden contenir els números 8 i 9.

TCP/IP requereix una adreça d'Internet exclusiva per a cada interfície de xarxa (adaptador) d'una xarxa. Aquestes adreces estan determinades per les entrades de la base de dades de configuració, que han de concordar amb les entrades del fitxer `/etc/hosts` o de la base de dades **named** si la xarxa utilitza un servidor de noms.

Adreces d'Internet utilitzant zeros:

Quan una adreça d'Internet conté un 0 a la part d'adreça d'amfitrió, (per exemple, 192.9.200.0), TCP/IP envia una adreça comodí a la xarxa.

Totes les màquines amb una adreça de Classe C de 192.9.200.*X* (on *X* representa un valor entre 0 i 254) han de respondre a la sol•licitud. Això dóna com a conseqüència una xarxa inundada de sol•licituds a màquines no existents.

De la mateixa manera, es produeixen problemes en les adreces de Classe B com ara 129.5.0.0. Totes les màquines amb una adreça de Classe B de 129.5.*X*.*X* (on *X* representa un valor entre 0 i 254) estan obligades a respondre a la sol•licitud. En aquest cas, com que les adreces de Classe B representen xarxes més grans que les adreces de Classe C, la xarxa queda inundada d'un nombre significativament més gran de sol•licituds a màquines no existents que en una xarxa de Classe C.

Adreces de subxarxa

Les adreces de subxarxa permeten que un sistema autònom composat de diverses xarxes pugui compartir la mateixa adreça d'Internet.

La possibilitat de subxarxa de TCP/IP també permet dividir una xarxa en diverses xarxes lògiques (subxarxes). Per exemple, una organització pot tenir una única adreça de xarxa d'Internet que és coneguda pels usuaris externs a l'organització i, malgrat això, pot configurar internament la seva xarxa en subxarxes departamentals. En qualsevol cas, es necessiten menys adreces de xarxa d'Internet i alhora augmenten les possibilitats d'encaminament local.

Un camp d'adreces del protocol d'Internet estàndard té dues parts: una adreça de xarxa i una adreça local. Per fer possibles les subxarxes, la part d'adreça local d'una adreça d'Internet es divideix en un número de subxarxa i en un número d'amfitrió. La subxarxa s'identifica de tal manera que el sistema autònom local pot encaminar els missatges de manera fiable.

A l'adreça d'Internet de Classe A bàsica, que està formada per una adreça de xarxa de 8 bits i una adreça local de 24 bits, l'adreça local identifica la màquina d'amfitrió específica de la xarxa.

Adreça de xarxa (8 bits)	**Adreça de l'amfitrió local** (24 bits)		
01111101	00001101	01001001	00001111

Figura 18. Adreça de Classe A

Aquesta il•lustració mostra una estructura típica d'adreça de Classe A. Els primers 8 bits contenen l'adreça de xarxa (que sempre comença amb un zero). Els 24 bits restants contenen l'adreça d'amfitrió local.

Per crear una adreça de subxarxa per a aquesta adreça d'Internet de Classe A, l'adreça local pot dividir-se en un número que identifica la xarxa física (o subxarxa) i un número que identifica l'amfitrió de la subxarxa. Els emissors encaminen els missatges a l'adreça de xarxa anunciada, i el sistema local s'encarrega d'encaminar els missatges a les seves subxarxes i els seus amfitrions. A l'hora de decidir com particionar l'adreça local en adreça de xarxa i adreça d'amfitrió, heu de tenir en compte el nombre de subxarxes i el nombre d'amfitrions d'aquestes subxarxes.

A la figura següent, l'adreça local es particiona en una adreça de subxarxa de 12 bits i una adreça d'amfitrió de 12 bits.

Adreça de xarxa (8 bits)	**Adreça d'amfitrió local** (24 bits)	
Adreça de xarxa	**Adreça de subxarxa**	**Adreça d'amfitrió**
01111101	00001101 0100	1001 00001111

Nota: El bit d'ordre superior (o el primer bit) sempre serà 0 en una adreça de classe A.

Figura 19. Adreça de Classe A amb la corresponent adreça de subxarxa

Aquesta il•lustració mostra una estructura típica d'adreça de Classe A. Els primers 8 bits contenen l'adreça de xarxa (que sempre comença amb un zero). Els 24 bits restants contenen l'adreça d'amfitrió local amb l'adreça de subxarxa que ocupa els primers 8 bits i l'adreça d'amfitrió que ocupa els darrers 8 bits.

Teniu flexibilitat a l'hora d'assignar adreces de subxarxa i adreces d'amfitrió. Els bits de l'adreça local poden dividir-se segons les necessitats i el creixement potencial de l'organització i de la seva estructura de xarxa. Les úniques restriccions són les següents:

- `adreça_xarxa` és l'adreça d'Internet de la xarxa.
- `adreça_subxarxa` és un camp d'una amplada constant per a una xarxa determinada.
- `adreça_amfitrió` és un camp que té com a mínim una amplada d'1 bit.

Si l'amplada del camp `adreça_subxarxa` és 0, la xarxa no està organitzada en subxarxes, i l'adreçament a la xarxa es realitza utilitzant l'adreça de xarxa d'Internet.

Els bits que identifiquen la subxarxa s'especifiquen mitjançant una màscara de bits i, per tant, no cal que estiguin adjacents a l'adreça. No obstant això, normalment és desitjable que els bits de subxarxa estiguin contigus i col•locats com els bits més importants de l'adreça local.

Màscares de subxarxa:

Quan un amfitrió envia un missatge a una destinació, el sistema ha de determinar si la destinació es troba a la mateixa xarxa que l'origen o si es pot arribar directament a la destinació a través d'una de les interfícies locals. El sistema compara l'adreça de destinació amb l'adreça d'amfitrió utilitzant la *màscara de subxarxa*.

Si la destinació no és local, el sistema envia el missatge a una passarel•la. La passarel•la realitza la mateixa comparació per veure si l'adreça de destinació es troba en una xarxa a la que es pot accedir localment.

La màscara de subxarxa indica al sistema quin és l'esquema de particions de subxarxa. Aquesta màscara de bits està formada per la part d'adreça de xarxa i la part d'adreça de subxarxa de l'adreça d'Internet.

Adreça de xarxa (8 bits)	**Adreça de l'amfitrió local** (24 bits)			
Adreça de xarxa	**Adreça de subxarxa**		**Adreça d'amfitrió**	
01111101	00001101	0100	1001	00001111

Adreça de classe A amb l'adreça de subxarxa corresponent

Adreça de xarxa (8 bits)	**Adreça de l'amfitrió local** (24 bits)			
Adreça de xarxa	Adreça de subxarxa		Adreça d'amfitrió	
Màscara de subxarxa			**Adreça d'amfitrió**	
01111101	00001101	0100	1001	00001111

Adreça de classe A amb la màscara de subxarxa corresponent

Figura 20. Adreça de Classe A amb la corresponent adreça de subxarxa

Aquesta il•lustració mostra una estructura típica d'adreça de Classe A. Els primers 8 bits contenen l'adreça de xarxa (que sempre comença amb un zero). Els 24 bits restants contenen l'adreça d'amfitrió local amb l'adreça de subxarxa que ocupa els primers 8 bits i l'adreça d'amfitrió que ocupa els darrers 8 bits.

Per exemple, la màscara de subxarxa de l'adreça de Classe A amb l'esquema de particions definit abans es mostra en aquesta figura.

La màscara de subxarxa és un conjunt de 4 octets, igual que l'adreça d'Internet. La màscara de subxarxa està formada per bits alts (1) que corresponen a les posicions de bit de l'adreça de xarxa i subxarxa, i per bits baixos (0) que corresponen a les posicions de bit de l'adreça d'amfitrió. Una màscara de subxarxa per a l'adreça anterior té un aspecte semblant a la figura següent.

Adreça de xarxa (8 bits)	**Adreça de l'amfitrió local** (24 bits)			
Adreça de xarxa	**Adreça de subxarxa**		**Adreça d'amfitrió**	
11111111	11111111	1111	0000	00000000

Figura 21. Exemple de màscara de subxarxa

Aquesta il•lustració mostra un exemple d'una estructura de màscara de subxarxa. Els primers 8 bits contenen l'adreça de xarxa. Els 24 bits restants contenen l'adreça d'amfitrió local amb l'adreça de subxarxa que ocupa els primers 8 bits i l'adreça d'amfitrió que ocupa els darrers 8 bits.

Comparació d'adreces:

L'adreça de destinació i l'adreça de xarxa local es comparen realitzant les operacions AND lògica i OR exclusiva a la màscara de subxarxa de l'amfitrió d'origen.

El procés de comparació es descriu a continuació:

1. Realitzeu una operació AND lògica de l'adreça de destinació i la màscara de l'adreça de subxarxa local.
2. Realitzeu una operació OR exclusiva sobre el resultat de l'operació anterior i l'adreça de xarxa local de la interfície local. Si el resultat és tot 0, se suposa que es pot accedir directament a la destinació a través d'una de les interfícies locals.
3. Si un sistema autònom té més d'una interfície (per tant, més d'una adreça d'Internet), el procés de comparació es repeteix per a cada interfície local.

Per exemple, suposem que hi hagi dues interfícies locals definides per a una xarxa d'amfitrió, T125. Les seves adreces d'Internet i les representacions binàries d'aquestes adreces es mostren a l'exemple següent:

```
CLASSE A   73.1.5.2    =  01001001 00000001 00000101 00000010


CLASSE B   145.21.6.3  =  10010001 00010101 00000110 00000011
```

Les màscares de subxarxa corresponents per a les interfícies de xarxa locals es mostren a l'exemple següent:

```
CLASSE A   73.1.5.2    =  11111111 11111111 11100000 00000000


CLASSE B   145.21.6.3  =  11111111 11111111 11111111 11000000
```

Si se sol•licita a la xarxa d'origen, T125, que enviï un missatge a una xarxa de destinació amb l'adreça d'amfitrió 114.16.23.8 (representada en binari com a: 01110010 00010000 00010111 00001000), el sistema comprova si es pot accedir a la destinació a través d'una interfície local.

Nota: La paraula clau **subnetmask** s'ha d'establir a la base de dades de configuració de cada amfitrió que ha de donar suport a les subxarxes. Abans de que es pugui utilitzar la possibilitat de subxarxa , tots els amfitrions de la xarxa li han de donar suport. Establiu la màscara de subxarxa permanentment a la base de dades de configuració utilitzant el menú Selecció d'interfície de xarxa de la SMIT. La màscara de subxarxa també es pot establir en el sistema en execució utilitzant l'ordre **ifconfig**. La utilització de l'ordre **ifconfig** per establir la màscara de subxarxa no és un canvi permanent.

Adreces de difusió

TCP/IP pot enviar dades a tots els amfitrions d'una xarxa local o a tots els amfitrions de totes les xarxes connectades directament. Aquestes transmissions reben el nom de *missatges de difusió*.

Per exemple, el daemon d'encaminament **routed** utilitza missatges de difusió per consultar i respondre a les consultes d'encaminament.

Per difondre les dades a tots els amfitrions de totes les xarxes connectades directament, s'utilitzen els protocols UDP (User Datagram Protocol) i IP (Protocol d'Internet) per enviar les dades, i l'adreça de destinació de l'amfitrió de la capçalera IP té tots els bits establerts en 1. Per difondre les dades a tots els amfitrions d'una xarxa específica, tots els bits de la part d'adreça local de l'adreça IP estan establerts en 0. No hi ha ordres d'usuari que utilitzin la possibilitat de difusió, malgrat que es poden desenvolupar ordres, o programes, d'aquest tipus.

L'adreça de difusió pot canviar-se temporalment canviant el paràmetre *broadcast* de l'ordre **ifconfig**. Canvieu l'adreça de difusió de forma permanent utilitzant el camí d'accés ràpid de la SMIT `smit chinet`. El canvi d'adreça de difusió pot ser útil per la compatibilitat amb versions anteriors de programari que utilitza una adreça de difusió diferent; per exemple, els ID d'amfitrió estan tots establerts en 0.

Adreces de bucle de retorn local

El protocol d'Internet defineix l'adreça de xarxa especial, 127.0.0.1, com a adreça de bucle de retorn local.

Els amfitrions utilitzen adreces de bucle de retorn local per enviar-se missatges a si mateixos. El gestor de configuracions estableix l'adreça de bucle de retorn local durant el procés d'engegada del sistema. El bucle de retorn local s'implementa al kernel i també es pot establir amb l'ordre **ifconfig**. El bucle de retorn s'invoca quan s'inicia el sistema.

Traducció de noms del TCP/IP

Tot i que les adreces d'Internet de 32 bits proporcionen a les màquines un mitjà eficaç d'identificació de l'origen i la destinació dels datagrames enviats a través d'una internetwork, els usuaris prefereixen noms amb significat i fàcils de recordar. El **Transmission Control Protocol/Internet Protocol (TCP/IP)** proporciona un sistema de denominació que dóna suport tant a l'organització de xarxa jeràrquica com plana.

La denominació a les xarxes planes és molt senzilla. Els noms d'amfitrió consten d'un únic joc de caràcters i s'acostumen a administrar localment. A les xarxes **TCP/IP** planes, cada màquina de la xarxa té un fitxer (`/etc/hosts`) que conté la informació de mapatge de nom a adreça d'Internet de cada amfitrió de la xarxa. La càrrega administrativa de mantenir actualitzat el fitxer de denominació de cada màquina creix a mida que creix la xarxa **TCP/IP**. Quan les xarxes **TCP/IP** passen a ser molt grans, com a Internet, la denominació es divideix de forma jeràrquica. Normalment, les divisions segueixen l'organització de la xarxa. Al **TCP/IP**, la denominació jeràrquica es coneix com a *sistema de noms de domini* (DNS) i utilitza el protocol DOMAIN. Al **TCP/IP** és el daemon **named** qui implementa el protocol DOMAIN.

Igual que amb la denominació a les xarxes planes, la jerarquia de noms de domini proporciona l'assignació de noms simbòlics a xarxes i amfitrions que tenen significat i són fàcils de recordar per als usuaris. No obstant això, en comptes que cada màquina de la xarxa mantingui un fitxer que contingui el mapatge de nom a adreça per a tots els altres amfitrions de la xarxa, se selecciona un o més amfitrions perquè funcionin com a *servidors de noms.* Els servidors de noms tradueixen (resolen) els noms simbòlics assignats a les xarxes i amfitrions en les eficaces adreces d'Internet utilitzades per les màquines. Un servidor de noms té informació completa sobre alguna part del domini, anomenada *zona*, i té *autorització* per a la seva zona.

Autoritat de denominació

En una xarxa plana, tots els amfitrions de la xarxa estan administrats per una autoritat central. Aquesta forma de xarxa requereix que tots els amfitrions de la xarxa tinguin noms d'amfitrió exclusius. En una xarxa gran, aquest requisit crea una gran càrrega administrativa per a l'autoritat central.

En una xarxa de dominis, els grups d'amfitrions s'administren de forma independent en una jerarquia d'arbre de dominis i subdominis. En aquest cas, els noms d'amfitrió han de ser exclusius només dins del domini local, i només el *domini de root* està administrat per una autoritat central. Aquesta estructura permet que els subdominis estiguin administrats localment i redueix la càrrega de l'autoritat central. Per exemple, el domini de root d'Internet consta dels dominis `com` (organitzacions comercials), `edu` (organitzacions educatives), `gov` (organitzacions governamentals) i `mil` (grups militars). Només l'autoritat central pot afegir nous dominis de nivell superior. La denominació al segon nivell està delegada a determinats agents dins dels dominis respectius. Per exemple, a la figura següent, `com` té autoritat de denominació per a tots els subdominis d'organització comercial que té a sota. De la mateixa manera, la denominació al tercer nivell (i així successivament) està delegada a agents dins d'aquest nivell. Per exemple, a la figura Estructura de dominis d'Internet, Century té autoritat de denominació per als seus subdominis Austin, Hopkins i Charlotte.

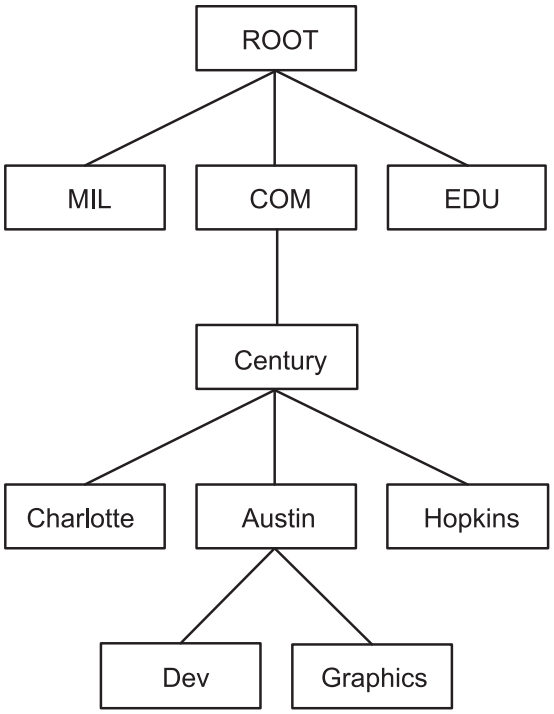


Figura 22. Estructura de dominis d'Internet

Aquesta figura il•lustra l'estructura jeràrquica d'Internet. Comença a la part superior i es bifurca cap al nivell següent que conté els dominis mil, com i edu. A sota del domini com hi ha un altre nivell que conté Charlotte, Austin i Hopkins. A sota d'Austin hi ha Dev i Graphics.

El subdomini Austin de Century també es pot dividir en zones, per exemple, Dev i Graphics. En aquest cas, la zona `austin.century.com` té totes les dades al domini `austin.century.com`, excepte les delegades a Dev i Graphics. La zona `dev.century.com` només contindria les dades delegades a Dev; no hi hauria res sobre Graphics, per exemple. La zona `austin.century.com` (en oposició al domini del mateix nom) contindria només les dades no delegades a altres zones.

Convenis de denominació

Al sistema jeràrquic de noms de dominis, els noms consten d'una seqüència de subnoms no sensibles a minúscules i majúscules separats per punts sense blancs intercalats.

El protocol DOMAIN especifica que un nom de domini local ha de tenir menys de 64 caràcters i que un nom d'amfitrió ha de tenir menys de 32 caràcters de longitud. El nom d'host es dóna primer, seguit d'un punt (.), una sèrie de noms de domini local separats per punts, i finalment el domini arrel. Un nom de domini especificat completament per a un amfitrió, inclosos els punts, ha de tenir menys de 255 caràcters de longitud i la forma següent:

```
host.subdomini1.[subdomini2 . . . subdomini].domini_de_root
```

Com que els noms d'amfitrió han de ser exclusius dins un domini, podeu utilitzar un nom abreujat a l'hora d'enviar missatges a un amfitrió dins el mateix domini. Per exemple, en comptes d'enviar un missatge a `smith.eng.lsu.edu`, un amfitrió dins del domini `eng` podria enviar un missatge a `smith`. A més, cada amfitrió pot tenir diversos àlies que els altres amfitrions poden utilitzar en enviar missatges.

Denominació d'amfitrions a la vostra xarxa

L'objectiu d'utilitzar noms per als amfitrions és proporcionar una forma ràpida, fàcil i gens ambigua de referir-se als ordinadors de la vostra xarxa. Els administradors de sistemes d'Internet han descobert que

hi ha bones opcions, tot i que pobres, per als noms d'amfitrió. Aquests suggeriments pretenen ajudar-vos a evitar riscos habituals a l'hora de triar noms d'amfitrió.

A continuació es mostren alguns suggeriments per triar noms d'amfitrió gens ambigus i fàcils de recordar:

- Termes d'ús poc freqüent, com per exemple, `esfinx` o `eclipsi`.
- Noms de temes, com ara colors, elements (per exemple, `heli`, `argó` o `zinc`), flors, peixos, i d'altres.
- Paraules reals (en oposició a sèries aleatòries de caràcters).

A continuació es mostren alguns exemples d'opcions pobres. En general, aquestes opcions són pobres perquè són difícils de recordar o confuses (sigui per als humans o per als ordinadors):

- Termes que ja estan en l'ús comú, per exemple, `amunt`, `avall`, o `caiguda`.
- Noms que només contenen xifres.
- Noms que contenen signes de puntuació.
- Noms que depenen de la distinció de majúscules i minúscules, per exemple, `Blanca` i `blanca`.
- El nom o les inicials de l'usuari principal del sistema.
- Noms de més de 8 caràcters.
- Ortografies inusuals o intencionadament incorrectes, per exemple, `chec`, que es podria confondre amb "xec" o "txec".
- Noms que són, o semblen, noms de domini, per exemple, `yale.edu`.

Servidors de noms

En un espai de nom pla, tots els noms han d'estar al fitxer `/etc/hosts` en cada amfitrió de la xarxa. Si la xarxa és molt gran, això pot suposar una càrrega en els recursos de cada màquina. En una xarxa jeràrquica, determinats amfitrions designats com a *servidors de noms* resolen els noms en adreces d'Internet per a altres amfitrions.

Això té dos avantatges per a l'espai de nom pla. Evita que els recursos de cada amfitrió de la xarxa estiguin ocupats en la traducció de noms, i evita que la persona que gestiona el sistema hagi de mantenir els fitxers de traducció de noms en cada màquina de la xarxa. El conjunt de noms gestionats per un únic servidor de noms es coneix com la seva *zona d'autorització*.

Nota: Tot i que la màquina d'amfitrió que realitza la funció de traducció de noms per a una zona d'autorització s'anomena habitualment amfitrió de *servidor de noms*, el procés que controla la funció, el daemon **named**, és el procés del servidor de noms real.

Per reduir més l'activitat de xarxa innecessària, tots els servidors de noms *posen a la memòria cau* (emmagatzemen durant un període de temps) els mapatges de nom a adreça. Quan un client demana a un servidor que resolgui un nom, el servidor comprova primer la seva memòria cau per veure si el nom s'ha resolt recentment. Com que els noms de domini i d'amfitrió canvien, cada element roman a la memòria cau durant un període de temps limitat especificat pel TTL de l'enregistrament. D'aquesta manera, les autoritzacions poden especificar quant de temps esperen que la traducció de noms sigui correcta.

A qualsevol sistema autònom hi poden haver múltiples servidors de noms. Normalment, els servidors de noms s'organitzen de forma jeràrquica i corresponen a l'organització de la xarxa. En referència a la figura "Estructura de dominis d'Internet", cada domini pot tenir un servidor de noms responsable de tots els subdominis del domini. Cada servidor de noms de subdominis es comunica amb el servidor de noms del domini de sobre (anomenat servidor de noms *superior*), així com amb els servidors de noms d'altres subdominis.

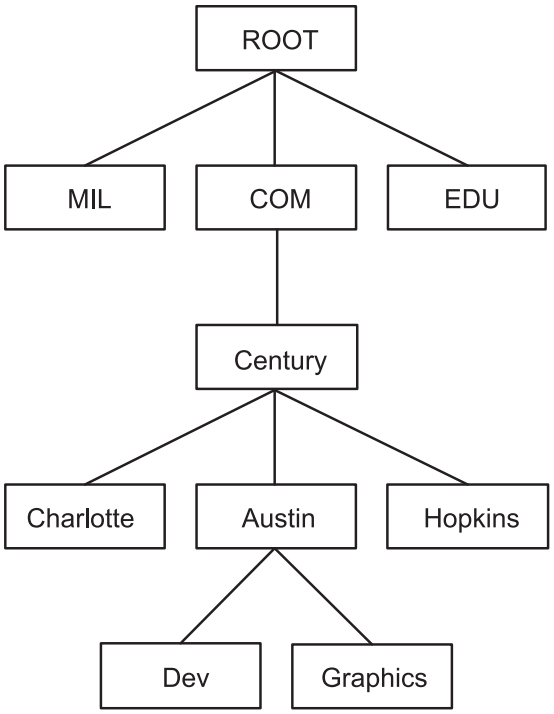


Figura 23. Estructura de dominis d'Internet

Aquesta figura il•lustra l'estructura jeràrquica d'Internet. Comença a la part superior i es bifurca cap al nivell següent que conté els dominis mil, com i edu. A sota del domini com hi ha un altre nivell que conté Charlotte, Austin i Hopkins. A sota d'Austin hi ha Dev i Graphics.

Per exemple, a la figura "Estructura de dominis d'Internet", Austin, Hopkins i Charlotte són tots tres subdominis del domini Century. Si se segueix la jerarquia d'arbre del disseny de la xarxa, el servidor de noms d'Austin es comunica amb els servidors de noms de Charlotte i Hopkins així com amb el servidor de noms de Century superior. El servidor de noms d'Austin també es comunica amb els servidors de noms responsables dels seus subdominis.

Hi ha diversos tipus de servidors de noms:

Element	Descripció
Servidor de noms mestre	Carrega les seves dades des d'un fitxer o disc i pot delegar l'autorització a altres servidors del seu domini.
Servidor de noms esclau	Rep la seva informació en el moment d'engegada del sistema per a la zona d'autorització determinada a partir d'un servidor de noms mestre i, a continuació, demana periòdicament al servidor mestre que actualitzi la seva informació. Quan caduqui el valor de renovació a l'enregistrament de recursos de l'inici d'autorització (SOA) en un servidor de noms esclau, o quan es rebi un missatge de notificació del servidor de noms mestre, l'esclau recarrega la base de dades del mestre si el número de sèrie de la base de dades del mestre és superior al número de sèrie de la base de dades actual de l'esclau. Si és necessari forçar una nova transferència de zona des del mestre, només cal que elimineu les bases de dades existents de l'esclau i renoveu el daemon **named** al servidor de noms esclau.
Servidor de noms stub	Tot i que el seu mètode de rèplica de bases de dades és semblant al del servidor de noms esclau, el servidor de noms stub només replica els enregistraments de servidor de noms de la base de dades mestra i no tota la base de dades sencera.

Element	Descripció
Servidor d'orientació	Indica un servidor de noms que només confia en les orientacions que ha muntat a partir de les consultes anteriors a altres servidors de noms. El servidor de noms d'orientació respon a les consultes preguntant a altres servidors que tenen autorització per proporcionar la informació necessària si un servidor de noms d'orientació no té a la seva memòria cau un mapatge de nom a adreça.
Servidor reenviador o client	Reenvia les consultes que no pot satisfer localment a una llista fixa de servidors de reenviament. Els servidors de només reenviament (un reenviador que obté informació i la passa a altres clients, però que realment no és un servidor) no interactuen amb els servidors de noms mestres per al domini de root i altres dominis. Les consultes als servidors de reenviament són recursives. Hi pot haver un o més servidors de reenviament, que es van provant per torn fins que s'esgota la llista. Una configuració de reenviador i client s'utilitza normalment quan no voleu que tots els servidors d'un lloc determinat interactuïn amb la resta de servidors d'Internet, o quan voleu muntar una memòria cau gran en un nombre seleccionat de servidors de noms.
Servidor remot	Executa tots els programes de xarxa que utilitzen el servidor de noms sense que el procés de servidor de noms s'executi a l'amfitrió local. Totes les consultes les processa un servidor de noms que s'executa en una altra màquina de la xarxa.

Un amfitrió de servidor de noms pot funcionar en capacitats diferents per a diferents zones d'autorització. Per exemple, un sol amfitrió de servidor de noms pot ser un servidor de noms mestre per a una zona i un servidor de noms esclau per a una altra zona.

Traducció de noms

El procés per obtenir una adreça d'Internet a partir d'un nom d'amfitrió es coneix com a traducció de noms i s'aconsegueix amb la subrutina **gethostbyname**.

El procés de traduir una adreça d'Internet en un nom d'amfitrió es coneix com a traducció de noms inversa i s'aconsegueix amb la subrutina **gethostbyaddr**. Essencialment aquestes rutines són objectes usuari d'una biblioteca de rutines de traducció de noms que es coneixen com a *solucionadors*.

Les rutines de solucionador dels amfitrions que executen el **TCP/IP** normalment intenten resoldre noms, mitjançant els orígens següents.

1. BIND/DNS (amb nom)
2. Network Information Service (NIS)
3. Fitxer `/etc/hosts` local

Per resoldre un nom en una xarxa de domini, la rutina de solucionador primer consulta la base de dades de servidors de noms de domini, que podria ser local si l'amfitrió és un servidor de noms de domini o es troba en un amfitrió extern. Els servidors de noms tradueixen els noms de domini en adreces d'Internet. El grup de noms del qual és responsable un servidor de noms és la seva zona d'autorització. Si la rutina de solucionador utilitza un servidor de noms remot, la rutina utilitza el protocol de noms de domini (DOMAIN) per consultar sobre el mapatge. Per resoldre un nom en una xarxa plana, la rutina de solucionador comprova si hi ha una entrada al fitxer `/etc/hosts` local. Quan s'utilitza el NIS, es comprova el fitxer `/etc/hosts` del servidor mestre.

Per defecte, les rutines de solucionador intenten resoldre els noms mitjançant els recursos anteriors. Primer es prova el BIND/DNS. Si el fitxer `/etc/resolv.conf` no existeix o si el BIND/DNS no ha pogut trobar el nom, es consulta al NIS si es troba en execució. El NIS està autoritzat per sobre del fitxer `/etc/hosts` local; per tant, la cerca finalitza aquí si es troba en execució. Si el NIS no està en execució, aleshores se cercarà al fitxer `/etc/hosts` local. Si cap d'aquests serveis pot trobar el nom, les rutines de solucionador tornen amb AMFITRIÓ_NO_TROBAT. Si cap dels serveis no està disponible, les rutines de solucionador tornen amb SERVEI_NO_DISPONIBLE.

L'ordre per defecte descrit més amunt es pot sobreescriure creant el fitxer de configuració /etc/irs.conf i especificant l'ordre desitjat. A més, tant l'ordre per defecte com el d'/etc/irs.conf es poden sobreescriure amb la variable d'entorn **NSORDER**. Si es defineix el fitxer /etc/irs.conf o bé la variable d'entorn **NSORDER**, cal especificar com a mínim un valor juntament amb l'opció.

Per especificar l'ordre d'amfitrió amb el fitxer /etc/irs.conf:

```
hosts valor [ continue ]
```

L'ordre s'especifica amb cada mètode indicat en una línia per si mateix. El *valor* és un dels mètodes llistats i la paraula clau **continue** indica que hi ha un altre mètode de solucionador que segueix a la línia següent.

Per especificar l'ordre d'amfitrió amb la variable d'entorn **NSORDER**:

```
NSORDER=valor,valor,valor
```

L'ordre s'especifica en una línia amb valors separats per comes. Estan permesos els espais en blanc entre les comes i el signe d'igual.

Per exemple, si la xarxa local està organitzada com una xarxa plana, només es necessita el fitxer /etc/hosts. En aquest exemple, el fitxer /etc/irs.conf conté la línia següent:

```
hosts local
```

Com a alternativa, es pot establir la variable d'entorn **NSORDER** com a:

```
NSORDER=local
```

Si la xarxa local és una xarxa de domini que utilitza un servidor de noms per a la traducció de noms i un fitxer /etc/hosts per a la còpia de seguretat, s'haurien d'especificar ambdós serveis. En aquest exemple, el fitxer /etc/irs.conf conté les línies següents:

```
hosts dns continue
hosts local
```

La variable d'entorn **NSORDER** s'estableix com a:

```
NSORDER=bind,local
```

Nota: Els valors llistats han d'estar en minúscules.

Quan se segueix qualsevol ordre de solucionador definit o per defecte, l'algorisme de cerca continua d'un solucionador al següent només si:

- El servei actual no està en execució, i per tant no està disponible.
- El servei actual no pot trobar el nom i no està autoritzat.

Si el fitxer /etc/resolv.conf no existeix, es considera que el BIND/DNS no està configurat o en execució i, per tant, no està disponible. Si les subrutines **getdomainname** i **yp_bind** fallen, es considera que el servei NIS no està configurat o en execució i, per tant, no està disponible. Si no s'ha pogut obrir el fitxer /etc/hosts, és impossible realitzar una cerca local i, per tant, el fitxer i el servei no estan disponibles.

Quan un servei apareix com a autoritzat (*authoritative*, significa que aquest servei és l'expert dels seus successors i té tots els noms i adreces pertinents. Les rutines de solucionador no proven els serveis de successors, perquè els successors poden contenir només un subconjunt de la informació del servei autoritzat. La traducció de noms finalitza al servei llistat com a autoritzat, fins i tot si no troba el nom (en aquest cas, la rutina de solucionador torna AMFITRIÓ_NO_TROBAT). Si un servei autoritzat no està disponible, es consulta el següent servei especificat.

Un origen autoritzat s'especifica amb la sèrie `=auth` directament darrere d'un valor. Es pot escriure tota la paraula `authoritative`, però només s'utilitza la sèrie `auth`. Per exemple, si la variable d'entorn **NSORDER** conté el següent:

```
hosts = nis=auth,dns,local
```

La cerca finalitza després de la consulta del NIS (si el NIS està en execució), independentment de si s'ha trobat el nom. Si el NIS no està en execució, aleshores es consultarà el següent origen, que és el DNS.

Els servidors de noms **TCP/IP** utilitzen memòries cau per reduir el cost de cerca de noms d'amfitrions en xarxa remotes. En comptes de cercar un nom d'amfitrió cada vegada que es realitza una sol•licitud, un servidor de noms primer cerca a la seva memòria cau per veure si el nom d'amfitrió s'ha resolt recentment. Com que els noms de domini i d'amfitrió canvien, cada element roman a la memòria cau durant un període de temps limitat especificat pel valor de duració (TTL) de l'enregistrament. D'aquesta manera, els servidors de noms poden especificar quant de temps esperen que les seves respostes es considerin autoritzades.

Conflicte potencial de noms d'amfitrió entre el servidor de noms i sendmail:

En un entorn DNS, un nom d'amfitrió establert mitjançant l'ordre **hostname** des de la línia d'ordres o en el format del fitxer `rc.net` ha de ser el nom oficial de l'amfitrió que torna el servidor de noms.

Generalment, aquest nom és el nom de domini complet de l'amfitrió amb la forma:

```
amfitrió.subdomini.subdomini.domini_root
```

Nota: Les rutines de solucionador requereixen que s'estableixi el domini per defecte. Si no s'estableix el domini per defecte a l'ordre **hostname**, s'ha d'establir al fitxer `/etc/resolv.conf`.

Si el nom de l'amfitrió no es configura com un nom de domini completament qualificat i si el sistema s'ha configurat per utilitzar un servidor de noms de domini juntament amb el programa **sendmail**, cal editar el fitxer de configuració de **sendmail** (`/etc/sendmail.cf`) perquè reflecteixi aquest nom d'amfitrió oficial. A més, s'ha d'establir que les macros de noms de domini d'aquest fitxer de configuració funcionin correctament per al programa **sendmail**.

Nota: El domini especificat al fitxer `/etc/sendmail.cf` té prioritat per damunt del domini establert per l'ordre **hostname** per a totes les funcions **sendmail**.

Conflicte potencial de noms de domini entre el servidor de noms i sendmail:

Els noms de domini locals i els servidors de noms de domini s'especifiquen en fitxers diferents, en funció de si l'amfitrió és un servidor de noms DOMAIN.

Per a un amfitrió que es troba en una xarxa DOMAIN però que no és un servidor de noms, el nom de domini local i el servidor de noms de domini s'especifiquen al fitxer `/etc/resolv.conf`. En un amfitrió de servidor de noms DOMAIN, el domini local i altres servidors de noms es defineixen en fitxers llegits pel daemon **named** quan s'inicia.

Protocol de resolució d'adreces inversa

El **Protocol de resolució d'adreces inversa (RARP)** tradueix adreces de maquinari exclusives en adreces d'Internet a l'adaptador Ethernet de xarxa d'àrea local (LAN) (només protocol Ethernet).

El protocol Ethernet estàndard està suportat amb les restriccions següents:

- El servidor només respon a sol•licituds **RARP**.
- El servidor només utilitza entrades de taula **ARP** permanents.
- El servidor no utilitza entrades de taula **ARP** dinàmiques.
- El servidor no respon automàticament per si mateix.

L'administrador del sistema ha de muntar i mantenir de forma manual una taula d'entrades **ARP** permanents mitjançant l'ordre **arp**. S'ha d'afegir al servidor una entrada de taula **ARP** específica per a cada amfitrió que requereixi respostes **RARP** d'un origen autoritzat.

Tasques de traducció de noms locals (/etc/hosts)

Configureu el fitxer `/etc/hosts` si la vostra xarxa és petita i feu servir un esquema de denominació plana.

Fins i tot si utilitzeu un esquema de denominació jeràrquica (o de dominis) amb servidors de noms, és possible que vulgueu configurar el fitxer `/etc/hosts` per identificar els amfitrions que els servidors de noms no coneixen.

Configureu el sistema per a la resolució d'amfitrions locals mitjançant la SMIT (System Management Interface Tool), o bé ordres. Si trieu el mètode de les ordres, assegureu-vos de preservar el format del fitxer `/etc/hosts`, tal com es descriu a l'apartat Hosts File Format for TCP/IP de la publicació *Files Reference*.

Taula 61. Tasques de traducció de noms locals

Tasca	Camí d'accés ràpid de la SMIT	Ordre o fitxer
Llistar tots els amfitrions	**smit lshostent**	Utilitzeu l'ordre **hostent** o **view** `/etc/hosts`
Afegir un amfitrió	**smit mkhostent**	Utilitzeu l'ordre **hostent** o **edit** `/etc/hosts`
Canviar/Mostrar característiques d'un amfitrió	**smit chhostent**	Utilitzeu l'ordre **hostent** o **edit** `/etc/hosts`
Eliminar un amfitrió	**smit rmhostent**	Utilitzeu l'ordre **hostent** o **edit** `/etc/hosts`

Planificació de la traducció de noms de domini

Aquests suggeriments us poden ajudar a planificar el vostre propi sistema de traducció de noms de domini.

Si formeu part d'una internetwork més gran, coordineu la configuració dels vostres servidors de noms i dominis amb l'autoritat central.

- A causa de les àmplies possibilitats en arquitectura i configuració, familiaritzeu-vos amb el **TCP/IP**, el DNS i el BIND abans de solidificar cap planificació. Si teniu la intenció d'utilitzar un servei d'informació de xarxa, familiaritzeu-vos també amb l'NFS i el NIS. Els manuals sobre aquests temes estan disponibles obertament.
- Comenceu la planificació.

  Canviar un nom és *molt* més difícil que configurar-ne l'inicial. Aconseguiu el consens de la vostra organització sobre els noms de xarxa, passarel•la, servidor de noms i amfitrió abans de configurar els fitxers.
- Configureu els servidors de noms redundants.

  Si no podeu configurar servidors de noms redundants, assegureu-vos de configurar servidors de noms d'orientació i esclaus per tenir algun tipus de còpia de seguretat.
- A l'hora de seleccionar els servidors de noms, tingueu present el següent:
  - Trieu màquines que es troben físicament més properes als sistemes exteriors.
  - Els servidors de noms haurien de ser tan independents com sigui possible. Proveu diferents fonts d'alimentació i cablatge independent.
  - Cerqueu una altra xarxa per fer una còpia de seguretat del servei de traducció de noms i feu el mateix amb les altres xarxes.
- Proveu els servidors.
  - Proveu tant la traducció de noms normal com la inversa.
  - Proveu la transferència de zona des dels servidors de noms mestres als esclaus.
  - Proveu cada servidor de noms després d'una caiguda i reengegada del sistema.

- Envieu sol•licituds de traducció de noms als servidors remitents abans que vagin als servidors de noms exteriors. Això permet als servidors de noms compartir memòries cau i millorar el rendiment reduint la càrrega dels servidors de noms mestres.

```
objectclass container
        requires
                objectclass,
                cn
objectclass hosts
        requires
                objectclass,
                hname
        allows
                addr
                halias,
                comment
```

Resolució de servidors de noms

En una xarxa jeràrquica, hi ha determinats amfitrions designats com a *servidors de noms*. Aquests amfitrions tradueixen els noms en adreces IP per a altres amfitrions.

El daemon **named** controla la funció de servidor de noms i, per tant, cal executar-lo en un amfitrió de servidor de noms.

Abans de configurar un servidor de noms, decidiu quin o quins tipus s'ajustaràn millor a la xarxa. Hi ha diversos tipus de servidors de noms.

Un *servidor de noms mestre* emmagatzema, de fet, la base de dades que conté la informació de mapatge de nom a adreça. Carrega les seves dades des d'un fitxer o disc i pot delegar l'autorització a altres servidors del seu domini. Un *servidor de noms esclau* o *servidor de noms stub* rep la seva informació en el moment d'engegada del sistema per a la zona d'autorització determinada a partir d'un servidor de noms mestre i, a continuació, demana periòdicament al servidor mestre que actualitzi la seva informació. Un *servidor de noms d'orientació* respon a les sol•licituds per resoldre noms consultant altres servidors que tenen autorització per proporcionar la informació necessària.

Nota: Les generacions anteriors del servidor de noms **named** especificaven el servidor de noms mestre com el servidor de noms primari, el servidor de noms esclau com el servidor de noms secundari, i el servidor de noms d'orientació com el servidor de noms només de memòria cau.

Tingueu present que un servidor de noms pot funcionar en capacitats diferents per a diferents zones d'autorització. Per exemple, un amfitrió de servidor de noms pot ser un servidor de noms mestre per a una zona i un servidor de noms esclau per a una altra zona. Si el vostre sistema té instal•lat el NIS, aquests serveis també poden proporcionar resolució de noms.

Hi ha diversos fitxers implicats en la configuració de servidors de noms.

Element	Descripció
`conf`	Aquest fitxer es llegeix quan s'inicia el daemon **named**. Els enregistraments del fitxer `conf` comuniquen al daemon **named** quin tipus de servidor és, sobre quins dominis té autorització (les seves zones d'autorització), i d'on es poden obtenir les dades per configurar inicialment la seva base de dades. El nom per defecte d'aquest fitxer és `/etc/named.conf`. No obstant això, podeu canviar-li el nom especificant el nom i el camí d'accés del fitxer a la línia d'ordres quan s'inicia el daemon **named**. Si teniu la intenció d'utilitzar el fitxer `/etc/named.conf` com el fitxer `conf` i no existeix, es generarà un missatge al fitxer `syslog` i **named** finalitzarà. No obstant això, si s'especifica un fitxer `conf` alternatiu i aquest fitxer alternatiu no existeix, no es generarà cap missatge d'error i **named** continuarà.
`cache`	Conté informació sobre la memòria cau local. El fitxer de memòria cau local conté els noms i les adreces dels servidors de noms de màxima autorització de la xarxa. El fitxer de memòria cau utilitza el format d'enregistrament de recursos estàndard. El nom del fitxer de memòria cau s'estableix al fitxer `conf`.

Element	Descripció

`domain data`	Hi ha tres fitxers de dades de domini típics, també anomenats com els fitxers de dades de **named**. El fitxer **named** *local* conté la informació de resolució d'adreces per al bucle de retorn local. El fitxer **named** *data* conté les dades de resolució d'adreces per a totes les màquines de la zona d'autorització del servidor de noms. El fitxer **named** *reverse data* conté la informació de resolució d'adreces inversa per a totes les màquines de la zona d'autorització del servidor de noms. Els fitxers de dades de domini utilitzen el format d'enregistrament de recursos estàndard. L'usuari pot definir els seus noms de fitxer, que s'estableixen al fitxer `conf`. Per conveni, els noms d'aquests fitxers generalment inclouen el nom del daemon (`named`), i el tipus de fitxer i el nom del domini ve determinat per l'extensió. Per exemple, el servidor de noms del domini `abc` podria tenir els fitxers següents:
	`named.abc.data`
	`named.abc.rev`
	`named.abc.local`
	
	Quan modifiqueu els fitxers de dades **named** cal incrementar el número de sèrie de l'enregistrament de recursos SOA perquè els servidors de noms esclaus realitzin correctament els canvis de la nova zona.

`resolv.conf`	La presència d'aquest fitxer indica a un amfitrió que vagi primer a un servidor de noms per resoldre un nom. Si el fitxer `resolv.conf` no existeix, l'amfitrió cerca al fitxer `/etc/hosts` la traducció del nom. En un servidor de noms, ha d'existir el fitxer `resolv.conf` i pot contenir l'adreça d'amfitrió local, l'adreça de bucle de retorn (127.0.0.1), o bé pot estar buit. **Nota:** Les rutines de solucionador requereixen que s'estableixi el domini per defecte. Si no s'estableix el domini per defecte al fitxer `/etc/resolv.conf`, cal que estigui establert a `hostname`.

La duració (TTL) s'especifica als enregistraments de recursos. Si TTL no s'especifica en un enregistrament, la longitud d'aquest període de temps serà per defecte el camp mínim definit a l'enregistrament de l'inici de l'autorització (SOA) d'aquella zona. TTL s'utilitza quan les dades s'emmagatzemen fora d'una zona (en una memòria cau) per assegurar-se que les dades no es retenen de forma indefinida.

Configuració de servidors de noms de domini:

En aquest escenari es configurarà un servidor de noms mestre, un servidor de noms esclau i un servidor de noms de suggeriments per dur a terme la resolució de noms. Cada servidor de noms serà una màquina independent i cadascuna tindrà un fitxer `/etc/named.conf` configurat, encara que la informació continguda en aquests fitxers serà diferent. El fitxer `/etc/named.conf` es llegeix cada vegada que s'inicia el dimoni **named** i especifica de quin tipus de servidor es tracta (mestre, esclau o suggeriment) i d'on obtindrà les seves dades per a la resolució de noms. A cadascun d'aquests servidors de noms s'executa BIND 8.

El servidor de noms mestre es configurarà per proporcionar la resolució de noms de la zona `abc.aus.century.com`. En aquest escenari, l'adreça IP del servidor de noms mestre és `192.9.201.1` i el seu nom d'amfitrió és `venus.abc.aus.century.com`. Proporcionarà la resolució de noms per als noms d'amfitrió venus, earth, mars i jupiter. El fitxer `/etc/named.conf` es configurarà per especificar que el dimoni **named** haurà de cercar els seus fitxers de dades al directori `/usr/local/domain`. Els fitxers de dades que es configuraran per al servidor de noms mestre són `named.ca`, `named.abc.local`, `named.abc.data` i `named.abc.rev`.

A continuació es configurarà un servidor de noms esclau. El nom d'amfitrió del servidor de noms esclau serà `earth.abc.aus.century.com` i la seva adreça IP `192.9.201.5`. Al fitxer `/etc/named.conf` del servidor de noms esclau especificarem l'adreça del servidor de noms mestre per tal que el servidor de noms esclau pugui replicar els fitxers `named.abc.data` i `named.abc.rev` del servidor de noms mestre. A més a més, els fitxers de dades `named.ca` i `named.abc.local` es configuraran per a aquest servidor.

A continuació es configurarà un servidor de noms de suggeriment. El servidor de noms de suggeriment emmagatzemarà una memòria cau local per al mapatge d'adreces i els noms d'amfitrió. Si una adreça o un nom d'amfitrió sol•licitat no es troba a la seva memòria cau, el servidor de suggeriment es posarà en contacte amb el servidor de noms mestre, obtindrà la informació de resolució i l'afegirà a la seva memòria cau. A més a més, els fitxers de dades `named.ca` i `named.abc.local` es configuraran per a aquest servidor.

Tota la informació dels fitxers de dades named (no del fitxer /etc/named.conf) dels mateixos servidors de noms ha de tenir el format Standard Resource Record Format. Per obtenir informació sobre els fitxers de dades named, vegeu Standard Resource Record Format for TCP/IP a *Files Reference*.

L'administrador de cada servidor de noms serà gail.zeus.abc.aus.century.com. Això està especificat als fitxers de dades locals de cada servidor de noms. A més a més, en aquest escenari, el servidor de noms de root és relay.century.com i la seva adreça IP 129.114.1.2.

Al final d'aquest escenari, es proporcionarà la resolució de noms dels amfitrions venus, earth, mars i jupiter. A més també es proporciona la resolució de noms inversa (adreça IP a nom d'amfitrió). Quan es rep una sol•licitud que no es pot resoldre, el servidor de noms mestre es posarà en contacte amb relay.century.com per trobar la informació necessària.

Informació que cal tenir en compte

- La informació d'aquest cas s'ha provat amb versions específiques de l'AIX. Els resultats obtinguts poden variar força segons la versió i el nivell de l'AIX.

Pas 1. Configuració del servidor de noms mestre

1. Al servidor de noms mestre, obriu el fitxer /etc/named.conf. Si no hi ha cap fitxer /etc/named.conf al directori /etc, executeu l'ordre següent per crear-ne un:

   ```
   touch /etc/named.conf
   ```

   Seguiu aquestes instruccions per configurar el fitxer /etc/named.conf:

   a. Especifiqueu una clàusula de directori a l'stanza d'opcions. Això permetrà que els fitxers de dades named utilitzin camins d'accés relatius al directori /usr/local/domain. En aquest escenari s'ha afegit el següent:

      ```
      options {
          directory "/usr/local/domain";
      };
      ```

      Si trieu que no voleu especificar un directori aquí, els fitxers de dades necessaris se cercaran al directori /etc.

   b. Per permetre que les dades dels registres s'emmagatzemin a la memòria cau fora de les zones definides, especifiqueu el nom del fitxer de zona de suggeriment. En aquest escenari s'ha afegit el següent:

      ```
      zone "." IN {
          type hint;
          file "named.ca";
      };
      ```

   c. Afegiu les stanzas següents per especificar cada zona, el tipus de servidor de noms que esteu configurant i el fitxer de dades del domini del servidor de noms. En aquest escenari, el servidor mestre per a les zones directa i inversa és el següent:

      ```
      zone "abc.aus.century.com" in {
          type master;
          file "named.abc.data";
      };
      zone "201.9.192.in-addr.arpa" in {
          type master;
          file "named.abc.rev";
      };
      ```

   d. Definiu el nom del fitxer local named. Per exemple:

      ```
      zone "0.0.127.in-addr.arpa" in {
          type master;
          file "named.abc.local";
      };
      ```

      Després d'editar el fitxer, deseu-lo i tanqueu-lo.

2. Obriu el fitxer /usr/local/domain/named.ca. Afegiu les adreces dels servidors de noms de root del domini. En aquest escenari s'ha afegit el següent:

```
; servidors de noms de root.
.                   IN    NS    relay.century.com.
relay.century.com.   3600000    IN    A     129.114.1.2
```

   Després d'editar el fitxer, deseu-lo i tanqueu-lo.

3. Obriu el fitxer /usr/local/domain/named.abc.local. Afegiu la informació següent:
   - L'inici d'autoritat (SOA) de la zona i la informació de la duració per defecte. En aquest escenari s'ha afegit el següent:

```
$TTL 3h    ;3 hour

@ IN    SOA     venus.abc.aus.century.com. gail.zeus.abc.aus.century.com. (

                           1       ;serial
                           3600    ;refresh
                           600     ;retry
                           3600000 ;expire
                           3600    ;negative caching TTL
)
```

   - El registre del servidor de noms (NS). Inseriu un espai de tabulació al principi de la línia; el dimoni **named** substituirà l'espai de tabulació amb el nom de la zona:

```
<tab> IN    NS     venus.abc.aus.century.com.
```

   - El registre del punter (PTR).

```
1      IN    PTR    localhost.
```

   Després d'editar el fitxer, deseu-lo i tanqueu-lo.

4. Obriu el fitxer /usr/local/domain/named.abc.data. Afegiu la informació següent:
   - L'inici d'autoritat de la zona i la informació de la duració per defecte de la zona. Aquest registre designa l'inici d'una zona. Només es permet un registre d'inici d'autoritat per zona. En aquest escenari s'ha afegit el següent:

```
$TTL 3h    ;3 hour

@ IN    SOA     venus.abc.aus.century.com. gail.zeus.abc.aus.century.com. (
                1       ;serial
                3600    ;refresh
                600     ;retry
                3600000 ;expire
                3600    ;negative caching TTL
)
```

   - Registre del servidor de noms de tots els servidors de noms mestre de la zona. Inseriu un espai de tabulació al principi de la línia; el dimoni **named** substituirà l'espai de tabulació amb el nom de la zona:

```
<tab> IN    NS     venus.abc.aus.century.com.
```

   - Informació de resolució de nom a adreça a tots els amfitrions de la zona d'autoritat del servidor de noms:

```
venus   IN      A       192.9.201.1
earth       IN    A         192.9.201.5
mars        IN    A         192.9.201.3
jupiter     IN    A         192.9.201.7
```

   Inclou altres tipus d'entrades, com ara registres de noms canònics i registres intercanviadors de correu segons convingui.

   Després d'editar el fitxer, deseu-lo i tanqueu-lo.

5. Obriu el fitxer /usr/local/domain/named.abc.rev. Afegiu la informació següent:

- L'inici d'autoritat de la zona i la informació de la duració per defecte. Aquest registre designa l'inici d'una zona. Només es permet un registre d'inici d'autoritat per zona:

```
$TTL 3h    ;3 hour

@ IN    SOA     venus.abc.aus.century.com. gail.zeus.abc.aus.century.com. (
                            1       ;serial
                            3600    ;refresh
                            600     ;retry
                            3600000 ;expire
                            3600    ;negative caching TTL
)
```

- Inclou altres tipus d'entrades, com ara registres de servidors de noms. Si voleu incloure aquests registres, inseriu un espai de tabulació al principi de la línia; el dimoni **named** substituirà l'espai de tabulació amb el nom de la zona. En aquest escenari s'ha afegit el següent:

```
<tab> IN    NS     venus.abc.aus.century.com.
```

- Informació de resolució d'adreça a nom a tots els amfitrions de la zona que són a la zona d'autoritat del servidor de noms.

```
1                       IN    PTR    venus.abc.aus.century.com.
5                       IN    PTR    earth.abc.aus.century.com.
3                       IN    PTR    mars.abc.aus.century.com.
7                       IN    PTR    jupiter.abc.aus.century.com.
```

  Després d'editar el fitxer, deseu-lo i tanqueu-lo.

6. Creeu un fitxer `/etc/resolv.conf` executant l'ordre següent:

   ```
   touch /etc/resolv.conf
   ```

   La presència d'aquest fitxer indica que l'amfitrió hauria d'utilitzar un servidor de noms per la resolució de noms.

7. Afegiu l'entrada següent al fitxer `/etc/resolv.conf`:

   ```
   nameserver 127.0.0.1
   ```

   L'adreça `127.0.0.1` és l'adreça de bucle de retorn que fa que l'amfitrió accedeixi ell mateix com a servidor de noms. El fitxer `/etc/resolv.conf` també pot contenir una entrada com ara:

   ```
   domain abc.aus.century.com
   ```

   En aquest cas, `abc.aus.century.com` és el nom de domini.

   Després d'editar el fitxer, deseu-lo i tanqueu-lo.

8. Utilitzeu el camí d'accés ràpid de l'SMIT `smit stnamed` per habilitar el dimoni **named**. Així s'inicialitza el daemon cada vegada que s'engegui el sistema. Indiqueu si voleu iniciar el daemon **named** ara, quan es torni a engegar el sistema o les dues coses.

Pas 2. Configuració del servidor de noms esclau

Per configurar un servidor de noms esclau, seguiu aquest procediment. Haureu d'editar uns quants fitxers i després utilitzar l'SMIT per iniciar el dimoni **named**.

1. Al servidor de noms esclau, obriu el fitxer `/etc/named.conf`. Si no hi ha cap fitxer `/etc/named.conf` al directori `/etc`, executeu l'ordre següent per crear-ne un:

   ```
   touch /etc/named.conf
   ```

   Seguiu aquestes instruccions per configurar el fitxer `/etc/named.conf`:

   a. Especifiqueu una clàusula de directori a l'stanza d'opcions. Això permetrà que els fitxers de dades `named` utilitzin camins d'accés relatius al directori `/usr/local/domain`. En aquest escenari s'ha afegit el següent:

      ```
      options {
          directory "/usr/local/domain";
      };
      ```

Si trieu que no voleu especificar un directori aquí, el dimoni **named** els fitxers de dades necessaris se cercaran al directori /etc.

b. Per permetre que les dades dels registres s'emmagatzemin a la memòria cau fora de les zones definides, especifiqueu el nom del fitxer de zona de suggeriment per al servidor de noms.

```
zone "." IN {
    type hint;
    file "named.ca";
};
```

c. Especifiqueu les clàusules de la zona d'esclau. Cada stanza inclou el tipus de zona, un nom de fitxer en el qual el servidor de noms pot fer una còpia de seguretat de les seves dades i l'adreça IP del servidor de noms mestre, des del qual el servidor de noms esclau replicarà els seus fitxers de dades. En aquest cas, hem afegit les següents clàusules de la zona d'esclau:

```
zone "abc.aus.century.com" IN {
    type slave;
    file "named.abc.data.bak";
    masters { 192.9.201.1; };
};
zone "201.9.192.in-addr.arpa" IN {
    type slave;
    file "named.abc.rev.bak";
    masters { 192.9.201.1; };
};
```

d. Per admetre la resolució de l'adreça de xarxa de bucle de retorn, especifiqueu una zona de tipus *mestre* amb un origen named.abc.local, així com el domini del qual el servidor de noms n'és responsable.

```
zone "0.0.127.in-addr.arpa" in {
    type master;
    file "named.abc.local";
};
```

Després d'editar el fitxer, deseu-lo i tanqueu-lo.

2. Editeu el fitxer /usr/local/domain/named.ca.

   Aquest fitxer conté el servidor d'adreces que és el servidor de domini de root de la xarxa. En aquest escenari s'ha afegit el següent:

```
; servidors de noms de root.
.                   IN    NS    relay.century.com.
relay.century.com.   3600000    IN    A     129.114.1.2
```

   Després d'editar el fitxer, deseu-lo i tanqueu-lo.

3. Obriu el fitxer /usr/local/domain/named.abc.local. En aquest escenari s'ha afegit el següent:

   - L'inici d'autoritat (SOA) de la zona i la informació de la duració per defecte:

```
$TTL 3h    ;3 hour

@ IN SOA earth.abc.aus.century.com. gail.zeus.abc.aus.century.com.  (

                            1       ;serial
                            3600    ;refresh
                            600     ;retry
                            3600000 ;expire
                            3600    ;negative caching TTL
)
```

   - El registre del servidor de noms (NS). Inseriu un espai de tabulació al principi de la línia; el dimoni **named** substituirà l'espai de tabulació amb el nom de la zona. Per exemple:

```
<tab> IN    NS     earth.abc.aus.century.com.
```

   - El registre del punter (PTR).

```
1      IN    PTR    localhost.
```

   Després d'editar el fitxer, deseu-lo i tanqueu-lo.

4. Creeu un fitxer /etc/resolv.conf executant l'ordre següent:
   ```
   touch /etc/resolv.conf
   ```
5. Afegiu l'entrada següent al fitxer:
   ```
   nameserver 127.0.0.1
   domain abc.aus.century.com
   ```

   Després d'editar el fitxer, deseu-lo i tanqueu-lo.
6. Utilitzeu el camí d'accés ràpid de l'SMIT smit stnamed per habilitar el dimoni **named**. Així s'inicialitza el daemon cada vegada que s'engegui el sistema. Indiqueu si voleu iniciar el daemon **named** ara, quan es torni a engegar el sistema o les dues coses.

Pas 3. Configuració del servidor de noms de suggeriment

Per configurar un servidor de noms de suggeriment, o de *només de memòria cau*, utilitzeu el procediment següent, que edita una sèrie de fitxers i després utilitza l'SMIT o la línia d'ordres per iniciar el dimoni **named**.

1. Al servidor de noms de suggeriment, editeu el fitxer /etc/named.conf. Si no hi ha cap fitxer /etc/named.conf al directori /etc, executeu l'ordre següent per crear-ne un:
   ```
   touch /etc/named.conf
   ```
   Seguiu aquestes instruccions per configurar el fitxer /etc/named.conf:
   a. Especifiqueu una clàusula de directori a l'stanza d'opcions. Això permetrà que els fitxers de dades named utilitzin camins d'accés relatius al directori /usr/local/domain. En aquest escenari s'ha afegit el següent:
      ```
      options {
          directory "/usr/local/domain";
      };
      ```
   b. Per admetre la resolució de l'adreça de xarxa de bucle de retorn, especifiqueu una zona de tipus *mestre* amb un origen named.abc.local, així com el domini del qual el servidor de noms n'és responsable. En aquest exemple, la paraula clau del directori d'opcions s'ha especificat al fitxer /etc/named.conf.
      ```
      zone "0.0.127.in-addr.arpa" IN {
          type master;
         file "named.abc.local";
      };
      ```
   c. Especifiqueu el nom del fitxer de la zona de memòria cau. Per exemple:
      ```
      zone "." IN {
          type hint;
          file "named.ca";
      };
      ```

   Després d'editar el fitxer, deseu-lo i tanqueu-lo.
2. Editeu el fitxer /usr/local/domain/named.ca.

   Aquest fitxer conté les adreces dels servidors que són servidors de noms autoritzats pel domini de root de la xarxa. Per exemple:
   ```
   ; servidors de noms de root.
   .                   IN    NS    relay.century.com.
   relay.century.com.   3600000    IN    A     129.114.1.2
   ```

   Després d'editar el fitxer, deseu-lo i tanqueu-lo.
3. Editeu el fitxer /usr/local/domain/named.local. En aquest escenari s'ha afegit la informació següent a aquest fitxer:
   - L'inici d'autoritat (SOA) de la zona i la informació de la duració per defecte:
     ```
     $TTL 3h    ;3 hour

     @ IN    SOA     venus.abc.aus.century.com. gail.zeus.abc.aus.century.com. (
     ```

```
                                1       ;serial
                                3600    ;refresh
                                600     ;retry
                                3600000 ;expire
                                3600    ;negative caching TTL
)
```

- El registre del servidor de noms (NS). Inseriu un espai de tabulació al principi de la línia; el dimoni **named** substituirà l'espai de tabulació amb el nom de la zona:

  ```
  <tab> IN    NS     venus.abc.aus.century.com.
  ```

- El registre del punter (PTR).

  ```
  1      IN    PTR    localhost.
  ```

Després d'editar el fitxer, deseu-lo i tanqueu-lo.

4. Creeu un fitxer `/etc/resolv.conf` executant l'ordre següent:

   ```
   touch /etc/resolv.conf
   ```

5. Afegiu l'entrada següent al fitxer:

   ```
   nameserver 127.0.0.1
   domain abc.aus.century.com
   ```

   Després d'editar el fitxer, deseu-lo i tanqueu-lo.

6. Utilitzeu el camí d'accés ràpid de l'SMIT `smit stnamed` per habilitar el dimoni **named**. Així s'inicialitza el daemon cada vegada que s'engegui el sistema. Indiqueu si voleu iniciar el daemon **named** ara, quan es torni a engegar el sistema o les dues coses.

Quan reinicieu, la configuració d'IPv6 s'establirà. Repetiu aquest procés per a cada amfitrió.

Configuració d'un servidor de correu de domini:

La configuració d'un servidor de correu de domini proporciona a usuaris externs de la vostra organització un mètode simple d'adreçament de correu als vostres usuaris. És a dir, sense un servidor de correu de domini, l'adreça de correu ha d'especificar un amfitrió particular de la vostra organització.

Per exemple, `santi@lluna.widget.com`, en què `widget.com` és el nom de domini de la vostra organització i `lluna` és l'amfitrió que fa servir el `santi`. Però amb un servidor de correu de domini, els usuaris externs de la vostra organització només haurien d'especificar el nom d'usuari i el nom de domini, sense que hagin de saber quin amfitrió fa servir l'usuari, per exemple, `santi@widget.com`.

Per configurar un servidor de correu de domini, utilitzeu el procediment següent.

1. Creeu un enregistrament intercanviador de correu (MX) i un enregistrament d'adreces (A) pel sevidor de correu `black.widget.com`:

   ```
   widget.com           IN    MX     10 black.widget.com
   widget.com           IN     A     192.10.143.9
   black.widget.com     IN     A     192.10.143.9
   ```

2. Editeu el fitxer `sendmail.cf` del servidor de correu (`black.widget.com`) per afegir-hi els àlies de domini (la classe **w**):

   ```
   Cw $w $?D$w.$D$. widget.com
   ```

3. Els clients de correu han de saber on enviar el correu que no sigui local. Per tant, editeu el fitxer `sendmail.cf` a cada client per apuntar-lo al servidor de correu (la macro **S**):

   ```
   DRblack.widget.com
   ```

4. Utilitzeu l'opció **NameServOpt** per configurar el daemon **sendmail** de manera que tothom pugui utilitzar els enregistraments MX definits al servidor de noms `puig.widget.com`.
5. Afegiu àlies per usuaris del domini que no tinguin comptes al sevidor de correu utilitzant el fitxer d'àlies, per exemple:

```
santi:santi@lluna.widget.com
david:david@estel.widget.com
judit:judit@sol.widget.com
```

Nota: Els enregistraments de bústia (MB) poden fer la mateixa funció.

6. El número de sèrie de l'enregistrament de recursos SOA s'ha d'incrementar perquè la base de dades ha estat modificada.
7. Renoveu la base de dades del servidor de noms mitjançant l'ordre `refresh -s named`.
8. En els clients, executeu l'ordre `refresh -s sendmail` perquè els canvis entrin en vigor.

Hi ha altres mètodes per configurar un servidor de correu de domini. Aquests procediments impliquen fer servir els enregistraments de bústia (MB), canvi de nom de correu (MR) i grup de correu (MG).

Configuració d'un servidor de correu de domini utilitzant els enregistraments de bústia:

Utilitzeu el procediment següent per configurar un servidor de correu de domini utilitzant els enregistraments de bústia.

1. Definiu un enregistrament de bústia (MB) per a cada usuari del domini. Afegiu entrades del tipus:

   ```
   santi IN MB lluna.widget.com.
   ```

   al fitxer `/usr/local/domain/named.abc.data` de l'amfitrió `puig.widget.com`. Aquestes entrades identifiquen al servidor de correu `blanc.widget.com` on s'ha d'enviar el correu de cada usuari del domini.
2. Configureu el daemon **sendmail** del servidor de correu `blanc.widget.com` per utilitzar els enregistraments MB definits al servidor de noms `puig.widget.com`. Utilitzeu l'opció **NameServOpt**.
3. Augmenteu el número de sèrie de l'enregistrament de recursos SOA perquè la base de dades s'ha modificat.
4. Renoveu la base de dades del servidor de noms executant l'ordre `refresh -s named`.
5. Escriviu l'ordre `refresh -s sendmail` perquè els canvis entrin en vigor.

Definició un enregistrament de canvi de noms de correu per un usuari:

Utilitzeu el procediment següent per definir un enregistrament de canvi de noms de correu.

1. Editeu el fitxer `/usr/local/domain/named.abc.data` al vostre servidor de noms de domini.
2. Afegiu un enregistrament MR (Mail Rename) per a cada àlies. Per exemple, si un usuari `antoni` té l'àlies `toni`, l'enregistrament de canvi de nom és:

   ```
   toni IN MR antoni
   ```

   Aquest enregistrament fa que totes les adreces de correu que van a `toni` es lliurin a `antoni`. Cada enregistrament MR s'ha d'entrar en una línia sola.
3. El número de sèrie de l'enregistrament de recursos SOA s'ha d'incrementar perquè la base de dades ha estat modificada.
4. Renoveu la base de dades del servidor de noms escrivint l'ordre `refresh -s named`.
5. Escriviu l'ordre `refresh -s sendmail` perquè els canvis entrin en vigor.

Definició dels enregistraments de membres del grup de correu:

Utilitzeu el procediment següent per definir els enregistraments dels membres del grup de correu.

1. Editeu el fitxer `/usr/local/domain/named.abc.data` al servidor de noms de domini.
2. Afegiu enregistraments MG per cada grup de correu (MG). Els enregistraments MG funcionen igual que el fitxer `/etc/aliases`, conservant els àlies al servidor de noms. Per exemple:

```
users IN HINFO users-request widget.com
users IN MG santi
users IN MG david
users IN MG judit
```

Aquest exemple fa que el tot el correu adreçat a `users@widget.com` es lliuri a `santi`, `david` i `judit`. Escriviu cada enregistrament MG en una línia per si mateix.

Nota: Els usuaris `santi`, `david` i `judit` han de tenir definits enregistraments MB.

3. El número de sèrie de l'enregistrament de recursos SOA s'ha d'incrementar perquè la base de dades ha estat modificada.
4. Renoveu la base de dades del servidor de noms escrivint l'ordre `refresh -s named`.
5. Escriviu l'ordre `refresh -s sendmail` perquè els canvis entrin en vigor.

Definició dels enregistraments de l'intercanviador de correu:

Utilitzeu el procediment següent per definir els enregistraments de l'intercanviador de correu.

1. Editeu el fitxer `/usr/local/domain/named.abc.data` al vostre servidor de noms de domini.
2. Afegiu enregistraments d'intercanviador de correu (MX) per a cada màquina que no estigui connectada directament a la vostra xarxa i a la que vulgueu reenviar correu. Per exemple, si el correu enviat als usuaris de `lila.widget.com` s'hagués de reenviar a `oficina.correus.widget`, els enregistrament MX s'assemblarà al següent:

   ```
   lila.widget.com IN MX 0 oficina.correus.widget.
   ```

   Heu d'especificar els noms de l'amfitrió i de les màquines quan utilitzeu enregistraments MX. Escriviu cada enregistrament MG en una línia per si mateix. Podeu utilitzar comodins, per exemple:

   ```
   *.widget.com IN MX 0 oficina.correus.widget.
   ```

   En aquest exemple el que passa és que el correu enviat a un amfitrió desconegut (un amfitrió sense cap enregistrament MX explícit) del domini `widget.com` es reenviarà a `oficina.correus.widget`.

   Nota: Els enregistraments MX comodins no són adequats per utilitzar-los a Internet.
3. El número de sèrie de l'enregistrament de recursos SOA s'ha d'incrementar perquè la base de dades ha estat modificada.
4. Renoveu la base de dades del servidor de noms escrivint l'ordre `refresh -s named`.
5. Escriviu l'ordre `refresh -s sendmail` perquè els canvis entrin en vigor.

Configuració d'un reenviador

Per configurar un servidor remitent utilitzeu el procediment següent, que edita una sèrie de fitxers i després utilitza l'SMIT o la línia d'ordres per iniciar el dimoni **named**.

1. Editeu el fitxer `/etc/named.conf`. Si no hi ha cap fitxer `named.conf` al directori `/etc`, copieu el fitxer d'exemple `/usr/samples/tcpip/named.conf` al directori `/etc` i editeu-lo. Consulteu l'apartat "Format de fitxers named.conf pel TCP/IP" a *Files Reference* per obtenir més informació i un exemple detallat d'un fitxer de configuració.
   - Especifiqueu una línia dels reenviadors a la stanza d'opcions del fitxer `/etc/named.conf` que llista les adreces IP dels servidors de noms que haurien de rebre les sol•licituds reenviades. Per exemple:

     ```
     options {
         ...
         directory "/usr/local/domain";
         forwarders { 192.100.61.1; 129.35.128.222; };
         ...
     };
     ```
   - Especifiqueu la zona de bucle de retorn. Per exemple:

     ```
     zone "0.0.127.in-addr.arpa" in {
         type master;
         file "named.abc.local";
     };
     ```

- Especifiqueu la zona de suggeriment. Per exemple:

```
zone "." IN {
    type hint;
    file "named.ca";
};
```

2. Editeu el fitxer `/usr/local/domain/named.ca`. Consulteu l'apartat "Format de fitxers de memòria cache DOMAIN pel TCP/IP" a *Files Reference* per obtenir més informació i un exemple detallat d'un fitxer de memòria cau.

   Aquest fitxer conté les adreces dels servidors que són servidors de noms autoritzats pel domini de root de la xarxa. Per exemple:

```
; servidors de noms de root.
.                   IN    NS    relay.century.com.
relay.century.com.   3600000    IN    A     129.114.1.2
```

   Nota: Totes les línies d'aquest fitxer han de tenir el format d'enregistrament de recursos estàndard.

3. Editeu el fitxer `/usr/local/domain/named.abc.local`. Consulteu la secció Format de fitxer de dades local de DOMINI per a TCP/IP al *Files Reference* per obtenir més informació i un exemple d'un fitxer de dades local més detallat.

   a. Especifiqueu l'inici de l'autorització (SOA) de la zona i la informació de duració per defecte. Per exemple:

```
$TTL 3h    ;3 hores

@ IN    SOA     venus.abc.aus.century.com. gail.zeus.abc.aus.century.com. (

                            1       ;serial
                            3600    ;refresh
                            600     ;retry
                            3600000 ;expire
                            86400   ;negative caching TTL
)
```

   b. Especifiqueu l'enregistrament del servidor de noms (NS). Per exemple:

```
<tab> IN    NS      venus.abc.aus.century.com.
```

   c. Especifiqueu l'enregistrament punter (PTR).

```
1       IN    PTR    localhost.
```

   Nota: Totes les línies d'aquest fitxer han de tenir el format d'enregistrament de recursos estàndard.

4. Creeu un fitxer `/etc/resolv.conf` escrivint l'ordre següent:

```
touch /etc/resolv.conf
```

   La presència d'aquest fitxer indica que l'amfitrió hauria d'utilitzar un servidor de noms i no el fitxer `/etc/hosts` per la resolució de noms.

   De forma alternativa, el fitxer `/etc/resolv.conf` pot contenir l'entrada següent:

```
nameserver 127.0.0.1
```

   L'adreça `127.0.0.1` és l'adreça de bucle de retorn que fa que l'amfitrió accedeixi ell mateix com a servidor de noms. El fitxer `/etc/resolv.conf` també pot contenir una entrada com la següent:

```
domain domainname
```

   A l'exemple anterior, el valor *domainname* és `austin.century.com`.

5. Dueu a terme un dels passos següents:
   - Habiliteu el daemon **named** utilitzant el camí d'accés ràpid de la SMIT `smit stnamed`. Així s'inicialitza el daemon cada vegada que s'engegui el sistema. Indiqueu si voleu iniciar el daemon **named** ara, quan es torni a engegar el sistema o les dues coses.
   - Editeu el fitxer `/etc/rc.tcpip`. Descomenteu la línia del daemon **named** eliminant-ne el símbol de comentari (#) a la línia següent:

```
#start /etc/named "$src_running"
```

Així s'inicialitza el daemon cada vegada que s'engegui el sistema.

6. Si trieu no inicialitzar el daemon indicat mitjançant la SMIT, inicieu el daemon per aquesta sessió escrivint l'ordre següent:

```
startsrc -s named
```

Configuració d'un servidor de noms de només reenviament

Per configurar un servidor de noms que només sigui remitent, utilitzeu el procediment següent, que edita una sèrie de fitxers i després utilitza l'SMIT o la línia d'ordres per iniciar el dimoni **named**.

Nota: Podeu obtenir una configuració similar sense executar cap servidor de noms de només reenviament. Creeu, en canvi, un fitxer `/etc/resolv.conf` que contingui línies del servidor de noms que apuntin als reenviadors que volgueu utilitzar.

1. Editeu el fitxer `/etc/named.conf`. Si no hi ha cap fitxer `named.conf` al directori `/etc`, copieu el fitxer d'exemple `/usr/samples/tcpip/named.conf` al directori `/etc` i editeu-lo. Consulteu l'apartat Format de fitxers named.conf pel TCP/IP a *Files Reference* per obtenir més informació o un exemple detallat d'un fitxer de configuració.
   - Especifiqueu els reenviador i les línies només de reenviament a la stanza d'opcions del fitxer `/etc/named.conf` que llista les adreces ID dels servidors de nom que reben les sol•licitud reenviades. Per exemple:

     ```
     options {
         ...
         directory "/usr/local/domain";
         forwarders { 192.100.61.1;  129.35.128.222; };
         forward only;
         ...
     };
     ```

   - Especifiqueu la zona de bucle de retorn. Per exemple:

     ```
     zone "0.0.127.in-addr.arpa" in {
         type master;
         file "named.abc.local";
     };
     ```

   - Especifiqueu la zona de suggeriment. Per exemple:

     ```
     zone "." IN {
         type hint;
         file "named.ca";
     };
     ```

2. Editeu el fitxer `/usr/local/domain/named.ca`. Per exemple: Consulteu l'apartat Format de fitxers de memòria cache DOMAIN pel TCP/IP a *Files Reference* per obtenir més informació i un exemple detallat d'un fitxer de memòria cau. Aquest fitxer conté les adreces dels servidors que són servidors de noms autoritzats pel domini de root de la xarxa.

   ```
   ; servidors de noms de root.
   .                   IN    NS    relay.century.com.
   relay.century.com.   3600000    IN    A     129.114.1.2
   ```

   Nota: Totes les línies d'aquest fitxer han de tenir el format d'enregistrament de recursos estàndard.

3. Editeu el fitxer `/usr/local/domain/named.abc.local`. Consulteu la secció Format de fitxer de dades local de DOMINI per a TCP/IP al *Files Reference* per obtenir més informació i un exemple d'un fitxer de dades local més detallat.
   a. Especifiqueu l'inici de l'autorització (SOA) de la zona i la informació de duració per defecte. Per exemple:

      ```
      $TTL 3h    ;3 hores

      @ IN    SOA     venus.abc.aus.century.com. gail.zeus.abc.aus.century.com. (

                                1       ;serial
                                3600    ;refresh
      ```

```
                                600     ;retry
                                3600000 ;expire
                                86400   ;negative caching TTL
)
```

b. Especifiqueu l'enregistrament del servidor de noms (NS). Per exemple:

```
<tab> IN    NS     venus.abc.aus.century.com.
```

c. Especifiqueu l'enregistrament punter (PTR).

```
1      IN    PTR    localhost.
```

Nota: Totes les línies d'aquest fitxer han de tenir el format d'enregistrament de recursos estàndard.

4. Creeu un fitxer `/etc/resolv.conf` escrivint l'ordre següent:

   ```
   touch /etc/resolv.conf
   ```

   La presència d'aquest fitxer indica que l'amfitrió hauria d'utilitzar un servidor de noms i no el fitxer `/etc/hosts` per la resolució de noms.

   De forma alternativa, el fitxer `/etc/resolv.conf` pot contenir l'entrada següent:

   ```
   nameserver 127.0.0.1
   ```

   L'adreça `127.0.0.1` és l'adreça de bucle de retorn que fa que l'amfitrió accedeixi ell mateix com a servidor de noms. El fitxer `/etc/resolv.conf` també pot contenir una entrada com ara:

   ```
   domain domainname
   ```

   A l'exemple anterior, el valor *domainname* és `austin.century.com`.

5. Dueu a terme un dels passos següents:
   - Habiliteu el daemon **named** utilitzant el camí d'accés ràpid de la SMIT `smit stnamed`. Així s'inicialitza el daemon cada vegada que s'engegui el sistema. Indiqueu si voleu iniciar el daemon **named** ara, quan es torni a engegar el sistema o les dues coses.
   - Editeu el fitxer `/etc/rc.tcpip`. Descomenteu la línia del daemon **named** eliminant-ne el símbol de comentari (#) a la línia següent:

     ```
     #start /etc/named "$src_running"
     ```

     Així s'inicialitza el daemon cada vegada que s'engegui el sistema.

6. Si trieu no inicialitzar el daemon **named** mitjançant la SMIT, inicieu el daemon per aquesta sessió escrivint:

   ```
   startsrc -s named
   ```

Configuració d'un amfitrió perquè utilitzi un servidor de noms

Per configurar un amfitrió perquè utilitzi un servidor de noms, feu servir aquest procediment.

1. Creeu un fitxer `/etc/resolv.conf` executant l'ordre següent:

   ```
   touch /etc/resolv.conf
   ```

2. A la primera línia del fitxer `/etc/resolv.conf`, escriviu la paraula `domain` seguida del nom complet del domini al qual es troba l'amfitrió. Per exemple:

   ```
   domain abc.aus.century.com
   ```

3. En una línia en blanc que estigui sota la línia `domain`, escriviu la paraula `nameserver`, seguida al menys d'un espai, seguida de l'adreça amb notació decimal amb punt d'Internet del servidor de noms que l'amfitrió ha d'utilitzar (el servidor de noms ha de servir el domini indicat mitjançant la sentència `domain`). Podeu tenir fins a 3 entrades de servidors de noms. Per exemple, el vostre fitxer `/etc/resolv.conf` por tenir les entrades:

   ```
   servidor_de_noms 192.9.201.1
   servidor_de_noms 192.9.201.2
   ```

   El sistema llegeix els servidors de nom en l'ordre en què apareixen a la llista.

   ```
   search domainname_list
   ```

Una altra possibilitat és que la paraula clau es pugui fer servir per especificar l'ordre en què el solucionador consultarà la llista de dominis. En aquest cas, els valors `domainname_list` són `abc.aus.century.com` i `aus.century.com`. El valor `domainname_list` podria contenir un màxim de cadenes de 1024 caràcters, separades per un espai.

4. Pressuposem que el servidor de noms estigui funcionant, podeu provar la comunicació entre l'amfitrió i el servidor de noms escrivint l'ordre següent:

   ```
   host nom_sistema_principal
   ```

   Utilitzeu el nom d'un amfitrió que resoldria el servidor de noms per veure si el procés funciona. La sortida que rebeu hauria de ser similar a la següent:

   ```
   puig.abc.aus.century.com is 129.35.145.95
   ```

A la taula següent hi trobareu altres tasques de configuració.

Taula 62. Configuració d'un amfitrió perquè utilitzi tasques del servidor de noms

Tasca	Camí d'accés ràpid de la SMIT	Ordre o fitxer
Crear un fitxer `/etc/resolv.conf`	`smit stnamerslv2`	create i edit `/etc/resolv.conf`[1]
Llistar tots els servidors de noms que utilitza un amfitrió	`smit lsnamerslv`	view `/etc/resolv.conf`
Afegir un servidor de noms	`smit mknamerslv`	edit `/etc/resolv.conf`[2]
Eliminar un servidor de noms	`smit rmnamerslv`	edit `/etc/resolv.conf`
Iniciar/Reiniciar la utilització de la resolució de noms de domini	`smit stnamerslv`	
Aturar la utilització de la resolució de noms de domini	`smit spnamerslv`	
Canviar/Mostrar el domini	`smit mkdomain`	edit `/etc/resolv.conf`
Eliminar el domini	`smit rmdomain`	edit `/etc/resolv.conf`

Informació relacionada

Fitxer netsvc.conf

Zones dinàmiques al servidor de noms DNS

L'ordre **named** permet dur a terme actualitzacions dinàmiques. Cal configurar la base de dades named i els fitxers de configuració perquè les màquines client puguis emetre actualitzacions. Una zona es pot establir en dinàmica o estàtica. El valor per defecte de la zona és estàtica.

Perquè una zona sigui dinàmica, heu d'afegir la paraula clau **allow-update** a la stanza de la zona en qüestió al fitxer `/etc/named.conf`. La paraula clau **allow-update** especifica una llista de coincidències d'adreces d'Internet que defineix els amfitrions permesos perquè executin actualitzacions. Consulteu l'apartat Format de fitxers named.conf pel TCP/IP a *Files Reference* per obtenir més informació o un exemple detallat d'un fitxer de configuració. A l'exemple següent, tots els amfitrions podran actualitzar la zona dinàmica:

```
zone "abc.aus.century.com" IN {
    type master;
    file "named.abc.data";
    allow-update { any; };
};
```

Després que una zona s'hagi marcat com a dinàmica, es poden iniciar tres modalitats de seguretat:

Element	Descripció
Insegura	Permet que qualsevol persona en qualsevol moment actualitzi informació de la zona. **Atenció:** No es recomana la utilització d'aquesta modalitat. Pot implicar pèrdua de dades, intercepció de dades i frustració de l'usuari. Al menys, una zona insegura hauria d'estar limitada només a actualitzacions d'adreces específiques d'Internet.
Controlada	Permet crear nova informació i substituir la informació existent. Aquesta és probablement la modalitat més fàcil d'utilitzar per un entorn de transició segur. Aquesta modalitat també requereix que totes les actualitzacions d'entrada portin la indicació de l'hora i que tinguin signatures en clau.
Preassegurada	Requereix que totes les actualitzacions d'informació existent es substitueixin per informació similar. No permet la creació d'informació nova. Aquesta modalitat també requereix que totes les actualitzacions d'entrada portin la indicació de l'hora i que tinguin signatures en clau.

Una zona dinàmica pren per defecte la modalitat insegura. Per utilitzar una de les altres modalitats, escriviu `controlada` o `preassegurada` després de la paraula clau **update-security** de la stanza de la zona al fitxer `/etc/named.conf`. D'aquesta manera s'indica al servidor **named** el nivell de seguretat que ha d'utilitzar amb aquesta zona. Per exemple:

```
zone "abc.aus.century.com" IN {
    type master;
    file "named.abc.data";
    allow-update { any; };
    update-security controlada;
};
```

Després de triar una modalitat, caldrà modificar el nivell de seguretat dels fitxers de dades actuals. En la modalitat insegura, els fitxers de dades es fan servir "tal qual". Per les modalitats controlada o preassegurada, heu de generar un conjunt de parelles claus de noms de servidor mestre/amfitrió per cada nom de la zona. Això es fa amb l'ordre **nsupdate** utilitzant l'opció **-g**. Aquesta ordre genera una parella clau (una clau pública i privada). Aquestes claus són necessàries per signar amb fidelitat les actualitzacions. Després de generar totes les claus per la llista de noms de zona, haureu d'afegir-les al fitxer de dades. El format KEY és el següent:

Índex ttl Classe Tipus Senyaladors_clau Protocol Algoritme Dades_clau

en què:

Element	Descripció
Índex	Especifica el nom utilitzat per fer referència a les dades de la zona.
ttl	Especifica el valor de duració (TTL - time-to-live) per aquestes dades. Es tracta d'un camp opcional.
Classe	Especifica la classe de les dades. Depèn de la zona però normalment és IN.
Tipus	Indica el tipus d'enregistrament. En aquest cas, és KEY.
Senyaladors_clau	Ofereix informació sobre la clau. 0x0000 defineix l'enregistrament clau típic que utilitza un amfitrió. 0x0100 defineix l'enregistrament clau associat al nom de la zona.
Protocol	Especifica el protocol que s'ha d'utilitzar. Normalment, només n'hi ha un, `0`.
Algoritme	Especifica l'algorisme de la clau. Normalment, només n'hi ha un, 1. Es tracta del mètode d'autenticació MD5 públic/privat.
Dades_clau	Indica la clau en representació base64. L'ordre **nsupdate** genera tant claus públiques com privades en representació base64. La clau pública es llista al final del fitxer de sortida.

Per exemple, per tal de garantir la seguretat en un nom d'amfitrió d'una zona dinàmica, cal afegir al fitxer de la zona (la zona que conté el nom de l'amfitrió) una línia similar a la següent.

```
ossos    4660    IN    KEY    0x0000    0    1    AQOtg......
```

L'exemple anterior indica que `ossos` té definit un enregistrament KEY. Algú que volia actualitzar `ossos` hauria de signar-ne l'actualització amb la clau privada i fer-la coincidir amb la clau pública de la base de dades. Perquè l'ordre sigui satisfactòria **nsupdate**, la clau privada s'ha de col•locar al client en un fitxer de claus (per defecte, a `/etc/keyfile`). Hauria de tenir aquest format:

nom_sistema_principal nom_mestre base64 clau

Fa falta una entrada KEY similar en la secció de definició de zones. *Una clau de zona és necessària per les modalitats controlada i preassegurada si no, la modalitat es considerarà insegura.* Això es pot dur a terme tal com mostrava l'exemple anterior, `ossos`, però la clau privada s'ha de deixar perquè l'administrador l'utilitzi amb la modalitat administrativa de l'ordre **nsupdate**.

1. Per generar una parella de claus utilitzant l'ordre **nsupdate**, escriviu el següent:

   ```
   nsupdate -g -h Nom_zona -p Nom_Servidor -k Fitxer_Clau_Admin
   ```

   D'aquesta manera es genera una clau per la zona. En aquest exemple, **nsupdate** s'enllaça a **nsupdate4**, que es pot fer escrivint el següent:

   ```
   ln -fs /usr/sbin/nsupdate4 /usr/sbin/nsupdate
   ```

2. Col•loqueu la darrera clau de la parella a la secció del principi per la zona, tal com es mostra a continuació:

   ```
   IN     KEY     0x0100  0  1  Key
   ```

   L'entrada pel fitxer `named.abc.data` serà la següent:

   ```
   $TTL 3h    ;3 hour

   @ IN    SOA     venus.abc.aus.century.com. gail.zeus.abc.aus.century.com. (
                   1       ;serial
                   3600    ;refresh
                   600     ;retry
                   3600000 ;expire
                   86400   ;negative caching TTL
   )
           IN      NS      venus.abc.aus.century.com.
           IN      KEY     0x0100  0 1 AQPlwHmIQeZzRk6Q/nQYhs3xwnhfTgF/
                           8YlBVzKSoKxVKPNLINnYW0mB7attTcfhHaZZcZr4u/
                           vDNikKnhnZwgn/
   venus   IN      A       192.9.201.1
   terra   IN      A       192.9.201.5
   mart    IN      A       192.9.201.3
   ```

3. Ara la zona ja està a punt per a ser localitzada si es renova el servidor de noms. Poseu el fitxer de claus administratives al client o al servidor DHCP que actualitza la zona. La clau de zona que es troba al fitxer de claus administratives es pot utilitzar per a dur a terme actualitzacions i operacions de manteniment al servidor de noms.

Seguretat BIND 9

BIND 9 ofereix Signatures de transaccions (TSIG) i Signatures (SIG) com a mesures de seguretat per a **named**.

Per defecte, el servidor de noms amb BIND 9 no permet actualitzacions dinàmiques en zones autoritzades, de forma semblant a com ho fa el de BIND 8.

BIND 9 dóna suport principalment a les Signatures de transaccions (TSIG) per a la comunicació de servidor a servidor. Això inclou missatges de consulta recursiva, de notificació i de transferència de zona. TSIG també és útil per a les actualitzacions dinàmiques. Un servidor primari d'una zona dinàmica ha d'utilitzar el control d'accés per controlar les actualitzacions, però el control d'accés basat en IP no és suficient.

Gràcies a què utilitza l'encriptació base de claus en comptes del mètode actual de llistes control d'accés, TSIG pot utilitzar-se per restringir qui pot realitzar actualitzacions en les zones dinàmiques. A diferència del mètode ACL (llista de control d'accés) d'actualitzacions dinàmiques, la clau TSIG pot distribuir-se a altres actualitzadors sense haver de modificar els fitxers de configuració del servidor de noms, la qual cosa significa que el servidor de noms no ha de tornar a llegir els fitxers de configuració.

És important tenir en compte que BIND 9 no té totes les paraules clau implementades de BIND 8. En aquest exemple, utilitzem la configuració mestra simple de BIND 8.

Nota: Per tal d'utilitzar named 9, heu de tornar a enllaçar l'enllaç simbòlic amb el daemon **named** a **named9** i **nsupdate** a **nsupdate9** executant les ordres següents:

1. `ln -fs /usr/sbin/named9 /usr/sbin/named`
2. `ln -fs /usr/sbin/nsupdate9 /usr/sbin/nsupdate`

1. Genereu la clau utilitzant l'ordre **dnssec-keygen**:

   ```
   dnssec-keygen -a HMAC-MD5 -b 128 -n HOST keyname
   ```

   - `HMAC-MD5` és l'algorisme utilitzat per l'encriptació
   - `128` és la longitud de la clau que s'utilitzarà (o nombre de bits)
   - `HOST`: `HOST` és la paraula clau de TSIG que s'utilitza per generar una clau d'amfitrió per a l'encriptació de la clau compartida.

   L´ordre

   ```
   dnssec-keygen -a HMAC-MD5 -b 128 -n HOST venus-batman.abc.aus.century.com
   ```

   generarà dos fitxers de claus, tal com s'indica a continuació:

   ```
   Kvenus-batman.abc.aus.century.com.+157+35215.key
   Kvenus-batman.abc.aus.century.com.+157+35215.private
   ```

   - `157` és l'algorisme utilitzat (HMAC-MD5)
   - `35215` és l'empremta digital, que és útil a DNNSEC ja que es permeten diverses claus per zona

2. Afegiu l'entrada a named.conf del servidor de noms mestre .

   ```
   // Clau TSIG
   key venus-batman.abc.aus.century.com. {
           algorithm hmac-md5;
           secret "+UWSvbpxHWFdNwEAdy1Ktw==";
   };
   ```

   Suposant que s'utilitza HMAC-MD5, els dos fitxers de claus contenen la clau compartida, que s'emmagatzema com l'última entrada dels fitxers. Cerqueu una forma segura de copiar la clau secreta compartida al client. No cal que copieu el fitxer de claus, només la clau secreta compartida.

   A continuació es mostra l'entrada per al fitxer `Kvenus-batman.abc.aus.century.com.+157+35215.private`:

   ```
   Private-key-format: v1.2
   Algorithm: 157 (HMAC_MD5)
   Key: +UWSvbpxHWFdNwEAdy1Ktw==
   ```

   A continuació es mostra un exemple del fitxer `named.conf` per al servidor de noms mestre. La zona `abc.aus.century.com` permet la transferència de zona i les actualitzacions dinàmiques només als servidors amb la clau `venus-batman.abc.aus.century.com`. Feu el mateix a la zona inversa, que requereix que els actualitzadors tinguin la clau compartida.

   ```
   // Clau TSIG
   key venus-batman.abc.aus.century.com. {
           algorithm hmac-md5;
           secret "+UWSvbpxHWFdNwEAdy1Ktw==";
   };

   options {
           directory "/usr/local/domain";
   };

   zone "abc.aus.century.com" in {
           type master;
           file "named.abc.data";
           allow-transfer { key venus-batman.abc.aus.century.com.;};
           allow-update{ key venus-batman.abc.aus.century.com.; };
   };
   ```

   Com que les transferències de zona ara estan restringides a les que tenen una clau, també s'ha d'editar el fitxer `named.conf` del servidor de noms esclau. Totes les sol•licituds realitzades a 192.9.201.1

(venus.abc.aus.century.com) estan signades amb una clau. Tingueu en compte que el nom de la clau (venus-batman.abc.aus.century.com.) ha de coincidir amb les dels servidors que les utilitzen.

A continuació es mostra un exemple del fitxer `named.conf` del servidor de noms esclau:

```
// Clau TSIG
key venus-batman.abc.aus.century.com. {
        algorithm hmac-md5;
        secret "+UWSvbpxHWFdNwEAdy1Ktw==";
};

server 192.9.201.1{
        keys { venus-batman.abc.aus.century.com.;};
};

options {
        directory "/usr/local/domain";
};

zone "abc.aus.century.com" IN {
    type slave;
    file "named.abc.data.bak";
    masters { 192.9.201.1; };
};
```

Signatures de transaccions BIND 9:

BIND 9 dóna suport principalment a les Signatures de transaccions (TSIG) per a la comunicació de servidor a servidor.

Això inclou missatges de consulta recursiva, de notificació i de transferència de zona. TSIG també és útil per a les actualitzacions dinàmiques. Un servidor primari d'una zona dinàmica ha d'utilitzar el control d'accés per controlar les actualitzacions, però el control d'accés basat en IP no és suficient.

Gràcies a què utilitza l'encriptació base de claus en comptes del mètode actual de llistes de control d'accés, TSIG pot utilitzar-se per restringir qui pot realitzar actualitzacions en les zones dinàmiques. A diferència del mètode ACL (llista de control d'accés) d'actualitzacions dinàmiques, la clau TSIG pot distribuir-se a altres actualitzadors sense haver de modificar els fitxers de configuració del servidor de noms, la qual cosa significa que el servidor de noms no ha de tornar a llegir els fitxers de configuració.

És important tenir en compte que BIND 9 no té totes les paraules clau implementades de BIND 8. En aquest exemple, utilitzem la configuració mestra simple de BIND 8.

Nota: Per tal d'utilitzar named 9, heu de tornar a enllaçar l'enllaç simbòlic amb el daemon **named** a **named9** i **nsupdate** a **nsupdate9** executant les ordres següents:

1. `ln -fs /usr/sbin/named9 /usr/sbin/named`
2. `ln -fs /usr/sbin/nsupdate9 /usr/sbin/nsupdate`

1. Genereu la clau utilitzant l'ordre **dnssec-keygen**:

   ```
   dnssec-keygen -a HMAC-MD5 -b 128 -n HOST keyname
   ```

   - `HMAC-MD5` és l'algorisme utilitzat per l'encriptació
   - `128` és la longitud de la clau que s'utilitzarà (o nombre de bits)
   - `HOST`: `HOST` és la paraula clau de TSIG que s'utilitza per generar una clau d'amfitrió per a l'encriptació de la clau compartida.

   L´ordre

   ```
   dnssec-keygen -a HMAC-MD5 -b 128 -n HOST venus-batman.abc.aus.century.com
   ```

   generarà dos fitxers de claus, tal com s'indica a continuació:

   ```
   Kvenus-batman.abc.aus.century.com.+157+35215.key
   Kvenus-batman.abc.aus.century.com.+157+35215.private
   ```

- 157 és l'algorisme utilitzat (HMAC-MD5)
- 35215 és l'empremta digital, que és útil a DNNSEC ja que es permeten diverses claus per zona

2. Afegiu l'entrada a named.conf del servidor de noms mestre .

```
// Clau TSIG
key venus-batman.abc.aus.century.com. {
         algorithm hmac-md5;
         secret "+UWSvbpxHWFdNwEAdy1Ktw==";
};
```

Suposant que s'utilitza HMAC-MD5, els dos fitxers de claus contenen la clau compartida, que s'emmagatzema com l'última entrada dels fitxers. Cerqueu una forma segura de copiar la clau secreta compartida al client. No cal que copieu el fitxer de claus, només la clau secreta compartida.

A continuació es mostra l'entrada per al fitxer Kvenus-batman.abc.aus.century.com.+157+35215.private:

```
Private-key-format: v1.2
Algorithm: 157 (HMAC_MD5)
Key: +UWSvbpxHWFdNwEAdy1Ktw==
```

A continuació es mostra un exemple del fitxer named.conf per al servidor de noms mestre. La zona abc.aus.century.com permet la transferència de zona i les actualitzacions dinàmiques només als servidors amb la clau venus-batman.abc.aus.century.com. Feu el mateix a la zona inversa, que requereix que els actualitzadors tinguin la clau compartida.

```
// Clau TSIG
key venus-batman.abc.aus.century.com. {
         algorithm hmac-md5;
         secret "+UWSvbpxHWFdNwEAdy1Ktw==";
};

options {
         directory "/usr/local/domain";
};
zone "abc.aus.century.com" in {
         type master;
         file "named.abc.data";
         allow-transfer { key venus-batman.abc.aus.century.com.;};
         allow-update{ key venus-batman.abc.aus.century.com.; };
};
```

Com que les transferències de zona ara estan restringides a les que tenen una clau, també s'ha d'editar el fitxer named.conf del servidor de noms esclau. Totes les sol•licituds realitzades a 192.9.201.1 (venus.abc.aus.century.com) estan signades amb una clau. Tingueu en compte que el nom de la clau (venus-batman.abc.aus.century.com.) ha de coincidir amb les dels servidors que les utilitzen.

A continuació es mostra un exemple del fitxer named.conf del servidor de noms esclau:

```
// Clau TSIG
key venus-batman.abc.aus.century.com. {
         algorithm hmac-md5;
         secret "+UWSvbpxHWFdNwEAdy1Ktw==";
};

server 192.9.201.1{
         keys { venus-batman.abc.aus.century.com.;};
};

options {
         directory "/usr/local/domain";
};

zone "abc.aus.century.com" IN {
     type slave;
     file "named.abc.data.bak";
     masters { 192.9.201.1; };
};
```

Signatura BIND 9:

BIND 9 dóna suport parcialment a les signatures de transaccions SIG de DNSSEC, tal com s'especifica a l'RFC 2535.

SIG utilitza claus públiques i privades per autenticar missatges.

Els enregistraments SIG permeten als administradors signar les dades de la seva zona, indicant així que són autèntiques.

Protecció de la zona root:

Quan s'utilitzen aquests passos per protegir la zona root, es pressuposa que els altres servidors de noms d'Internet no utilitzen BIND 9, i voleu protegir les dades de la vostra zona i permetre que altres servidors verifiquin les dades de la vostra zona.

Voleu indicar que la vostra zona (en el nostre cas `aus.century.com`) és una zona root segura i validareu les dades de zona segura que estan sota d'ella

1. Genereu les claus utilitzant l'ordre **dnssec-keygen**:

   ```
   dnssec-keygen -a RSA -b 512 -r /usr/sbin/named -n ZONE aus.century.com.
   ```

   Nota: L'encriptació RSA pot utilitzar-se com l'algorisme per generar la clau si OpenSSL està instal•lat, malgrat que primer heu de tornar a enllaçar la biblioteca DNS amb una biblioteca DNS protegida executant l'ordre següent:

   ```
   ln -fs /usr/lib/libdns_secure.a /usr/lib/libdns.a
   ```

   - ZONE: ZONE és la paraula clau de DNSSEC que s'utilitza per generar claus de zona per a l'encriptació de claus privades/públiques
   - El senyalador `r` especifica un dispositiu aleatori
2. Afegiu l'entrada de clau pública semblant al fitxer `named.conf`. L'entrada utilitzada en el nostre cas és la següent. A continuació es mostra el contingut del fitxer de claus `Kaus.century.com.+001+03254.key`.

   ```
   abc.aus.century.com. IN KEY 256 3 1
   AQOnfGEAg0xpzSdNRe7KePq3Dl4NqQiq7HkwKl6TygUfaw6vz6ldmauB4UQFcGKOyL68/
   Zv5ZnEvyB1fMTAaDLYz
   ```

   La clau pública està continguda al fitxer `Kzonename.+algor.+fingerprint.key`, o en el nostre cas `Kaus.century.com.+001+03254.key`. Heu d'eliminar la classe IN i escriure KEY així com encerclar la clau entre cometes. Un cop hagueu afegit aquesta entrada al fitxer `/etc/named.conf` i renovat el servidor de noms, la zona `aus.century.com` serà una zona root segura.

   ```
   trusted-keys {
           aus.century.com. 256 3 1 "AQOnfGEAg0xpzSdNRe7KePq3Dl4NqQiq7HkwKl6Tyg
   Ufaw6vz6ldmauB 4UQFcGKOyL68/Zv5ZnEvyB1fMTAaDLYz";
   };
   options {
           directory "/usr/local/domain";
   };

   zone "abc.aus.century.com" in {
           type master;
           file "named.abc.data.signed";
           allow-update{192.9.201.1;};
   };
   ```

Aplicació de la cadena de confiança:

Ara que teniu una zona root protegida, podeu protegir la resta de les zones fill. En aquest cas, treballem per protegir la zona `abc.aus.century.com`.

Efectueu els passos següents per protegir la resta de zones fill:

1. Genereu les parelles de claus utilitzant l'ordre **dnssec-keygen**:

   ```
   dnssec-keygen -a RSA -b 512 -r /usr/sbin/named -n ZONE abc.aus.century.com.
   ```

   El senyalador `r` especifica un fitxer d'entrada aleatori.
2. Genereu un conjunt de claus executant l'ordre **dnssec-makekeyset**:

   ```
   dnssec-makekeyset -t 172800 Kabc.aus.century.com.+001+11515.key
   ```

   on *Kabc.aus.century.com.+001+11515.key* és la vostra pròpia clau pública.

   Això crea un fitxer de conjunt de claus anomenat `keyset-abc.aus.century.com`.
3. Envieu aquest fitxer de conjunt de claus a la zona pare per signar-la. En aquest cas, la nostra zona pare és la zona root segura `aus.century.com`.
4. El pare ha de signar la clau utilitzant la seva clau privada.

   ```
   dnssec-signkey keyset-abc.aus.century.com. Kaus.century.com.+001+03254.private
   ```

   Això generarà un fitxer anomenat `signedkey-abc.aus.century.com` i el pare haurà d'enviar aquest fitxer de tornada a la zona fill.
5. En el servidor de noms fill per a la zona `abc.aus.century.com`, afegiu `$INCLUDE Kabc.aus.century.com.+001+11515.key` al fitxer de zona sense format `named.abc.data`. Recordeu col•locar el fitxer `signedkey-abc.aus.century.com` a la mateixa ubicació que el fitxer de zona `named.abc.data`. Quan la zona se signi al pas següent, el programa sabrà que ha d'incloure `signedkey-abc.aus.century.com`, que ha rebut del pare.

   ```
   $TTL 3h    ;3 hour

   @ IN    SOA     venus.abc.aus.century.com. gail.zeus.abc.aus.century.com. (
                   1       ;serial
                   3600    ;refresh
                   600     ;retry
                   3600000 ;expire
                   86400   ;negative caching TTL
   )
   $INCLUDE Kabc.aus.century.com.+001+03254.key
   ```
6. Signeu la zona utilitzant l'ordre **dnssec-signzone**:

   ```
   dnssec-signzone -o abc.aus.century.com. named.abc.data
   ```
7. Modifiqueu el fitxer **named.conf** de la zona fill `abc.aus.century.com` per tal d'utilitzar el nou fitxer de zona signat (`named.abc.data.signed`). Per exemple:

   ```
   options {
           directory "/usr/local/domain";
   };

   zone "abc.aus.century.com" in {
           type master;
           file "named.abc.data.signed";
           allow-update{192.9.201.1;};
   };
   ```
8. Renoveu el servidor de noms.

Per obtenir informació sobre resolució de problemes, consulteu l'apartat “Problemes de la traducció de noms” a la pàgina 419.

Planificació i configuració per la resolució de noms LDAP (esquema d'IBM SecureWay Directory schema)

El **Lightweight Directory Access Protocol (LDAP)** és un estàndard de mercat obert que defineix un mètode per accedir i actualitzar informació d'un directori.

Un esquema **LDAP** defineix les normes per l'ordenació de les dades. La classe d'objecte **ibm-HostTable**, part de l'esquema IBM SecureWay Directory, es pot utilitzar per emmagatzemar la informació de mapatge nom a adreça d'Internet per a cada amfitrió de la xarxa.

La classe d'objecte **ibm-HostTable** es defineix tal com s'indica a continuació:

```
Nom de classe d'objecte:     ibm-HostTable
Descripció:            L'entrada de la taula de l'amfitrió té una recopilació de mapatges de noms de
                       amfitrió a adreces IP.
OID:                   TBD
RDN:                   ipAddress
Classe d'objecte superior: top
Atributs necessaris:   host, ipAddress
Atributs opcionals:    ibm-hostAlias, ipAddressType, description
```

Les definicions de l'atribut són:

```
Nom d'atribut: ipAddress
Descripció:     Adreça IP del nom d'amfitrió de la taula d'amfitrions
OID:            TBD
Sintaxi:        caseIgnoreString
Longitud:       256
Amb valor simple: Yes
Nom atribut:    ibm-hostAlias
Descripció:     Àlies del nom d'amfitrió de la taula d'amfitrions
OID:            TBD
Sintaxi:        caseIgnoreString
Longitud:       256
Amb valor simple:  Multi-valued
Nom atribut:    ipAddressType
Descripció:    Família d'adreces de l'adreça IP (1=IPv4, 2=IPv6)
OID:            TBD
Sintaxi:        Integer
Longitud:       11
Amb valor simple: Yes
Nom d'atribut: host
Descripció:     El nom d'amfitrió d'un sistema de l'ordinador.
OID:            1.13.18.0.2.4.486
Sintaxi:        caseIgnoreString
Longitud:       256
Amb valor simple:  Multi-valued
Nom atribut:    description
Descripció:     Comentaris que proporcionen una descripció d'una entrada d'objectes d'un directori.
OID:            2.5.4.13
Sintaxi:        caseIgnoreString
Longitud:       1024
Amb valor simple:  Multi-valued
```

Utilitzeu el procediment següent per configurar el servidor **LDAP** que respecta els estàndards de l'esquema de l'IBM SecureWay Directory, per emmagatzemar la informació de l'amfitrió de mapatges nom a adreça d'Internet.

1. Afegiu un sufix al servidor **LDAP**. El sufix és el punt de partida de la base de dades d'amfitrions. Per exemple, "cn=hosts". Això es pot fer utilitzant l'eina basada en la web IBM SecureWay Directory Server Administration.
2. Creeu un fitxer LDIF (LDAP Data Interchange Format). Això es pot fer manualment o amb l'ordre **hosts2ldif**, que crea un fitxer LDIF a partir del fitxer `/etc/hosts`. Consulti l'apartat Ordre hosts2ldif per obtenir més informació. A continuació trobareu un exemple d'un fitxer LDIF:

   ```
   dn: cn=hosts
   objectclass: top
   objectclass: container
   cn: hosts
   dn: ipAddress=1.1.1.1, cn=hosts
   host: test
   ipAddress: 1.1.1.1
   ```

```
objectclass: ibm-HostTable
ipAddressType: 1
ibm-hostAlias: e-test
ibm-hostAlias: test.austin.ibm.com
description: first ethernet interface
dn: ipAddress=fe80::dead, cn=hosts
host: test
ipAddress: fe80::dead
objectclass: ibm-HostTable
ipAddressType: 2
ibm-hostAlias: test-ll
ibm-hostAlias: test-ll.austin.ibm.com
description: v6 link level interface
```

3. Importeu les dades del directori d'amfitrions del fitxer LDIF que es troba al servidor **LDAP**. Això es pot fer amb l'ordre **ldif2db** o mitjançant l'eina basada en la web IBM SecureWay Directory Server Administration.

Per configurar el client perquè pugui accedir a la base de dades dels amfitrions del servidor LDAP, utilitzant el mecanisme de l'**LDAP**, seguiu aquestes passos:

1. Creeu el fitxer `/etc/resolv.ldap`. Consulteu l'apartat Format de fitxers resolv.ldap pel TCP/IP a *Files Reference* per obtenir més informació i un exemple detallat d'un fitxer `resolv.ldap`.
2. Canvieu la resolució de noms per defecte a través de la variable d'entorn **NSORDER**, el fitxer `/etc/netsvc.conf` o el fitxer `/etc/irs.conf`. Consulteu l'apartat Format de fitxers netsvc.conf del TCP/IP o l'apartat Format de fitxers irs.conf a *Files Reference* per obtenir més informació.

Tot i que se'n dona suport, es desaprova la utilització del mecanisme `ldap`. El mecanisme `ldap` existent funciona amb l'esquema d'IBM SecureWay Directory, mentre que el `nis_ldap` (NIS_LDAP) funciona amb l'esquema RFC 2307. Es recomana utilitzar el mecanisme `nis_ldap` per comptes del mecanisme `ldap`. Per obtenir informació sobre la resolució de noms del `nis_ldap`, consulteu la publicació "Planificació i configuració de la resolució de noms NIS_LDAP (esquema RFC 2307)".

Planificació i configuració de la resolució de noms NIS_LDAP (esquema RFC 2307)

AIX 5.2 ofereix un nou mecanisme de denominació anomenat NIS_LDAP.

La diferència entre el mecanisme LDAP existent i el nou mecanisme NIS_LDAP es troba a l'esquema LDAP (el conjunt d'atributs i de classes d'objecte que determinen la manera en què s'agrupen els atributs per descriure una entitat). El mecanisme LDAP existent funciona amb el servidor LDAP compatible amb l'esquema del directori IBM SecureWay i dóna suport només al servei de denominació d'amfitrió. Els mecanismes NIS_LDAP funcionen amb el servidor LDAP compatible amb l'esquema RFC 2307 i donen suport a tots els serveis NIS: usuaris i grups, amfitrions, serveis, protocols, xarxes i grup de xarxes. RFC 2307 defineix un conjunt d'atributs i classes d'objecte que es poden utilitzar per descriure serveis d'informació de xarxa, incloent usuaris i grups.

- Per configurar el servidor LDAP, haureu de configurar el servidor LDAP i migrar les dades necessàries al servidor.
  1. Utilitzeu l'ordre **mksecldap** per configurar un servidor. El mecanisme `nis_ldap` funciona només amb l'esquema RFC 2307. Mentre es configura el servidor LDAP, s'hauria d'invocar l'ordre **mksecldap** amb l'opció `-S rfc2307` o `-S rfc2307aix` (no l'opció `-S aix`, la qual especifica l'esquema del directori IBM SecureWay). Per defecte, l'ordre **mksecldap** migra els usuaris i grups definits al sistema local al servidor LDAP. Si desitgeu inhabilitar aquesta migració, utilitzeu l'opció `-u NONE`.

     ```
     mksecldap -s -a cn=admin -p adminpwd -S rfc2307aix
     ```

     Això configura el servidor LDAP amb el DN d'administrador `cn=admin` i la paraula clau `adminpwd`. El sufix per defecte, `cn=aixdata`, també s'afegeix al fitxer `/etc/slapd32.conf`, el fitxer de configuració del servidor LDAP.

Per defecte, l'ordre **mksecldap** migra els usuaris i grups definits al sistema local al servidor LDAP. Si desitgeu inhabilitar aquesta migració, utilitzeu l'opció `-u NONE`, la qual evita la migració d'usuaris i grups locals al servidor LDAP per tal que només es pugui afegir usuaris i grups NIS més endavant.

```
mksecldap -s -a cn=admin -p adminpwd -u NONE
```

Per obtenir més informació sobre l'ordre **mksecldap**, consulteu la descripció que apareix a *Commands Reference, Volume 3*.

2. Migreu les dades NIS. Utilitzeu l'ordre **nistoldif** des del servidor NIS per migrar els mapatges NIS al servidor LDAP. L'ordre **nistoldif** també es pot fer servir per migrar les dades de fitxers plans. Executeu l'ordre **nistoldif** en un sistema que contingui dades NIS que s'hagin de migrar al servidor LDAP.

   ```
   nistoldif -h server1.ibm.com -a cn=admin -p adminpwd -d cn=aixdata
   ```

   Això fa que es migrin els mapatges NIS del sistema local al servidor LDAP, `server1.ibm.com`. Les dades NIS es col•loquen al DN `cn=aixdata`. També podeu executar l'ordre **nistoldif** per migrar dades de fitxers plans de qualsevol sistema al servidor LDAP. Els fitxers plans s'utilitzaran per qualsevol correlació que falti del servidor NIS.

   Per obtenir més informació sobre l'ordre **nistoldif**, consulteu la descripció d'ordres que apareix a *Commands Reference, Volume 4*.

   Nota: Els noms es representen mitjançant l'atribut `cn` del servidor LDAP. L'atribut `cn` definit per RFC 2307 no reconeix majúscules i minúscules. Els noms que només es diferencien per les majúscules i minúscules es fusionaran al servidor. Les coincidències tampoc reconeixen majúscules i minúscules. Si es busca `TCP`, `tcp` o `Tcp` es retornarà l'entrada de protocol de TCP.

- Per configurar el client LDAP per accedir a noms des del servidor LDAP, executeu l'ordre **mksecldap** amb les opcions de configuració de client.

  1. L'ordre **mksecldap** desa el nom, el port, el dn d'administrador, la paraula clau i el dn de base del servidor LDAP al fitxer `/etc/security/ldap/ldap.cfg`, el qual només es pot llegir mitjançant el daemon **secldapclntd** quan es reinicia. L'ordre **mksecldap** inicia el daemon **secldapclntd** automàticament, en el cas que la configuració s'hagi realitzat correctament.

     Consulteu el fitxer `/etc/security/ldap/ldap.cfg` a *Files Reference* i el dimoni **secldapclntd** a la secció *Commands Reference, Volume 5* per obtenir més informació.

  2. L'ordre **mksecldap** afegeix el mecanisme `nis_ldap` al fitxer `/etc/netsvc.conf` i al fitxer `/etc/irs.conf` per tal que es pugui dirigir la resolució de noms a LDAP. També podeu establir manualment la variable d'entorn **NSORDER** en `nis_ldap` per utilitzar la resolució de noms NIS_LDAP.

     ```
     mksecldap -c -a cn=admin -p adminpwd -h server1.ibm.com
     ```

     Això fa que es configuri el sistema local per utilitzar el servidor LDAP `server1.ibm.com`. El DN i la paraula clau de l'administrador de servidor LDAP s'han de proporcionar per a aquest client per l'autenticació al servidor. Els fitxers `/etc/netsvc.conf` i `/etc/irs.conf` s'actualitzen per tal que la resolució de noms es resolgui a través de NIS_LDAP.

     Consulteu el format del fitxer `/etc/netsvc.conf` per TCP/IP o el format del fitxer `/etc/irs.conf` per TCP/IP que es troben a *Files Reference* per obtenir més informació.

  3. La resolució de noms per usuaris i grups no es controlen mitjançant els fitxer `/etc/netsvc.conf` ni `/etc/irs.conf`. Enlloc d'això, es realitza a través del fitxer `/etc/security/user`. Per habilitar un usuari LDAP per tal que inicií sessió a un sistema AIX, configureu les variables `SYSTEM` i `registry` de l'usuari en `LDAP` al fitxer `/etc/security/user` del sistema del client. Podeu executar l'ordre **chuser** per fer-ho.

     ```
     chuser -R LDAP SYSTEM=LDAP registry=LDAP foo
     ```

     Podeu configurar el vostre sistema per tal que permeti als usuaris LDAP iniciar sessió a un sistema. Per fer-ho, editeu el fitxer `/etc/security/user`. Afegiu `registry = files` a la stanza root. A continuació, afegiu `SYSTEM = LDAP` i `registry = LDAP` a la stanza per defecte.

Per obtenir més informació sobre l'autenticació d'usuaris, consulteu Protocol LDAP que es troba a *Security*.

Informació relacionada:

Migració de NIS a serveis de LDAP conformes amb la RFC 2307

Assignació d'adreces i de paràmetres TCP/IP - Protocol de Configuració d'Amfitrió Dinàmic

El **Transmission Control Protocol/Internet Protocol (TCP/IP)** permet la comunicació entre màquines amb adreces configurades. Una part de la càrrega que un administrador de la xarxa ha d'afrontar és l'assignació d'adreces i la distribució de paràmetres de totes les màquines de la xarxa. Normalment, aquest és un procés en què l'administrador dicta la configuració a cada usuari i així li permet configurar la màquina. No obstant això, les configuracions errònies i els malentesos poden generar trucades de servei que l'administrador ha de tractar individualment. El **Protocol de Configuració d'Amfitrió Dinàmic (DHCP)** proporciona a l'administrador de la xarxa un mètode per treure l'usuari final d'aquest problema de configuració i mantenir la configuració de la xarxa en una ubicació centralitzada.

El **DHCP** és un protocol de capa d'aplicació que permet a una màquina client de la xarxa obtenir una adreça IP i altres paràmetres de configuració del servidor. Obté informació mitjançant l'intercanvi de paquets entre un daemon del client i un altre del servidor. Actualment, la majoria de sistemes operatius proporcionen un client **DHCP** al paquet de base.

Per obtenir una adreça, el daemon de client **DHCP** (**dhcpcd**) envia un missatge de descobriment **DHCP** que el servidor rep i processa. (Es poden configurar diversos servidors a la xarxa per redundància.) Si el client té a disposició una adreça lliure, es crea un missatge d'oferiment **DHCP**. Aquest missatge conté una adreça IP i altres opcions apropiades per a aquell client. El client rep l'oferiment del servidor **DHCP** i l'emmagatzema mentre n'espera d'altres. Quan el client escull el millor oferiment, envia una sol•licitud **DHCP** que especifica l'oferiment de servidor que desitja.

Tots els servidors **DHCP** configurats reben la sol•licitud. Cadascun comprova si es tracta del servidor sol•licitat. Si no, el servidor allibera l'adreça assignada al client en qüestió. El servidor sol•licitat marca l'adreça com a assignada i torna un reconeixement **DHCP** amb el qual es completa la transacció. El client té una adreça durant el període de temps (lloguer) designat pel servidor.

Quan ja s'ha consumit la meitat del temps de lloguer, el client envia al servidor un paquet de *renovació* per estendre'l. Si el servidor accepta la renovació, envia un reconeixement **DHCP**. Si el client no rep una resposta del servidor al qual pertany la seva adreça actual, envia un paquet de revinculació **DHCP** per arribar al servidor si, per exemple, aquest darrer s'ha traslladat d'una xarxa a una altra. Si el client no ha renovat l'adreça després de tot el període de lloguer, s'atura la interfície i es reinicia el procés. Aquest cicle evita que s'assigni la mateixa adreça a diversos clients d'una xarxa.

El servidor **DHCP** assigna adreces basades en claus. Les quatre claus comuns són la xarxa, la classe, el proveïdor i l'ID de client. El servidor utilitza aquestes claus per obtenir una adreça i un grup d'opcions de configuració per tornar al client.

xarxa Identifica el segment de xarxa del qual procedeix el paquet. La clau de xarxa permet al servidor comprovar la base de dades d'adreces i assignar una adreça per segment de xarxa.

classe És completament configurable a nivell de client. Pot especificar una adreça i opcions. Aquesta clau es pot utilitzar per denotar la funció de màquina a la xarxa o bé per descriure com s'agrupen les màquines amb propòsits administratius. Per exemple, pot ser que l'administrador de la xarxa vulgui crear una classe `netbios` que contingui opcions per als clients NetBIOS o una classe `comptabilitat` que representi a les màquines del departament de Comptabilitat que necessiten accedir a una determinada impressora.

proveïdor
Ajuda a identificar el client per la seva plataforma de programari/maquinari (per exemple, el client Microsoft Windows 95 o bé un client OS/2 Warp.

ID de client
Identifica el client mitjançant el nom de l'amfitrió de la màquina o bé mitjançant l'adreça de capa de control d'accés al medi (MAC). L'ID de client s'especifica al fitxer de configuració del daemon **dhcpcd**. El servidor també pot utilitzar l'ID de client per passar opcions a un client específic o prohibir que un client en concret rebi cap paràmetre.

La configuració pot emprar aquestes claus tant individualment com en combinacions. Si el client proporciona diverses claus i es poden assignar diverses adreces, només se'n selecciona una i l'opció establerta es deriva primerament de la clau seleccionada. Per obtenir informació més detallada sobre la selecció de claus i adreces, consulteu l'apartat "Configuració del DHCP" a la pàgina 212.

Es necessita un agent de retransmissió per tal que les difusions inicials del client abandonin la xarxa local. Aquest agent s'anomena l'agent de retransmissió BOOTP. Els agents de retransmissió actuen com a agents de reenviament dels paquets **DHCP** i **BOOTP**.

Servidors DHCP

A l'AIX, el servidor **DHCP** s'ha segmentat en tres parts principals:

Els components principals del servidor **DHCP** són una base de dades, un motor de protocol i un conjunt de fils de servei, cadascun d'ells amb la seva informació de configuració.

Base de dades DHCP:

La base de dades `db_file.dhcpo` s'utilitza per fer un seguiment dels clients i de les adreces, així com per al control d'accés (per exemple, permetre l'accés de determinats clients a només algunes xarxes o bé inhabilitar els clients **BOOTP** en una xarxa en concret).

Les opcions també s'emmagatzemen a la base de dades per a la recuperació i lliurament als clients. La base de dades s'implementa com un objecte dinàmicament carregable, que permet una millora i un manteniment fàcils del servidor.

La base de dades s'actualitza i verifica per coherència mitjançant la informació del fitxer de configuració. Un conjunt de fitxers de punt de comprovació gestiona les actualitzacions de la base de dades i disminueix la sobrecàrrega d'enregistraments del fitxer d'emmagatzematge principal. La base de dades també conté les agrupacions d'adreces i d'opcions, les quals són estàtiques i se'n parla a l'apartat "Configuració del DHCP" a la pàgina 212.

El fitxer d'emmagatzematge principal i la còpia de seguretat són fitxers ASCII plans que es poden editar. El format dels fitxers d'emmagatzematge principal de base de dades és el següent:

```
DF01
"ID DE CLIENT" "0.0.0.0" Estat Inici_temps_lloguer Durada_temps_lloguer Fi_temps_lloguer
  "Adreça IP del servidor" "ID de classe" "ID de proveïdor" "Nom_amfitrió" "Nom de domini"
"ID DE CLIENT" "0.0.0.0" Estat Inici_temps_lloguer Durada_temps_lloguer Fi_temps_lloguer
  "Adreça IP del servidor" "ID de classe" "ID de proveïdor" "Nom d'amfitrió" "Nom de domini"
...
```

La primera línia és un identificador de versió del fitxer `DF01c`. Les línies següents són de definició d'enregistrament del client. El servidor llegeix des de la segona línia fins al final del fitxer. (Els paràmetres entre cometes s'han d'incloure entre cometes).

"*ID DE CLIENT***"**
És l'ID que el client utilitza per representar-se al servidor.

"0.0.0.0"
és l'adreça IP assignada actualment al servidor **DHCP**. Si no s'ha assignat cap adreça, és "0.0.0.0".

Estat És l'estat actual del client. El motor de protocol **DHCP** conté el conjunt permès i els estats es mantenen a la base de dades **DHCP**. El nombre a la vora d'*Estat* en representa el valor. Els estats poden ser:

(1) LLIURE
Representa les adreces disponibles per a l'ús. En general, els clients no tenen aquest estat a no ser que no tinguin assignada cap adreça. El **dadmin** i la sortida del **lssrc** informen sobre aquest estat com a `Lliure`.

(2) VINCULAT
Indica que el client i l'adreça estan enllaçats i que s'ha assignat aquesta adreça al client durant un determinat període de temps. El **dadmin** i la sortida del **lssrc** informen sobre aquest estat com a `Llogat`.

(3) CADUCAT
Indica que el client i l'adreça estan enllaçats, però només per motius d'informació, d'una manera semblant a les adreces alliberades. No obstant això, l'estat de caducat representa els clients que es deixen caducar els lloguers. Una adreça caducada es pot utilitzar i es torna a assignar quan cap de les adreces lliures està disponible i abans que es tornin a assignar les adreces alliberades. El **dadmin** i la sortida del **lssrc** informen sobre aquest estat com a `Caducat`.

(4) ALLIBERAT
Indica que el client i l'adreça estan enllaçats només per motius d'informació. El protocol **DHCP** aconsella que els servidors **DHCP** mantinguin la informació dels clients per a futures consultes (sobretot per intentar donar la mateixa adreça al client al qual ja se li havia assignat anteriorment). Aquest estat indica que el client ha alliberat l'adreça. Els altres clients poden utilitzar l'adreça si no n'hi ha cap més de disponible. El **dadmin** i la sortida del **lssrc** informen sobre aquest estat com a `Alliberat`.

(5) RESERVAT
Indica que el client i l'adreça estan enllaçats, però de manera suau. El client ha enviat un missatge de descobriment **DHCP** i el servidor **DHCP** ha respost, però el client encara no ha respost amb una sol•licitud **DHCP** per a l'adreça. El **dadmin** i la sortida del **lssrc** informen sobre aquest estat com a `Reservat`.

(6) ERRONI
Representa una adreça que s'utilitza a la xarxa, però que el servidor **DHCP** no ha distribuït. Aquest estat també representa les adreces que els clients han rebutjat. Aquest estat no fa referència als clients. El **dadmin** i la sortida del **lssrc** informen sobre aquest estat com a `Utilitzat` i `Erroni`, respectivament.

Inici_temps_lloguer
És l'inici del període de lloguer actual (en segons des de l'1 de gener del 1970).

Durada_temps_lloguer
Representa la durada del lloguer (en segons).

Fi_temps_lloguer
Utilitza el mateix format que l'*Inici_temps_lloguer*, però representa la fi del lloguer. Algunes opcions de configuració utilitzen valors diferents per a l'inici i el final d'un lloguer que es poden veure alterats temporalment a causa de les opcions de fitxer de configuració. Consulteu l'apartat “Sintaxi de fitxer del servidor DHCP per a la base de dades db_file” a la pàgina 229.

"*Adreça IP del servidor***"**
És l'adreça IP del servidor DHCP al qual pertany aquest enregistrament.

"*ID de classe***" "***ID de proveïdor***" "***Nom d'amfitrió***" "***Nom de domini***"**
Són valors que el servidor utilitza per determinar les opcions que s'envien al servidor

(emmagatzemades com a sèries entre cometes). Aquests paràmetres augmenten el rendiment perquè es poden pregenerar llistes d'opcions per a aquests clients quan s'engega el servidor **DHCP**.

Fitxers de punt de comprovació DHCP:

La sintaxi dels fitxers de punt de comprovació no està especificada.

Si cau el servidor o bé heu d'aturar el sistema i no podeu tancar la base de dades amb normalitat, el servidor pot processar els fitxers de punt de comprovació i de còpia de seguretat per tornar a construir una base de dades vàlida. El client que s'estava enregistrant al fitxer de punt de comprovació quan el servidor cau es perd. Els fitxers de valors per defecte són:

/etc/db_file.cr
operació de base de dades normal

/etc/db_file.crbk
còpies de seguretat per a la base de dades

/etc/db_file.chkpt i /etc/db_file.chkpt2
fitxers de punt de comprovació giratoris

El servidor **DHCP** funciona amb fils. Per mantenir una productivitat alta, les operacions de base de dades (incloses les operacions de desament) tenen un sistema eficient de fils. Quan se sol•licita un desament, el fitxer de punt de comprovació existent es gira al següent fitxer d'aquest tipus, el fitxer de base de dades existent es copia al fitxer de còpia de seguretat i es crea el nou fitxer per desar. A continuació, cada enregistrament de client s'enregistra i es commuta un bit per indicar que el client hauria d'utilitzar el nou fitxer de punt de comprovació per iniciar la sessió. Quan tots els enregistraments de client s'han enregistrat, es tanca l'operació de desament i els fitxers de còpia de seguretat i de punt de comprovació antics se suprimeixen. Els clients encara es poden processar i, segons on s'hagi desat l'enregistrament de client, els canvis de la base de dades es traslladen en un fitxer de desament o de punt de comprovació nous.

Motor de protocol DHCP:

El motor de protocol **DHCP** protocol dóna suport a l'RFC 2131 i és encara compatible amb l'RFC 1541. (El servidor també pot processar opcions tal i com es defineixen al RFC 2132.) El motor de protocol utilitza la base de dades per determinar la informació que es torna al client.

La configuració de les agrupacions d'adreces tenen algunes opcions de configuració que afecten l'estat de cada màquina. Per exemple, el servidor **DHCP** fa ping a les adreces abans de lliurar-les. La quantitat de temps durant la qual el servidor espera una resposta es pot configurar ara per a cada agrupació d'adreces.

Operacions de fils DHCP:

La darrera part del servidor **DHCP** és un conjunt d'operacions que s'utilitzen per mantenir el funcionament. Atès que el **DHCP** és un servidor de fils, aquestes operacions realment estan configurades com a fils que de tant en tant realitzen certes tasques per assegurar-se que tot està enllaçat correctament.

El primer fil, el **main**, gestiona les sol•licituds SRC (com ara les **startsrc**, **stopsrc**, **lssrc**, **traceson** i **refresh**). Aquest fil coordina també totes les operacions que afecten tots els fils i gestiona els senyals. Per exemple,

- Un SIGHUP (-1) provoca una renovació de totes les bases de dades del fitxer de configuració.
- Un SIGTERM (-15) fa que el servidor s'aturi correctament.

El fil següent, el **dadmin**, opera interactivament amb el programa de client **dadmin** i el servidor **DHCP**. Es pot utilitzar l'eina **dadmin** per aconseguir un estat, així com per modificar la base de dades per evitar

l'edició manual dels fitxers de la base de dades. Les versions anteriors del servidor **DHCP** evitaven que els clients obtinguessin adreces si s'estava executant una sol•licitud d'estat. Havent inclòs els fils **dadmin** i **src**, el servidor pot gestionar les sol•licituds de servei i també les dels clients.

El fil següent és el **garbage**, el qual executa temporitzadors que netegen periòdicament la base de dades, la desen, depuren els clients que no tenen adreces i eliminen les adreces reservades que han estat massa temps en estat reservat. Tots aquests temporitzadors són configurables (consulteu l'apartat "Configuració del DHCP"). La resta de fils són processadors de paquets. El nombre d'aquests és configurable; El valor per defecte és 10. Cadascun d'ells pot gestionar una sol•licitud d'un client **DHCP**. El nombre de processadors de paquets necessari depèn, en certa manera, de la càrrega i de la màquina. Si s'utilitza la màquina per a altres serveis al marge del **DHCP**, no és recomanable engegar 500 fils.

Planificació DHCP

Per utilitzar aquest protocol, l'administrador de la xarxa necessita configurar un servidor **DHCP** i agents de retransmissió BOOTP als enllaços que no tenen un servidor **DHCP**. Una planificació avançada pot reduir la càrrega **DHCP** de la xarxa.

Per exemple, es pot configurar un servidor per gestionar tots els clients, però tots els paquets han de passar a través seu. Si teniu un sol encaminador entre dues xarxes grans, és millor col•locar dos servidors a la xarxa, un a cada enllaç.

Un altre aspecte que cal tenir en compte és el fet que el **DHCP** implica un patró de trànsit. Per exemple, si establiu el temps de lloguer per defecte a menys de dos dies i les màquines no reben corrent elèctric durant el cap de setmana, dilluns al matí serà un període d'elevat trànsit **DHCP**. Tot i que el trànsit **DHCP** no sobrecarrega excessivament la xarxa, s'ha de tenir en compte quan es decideix on col•locar els servidors **DHCP** en una xarxa i quants se n'utilitzaran.

Després d'habilitar el **DHCP** per tal que admeti el client a la xarxa, el client ja no ha d'introduir res més. El client **DHCP**, `dhcpcd`, llegeix el fitxer `dhcpcd.ini`, que conté informació sobre l'inici de sessió i altres paràmetres necessaris per iniciar l'execució. Després de la instal•lació, decidiu el mètode que voleu utilitzar per a la configuració **TCP/IP**: la configuració mínima o bé el **DHCP**. Si seleccioneu el **DHCP**, trieu una interfície i especifiqueu uns quants paràmetres opcionals. Per triar la interfície, seleccioneu la paraula clau **any**, que mana al `dhcpcd` que cerqui la primera interfície en funcionament i que l'empri. Aquest mètode minimitza la quantitat d'entrades a la banda del client.

Configuració del DHCP

Per defecte, el servidor **DHCP** es configura mitjançant la lectura del fitxer `/etc/dhcpsd.cnf`, el qual especifica la base de dades inicial d'opcions i adreces.

El servidor s'inicia al fitxer `/etc/rc.tcpip`. També es pot iniciar des de la SMIT o mitjançant ordres SRC. És possible configurar el client **DHCP** executant la System Management Interface Tool (SMIT) o bé editant un fitxer ASCII pla.

Normalment, la configuració del servidor **DHCP** és la part més complexa pel que fa a l'ús del **DHCP** a la xarxa. Primerament, decidiu les xarxes en què voleu tenir els clients **DHCP**. Cada subxarxa de la xarxa representa una agrupació d'adreces que el servidor **DHCP** ha d'afegir a la seva base de dades. Per exemple:

```
database db_file
{

    subxarxa 9.3.149.0 255.255.255.0
      {  opció 3 9.3.149.1 # Els clients de passarel•la per defecte d'aquesta xarxa haurien d'utilitzar
         opció 6 9.3.149.2 # Els clients de servidor de noms d'aquesta xarxa haurien d'utilitzar
      }
    ... les opcions o altres contenidors afegits posteriorment
}
```

L'exemple anterior mostra una subxarxa, la `9.3.149.0`, amb una màscara de subxarxa `255.255.255.0`. Totes les adreces d'aquesta subxarxa, de la 9.3.149.1 a la 9.3.149.254, són a l'agrupació. Opcionalment, es pot especificar un abast al final de la línia o bé es pot incloure al contenidor de subxarxes un abast o una sentència d'exclusió. Consulteu l'apartat “Opcions conegudes de fitxer del servidor DHCP” a la pàgina 221 pel que fa als mètodes habituals de configuració i a les definicions.

La clàusula de base de dades amb el `db_file` indica el mètode de base de dades que cal utilitzar per processar aquesta part del fitxer de configuració. Els comentaris comencen amb el signe #. El servidor **DHCP** obvia el text des del # inicial fins al final de la línia. El servidor utilitza cada línia d'`opció` per indicar al client el que ha de fer.“Opcions conegudes de fitxer del servidor DHCP” a la pàgina 221 descriu les opcions conegudes i suportades actualment. Consulteu l'apartat “Sintaxi de fitxer del servidor DHCP per al funcionament general del servidor” a la pàgina 225 sobre els mètodes per especificar opcions que el servidor no coneix.

Si el servidor no entén la manera d'analitzar una opció, utilitza mètodes per defecte per enviar l'opció al client. Això també permet al servidor **DHCP** enviar opcions d'indrets específics no definides pel RFC, però que poden ser utilitzades per certs clients o configuracions de clients.

Fitxer de configuració DHCP:

El fitxer de configuració té una secció d'adreces i una altra de definició d'opcions. Aquestes seccions utilitzen contenidors per retenir opcions, modificadors i, potencialment, altres contenidors.

Un *contenidor* (que és, bàsicament, un mètode per agrupar opcions) utilitza un identificador per classificar els clients en grups. Els tipus de contenidor són els de subxarxes, classes, proveïdors i clients. Actualment, no hi ha un contenidor genèric que l'usuari pugui definir. L'identificador només defineix el client perquè se'l pugui seguir si, per exemple, es desplaça entre subxarxes. Es pot utilitzar més d'un tipus de contenidor per definir l'accés del client.

Les *Opcions* són identificadors que es tornen al client, com ara la passarel•la per defecte i l'adreça DNS.

Els *modificadors* són sentències úniques que modifiquen algun aspecte d'un contenidor, com ara el valor per defecte del període de lloguer.

Contenidors DHCP:

Quan el servidor **DHCP** rep una sol•licitud, s'analitza el paquet i les claus d'identificació determinen els contenidors, les opcions i les adreces que cal extreure.

L'exemple de la “Configuració del DHCP” a la pàgina 212mostra un contenidor de subxarxes. La clau d'identificació és la posició del client a la xarxa. Si el client és d'aquesta xarxa, cau en aquest contenidor.

Cada tipus de contenidor utilitza una opció diferent per identificar un client:

- El contenidor de subxarxes utilitza el camp **giaddr** o l'adreça d'interfície de la interfície receptora per determinar la subxarxa de la qual procedeix el client.
- El contenidor de classes utilitza el valor de l'opció 77 (Identificador de classes d'indret d'usuari).
- El proveïdor utilitza el valor de l'opció 60 (Identificador de classes de proveïdor).
- El contenidor de clients utilitza l'opció 61 (Identificador de clients) per als clients **DHCP** i el camp **chaddr** del paquet **BOOTP** per als clients **BOOTP**.

A excepció de les subxarxes, cada contenidor permet l'especificació del valor amb el qual coincideix, incloses les coincidències d'expressió regular.

També hi ha un contenidor implícit, el contenidor *global*. Les opcions i els modificadors estan situats al contenidor global a no ser que estiguin alterats temporalment o denegats. La major part dels contenidors

es poden col•locar a dins d'altres contenidors que impliquen un àmbit de visibilitat. Tant pot ser que els contenidors tinguin abasts d'adreces associats com no. Les subxarxes tenen, per naturalesa, abasts associats.

Les normes bàsiques dels contenidors i subcontenidors són les següents:

- Tots els contenidors són vàlids a nivell global.
- Les subxarxes no es poden col•locar dins d'altres contenidors.
- Els contenidors restringits no poden tenir contenidors regulars del mateix tipus. (Per exemple, un contenidor amb una opció que només permet una classe de `Comptabilitat` no pot incloure un contenidor amb una opció que permeti totes les classes que comencen amb la lletra "a". Això no és permès.)
- Els contenidors de clients restringits no poden tenir subcontenidors.

Segons aquestes normes, podeu generar una jerarquia de contenidors que segmenti les opcions en grups per a clients específics o grups de clients.

Si un client coincideix amb diversos contenidors, com es distribueixen les opcions i les adreces? El servidor **DHCP** rep els missatges, passa la sol•licitud a la base de dades (`db_file`, en aquest cas) i es genera una llista de contenidors. La llista es presenta per ordre de profunditat i de prioritat. La prioritat es defineix com una jerarquia implícita als contenidors. Els contenidors estrictes tenen una prioritat major que els contenidors regulars. Els clients, les classes, els proveïdors i finalment les subxarxes es classifiquen per aquest ordre i dins el tipus de contenidor segons la profunditat. Això genera una llista ordenada de més específic a menys específic. Per exemple:

```
Subxarxa 1
--Classe 1
--Client 1
Subxarxa 2
--Classe 1
----Proveïdor 1
----Client 1
--Client 1
```

L'exemple mostra dues subxarxes, la `Subxarxa 1` i la `Subxarxa 2`. Hi ha un nom de classe, `Classe 1`, un nom de proveïdor, `Proveïdor 1` i un nom de client `Client 1`. La `Classe 1` i el `Client 1` estan definits en diversos llocs. Com que es troben en contenidors diferents, pot ser que tinguin el mateix nom, però que els valors al seu interior siguin diferents. Si el `Client 1` envia un missatge al servidor **DHCP** des de la `Subxarxa 1` amb la `Classe 1` especificada a la llista d'opcions, el servidor **DHCP** generarà el següent camí d'accés del contenidor:

`Subxarxa 1, Classe 1, Client 1`

El contenidor més específic és l'últim de la llista. Per obtenir una adreça, s'examina la llista en jerarquia invertida per trobar la primera adreça disponible. Seguidament, la llista s'examina en jerarquia cap endavant per obtenir les opcions. Les opcions alteren temporalment els valors precedents a no ser que hi hagi una opció **deny** al contenidor. Així mateix, com que la `Classe 1` i el `Client 1` són a la `Subxarxa 1`, s'ordenen segons la prioritat de contenidor. Si el mateix client és a la `Subxarxa 2` i envia el mateix missatge, la llista de contenidor que es genera és:

`Subxarxa 2, Classe 1, Client 1` (al nivell de la `Subxarxa 2`), `Client 1` (al nivell de la `Classe 1`)

Primer es fa una llista de la `Subxarxa 2`, després de la `Classe 1`, seguidament del `Client 1` a nivell de la `Subxarxa 2` (perquè aquesta sentència de client només es troba un nivell per sota de la jerarquia). La jerarquia implica que un client que coincideix amb la primera sentència de client és menys específic que el client que coincideix amb el `Client 1` de la `Classe 1` a la `Subxarxa 2`.

La prioritat dels contenidors no substitueix la prioritat seleccionada per profunditat dins la jerarquia. Per exemple, si el mateix client executa el mateix missatge i especifica un identificador de proveïdor, la llista de contenidor és:

`Subxarxa 2, Classe 1, Proveïdor 1, Client 1` (al nivell de la `Subxarxa 2`), `Client 1` (al nivell de la `Classe 1`)

La prioritat de contenidor millora el rendiment de cerca ja que segueix el concepte general segons el qual els contenidors de clients són la manera més específica de definir un o més clients. El contenidor de classes reté menys adreces específiques que un contenidor de clients; el de proveïdors és encara menys específic i el de subxarxes, el menys específic de tots.

Adreces i abasts d'adreces DHCP:

Qualsevol tipus de contenidor pot tenir associats abasts d'adreces; les subxarxes han de tenir abasts d'adreces associats. Cada abast d'un contenidor ha de ser un subconjunt de l'abast i no s'ha de superposar amb els abasts dels altres contenidors.

Per exemple, si una classe es troba definida en una subxarxa i té un abast, aquest abast ha de ser un subconjunt de l'abast de la subxarxa. De la mateixa manera, l'abast d'aquest contenidor de classes no es pot superposar amb cap altre abast del seu nivell.

Els abasts poden expressar-se a la línia del contenidor i modificar-se per abast, així com excloure sentències per permetre conjunts d'adreces desunits associats a un contenidor. Si teniu disponibles les deu adreces principals i les segones deu adreces d'una subxarxa, la subxarxa pot especificar aquestes adreces per abast a la clàusula de la subxarxa per reduir tant l'ús de la memòria com el risc de col•lisió d'adreces amb altres clients fora dels abasts especificats.

Després de seleccionar una adreça, s'elimina de la llista qualsevol contenidor subseqüent de la llista que contingui abasts d'adreces juntament amb els seus subordinats. Les opcions específiques de xarxa dels contenidors eliminats no són vàlides si no s'utilitza una adreça des d'aquell contenidor.

Opcions del fitxer de configuració DHCP:

Després d'haver netejat la llista per determinar les adreces, es genera un conjunt d'opcions per al client.

En aquest procés de selecció, les opcions sobreescriuen les opcions seleccionades prèviament a no ser aparegui un *deny*; en aquest cas, l'opció denegada s'elimina de la llista que s'està enviant al client. Aquest mètode permet l'herència dels contenidors superiors per reduir la quantitat de dades que cal especificar.

Modificadors DHCP:

Els modificadors són elements que canvien algun aspecte d'un contenidor en qüestió, com ara l'accés o el període de lloguer.

Definiu les agrupacions d'adreces i d'opcions abans de modificar el contenidor. Els modificadors més comuns són el **leasetimedefault**, el **supportBootp** i el **supportUnlistedclients**.

leasetimedefault
: Defineix la quantitat de temps que una adreça s'ha de llogar a un client.

supportBootp
: Defineix si el servidor respon o no als clients **BOOTP**.

supportUnlistedclients
: Indica si els clients s'han de definir explícitament mitjançant una sentència de client per rebre adreces. El valor del **supportUnlistedClients** pot ser **none**, **dhcp**, **bootp** o **both**. Això us permet restringir l'accés al client bootp i que tots els clients DHCP obtinguin adreces.

A l'apartat “Sintaxi de fitxer del servidor DHCP per a la base de dades db_file” a la pàgina 229, apareix una llista d'altres modificadors.

Inici de sessió DHCP:

Després de seleccionar els modificadors, el següent element que cal configurar és l'inici de sessió.

Els paràmetres d'inici de sessió s'especifiquen en un contenidor com la base de dades, però la paraula clau del contenidor és **logging_info**. Quan s'aprèn a configurar el **DHCP**, és aconsellable posar l'inici de sessió al nivell superior. Així mateix, és millor especificar la configuració d'inici de sessió abans que qualsevol altra dada del fitxer de configuració per assegurar-se que els errors de configuració s'enregistren després que s'hagi inicialitzat el subsistema d'inici de sessió. Utilitzeu la paraula clau **logitem** per habilitar un nivell d'inici de sessió o elimineu la paraula clau **logitem** per inhabilitar un nivell d'inici de sessió. Altres paraules clau per a l'inici de sessió permeten especificar el nom de fitxer de registre, la grandària del fitxer i el nombre de fitxers de registre giratoris.

Opcions específiques de servidor DHCP:

El darrer conjunt de paràmetres que cal especificar són opcions específiques de servidor que permeten a l'usuari controlar el nombre de processadors de paquet, la freqüència d'execució dels fils de recollida de deixalles, etcètera.

Per exemple, dos opcions específiques de servidor són:

reservedTime
: Indica el temps que una adreça roman en estat reservat després d'enviar un OFFER al client **DHCP**

reservedTimeInterval
: Indica la freqüència amb la qual el servidor **DHCP** escaneja les adreces per veure si n'hi ha que han estat més temps en estat reservat que no pas en **reservedTime**.

Aquestes opcions són útils si teniu diversos clients que envien missatges de DESCOBRIMENT i, o bé no envien el missatge de PETICIÓ, o bé el missatge de PETICIÓ es perd a la xarxa. L'ús d'aquests paràmetres evita que les adreces estiguin reservades indefinidament per a un client incomplidor.

Un altra opció especialment útil é **SaveInterval**, que indica la freqüència dels desaments. Totes les opcions específiques de servidor es troben a l'apartat “Sintaxi de fitxer del servidor DHCP per al funcionament general del servidor” a la pàgina 225 amb les paraules claus d'inici de sessió.

Consideracions de rendiment del DHCP:

És important entendre que determinades paraules clau de configuració i l'estructura del fitxer de configuració tenen un efecte en l'ús de la memòria i el rendiment del servidor **DHCP**.

Primerament, es pot evitar l'ús excessiu de la memòria si entenem el model d'herència d'opcions dels contenidors superiors als subordinats. En un entorn que no dóna suport als clients que no figuren a la llista, l'administrador ha de mostrar explícitament a la llista cada client del fitxer. Quan es realitza una llista d'opcions per a qualsevol client específic, el servidor utilitza més memòria per emmagatzemar aquest arbre de configuració que quan les opcions s'hereten d'un contenidor superior (per exemple, la subxarxa, la xarxa o els contenidors globals). Per tant, l'administrador hauria de comprovar si hi ha opcions repetides al nivell de client en el fitxer de configuració i determinar si aquestes opcions es poden especificar al contenidor superior i compartir per tot el grup de clients.

Així mateix, quan s'utilitzen les entrades **logItem** INFO i TRACE, s'enregistren nombrosos missatges durant el processament de cada missatge d'un client **DHCP**. Afegir una línia al fitxer de registre pot ser

una operació costosa; per tant, limitar la quantitat d'inicis de sessió millora el rendiment del servidor **DHCP**. Quan se sospita un error amb el servidor **DHCP**, es pot tornar a habilitar dinàmicament l'inici de sessió mitjançant les ordres SRC **traceson** o **dadmin**.

Finalment, la selecció d'un valor **numprocessors** depèn de la grandària de la xarxa suportada pel **DHCP**, el paràmetre de configuració **pingTime db_file** i el retard de propagació normal de la xarxa. Com que cada fil processador de paquets envia una Sol•licitud d'eco ICMP per comprovar l'estat d'una adreça propietat del servidor abans d'oferir-la a un client, el temps d'espera d'una Resposta d'eco afecta directament la quantitat de temps de processament d'un missatge de DESCOBRIMENT. Bàsicament, el fil de processador de paquets és capaç de només esperar una resposta o el temps d'espera **pingTime**. Abaixar el valor **numprocessors** millora el temps de resposta del servidor abaixant el nombre de retransmissions de client, però mantenint la utilitat del ping del disseny de servidor.

Per obtenir un rendiment millor, seleccioneu un **pingTime** basat en el retard de propagació de qualsevol xarxa remota suportada pel servidor **DHCP**. Així mateix, seleccioneu el valor **numprocessors** basat en aquest valor **pingTime** i en la grandària de la xarxa. Seleccionar un valor massa petit pot provocar l'aturada de tots els fils de processament de paquets. Aleshores, el servidor ha d'esperar les Respostes d'eco mentre els missatges dels clients **DHCP** fan cua al port del servidor. Això fa que el servidor gestioni els missatges dels clients en lots i no en un corrent constant.

Seleccionar un valor massa petit pot provocar l'aturada de tots els fils de processament de paquets a l'espera de Respostes d'eco.

Per evitar aquesta situació, establiu el valor del **numprocessors** en un nombre superior al nombre estimat de missatges de DESCOBRIMENT que es poden rebre en un interval **pingTime** durant un període d'alta activitat del client **DHCP**. No obstant això, no establiu un valor **numprocessors** massa elevat, ja que podria carregar el kernel amb la gestió de fils.

Per exemple, els valors **numprocessors 5** i **pingTime 300** provoquen un baix rendiment en un entorn amb 10 missatges de DESCOBRIMENT potencials per segon perquè, en el punt de màxima demanda, només es gestionen 5 missatges cada 3 segons. Configureu aquest entorn amb valors semblants a **numprocessors 20** i **pingTime 80**.

Personalització del fitxer de configuració DHCP:

Hi ha diversos factors implicats en la personalització del fitxer de configuració **DHCP**.

Moltes xarxes inclouen diversos tipus de client; per exemple, una sola xarxa pot incloure sistemes que executen diversos sistemes operatius, com ara el Windows, l'OS/2, el Java™ OS i l'UNIX. Cadascun requereix identificadors de proveïdor exclusius (el camp utilitzat per identificar el tipus de màquina al servidor DHCP). Pot ser que els clients del Java OS i les màquines de l'IBM Thin Client requereixin paràmetres exclusius com ara fitxers d'engegada i opcions de configuració que cal adaptar concretament. Els sistemes del Windows 95 no gestionen bé les opcions específiques del Java.

Les opcions específiques de màquina es poden encapsular en contenidors de proveïdors si l'ús principal per a certes màquines es basa en el tipus d'usuari. Per exemple, el personal de desenvolupament pot utilitzar els clients d'aquest sistema operatiu per programar; el personal de màrqueting pot emprar els clients de l'OS/2; el de vendes, els clients del Java OS i les màquines de l'IBM i el personal de comptabilitat, les màquines del Windows 95. És possible que cadascuna d'aquestes famílies d'usuari necessiti opcions de configuració diferents (impressores, servidors de noms o servidors web per defecte, etcètera). En aquest cas, aquestes opcions es podrien incloure al contenidor de proveïdors, ja que cada grup utilitza un tipus de màquina diferent.

Si diversos grups utilitzessin el mateix tipus de màquina, la col•locació de les opcions en un identificador de classe subordinat permetria als caps del màrqueting, per exemple, utilitzar un conjunt específic d'impressores al qual no tindrien accés els altres treballadors.

Nota: El següent exemple fictici representa part d'un fitxer de configuració. El signe # precedeix els comentaris, que descriuen la manera en què cada línia defineix la instal•lació.

```
proveïdor "AIX_CLIENT"
{
# Cap opció específica; gestiona elements basats en la classe
}

proveïdor "OS/2 Client"
{
# Cap opció específica; gestiona elements basats en la classe
}

proveïdor "Windows 95"
{ opció 44 9.3.150.3          # Servidor de noms NetBIOS per defecte
}

proveïdor "Java OS"
{ servidor_enceb 9.3.150.4    # Servidor TFTP per defecte dels requadres del Java OS
  opció 67 "javaos.bin"       # El fitxer d'engegada del requadre del Java OS
}

proveïdor "IBM Thin Client"
{ servidor_enceb 9.3.150.5    # Servidor TFTP per defecte dels requadres Thin Client
  opció 67 "thinos.bin"       # Fitxer d'engegada per defecte dels requadres Thin Client
}

subxarxa 9.3.149.0 255.255.255.0
{ opció 3 9.3.149.1           # La passarel•la per defecte de la subxarxa
  opció 6 9.3.150.2           # És el servidor de noms de la subxarxa
  comptabilitat de classe 9.3.149.5-9.3.149.20
  {       # La classe de comptabilitat està limitada a l'abast d'adreces 9.3.149.5-9.3.149.20
          # La impressora d'aquest grup també està en aquest abast, de manera que s'exclou.
     exclusió 9.3.149.15
     opció 9 9.3.149.15       # El servidor LPR (servidor d'impressió)
     proveïdor "Windows 95"
     {
     opció 9 denegar            # Aquesta instal•lació del Windows 95 no dóna suport a
                                # aquesta impressora, de manera que es denega l'opció.
     }
  }
 . . .
}
```

El DHCP i el Sistema de noms de domini dinàmic

El servidor **DHCP** ofereix opcions que permeten operar en un entorn de Sistema de noms de domini dinàmic (DDNS).

Per utilitzar el **DHCP** en un entorn DDNS, heu de configurar i utilitzar una Zona dinàmica en un servidor DNS.

Un cop s'hagi configurat el servidor DDNS, decidiu si el servidor **DHCP** farà les actualitzacions d'enregistrament A, les d'enregistrament PTR, les actualitzacions d'ambdós tipus, o bé cap. Aquesta decisió depèn de si la màquina client pot realitzar una part d'aquesta tasca o bé la totalitat.

- Si el client pot compartir la responsabilitat d'actualització, configureu el servidor perquè dugui a terme les actualitzacions d'enregistrament PTR i configureu el client per tal que en realitzi les d'enregistrament A.
- Si el client pot dur a terme ambdues actualitzacions, configureu el servidor de manera que no en faci cap.
- Si el client no pot realitzar actualitzacions , configureu el servidor perquè les faci totes dues.

El servidor **DHCP** té una sèrie de paraules claus de configuració que us permeten especificar una ordre que s'executi quan se sol•licita una actualització. Les paraules clau són les següents:

updatedns
(Desaprovada). Representa l'ordre que cal executar per realitzar qualsevol tipus d'actualització. Es crida tant per a l'actualització d'enregistrament PTR com per a la d'enregistrament A.

updatednsA
Especifica l'ordre per actualitzar l'enregistrament A.

updatednsP
Especifica l'ordre per actualitzar l'enregistrament PTR.

Aquestes paraules clau especifiquen sèries executables que el servidor **DHCP** executa quan és necessària una actualització. Les sèries de paraules clau han de contenir quatre %s (el símbol de percentatge, la lletra s). El primer %s és el nom d'amfitrió; el segon és el nom de domini; el tercer és l'adreça IP i el quart, el període de lloguer. S'utilitzen com a primers quatre paràmetres de l'ordre **dhcpaction**. Els dos paràmetres restants de l'ordre **dhcpaction** indiquen l'enregistrament que cal actualitzar (A, PTR, NONE, o BOTH) i si cal actualitzar el NIM (NIM o NONIM). Consulteu l'apartat "Suggeriments de Gestió d'instal•lació de xarxa i DHCP" a la pàgina 276 per obtenir més informació sobre la interacció entre el NIM i el **DHCP**. Per exemple:

```
updatednsA "/usr/sbin/dhcpaction '%s' '%s' '%s' '%s' '%s' A NONIM"
                    # Només realitza l'ordre dhcpaction a l'enregistrament A
updatednsP "/usr/sbin/dhcpaction '%s' '%s' '%s' '%s' '%s' PTR NONIM"
                    # Només realitza l'ordre a l'enregistrament PTR
updatedns "/usr/sbin/dhcpaction '%s' '%s' '%s' '%s' '%s' BOTH NIM"
                    # Realitza l'ordre en ambdós enregistraments i actualitza el NIM
```

El servidor **DHCP** també té un conjunt de paraules clau per eliminar les entrades DNS quan un lloguer s'allibera o caduca. Les paraules clau són:

releasednsA
Elimina l'enregistrament A.

releasednsP
Elimina l'enregistrament PTR.

removedns
Elimina tots dos tipus d'enregistrament.

Aquestes paraules clau especifiquen sèries executables que el servidor **DHCP** executa quan s'allibera o caduca una adreça. L'ordre **dhcpremove** funciona de manera semblant a la **dhcpaction**, però només té tres paràmetres:

1. L'adreça IP, especificada com a %s a la sèrie d'ordres
2. L'enregistrament que cal eliminar (A, PTR, NONE, o BOTH).
3. Si cal actualitzar el NIM (NIM o NONIM).

Per exemple:

```
releasednsA "/usr/sbin/dhcpremove '%s' A NONIM"
                     # Només realitza l'ordre dhcpremove a l'enregistrament A
releasednsP "/usr/sbin/dhcpremove '%s' PTR NONIM"
                     # Només realitza l'ordre a l'enregistrament PTR
removedns "/usr/sbin/dhcpremove '%s' BOTH NIM"
                     # Realitza l'ordre en ambdós enregistraments i actualitza el NIM
```

Les seqüències **dhcpaction** i **dhcpremove** duen a terme una comprovació de paràmetres i, a continuació, fa una crida al **nsupdate**, el qual ha estat actualitzat per operar amb els servidors d'aquest sistema operatiu i amb els servidors DDNS de l'OS/2. Consulteu la descripció de l'ordre **nsupdate** per obtenir més informació.

Si l'actualització de nom **NO** requereix la interacció del NIM, es pot configurar el servidor DHCP per utilitzar una transferència de sòcol entre el daemon **DHCP** i l'ordre **nsupdate** per millorar el rendiment i

permetre que es reintentin les actualitzacions DNS en cas d'anomalia. Per configurar aquesta opció, les paraules clau **updateDNSA**, **updateDNSP**, **releaseDNSA** o **releaseDNSP** han d'especificar "nsupdate_daemon" com a primera paraula entre cometes. Els paràmetres i senyaladors d'aquesta actualització són idèntics als que l'ordre **nsupdate** accepta. Addicionalment, es poden emprar com a substituts els següents noms variables:

Element	Descripció
$nom_amfitrió	Substituït pel nom d'amfitrió del client a l'actualització DNS o bé el nom d'amfitrió associat anteriorment amb el client per a l'extracció DNS.
$domini	Substituït pel domini DNS per a l'actualització o bé pel domini utilitzat anteriorment del nom d'amfitrió del client per a l'extracció DNS.
$adreça_ip	Substituït per l'adreça IP que cal associar o desassociar del nom de client **DHCP**.
$temps_lloguer	Substituït pel temps de lloguer (en segons).
$id_client	Substituït per la representació en sèrie de l'identificador de clients **DHCP** o bé la combinació del tipus de maquinari i l'adreça de maquinari dels clients **BOOTP**.

Per exemple:

```
updateDNSA "nsupdate_daemon -p 9.3.149.2 -h $nom_amfitrió -d $domini
 -s"d;a;*;a;a;$adreça_ip;s;$t4emps_lloguer;3110400""

updateDNSP "nsupdate_daemon -p 9.3.149.2 -r $adreça_ip
 -s"d;ptr;*;a;ptr;$nom_amfitrió.$domini.;s;$temps_lloguer;3110400""

releaseDNSA "nsupdate_daemon -p 9.3.149.2 -h $nom_amfitrió -d $domini -s"d;a;*;s;1;3110400""

releaseDNSP "nsupdate_daemon -p 9.3.149.2 -r $adreça_ip -s"d;ptr;*;s;1;3110400""
```

Consulteu la descripció de l'ordre **nsupdate** per obtenir més informació.

Així mateix, s'han afegit polítiques definides per l'administrador per als intercanvis de nom d'amfitrió entre el servidor i els clients. Per defecte, el nom d'amfitrió que es torna al client i s'utilitza per a una actualització DDNS és l'opció 12 (definida al fitxer de configuració del servidor). Alternativament, el nom d'amfitrió per defecte pot ser el nom d'amfitrió suggerit pel client, mitjançant l'opció 81 (l'opció DHCPDDNS) o la 12 (l'opció NOM D'AMFITRIÓ). No obstant això, l'administrador pot alterar temporalment el nom d'amfitrió per defecte mitjançant les paraules clau de configuració **hostnamepolicy**, **proxyarec** i **appenddomain**. Aquestes opcions i els seus paràmetres es defineixen a l'apartat "Sintaxi de fitxer del servidor DHCP per a la base de dades db_file" a la pàgina 229.

Compatibilitat del DHCP amb versions antigues

El servidor **DHCP** reconeix la configuració de les versions anteriors i els fitxers de base de dades `dhcps.ar` i `dhcps.cr`.

Analitza els fitxers de configuració antics i genera fitxers de bases de dades nous a les ubicacions antigues. Les bases de dades antigues es converteixen automàticament al nou fitxer. El fitxer de configuració no es converteix.

El mòdul de base de dades del servidor **DHCP**, el `db_file`, pot llegir el format antic. El servidor **DHCP** reconeix quan un contenidor de base de dades no es troba al fitxer de configuració i tracta tot el fitxer a mesura que configura els paràmetres del servidor, d'inici de sessió i de la base de dades `db_file`.

Nota:

1. De vegades, es desaprova la sintaxi de fitxers de configuració antiga, però igualment se li dóna suport. Altres desaprovacions són les següents:
2. El contenidor de xarxa està desaprovat completament. Per dur a terme una especificació correcta, convertiu la clàusula de xarxa amb un abast en un contenidor de subxarxes vàlid amb una adreça de subxarxa, una màscara de xarxa i l'abast. Si el contenidor de xarxa té contenidors de subxarxes, elimineu la paraula clau de contenidor de xarxa juntament amb les claus i, a continuació, col•loqueu

la màscara de subxarxa a la posició apropiada de la línia. Per començar a utilitzar el contenidor de base de dades, agrupeu tot allò que pertanyi a les xarxes i a l'accés de clients en un contenidor de base de dades de tipus `db_file`.

3. Les paraules clau **updatedns** i **removedns** es desaproven i substitueixen a favor de l'especificació de l'acció dels enregistraments A i PTR de manera separada.
4. Les paraules clau **clientrecorddb** i **addressrecorddb** s'han desaprovat al **clientrecorddb** i al **backupfile**, respectivament.
5. Les paraules clau **bootstrapserver** i **giaddrfield** substitueixen les paraules clau **option sa** i **option ga**, respectivament. Consulteu l'apartat "Sintaxi de fitxer del servidor DHCP per al funcionament general del servidor" a la pàgina 225 i "Sintaxi de fitxer del servidor DHCP per a la base de dades db_file" a la pàgina 229 per obtenir més informació.

Opcions conegudes de fitxer del servidor DHCP

Tot seguit s'identifiquen les opcions conegudes de fitxer del servidor **DHCP**.

Nota: Les opcions que es mostren en aquesta taula tot indicant que no se'n permet l'especificació (amb un No a la columna Es pot especificar?) es poden especificar al fitxer de configuració, però se sobreescriuen amb el valor correcte. Per obtenir una definició millor de cada opció, consulteu l'RFC 2132.

Número d'opció	Tipus de dades per defecte	Es pot especificar?	Descripció/Ús
0	Cap	No	El servidor omple el camp opció, si cal.
1	Quartet amb punt	No	Màscara de xarxa de la subxarxa des d'on s'ha dibuixat l'adreça.
2	enter de 32 bits	Sí	Especifica el desplaçament de la subxarxa de client en segons del Coordinated Universal Time (UTC).
3	Un quartet amb punt o més	Sí	Llista d'adreces IP de les passarel•les per defecte.
4	Un quartet amb punt o més	Sí	Llista d'adreces IP del servidor horari.
5	Un quartet amb punt o més	Sí	Llista d'adreces IP del servidor de noms.
6	Un quartet amb punt o més	Sí	Llista d'adreces IP del DNS.
7	Un quartet amb punt o més	Sí	Llista d'adreces IP del servidor d'enregistraments.
8	Un quartet amb punt o més	Sí	Llista d'adreces IP del servidor cookie.
9	Un quartet amb punt o més	Sí	Llista d'adreces IP del servidor LPR.
10	Un quartet amb punt o més	Sí	Llista d'adreces IP del servidor Impress.
11	Un quartet amb punt o més	Sí	Llista d'adreces IP del servidor d'Ubicació de recursos.
12	Una sèrie ASCII	Sí	Nom d'amfitrió que l'usuari utilitzi.
13	Enter sense signe de 16 bits	Sí	La grandària del fitxer d'engegada.
14	Una sèrie ASCII	Sí	El camí d'accés per al fitxer de buidatge Merit.
15	Una sèrie ASCII	Sí	Nom de domini DNS per defecte.
16	Una adreça IP	Sí	Adreça del servidor d'Intercanvis.
17	Una sèrie ASCII	Sí	Camí d'accés arrel per defecte.
18	Una sèrie ASCII	Sí	Camí d'accés a les extensions per al client.
19	Sí, No, Cert, Fals, 1, 0	Sí	Especifica si s'ha d'engegar l'IP Forwarding.
20	Sí, No, Cert, Fals, 1, 0	Sí	Especifica si s'ha d'utilitzar encaminament d'origen no local.
21	Una parella o més de quartets amb punt, amb la forma *QuartetPunt*:*QuartetPunt*	Sí	Política de filtres de les adreces IP.
22	Enter sense signe de 16 bits	Sí	La grandària màxima que permeti fragments de datagrama.
23	Enter sense signe de 8 bits	Sí	La duració IP (TTL).
24	Enter sense signe de 32 bits	Sí	Nombre de segons que cal utilitzar al temps d'espera per antiguitat d'MTU del camí d'accés.
25	Llista d'un enter sense signe de 16 bits o més	Sí	Taula Plateau MTU del camí d'accés. Especifica un conjunt de valors que representa les grandàries MTU que cal emprar quan s'utilitza el descobriment MTU del camí d'accés.
26	Enter sense signe de 16 bits	Sí	Especifica la grandària MTU de la interfície receptora.
27	Sí, No, Cert, Fals, 1, 0	Sí	Especifica si totes les subxarxes són locals.
28	Una adreça IP (quartet amb punt)	Sí	Especifica l'adreça de difusió de la interfície.

Número d'opció	Tipus de dades per defecte	Es pot especificar?	Descripció/Ús
29	Sí, No, Cert, Fals, 1, 0	Sí	Especifica si s'ha d'utilitzar el descobriment de màscares de xarxa ICMP.
30	Sí, No, Cert, Fals, 1, 0	Sí	Especifica si el client ha de convertir-se en proveïdor de màscares de xarxa ICMP.
31	Sí, No, Cert, Fals, 1, 0	Sí	Especifica si s'han d'utilitzar missatges de Descobriment d'encaminaments ICMP.
32	Adreça IP (quartet amb punt)	Sí	Especifica l'adreça que cal utilitzar per a la sol•licitació d'encaminador.
33	Una parella o més d'adreces IP, amb la forma *DottedQuad*:*DottedQuad*	Sí	Cada parella d'adreces representa un encaminament estàtic.
34	Sí/No, Cert/Fals, 1/0	Sí	Especifica si s'ha d'utilitzar l'encapsulació de cua.
35	Enter sense signe de 32 bits	Sí	Valor de temps d'espera sobrepassat de cache ARP.
36	Sí/No, Cert/Fals, 1/0	Sí	Especifica si s'ha d'utilitzar l'encapsulació Ethernet.
37	Enter sense signe de 8 bits	Sí	La duració TCP (TTL).
38	Enter sense signe de 32 bits	Sí	L'interval keepalive **TCP**.
39	Sí/No, Cert/Fals, 1/0	Sí	Especifica si s'ha d'utilitzar el keepalive TCP.
40	Una sèrie ASCII	Sí	El domini per defecte NIS.
41	Un quartet amb punt o més	Sí	Especifica les adreces IP dels servidors NIS.
42	Un quartet amb punt o més	Sí	Especifica les adreces IP dels servidors NTP.
43	sèrie hex de dígits, en forma d'hex "*dígits*", hex "*dígits*" o 0x*dígits*	Sí, però només especificat realment amb contenidor de proveïdors	Contenidor d'opció encapsulat per al contenidor de proveïdors.
44	Un quartet amb punt o més	Sí	Especifica les adreces IP del servidor de noms NetBIOS.
45	Un quartet amb punt o més	Sí	Especifica les adreces IP del servidor de distribució de datagrama NetBIOS.
46	Enter sense signe de 8 bits	Sí	Especifica el Tipus de node NetBIOS.
47	sèrie hexadecimal de dígits, en forma d'hex "*dígits*", hex "*dígits*" o 0x*dígits*	Sí	Àmbit NetBIOS.
48	Un quartet amb punt o més	Sí	Especifica les adreces IP del servidor de tipus de lletra X Windows.
49	Un quartet amb punt o més	Sí	Especifica l'X Windows Display Manager.
50	Cap	No	Adreça IP sol•licitada utilitzada pel client per indicar l'adreça que desitja.
51	enter sense signe de 32 bits	Sí	Període de lloguer de l'adreça tornada. Per defecte, el servidor **DHCP** utilitza la paraula clau **leasetimedefault**, però l'altera temporalment l'especificació directa de l'opció 51.
52	Cap	No	Sobrecàrrega d'opcions. El client l'utilitza per indicar que els camps **sname** i **file** del paquet **BOOTP** poden tenir opcions.
53	Cap	No	El servidor o client **DHCP** utilitza aquesta opció per indicar el tipus de missatge **DHCP**.
54	Cap	No	El servidor o client **DHCP** utilitza aquesta opció per indicar l'adreça de servidor o el servidor al qual es dirigeix el missatge.
55	Cap	No	El client **DHCP** l'utilitza per indicar les opcions desitjades.
56	Una sèrie ASCII	Sí	Sèrie que el servidor **DHCP** envia al client. En general, el servidor i el client **DHCP** la poden utilitzar per indicar problemes.
57	No	No	El client **DHCP** utilitza aquesta opció per comunicar al servidor **DHCP** la grandària de paquet **DHCP** màxima que pot rebre el client.
58	Enter sense signe de 32 bits	Sí	Especifica el nombre de segons que han de passar fins que el client pugui enviar un paquet de renovació.
59	Enter sense signe de 32 bits	Sí	Especifica el nombre de segons que han de passar fins que el client pugui enviar un paquet de revinculació.
60	Cap	No	El client **DHCP** utilitza aquesta opció per indicar el tipus de proveïdor. El servidor **DHCP** utilitza aquest camp per fer coincidir contenidors de proveïdors.

Número d'opció	Tipus de dades per defecte	Es pot especificar?	Descripció/Ús
61	Cap	No	El client **DHCP** l'utilitza per identificar-se especialment. El servidor **DHCP** utilitza aquest camp per fer coincidir contenidors de clients.
66	Una sèrie ASCII	Sí	Especifica el nom de servidor **TFTP**. Aquest és un nom d'amfitrió i s'utilitza en lloc del camp **siaddr** si el client entén aquesta opció.
67	Una sèrie ASCII	Sí	Especifica el nom de fitxer d'engegada. Es pot utilitzar en lloc de la paraula clau **bootfile**, la qual situa el fitxer al camp **filename** del paquet.
68	Un quartet amb punt o més, o bé CAP	Sí	Especifica les adreces dels agents d'inici.
69	Un quartet amb punt o més	Sí	Especifica els servidors SMTP per defecte que cal utilitzar.
70	Un quartet amb punt o més	Sí	Especifica els servidors POP3 per defecte que cal utilitzar.
71	Un quartet amb punt o més	Sí	Especifica els servidors NNTP per defecte que cal utilitzar.
72	Un quartet amb punt o més	Sí	Especifica els servidors WWW per defecte que cal utilitzar.
73	Un quartet amb punt o més	Sí	Especifica els servidors Finger per defecte que cal utilitzar.
74	Un quartet amb punt o més	Sí	Especifica els servidors IRC per defecte que cal utilitzar.
75	Un quartet amb punt o més	Sí	Especifica els servidors Street Talk per defecte que cal utilitzar.
76	Un quartet amb punt o més	Sí	Especifica els servidors d'assistència de directori Street Talk per defecte que cal utilitzar.
77	Una sèrie ASCII	Sí	L'identificador de classe d'indret d'usuari. El servidor **DHCP** utilitza aquest camp per fer coincidir contenidors de classes.
78	Octet obligatori, un quartet amb punt o més	Sí	L'Opció d'agents de directoris SLP especifica una llista d'adreces IP per als Agents de directoris
79	Octet obligatori i una sèrie ASCII	Sí	La sèrie ASCII és una llista d'àmbits, és a dir, una llista delimitada per comes que indica els àmbits per a l'ús dels quals s'ha configurat un Agent SLP
81	Una sèrie ASCII més altres elements	No	El client DHCP utilitza aquesta opció per definir la política que el servidor **DHCP** hauria d'emprar pel que fa al DDNS.
85	Un quartet amb punt o més	Sí	L'opció de servidor NDS especifica el servidor o els servidors NDS que el client ha de contactar per accedir a la base de dades DNS. Caldria fer una llista de servidors per ordre de preferència.
86	Una sèrie ASCII	Sí	L'opció nom d'arbre NDS especifica el nom de l'arbre NDS que el client contactarà.
87	Una sèrie ASCII	Sí	L'opció context NDS especifica el context NDS inicial que el client hauria d'utilitzar.
93	Cap	No	El client DHCP utilitza aquesta opció per definir l'arquitectura del sistema client.
94	Cap	No	El client DHCP utilitza aquesta opció per definir l'identificador d'interfície de xarxa del client.

117	Un o més enters sense signe de 16 bits	Sí	L'Opció de cerca de serveis de nom dóna l'ordre preferida de codi d'opció d'enters dels serveis de nom. Per exemple:
			`Name services value`
			`Domain Name Server Option 6`
			`NIS Option 41`

118	Un quartet amb punt	No	L'Opció de selecció de subxarxa és una opció que el client envia amb la qual demana al servidor dhcp l'assignació de l'adreça IP des de la subxarxa especificada.
255	Cap	No	El client i el servidor DHCP utilitzen aquesta opció per indicar el final d'una llista d'opcions.

Subopció de contenidor de proveïdors PXE

Quan dóna suport a un client PXE (preboot execution environment), el servidor **DHCP** passa l'opció següent al servidor BINLD, que el BINLD utilitza per configurar-se.

Núm. Opc	Tipus de dades per defecte	Es pot especificar?	Descripció
7	Un quartet amb punt	Sí	Adreça IP de multidifusió. Adreça IP de multidifusió de descobriment de servidors d'engegada.

A l'exemple següent es mostra com es pot utilitzar aquesta opció:

```
pxeservertype    proxy_on_dhcp_server

Vendor pxeserver
{
     option   7    9.3.4.68
}
```

A l'exemple de dalt, el servidor **DHCP** comunica al client que el servidor proxy s'està executant a la mateixa màquina, però està rebent les sol•licituds de clients al port 4011. Aquí es requereix el contenidor de proveïdors perquè el servidor BINLD envia un missatge d'INFORMACIÓ/PETICIÓ al port 67 amb l'opció 60 establerta en "PXEServer." Com a resposta, el servidor **DHCP** envia l'adreça IP de multidifusió on el BINLD ha de rebre la sol•licitud del Client PXE.

A l'exemple següent, el servidor **dhcpsd** dóna el nom de fitxer d'engegada al Client PXE o dirigeix el Client PXE al servidor BINLD enviant subopcions. La paraula clau **pxeboofile** s'utilitza per crear una llista de fitxers d'engegada per a una arquitectura de client determinada i versions majors i menors del sistema client.

```
pxeservertype     dhcp_pxe_binld

subnet default
{
     vendor pxe
     {
         option 6 2    # Disable Multicast
         option 8 5 4 10.10.10.1 12.1.1.15 12.5.5.5 12.6.6.6\
                  2 2 10.1.1.10 9.3.4.5 1 1 10.5.5.9\
                  1 1 9.3.149.15\
                  4 0
         option 9 5 "WorkSpace On Demand" 2 "Intel"\
                  1 "Microsoft Windows NT" 4 "NEC ESMPRO"
         option 10 2 "Press F8 to View Menu"
     }
     vendor pxeserver
     {
         option 7 239.0.0.239
     }

}

subnet  9.3.149.0  255.255.255.0
{
     option 3   9.3.149.1
     option 6   9.3.149.15

     vendor pxe
     {
       option    6    4    # bootfile is present in the offer packet
       pxebootfile   1   2   1   os2.one
       pxebootfile   2   2   1   aix.one
     }
}
```

El servidor utilitza cada entrada de línia del contenidor per indicar al client el que ha de fer. “Subopcions del contenidor de proveïdors del PXE” a la pàgina 303 descriu les subopcions PXE conegudes i suportades actualment.

Sintaxi de fitxer del servidor DHCP per al funcionament general del servidor

A continuació es defineix la sintaxi de fitxer **DHCP** per al funcionament general del servidor i els valors vàlids de cada camp.

Nota: Les Unitats de temps (*unitats_temps*) que es mostren a la taula següent són opcionals i representen un modificador de l'hora actual. La unitat de temps per defecte és els minuts. Són valors vàlids els segons (1), els minuts (60), les hores (3600), els dies (86400), les setmanes (604800), els mesos (2392000) i els anys (31536000). El nombre que apareix entre parèntesis és un multiplicador aplicat al valor específic *n* per expressar el valor en segons.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
database	database *tipus_db*	Sí	Cap	El contenidor primari que reté les definicions de les agrupacions d'adreces, les opcions i les sentències d'accés de client. El *tipus_db* és el nom d'un mòdul que es carrega per processar aquesta part del fitxer. L'únic valor disponible actualment és el **db_file**.
logging_info	logging_info	Sí	Cap	El contenidor d'inici de sessió primari que defineix els paràmetres d'inici de sessió.
logitem	logitem NONE	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies.
logitem	logitem SYSERR	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies.
logitem	logitem OBJERR	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies.
logitem	logitem PROTOCOL	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies.
logitem	logitem PROTERR	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies.
logitem	logitem WARN	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies.
logitem	logitem WARNING	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
logitem	logitem CONFIG	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies.
logitem	logitem EVENT	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies.
logitem	logitem PARSEERR	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies.
logitem	logitem ACTION	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies.
logitem	logitem ACNTING	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies.
logitem	logitem STAT	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies.
logitem	logitem TRACE	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies.
logitem	logitem RTRACE	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies.
logitem	logitem START	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies.
numLogFiles	numLogFiles *n*	No	0	Especifica el nombre de fitxers de registre que cal crear. L'enregistrament gira quan s'emplena el primer. *n* és el nombre de fitxers que cal crear.
logFileSize	logFileSize *n*	No	0	Especifica la grandària de cada fitxer de registre en unitats de 1024 octets.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
logFileName	logFileName *camí d'accés*	No	Cap	Especifica el camí d'accés al primer fitxer de registre. El fitxer de registre original s'anomena *nom_fitxer* o *nom_fitxer.extensió*. Quan es gira un fitxer, es canvia de nom començant amb la base *nom_fitxer* i, a continuació, afegint un nombre o substituint l'extensió per un nombre. Per exemple, si el nom de fitxer original és `fitxer`, el nom de fitxer girat esdevé `fitxer01`. Si el nom de fitxer original és `fitxer.log`, esdevé `fitxer.01`.
CharFlag	charflag yes	No	cert	No aplicable al servidor **DHCP** d'aquest sistema operatiu, però el servidor **DHCP** de l'OS/2 l'utilitza per produir finestres de depuració.
CharFlag	charflag true	No	cert	No aplicable al servidor **DHCP** d'aquest sistema operatiu, però el servidor **DHCP** de l'OS/2 l'utilitza per produir finestres de depuració.
CharFlag	charflag false	No	cert	No aplicable al servidor **DHCP** d'aquest sistema operatiu, però el servidor **DHCP** de l'OS/2 l'utilitza per produir finestres de depuració.
CharFlag	charflag no	No	cert	No aplicable al servidor **DHCP** d'aquest sistema operatiu, però el servidor **DHCP** de l'OS/2 l'utilitza per produir finestres de depuració.
StatisticSnapShot	StatisticSnapShot *n*	No	-1, mai	Especifica la freqüència amb la qual les estadístiques s'escriuen al fitxer de registre en segons.
UsedIpAddressExpireInterval	UsedIpAddressExpireInterval *n time_units*	No	-1, mai	Especifica la freqüència amb la qual les adreces situades a l'estat ERRONI es recobren i es tornen a provar per validar-les.
leaseExpireInterval	leaseExpireInterval *n unitats_temps*	No	900 segons	Especifica la freqüència amb la qual les adreces de l'estat VINCULAT es comproven per veure si han caducat. Si l'adreça ha caducat, l'estat passa a CADUCAT.
reservedTime	reservedTime *n unitats_temps*	No	-1, mai	Especifica la freqüència amb la qual les adreces haurien de mantenir-se en estat RESERVAT abans de recobrar-se a l'estat LLIURE.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
reservedTimeInterval	reservedTimeInterval *n unitats_temps*	No	900 segons	Especifica la freqüència amb la qual les adreces de l'estat RESERVAT es comproven per veure si s'han de recobrar a l'estat LLIURE.
saveInterval	saveInterval *n unitats_temps*	No	3600 segons	Especifica la freqüència amb la qual el servidor **DHCP** hauria d'imposar un desament de les bases de dades obertes. Per als servidors molt carregats, hauria de ser 60 o 120 segons.
clientpruneintv	clientpruneintv *n unitats_temps*	No	3600 segons	Especifica la freqüència amb la qual el servidor **DHCP** fa que les bases de dades eliminin clients que no estan associats a cap adreça (a l'estat DESCONEGUT). Això redueix l'ús de memòria del servidor **DHCP**.
numprocessors	numprocessors *n*	No	10	Especifica el nombre de processadors de paquet que cal crear. Un com a mínim.
userObject	userObject *nom_obj*	Sí	Cap	Indica que el servidor hauria de carregar un objecte compartit definit per l'usuari i cridar les rutines dins l'objecte mitjançant cada interacció amb els clients **DHCP**. L'objecte que s'ha de carregar està localitzat al directori `/usr/sbin` amb el nom `obj_name.dhcpo`. Consulteu l'API d'extensió definida per l'usuari del servidor DHCP per obtenir més informació.
pxeservertype	pxeservertype *tipus_servidor*	No	dhcp_only	Indica el tipus de servidor **dhcpd** de què es tracta. El *tipus_servidor* pot ser un dels següents: **dhcp_pxe_binld** El **DHCP** du a terme les funcions **dhcpsd**, **pxed** i **bindl**. **proxy_on_dhcp_server** El **DHCP** remet el client PXE al port de servidor proxy de la mateixa màquina. El valor per defecte és `dhcp_only` i significa que el **dhcpsd** no dóna suport als clients PXE de la modalitat per defecte.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
supportsubnetselection	supportsubnetselection **global** supportsubnetselection **subnetlevel** supportsubnetselection **no**	No	Cap	Indica si el servidor dhcp donarà suport a l'opció 118 (opció de selecció de subxarxa) al paquet de DESCOBRIMENT o PETICIÓ dels clients. **global**: totes les subxarxes del fitxer de configuració donaran suport a l'opció 118. **subnetlevel**: les subxarxes que han estat configurades per donar suport a aquesta opció mitjançant la paraula clau supportoption118 li donaran suport. **no**: no dóna suport a l'opció 118.

Sintaxi de fitxer del servidor DHCP per a la base de dades db_file

La sintaxi de fitxer de la base de dades `db_file` té les propietats següents.

Nota:

1. Les Unitats de temps (*unitats_temps*) que es mostren a la taula següent són opcionals i representen un modificador de l'hora actual. La unitat de temps per defecte és els minuts. Són valors vàlids els segons (1), els minuts (60), les hores (3600), els dies (86400), les setmanes (604800), els mesos (2392000) i els anys (31536000). El nombre que apareix entre parèntesis és un multiplicador aplicat al valor específic *n* per expressar el valor en segons.
2. Pot ser que els elements que s'especifiquen en un contenidor s'alterin temporalment dins un subcontenidor. Per exemple, podríeu definir globalment els clients **BOOTP**, però permetre els clients **BOOTP** en una subxarxa determinada tot especificant la paraula clau supportBootp en ambdós contenidors.
3. Els contenidors de clients, classe i proveïdor permeten un suport d'expressió regular. Per als de classe i proveïdor, una sèrie entre cometes. El primer caràcter després de les cometes és un signe d'admiració (!) que indica que la resta de la sèrie s'ha de tractar com una expressió regular. El contenidor de clients permet les expressions regulars tant al camp tipus maquinari com al camp adreça maquinari. S'utilitza una sèrie simple per representar ambdós camps amb el format següent:

   ```
   decimal_number-data
   ```

   Si el nombre_decimal és el zero, aleshores la dada és una sèrie ASCII. Si és qualsevol altre nombre, la dada és en dígits hexadecimals.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
subnet	subxarxa per defecte	Sí	Cap	Especifica una subxarxa sense un abast associat. El servidor utilitza la subxarxa només quan respon a un paquet d' INFORMACIÓ/PETICIÓ del client i l'adreça del client no té cap altre contenidor de subxarxes coincident.
subnet	subnet*id de subxarxa màscara de xarxa*	Sí	Cap	Especifica una subxarxa i una agrupació d'adreces. Es pressuposa que totes les adreces són a l'agrupació a no ser que s'especifiqui un abast en la línia o que les adreces es modifiquin posteriorment al contenidor mitjançant un abast o una sentència d'exclusió. L'abast opcional és un parell d'adreces IP en format de quartet amb punt separades per un guió. Es pot especificar una etiqueta opcional i la prioritat. Les subxarxes virtuals les utilitzen per identificar i ordenar les subxarxes de la subxarxa virtual. Dos punts separen l'etiqueta de la prioritat. Aquests contenidors només es permeten a nivell de contenidor de base de dades o global.
subnet	subnet *id de subxarxa màscara de xarxa abast*	Sí	Cap	Especifica una subxarxa i una agrupació d'adreces. Es pressuposa que totes les adreces són a l'agrupació a no ser que s'especifiqui un abast en la línia o que les adreces es modifiquin posteriorment al contenidor mitjançant un abast o una sentència d'exclusió. L'abast opcional és un parell d'adreces IP en format de quartet amb punt separades per un guió. Es pot especificar una etiqueta opcional i la prioritat. Les subxarxes virtuals les utilitzen per identificar i ordenar les subxarxes de la subxarxa virtual. Dos punts separen l'etiqueta de la prioritat. Aquests contenidors només es permeten a nivell de contenidor de base de dades o global.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
subnet	subnet *id de subxarxa màscara de xarxa etiqueta:prioritat*	Sí	Cap	Especifica una subxarxa i una agrupació d'adreces. Es pressuposa que totes les adreces són a l'agrupació a no ser que s'especifiqui un abast en la línia o que les adreces es modifiquin posteriorment al contenidor mitjançant un abast o una sentència d'exclusió. L'abast opcional és un parell d'adreces IP en format de quartet amb punt separades per un guió. Es pot especificar una etiqueta opcional i la prioritat. Les subxarxes virtuals les utilitzen per identificar i ordenar les subxarxes de la subxarxa virtual. Dos punts separen l'etiqueta de la prioritat. Aquests contenidors només es permeten a nivell de contenidor de base de dades o global.
subnet	subnet *id de subxarxa màscara de xarxa abast etiqueta:prioritat*	Sí	Cap	Especifica una subxarxa i una agrupació d'adreces. Es pressuposa que totes les adreces són a l'agrupació a no ser que s'especifiqui un abast en la línia o que les adreces es modifiquin posteriorment al contenidor mitjançant un abast o una sentència d'exclusió. L'abast opcional és un parell d'adreces IP en format de quartet amb punt separades per un guió. Es pot especificar una etiqueta opcional i la prioritat. Les subxarxes virtuals les utilitzen per identificar i ordenar les subxarxes de la subxarxa virtual. Dos punts separen l'etiqueta de la prioritat. Aquests contenidors només es permeten a nivell de contenidor de base de dades o global.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
subnet	subnet *id de subxarxa abast*	Sí	Cap	Especifica una subxarxa que va en un contenidor de xarxa. Defineix un abast d'adreces que és tota la subxarxa a no ser que s'especifiqui la part d'abast opcional. La màscara de xarxa associada a la subxarxa s'agafa del contenidor de xarxa circumdant. **Nota:** Aquest mètode es desaprova a favor de les altres formes de subxarxa.
option	option *nombre dades* ...	No	Cap	Especifica una opció per enviar-la a un client o, en cas que s'hagi denegat, una opció que eviti l'enviament al client. L'opció `* deny` la clàusula significa que totes les opcions que no s'especifiquin al contenidor actual no es retornaran al client. L'opció *nombre*deny només denega l'opció especificada. *nombre* és un enter de 8 bits sense signe. *dades* és específic de l'opció (consulteu més amunt) o bé es pot especificar com a sèrie entre cometes (que indiqui el text ASCII) o 0x*dígits_hexadecimals* o hex"*dígits_hexadecimals*" o hex "*dígits_hexadecimals*". Si l'opció es troba en un contenidor de proveïdors, s'encapsularà amb altres opcions en una opció 43.
option	option *nombre*deny	No	Cap	Especifica una opció per enviar-la a un client o, en cas que s'hagi denegat, una opció que eviti l'enviament al client. L'opció `* deny` la clàusula significa que totes les opcions que no s'especifiquin al contenidor actual no es retornaran al client. L'opció *nombre*deny només denega l'opció especificada. *nombre* és un enter de 8 bits sense signe. *dades* és específic de l'opció (consulteu més amunt) o bé es pot especificar com a sèrie entre cometes (que indiqui el text ASCII) o 0x*dígits_hexadecimals* o hex"*dígits_hexadecimals*" o hex "*dígits_hexadecimals*". Si l'opció es troba en un contenidor de proveïdors, s'encapsularà amb altres opcions en una opció 43.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
option	option * deny	No	Cap	Especifica una opció per enviar-la a un client o, en cas que s'hagi denegat, una opció que eviti l'enviament al client. L'opció `* deny` la clàusula significa que totes les opcions que no s'especifiquin al contenidor actual no es retornaran al client. L'opció *nombre*deny només denega l'opció especificada. *nombre* és un enter de 8 bits sense signe. *dades* és específic de l'opció (consulteu més amunt) o bé es pot especificar com a sèrie entre cometes (que indiqui el text ASCII) o 0x*dígits_hexadecimals* o hex"*dígits_hexadecimals*" o hex "*dígits_hexadecimals*". Si l'opció es troba en un contenidor de proveïdors, s'encapsularà amb altres opcions en una opció 43.
exclude	exclude *una adreça IP*	No	Cap	Modifica l'abast al contenidor on hi ha la sentència d'exclusió. Als nivells de contenidor de base de dades o global, la sentència d'exclusió no és vàlida. Aquesta sentència elimina de l'abast actual del contenidor l'adreça o abast especificats. La sentència d'exclusió us permet crear abasts no contigus per a les subxarxes o altres contenidors.
exclude	exclude *quartet_amb_punt-quartet_amb_punt*	No	Cap	Modifica l'abast al contenidor on hi ha la sentència d'exclusió. Als nivells de contenidor de base de dades o global, la sentència d'exclusió no és vàlida. Aquesta sentència elimina de l'abast actual del contenidor l'adreça o abast especificats. La sentència d'exclusió us permet crear abasts no contigus per a les subxarxes o altres contenidors.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
range	range *adreça_IP*	No	Cap	Modifica l'abast al contenidor on hi ha la sentència d'abast. Als nivells de contenidor de base de dades o global, la sentència d'abast no és vàlida. Si l'abast és el primer del contenidor que no especifica un abast a la línia de definició del contenidor, aleshores l'abast per al contenidor esdevé l'abast especificat per la sentència d'abast. S'afegeixen a l'abast actual qualsevol sentència d'abast després del primer abast o totes les sentències d'abast per a un contenidor que especifiqui abasts a la definició. Amb la sentència d'abast, es poden afegir a l'abast una sola adreça o bé un grup d'adreces. L'abast ha d'encaixar dins la definició de contenidor de subxarxes.
range	range *quartet_amb_punt-quartet_amb_punt*	No	Cap	Modifica l'abast al contenidor on hi ha la sentència d'abast. Als nivells de contenidor de base de dades o global, la sentència d'abast no és vàlida. Si l'abast és el primer del contenidor que no especifica un abast a la línia de definició del contenidor, aleshores l'abast per al contenidor esdevé l'abast especificat per la sentència d'abast. S'afegeixen a l'abast actual qualsevol sentència d'abast després del primer abast o totes les sentències d'abast per a un contenidor que especifiqui abasts a la definició. Amb la sentència d'abast, es poden afegir a l'abast una sola adreça o bé un grup d'adreces. L'abast ha d'encaixar dins la definició de contenidor de subxarxes.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
client	client *tipus maquinari adreça maquinari* NONE	Sí	Cap	Especifica un contenidor de clients que denega al client especificat per l'*adreça maquinari* i el *tipus maquinari* l'obtenció d'una adreça. Si el *tipus maquinari* és igual a 0, llavors l'*adreça maquinari* és una sèrie ASCII. Altrament, el *tipus maquinari* és el tipus de maquinari per al client i l'*adreça maquinari* és l'adreça de maquinari del client. Si l'*adreça maquinari* és una sèrie, s'accepten els caràcters de cometes al voltant de la sèrie. Si l'*adreça maquinari* és una sèrie hexadecimal, llavors l'adreça es pot especificar amb 0x*dígits_hexadecimals* o hex *dígits*. L'*abast* fa que el client especificat mitjançant l'*adreça maquinari* i el *tipus maquinari* obtingui una adreça a l'*abast*. Per coincidir amb diversos clients, han de ser expressions regulars.
client	client *tipus maquinari adreça maquinari* ANY	Sí	Cap	Especifica un contenidor de clients que denega al client especificat per l'*adreça maquinari* i el *tipus maquinari* l'obtenció d'una adreça. Si el *tipus maquinari* és igual a 0, llavors l'*adreça maquinari* és una sèrie ASCII. Altrament, el *tipus maquinari* és el tipus de maquinari per al client i l'*adreça maquinari* és l'adreça de maquinari del client. Si l'*adreça maquinari* és una sèrie, s'accepten els caràcters de cometes al voltant de la sèrie. Si l'*adreça maquinari* és una sèrie hexadecimal, llavors l'adreça es pot especificar amb 0x*dígits_hexadecimals* o hex *dígits*. L'*abast* fa que el client especificat mitjançant l'*adreça maquinari* i el *tipus maquinari* obtingui una adreça a l'*abast*. Per coincidir amb diversos clients, han de ser expressions regulars.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
client	client *tipus maquinari adreça maquinari quartet_amb_punt*	Sí	Cap	Especifica un contenidor de clients que denega al client especificat per l'*adreça maquinari* i el *tipus maquinari* l'obtenció d'una adreça. Si el *tipus maquinari* és igual a 0, llavors l'*adreça maquinari* és una sèrie ASCII. Altrament, el *tipus maquinari* és el tipus de maquinari per al client i l'*adreça maquinari* és l'adreça de maquinari del client. Si l'*adreça maquinari* és una sèrie, s'accepten els caràcters de cometes al voltant de la sèrie. Si l'*adreça maquinari* és una sèrie hexadecimal, llavors l'adreça es pot especificar amb 0x*dígits_hexadecimals* o hex *dígits*. L'*abast* fa que el client especificat mitjançant l'*adreça maquinari* i el *tipus maquinari* obtingui una adreça a l'*abast*. Per coincidir amb diversos clients, han de ser expressions regulars.
client	client *tipus maquinari adreça maquinari abast*	Sí	Cap	Especifica un contenidor de clients que denega al client especificat per l'*adreça maquinari* i el *tipus maquinari* l'obtenció d'una adreça. Si el *tipus maquinari* és igual a 0, llavors l'*adreça maquinari* és una sèrie ASCII. Altrament, el *tipus maquinari* és el tipus de maquinari per al client i l'*adreça maquinari* és l'adreça de maquinari del client. Si l'*adreça maquinari* és una sèrie, s'accepten els caràcters de cometes al voltant de la sèrie. Si l'*adreça maquinari* és una sèrie hexadecimal, llavors l'adreça es pot especificar amb 0x*dígits_hexadecimals* o hex *dígits*. L'*abast* fa que el client especificat mitjançant l'*adreça maquinari* i el *tipus maquinari* obtingui una adreça a l'*abast*. Per coincidir amb diversos clients, han de ser expressions regulars.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
class	class *sèrie*	Sí	Cap	Especifica un contenidor de classes amb *sèrie* de nom. La sèrie pot estar entre cometes o no. Si està entre cometes, les cometes s'eliminen abans de la comparació. Les cometes són necessàries en les sèries amb espais o tabuladors. Aquest contenidor és vàlid a qualsevol nivell. Es pot especificar un abast per indicar un conjunt d'adreces que es lliuren a un client amb aquesta classe. L'abast és només una adreça IP de quartet amb punt o bé dues adreces IP de quartet amb punt separades per un guió.
class	class *sèrie abast*	Sí	Cap	Especifica un contenidor de classes amb *sèrie* de nom. La sèrie pot estar entre cometes o no. Si està entre cometes, les cometes s'eliminen abans de la comparació. Les cometes són necessàries en les sèries amb espais o tabuladors. Aquest contenidor és vàlid a qualsevol nivell. Es pot especificar un abast per indicar un conjunt d'adreces que es lliuren a un client amb aquesta classe. L'abast és només una adreça IP de quartet amb punt o bé dues adreces IP de quartet amb punt separades per un guió.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
network	network *id de xarxa màscara de xarxa*	Sí	Cap	Especifica un contenidor que cal fer coincidir amb qualsevol opció d'entrada arbitrària especificada pel client. El *nombre* especifica el nombre d'opció. *dades_opció* especifica la clau que cal fer coincidir per tal que se seleccioni aquest contenidor durant la selecció d'opció i d'adreça per al client. *dades_opció* s'especifica de forma esperada — amb una sèrie entre cometes, una adreça IP, un valor enter — en les opcions conegudes o bé es pot especificar opcionalment mitjançant una sèrie hexadecimal d'octets si la precedeixen els caràcters `0x`. Pel que fa a les opcions que el servidor no coneix, es pot especificar una sèrie hexadecimal d'octets de la mateixa manera. Addicionalment, *dades_opció* pot indicar una expressió regular que cal comparar amb la representació de sèrie de les dades d'opció del client. Les expressions regulars s'especifiquen en una sèrie entre cometes que comença amb `"!` (caràcter de cometes dobles seguit d'un signe d'exclamació). La forma en sèrie d'opcions menys conegudes pel servidor és una sèrie hexadecimal d'octets SENSE els caràcters `0x` al davant

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
network	network *id de xarxa*	Sí	Cap	Especifica un contenidor que cal fer coincidir amb qualsevol opció d'entrada arbitrària especificada pel client. El *nombre* especifica el nombre d'opció. *dades_opció* especifica la clau que cal fer coincidir per tal que se seleccioni aquest contenidor durant la selecció d'opció i d'adreça per al client. *dades_opció* s'especifica de forma esperada — amb una sèrie entre cometes, una adreça IP, un valor enter — en les opcions conegudes o bé es pot especificar opcionalment mitjançant una sèrie hexadecimal d'octets si la precedeixen els caràcters `0x`. Pel que fa a les opcions que el servidor no coneix, es pot especificar una sèrie hexadecimal d'octets de la mateixa manera. Addicionalment, *dades_opció* pot indicar una expressió regular que cal comparar amb la representació de sèrie de les dades d'opció del client. Les expressions regulars s'especifiquen en una sèrie entre cometes que comença amb `"!` (caràcter de cometes dobles seguit d'un signe d'exclamació). La forma en sèrie d'opcions menys conegudes pel servidor és una sèrie hexadecimal d'octets SENSE els caràcters `0x` al davant

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
network	network *id de xarxa abast*	Sí	Cap	Especifica un contenidor que cal fer coincidir amb qualsevol opció d'entrada arbitrària especificada pel client. El *nombre* especifica el nombre d'opció. *dades_opció* especifica la clau que cal fer coincidir per tal que se seleccioni aquest contenidor durant la selecció d'opció i d'adreça per al client. *dades_opció* s'especifica de forma esperada — amb una sèrie entre cometes, una adreça IP, un valor enter — en les opcions conegudes o bé es pot especificar opcionalment mitjançant una sèrie hexadecimal d'octets si la precedeixen els caràcters `0x`. Pel que fa a les opcions que el servidor no coneix, es pot especificar una sèrie hexadecimal d'octets de la mateixa manera. Addicionalment, *dades_opció* pot indicar una expressió regular que cal comparar amb la representació de sèrie de les dades d'opció del client. Les expressions regulars s'especifiquen en una sèrie entre cometes que comença amb `"!` (caràcter de cometes dobles seguit d'un signe d'exclamació). La forma en sèrie d'opcions menys conegudes pel servidor és una sèrie hexadecimal d'octets SENSE els caràcters `0x` al davant

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
vendor	vendor *id_proveïdor*	Sí	Cap	Especifica un contenidor que cal fer coincidir amb qualsevol opció d'entrada arbitrària especificada pel client. El *nombre* especifica el nombre d'opció. *dades_opció* especifica la clau que cal fer coincidir per tal que se seleccioni aquest contenidor durant la selecció d'opció i d'adreça per al client. *dades_opció* s'especifica de forma esperada — amb una sèrie entre cometes, una adreça IP, un valor enter — en les opcions conegudes o bé es pot especificar opcionalment mitjançant una sèrie hexadecimal d'octets si la precedeixen els caràcters `0x`. Pel que fa a les opcions que el servidor no coneix, es pot especificar una sèrie hexadecimal d'octets de la mateixa manera. Addicionalment, *dades_opció* pot indicar una expressió regular que cal comparar amb la representació de sèrie de les dades d'opció del client. Les expressions regulars s'especifiquen en una sèrie entre cometes que comença amb `"!` (caràcter de cometes dobles seguit d'un signe d'exclamació). La forma en sèrie d'opcions menys conegudes pel servidor és una sèrie hexadecimal d'octets SENSE els caràcters `0x` al davant

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
vendor	vendor *id_proveïdor* hex""	Sí	Cap	Especifica un contenidor que cal fer coincidir amb qualsevol opció d'entrada arbitrària especificada pel client. El *nombre* especifica el nombre d'opció. *dades_opció* especifica la clau que cal fer coincidir per tal que se seleccioni aquest contenidor durant la selecció d'opció i d'adreça per al client. *dades_opció* s'especifica de forma esperada — amb una sèrie entre cometes, una adreça IP, un valor enter — en les opcions conegudes o bé es pot especificar opcionalment mitjançant una sèrie hexadecimal d'octets si la precedeixen els caràcters `0x`. Pel que fa a les opcions que el servidor no coneix, es pot especificar una sèrie hexadecimal d'octets de la mateixa manera. Addicionalment, *dades_opció* pot indicar una expressió regular que cal comparar amb la representació de sèrie de les dades d'opció del client. Les expressions regulars s'especifiquen en una sèrie entre cometes que comença amb `"!` (caràcter de cometes dobles seguit d'un signe d'exclamació). La forma en sèrie d'opcions menys conegudes pel servidor és una sèrie hexadecimal d'octets SENSE els caràcters `0x` al davant

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
vendor	vendor *id_proveïdor* hex ""	Sí	Cap	Especifica un contenidor que cal fer coincidir amb qualsevol opció d'entrada arbitrària especificada pel client. El *nombre* especifica el nombre d'opció. *dades_opció* especifica la clau que cal fer coincidir per tal que se seleccioni aquest contenidor durant la selecció d'opció i d'adreça per al client. *dades_opció* s'especifica de forma esperada — amb una sèrie entre cometes, una adreça IP, un valor enter — en les opcions conegudes o bé es pot especificar opcionalment mitjançant una sèrie hexadecimal d'octets si la precedeixen els caràcters `0x`. Pel que fa a les opcions que el servidor no coneix, es pot especificar una sèrie hexadecimal d'octets de la mateixa manera. Addicionalment, *dades_opció* pot indicar una expressió regular que cal comparar amb la representació de sèrie de les dades d'opció del client. Les expressions regulars s'especifiquen en una sèrie entre cometes que comença amb `"!` (caràcter de cometes dobles seguit d'un signe d'exclamació). La forma en sèrie d'opcions menys conegudes pel servidor és una sèrie hexadecimal d'octets SENSE els caràcters `0x` al davant

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
vendor	vendor *id_proveïdor* 0xdata	Sí	Cap	Especifica un contenidor que cal fer coincidir amb qualsevol opció d'entrada arbitrària especificada pel client. El *nombre* especifica el nombre d'opció. *dades_opció* especifica la clau que cal fer coincidir per tal que se seleccioni aquest contenidor durant la selecció d'opció i d'adreça per al client. *dades_opció* s'especifica de forma esperada — amb una sèrie entre cometes, una adreça IP, un valor enter — en les opcions conegudes o bé es pot especificar opcionalment mitjançant una sèrie hexadecimal d'octets si la precedeixen els caràcters `0x`. Pel que fa a les opcions que el servidor no coneix, es pot especificar una sèrie hexadecimal d'octets de la mateixa manera. Addicionalment, *dades_opció* pot indicar una expressió regular que cal comparar amb la representació de sèrie de les dades d'opció del client. Les expressions regulars s'especifiquen en una sèrie entre cometes que comença amb `"!` (caràcter de cometes dobles seguit d'un signe d'exclamació). La forma en sèrie d'opcions menys conegudes pel servidor és una sèrie hexadecimal d'octets SENSE els caràcters `0x` al davant

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
vendor	vendor *id_proveïdor* ""	Sí	Cap	Especifica un contenidor que cal fer coincidir amb qualsevol opció d'entrada arbitrària especificada pel client. El *nombre* especifica el nombre d'opció. *dades_opció* especifica la clau que cal fer coincidir per tal que se seleccioni aquest contenidor durant la selecció d'opció i d'adreça per al client. *dades_opció* s'especifica de forma esperada — amb una sèrie entre cometes, una adreça IP, un valor enter — en les opcions conegudes o bé es pot especificar opcionalment mitjançant una sèrie hexadecimal d'octets si la precedeixen els caràcters `0x`. Pel que fa a les opcions que el servidor no coneix, es pot especificar una sèrie hexadecimal d'octets de la mateixa manera. Addicionalment, *dades_opció* pot indicar una expressió regular que cal comparar amb la representació de sèrie de les dades d'opció del client. Les expressions regulars s'especifiquen en una sèrie entre cometes que comença amb `"!` (caràcter de cometes dobles seguit d'un signe d'exclamació). La forma en sèrie d'opcions menys conegudes pel servidor és una sèrie hexadecimal d'octets SENSE els caràcters `0x` al davant

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
vendor	vendor *id_proveïdor abast*	Sí	Cap	Especifica un contenidor que cal fer coincidir amb qualsevol opció d'entrada arbitrària especificada pel client. El *nombre* especifica el nombre d'opció. *dades_opció* especifica la clau que cal fer coincidir per tal que se seleccioni aquest contenidor durant la selecció d'opció i d'adreça per al client. *dades_opció* s'especifica de forma esperada — amb una sèrie entre cometes, una adreça IP, un valor enter — en les opcions conegudes o bé es pot especificar opcionalment mitjançant una sèrie hexadecimal d'octets si la precedeixen els caràcters `0x`. Pel que fa a les opcions que el servidor no coneix, es pot especificar una sèrie hexadecimal d'octets de la mateixa manera. Addicionalment, *dades_opció* pot indicar una expressió regular que cal comparar amb la representació de sèrie de les dades d'opció del client. Les expressions regulars s'especifiquen en una sèrie entre cometes que comença amb `"!` (caràcter de cometes dobles seguit d'un signe d'exclamació). La forma en sèrie d'opcions menys conegudes pel servidor és una sèrie hexadecimal d'octets SENSE els caràcters `0x` al davant

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
vendor	vendor *id_proveïdor abast* hex""	Sí	Cap	Especifica un contenidor que cal fer coincidir amb qualsevol opció d'entrada arbitrària especificada pel client. El *nombre* especifica el nombre d'opció. *dades_opció* especifica la clau que cal fer coincidir per tal que se seleccioni aquest contenidor durant la selecció d'opció i d'adreça per al client. *dades_opció* s'especifica de forma esperada — amb una sèrie entre cometes, una adreça IP, un valor enter — en les opcions conegudes o bé es pot especificar opcionalment mitjançant una sèrie hexadecimal d'octets si la precedeixen els caràcters `0x`. Pel que fa a les opcions que el servidor no coneix, es pot especificar una sèrie hexadecimal d'octets de la mateixa manera. Addicionalment, *dades_opció* pot indicar una expressió regular que cal comparar amb la representació de sèrie de les dades d'opció del client. Les expressions regulars s'especifiquen en una sèrie entre cometes que comença amb `"!` (caràcter de cometes dobles seguit d'un signe d'exclamació). La forma en sèrie d'opcions menys conegudes pel servidor és una sèrie hexadecimal d'octets SENSE els caràcters `0x` al davant

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
vendor	vendor *id_proveïdor abast* hex ""	Sí	Cap	Especifica un contenidor que cal fer coincidir amb qualsevol opció d'entrada arbitrària especificada pel client. El *nombre* especifica el nombre d'opció. *dades_opció* especifica la clau que cal fer coincidir per tal que se seleccioni aquest contenidor durant la selecció d'opció i d'adreça per al client. *dades_opció* s'especifica de forma esperada — amb una sèrie entre cometes, una adreça IP, un valor enter — en les opcions conegudes o bé es pot especificar opcionalment mitjançant una sèrie hexadecimal d'octets si la precedeixen els caràcters `0x`. Pel que fa a les opcions que el servidor no coneix, es pot especificar una sèrie hexadecimal d'octets de la mateixa manera. Addicionalment, *dades_opció* pot indicar una expressió regular que cal comparar amb la representació de sèrie de les dades d'opció del client. Les expressions regulars s'especifiquen en una sèrie entre cometes que comença amb `"!` (caràcter de cometes dobles seguit d'un signe d'exclamació). La forma en sèrie d'opcions menys conegudes pel servidor és una sèrie hexadecimal d'octets SENSE els caràcters `0x` al davant

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
vendor	vendor *id_proveïdor abast* 0xdata	Sí	Cap	Especifica un contenidor que cal fer coincidir amb qualsevol opció d'entrada arbitrària especificada pel client. El *nombre* especifica el nombre d'opció. *dades_opció* especifica la clau que cal fer coincidir per tal que se seleccioni aquest contenidor durant la selecció d'opció i d'adreça per al client. *dades_opció* s'especifica de forma esperada — amb una sèrie entre cometes, una adreça IP, un valor enter — en les opcions conegudes o bé es pot especificar opcionalment mitjançant una sèrie hexadecimal d'octets si la precedeixen els caràcters `0x`. Pel que fa a les opcions que el servidor no coneix, es pot especificar una sèrie hexadecimal d'octets de la mateixa manera. Addicionalment, *dades_opció* pot indicar una expressió regular que cal comparar amb la representació de sèrie de les dades d'opció del client. Les expressions regulars s'especifiquen en una sèrie entre cometes que comença amb `"!` (caràcter de cometes dobles seguit d'un signe d'exclamació). La forma en sèrie d'opcions menys conegudes pel servidor és una sèrie hexadecimal d'octets SENSE els caràcters `0x` al davant

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
vendor	vendor *id_proveïdor abast* ""	Sí	Cap	Especifica un contenidor que cal fer coincidir amb qualsevol opció d'entrada arbitrària especificada pel client. El *nombre* especifica el nombre d'opció. *dades_opció* especifica la clau que cal fer coincidir per tal que se seleccioni aquest contenidor durant la selecció d'opció i d'adreça per al client. *dades_opció* s'especifica de forma esperada — amb una sèrie entre cometes, una adreça IP, un valor enter — en les opcions conegudes o bé es pot especificar opcionalment mitjançant una sèrie hexadecimal d'octets si la precedeixen els caràcters `0x`. Pel que fa a les opcions que el servidor no coneix, es pot especificar una sèrie hexadecimal d'octets de la mateixa manera. Addicionalment, *dades_opció* pot indicar una expressió regular que cal comparar amb la representació de sèrie de les dades d'opció del client. Les expressions regulars s'especifiquen en una sèrie entre cometes que comença amb `"!` (caràcter de cometes dobles seguit d'un signe d'exclamació). La forma en sèrie d'opcions menys conegudes pel servidor és una sèrie hexadecimal d'octets SENSE els caràcters `0x` al davant

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
inoption	inoption *nombre dades_opció*	Sí	Cap	Especifica un contenidor que cal fer coincidir amb qualsevol opció d'entrada arbitrària especificada pel client. El *nombre* especifica el nombre d'opció. *dades_opció* especifica la clau que cal fer coincidir per tal que se seleccioni aquest contenidor durant la selecció d'opció i d'adreça per al client. *dades_opció* s'especifica de forma esperada — amb una sèrie entre cometes, una adreça IP, un valor enter — en les opcions conegudes o bé es pot especificar opcionalment mitjançant una sèrie hexadecimal d'octets si la precedeixen els caràcters `0x`. Pel que fa a les opcions que el servidor no coneix, es pot especificar una sèrie hexadecimal d'octets de la mateixa manera. Addicionalment, *dades_opció* pot indicar una expressió regular que cal comparar amb la representació de sèrie de les dades d'opció del client. Les expressions regulars s'especifiquen en una sèrie entre cometes que comença amb `"!` (caràcter de cometes dobles seguit d'un signe d'exclamació). La forma en sèrie d'opcions menys conegudes pel servidor és una sèrie hexadecimal d'octets SENSE els caràcters `0x` al davant

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
inoption	inoption *nombre dades_opció abast*	Sí	Cap	Especifica un contenidor que cal fer coincidir amb qualsevol opció d'entrada arbitrària especificada pel client. El *nombre* especifica el nombre d'opció. *dades_opció* especifica la clau que cal fer coincidir per tal que se seleccioni aquest contenidor durant la selecció d'opció i d'adreça per al client. *dades_opció* s'especifica de forma esperada — amb una sèrie entre cometes, una adreça IP, un valor enter — en les opcions conegudes o bé es pot especificar opcionalment mitjançant una sèrie hexadecimal d'octets si la precedeixen els caràcters `0x`. Pel que fa a les opcions que el servidor no coneix, es pot especificar una sèrie hexadecimal d'octets de la mateixa manera. Addicionalment, *dades_opció* pot indicar una expressió regular que cal comparar amb la representació de sèrie de les dades d'opció del client. Les expressions regulars s'especifiquen en una sèrie entre cometes que comença amb `"!` (caràcter de cometes dobles seguit d'un signe d'exclamació). La forma en sèrie d'opcions menys conegudes pel servidor és una sèrie hexadecimal d'octets SENSE els caràcters `0x` al davant

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
virtual	virtual fill *id id* ...	No	Cap	Especifica una subxarxa virtual amb una política. `fill` significa utilitzar totes les adreces del contenidor abans d'anar al contenidor següent. `rotate` significa seleccionar una adreça de l'agrupació següent de la llista a cada sol•licitud. `sfill` i `srotate` són el mateix que `fill` i `rotate`, però es realitza una cerca per veure si el client coincideix amb els contenidors, els proveïdors o les classes de la subxarxa. Si es troba una coincidència que pot subministrar una adreça, s'agafa l'adreça d'aquest contenidor en lloc de seguir les normes. Hi pot haver tots els IDs que calgui. L'*id* és l'ID de subxarxa de la definició de subxarxa o l'etiqueta de la definició de subxarxa. L'etiqueta és necessària si hi ha diverses subxarxes amb el mateix id de subxarxa.
virtual	virtual sfill *id id* ...	No	Cap	Especifica una subxarxa virtual amb una política. `fill` significa utilitzar totes les adreces del contenidor abans d'anar al contenidor següent. `rotate` significa seleccionar una adreça de l'agrupació següent de la llista a cada sol•licitud. `sfill` i `srotate` són el mateix que `fill` i `rotate`, però es realitza una cerca per veure si el client coincideix amb els contenidors, els proveïdors o les classes de la subxarxa. Si es troba una coincidència que pot subministrar una adreça, s'agafa l'adreça d'aquest contenidor en lloc de seguir les normes. Hi pot haver tots els IDs que calgui. L'*id* és l'ID de subxarxa de la definició de subxarxa o l'etiqueta de la definició de subxarxa. L'etiqueta és necessària si hi ha diverses subxarxes amb el mateix id de subxarxa.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
virtual	virtual rotate *id id* ...	No	Cap	Especifica una subxarxa virtual amb una política. `fill` significa utilitzar totes les adreces del contenidor abans d'anar al contenidor següent. `rotate` significa seleccionar una adreça de l'agrupació següent de la llista a cada sol•licitud. `sfill` i `srotate` són el mateix que `fill` i `rotate`, però es realitza una cerca per veure si el client coincideix amb els contenidors, els proveïdors o les classes de la subxarxa. Si es troba una coincidència que pot subministrar una adreça, s'agafa l'adreça d'aquest contenidor en lloc de seguir les normes. Hi pot haver tots els IDs que calgui. L'*id* és l'ID de subxarxa de la definició de subxarxa o l'etiqueta de la definició de subxarxa. L'etiqueta és necessària si hi ha diverses subxarxes amb el mateix id de subxarxa.
virtual	virtual srotate *id id* ...	No	Cap	Especifica una subxarxa virtual amb una política. `fill` significa utilitzar totes les adreces del contenidor abans d'anar al contenidor següent. `rotate` significa seleccionar una adreça de l'agrupació següent de la llista a cada sol•licitud. `sfill` i `srotate` són el mateix que `fill` i `rotate`, però es realitza una cerca per veure si el client coincideix amb els contenidors, els proveïdors o les classes de la subxarxa. Si es troba una coincidència que pot subministrar una adreça, s'agafa l'adreça d'aquest contenidor en lloc de seguir les normes. Hi pot haver tots els IDs que calgui. L'*id* és l'ID de subxarxa de la definició de subxarxa o l'etiqueta de la definició de subxarxa. L'etiqueta és necessària si hi ha diverses subxarxes amb el mateix id de subxarxa.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
inorder:	inorder: *id id ...*	No	Cap	Especifica una subxarxa virtual amb unes normes d'emplenament. Això vol dir que s'han d'utilitzar totes les adreces del contenidor abans d'anar al següent. Hi pot haver tots els IDs que calgui. L'*id* és l'ID de subxarxa de la definició de subxarxa o l'etiqueta de la definició de subxarxa. L'etiqueta és necessària si hi ha diverses subxarxes amb el mateix ID de subxarxa.
balance:	balance: *id id ...*	No	Cap	Especifica una subxarxa virtual amb unes normes de rotació. Això vol dir que s'ha d'utilitzar l'adreça següent al contenidor següent. Hi pot haver tots els IDs que calgui. L'*id* és l'ID de subxarxa de la definició de subxarxa o l'etiqueta de la definició de subxarxa. L'etiqueta és necessària si hi ha diverses subxarxes amb el mateix ID de subxarxa.
supportBootp	supportBootp true	No	Sí	Especifica si el contenidor corrent i tots els de sota (fins que no s'alterin temporalment) han de donar suport als clients **BOOTP**.
supportBootp	supportBootp 1	No	Sí	Especifica si el contenidor corrent i tots els de sota (fins que no s'alterin temporalment) han de donar suport als clients **BOOTP**.
supportBootp	supportBootp yes	No	Sí	Especifica si el contenidor corrent i tots els de sota (fins que no s'alterin temporalment) han de donar suport als clients **BOOTP**.
supportBootp	supportBootp false	No	Sí	Especifica si el contenidor corrent i tots els de sota (fins que no s'alterin temporalment) han de donar suport als clients **BOOTP**.
supportBootp	supportBootp 0	No	Sí	Especifica si el contenidor corrent i tots els de sota (fins que no s'alterin temporalment) han de donar suport als clients **BOOTP**.
supportBootp	supportBootp no	No	Sí	Especifica si el contenidor corrent i tots els de sota (fins que no s'alterin temporalment) han de donar suport als clients **BOOTP**.
supportBootp				Especifica si el contenidor corrent i tots els de sota (fins que no s'alterin temporalment) han de donar suport als clients **BOOTP**.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
supportUnlistedclients	supportUnlistedclients BOTH	No	Ambdós	Especifica si el contenidor corrent i tots els de sota (fins que no s'alterin temporalment) han de donar suport als clients que no apareixen a la llista. El valor indica si tots els clients haurien de tenir accés sense sentències de client específic, només els clients **DHCP**, només els clients **BOOTP** o bé cap. **Nota:** Els valors certs i falsos són suportats per compatibilitat amb versions anteriors i es desaproven. El valor cert correspon a AMBDÓS i el valor fals, a CAP.
supportUnlistedclients	supportUnlistedclients DHCP	No	Ambdós	Especifica si el contenidor corrent i tots els de sota (fins que no s'alterin temporalment) han de donar suport als clients que no apareixen a la llista. El valor indica si tots els clients haurien de tenir accés sense sentències de client específic, només els clients **DHCP**, només els clients **BOOTP** o bé cap. **Nota:** Els valors certs i falsos són suportats per compatibilitat amb versions anteriors i es desaproven. El valor cert correspon a AMBDÓS i el valor fals, a CAP.
supportUnlistedclients	supportUnlistedclients BOOTP	No	Ambdós	Especifica si el contenidor corrent i tots els de sota (fins que no s'alterin temporalment) han de donar suport als clients que no apareixen a la llista. El valor indica si tots els clients haurien de tenir accés sense sentències de client específic, només els clients **DHCP**, només els clients **BOOTP** o bé cap. **Nota:** Els valors certs i falsos són suportats per compatibilitat amb versions anteriors i es desaproven. El valor cert correspon a AMBDÓS i el valor fals, a CAP.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
supportUnlistedclients	supportUnlistedclients NONE	No	Ambdós	Especifica si el contenidor corrent i tots els de sota (fins que no s'alterin temporalment) han de donar suport als clients que no apareixen a la llista. El valor indica si tots els clients haurien de tenir accés sense sentències de client específic, només els clients **DHCP**, només els clients **BOOTP** o bé cap. **Nota:** Els valors certs i falsos són suportats per compatibilitat amb versions anteriors i es desaproven. El valor cert correspon a AMBDÓS i el valor fals, a CAP.
supportUnlistedclients	supportUnlistedclients true	No	Ambdós	Especifica si el contenidor corrent i tots els de sota (fins que no s'alterin temporalment) han de donar suport als clients que no apareixen a la llista. El valor indica si tots els clients haurien de tenir accés sense sentències de client específic, només els clients **DHCP**, només els clients **BOOTP** o bé cap. **Nota:** Els valors certs i falsos són suportats per compatibilitat amb versions anteriors i es desaproven. El valor cert correspon a AMBDÓS i el valor fals, a CAP.
supportUnlistedclients	supportUnlistedclients yes	No	Ambdós	Especifica si el contenidor corrent i tots els de sota (fins que no s'alterin temporalment) han de donar suport als clients que no apareixen a la llista. El valor indica si tots els clients haurien de tenir accés sense sentències de client específic, només els clients **DHCP**, només els clients **BOOTP** o bé cap. **Nota:** Els valors certs i falsos són suportats per compatibilitat amb versions anteriors i es desaproven. El valor cert correspon a AMBDÓS i el valor fals, a CAP.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
supportUnlistedclients	supportUnlistedclients 1	No	Ambdós	Especifica si el contenidor corrent i tots els de sota (fins que no s'alterin temporalment) han de donar suport als clients que no apareixen a la llista. El valor indica si tots els clients haurien de tenir accés sense sentències de client específic, només els clients **DHCP**, només els clients **BOOTP** o bé cap. **Nota:** Els valors certs i falsos són suportats per compatibilitat amb versions anteriors i es desaproven. El valor cert correspon a AMBDÓS i el valor fals, a CAP.
supportUnlistedclients	supportUnlistedclients false	No	Ambdós	Especifica si el contenidor corrent i tots els de sota (fins que no s'alterin temporalment) han de donar suport als clients que no apareixen a la llista. El valor indica si tots els clients haurien de tenir accés sense sentències de client específic, només els clients **DHCP**, només els clients **BOOTP** o bé cap. **Nota:** Els valors certs i falsos són suportats per compatibilitat amb versions anteriors i es desaproven. El valor cert correspon a AMBDÓS i el valor fals, a CAP.
supportUnlistedclients	supportUnlistedclients no	No	Ambdós	Especifica si el contenidor corrent i tots els de sota (fins que no s'alterin temporalment) han de donar suport als clients que no apareixen a la llista. El valor indica si tots els clients haurien de tenir accés sense sentències de client específic, només els clients **DHCP**, només els clients **BOOTP** o bé cap. **Nota:** Els valors certs i falsos són suportats per compatibilitat amb versions anteriors i es desaproven. El valor cert correspon a AMBDÓS i el valor fals, a CAP.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
supportUnlistedclients	supportUnlistedclients 0	No	Ambdós	Especifica si el contenidor corrent i tots els de sota (fins que no s'alterin temporalment) han de donar suport als clients que no apareixen a la llista. El valor indica si tots els clients haurien de tenir accés sense sentències de client específic, només els clients **DHCP**, només els clients **BOOTP** o bé cap. **Nota:** Els valors certs i falsos són suportats per compatibilitat amb versions anteriors i es desaproven. El valor cert correspon a AMBDÓS i el valor fals, a CAP.
addressrecorddb	addressrecrddb *camí d'accés*	No	Cap	Si està especificat, funciona com la paraula clau **backupfile**. Només és vàlid a nivell de contenidor global o de base de dades. **Nota:** es desaconsella aquest mètode.
backupfile	backupfile *camí d'accés*	No	/etc/db_file.crbk	Especifica el fitxer que cal utilitzar per a les còpies de seguretat de la base de dades. Només és vàlid a nivell de contenidor global o de base de dades.
checkpointfile	checkpointfile *camí d'accés*	No	/etc/db_file.chkpt	Especifica els fitxers de punt de comprovació de la base de dades. El primer fitxer de punt de comprovació és el *camí d'accés*. El segon fitxer de punt de comprovació és el *camí d'accés* amb el darrer caràcter substituït per un 2. Per tant, el fitxer de punt de comprovació no hauria d'acabar en 2. Només és vàlid a nivell de contenidor global o de base de dades.
clientrecorddb	clientrecorddb *camí d'accés*	No	/etc/db_file.cr	Especifica el fitxer de desament de la base de dades. El fitxer conté tots els enregistraments de client que el servidor **DHCP** ha revisat. Només és vàlid a nivell de contenidor global o de base de dades.
bootstrapserver	bootstrapserver *adreça IP*	No	Cap	Especifica el servidor que els clients haurien d'utilitzar als fitxers **TFTP** després de rebre els paquets **BOOTP** o **DHCP**. Aquest valor emplena el camp **siaddr** del paquet. Això és vàlid a qualsevol nivell de contenidor.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
giaddrfield	giaddrfield *adreça IP*	No	Cap	Especifica el giaddrfield per als paquets de resposta. **Nota:** Aquesta especificació no es permet als protocols **BOOTP** i **DHCP**, però alguns clients demanen que el camp **giaddr** sigui la passarel•la per defecte de la xarxa. A causa d'aquest conflicte potencial, el giaddrfield només s'hauria d'utilitzar dins d'un contenidor de clients, tot i que pot funcionar a qualsevol nivell.
pingTime	pingTime *n unitat_temps*	No	3 segons	Especifica el temps que cal esperar una resposta ping abans de lliurar una adreça. La unitat de temps per defecte és els centèsims de segon. El valor d'unitat de temps es defineix a la nota abans d'aquesta taula. Això és vàlid a qualsevol nivell de contenidor. El paràmetre *unitat_temps* és opcional.
bootptime	bootptime *n unitat_temps*	No	-1, infinit	Especifica la quantitat de temps per llogar una adreça a un client **BOOTP**. El valor per defecte és -1, que vol dir infinit. Els valors d'unitat de temps normals estan disponibles. El paràmetre *unitat de temps* és opcional. Això és vàlid a qualsevol nivell de contenidor.
AllRoutesBroadcast	allroutesbroadcast no	No	0	Especifica si cal enviar les respostes a tots els camins, en cas que es demani una resposta de difusió. Això és vàlid a qualsevol nivell de contenidor. Els servidors **DHCP** del sistema operatiu ignoren aquest fet, perquè l'adreça MAC efectiva del client, inclosos els RIFs, s'emmagatzemen per al paquet de retorn. Això és vàlid a qualsevol nivell de contenidor.
AllRoutesBroadcast	allroutesbroadcast false	No	0	Especifica si cal enviar les respostes a tots els camins, en cas que es demani una resposta de difusió. Això és vàlid a qualsevol nivell de contenidor. Els servidors **DHCP** del sistema operatiu ignoren aquest fet, perquè l'adreça MAC efectiva del client, inclosos els RIFs, s'emmagatzemen per al paquet de retorn. Això és vàlid a qualsevol nivell de contenidor.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
AllRoutesBroadcast	allroutesbroadcast 0	No	0	Especifica si cal enviar les respostes a tots els camins, en cas que es demani una resposta de difusió. Això és vàlid a qualsevol nivell de contenidor. Els servidors **DHCP** del sistema operatiu ignoren aquest fet, perquè l'adreça MAC efectiva del client, inclosos els RIFs, s'emmagatzemen per al paquet de retorn. Això és vàlid a qualsevol nivell de contenidor.
AllRoutesBroadcast	allroutesbroadcast yes	No	0	Especifica si cal enviar les respostes a tots els camins, en cas que es demani una resposta de difusió. Això és vàlid a qualsevol nivell de contenidor. Els servidors **DHCP** del sistema operatiu ignoren aquest fet, perquè l'adreça MAC efectiva del client, inclosos els RIFs, s'emmagatzemen per al paquet de retorn. Això és vàlid a qualsevol nivell de contenidor.
AllRoutesBroadcast	allroutesbroadcast true	No	0	Especifica si cal enviar les respostes a tots els camins, en cas que es demani una resposta de difusió. Això és vàlid a qualsevol nivell de contenidor. Els servidors **DHCP** del sistema operatiu ignoren aquest fet, perquè l'adreça MAC efectiva del client, inclosos els RIFs, s'emmagatzemen per al paquet de retorn. Això és vàlid a qualsevol nivell de contenidor.
AllRoutesBroadcast	allroutesbroadcast 1	No	0	Especifica si cal enviar les respostes a tots els camins, en cas que es demani una resposta de difusió. Això és vàlid a qualsevol nivell de contenidor. Els servidors **DHCP** del sistema operatiu ignoren aquest fet, perquè l'adreça MAC efectiva del client, inclosos els RIFs, s'emmagatzemen per al paquet de retorn. Això és vàlid a qualsevol nivell de contenidor.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
addressassigned	addressassigned "*sèrie*"	No	Cap	Especifica una sèrie entre cometes que s'executa quan s'assigna una adreça a un client. La sèrie hauria de tenir dos %s. El primer %s és l'id de client amb la forma *tipus-sèrie*. El segon %s és una adreça IP en format de quartet amb punt. Això és vàlid a qualsevol nivell de contenidor.
addressreleased	addressreleased "*sèrie*"	No	Cap	Especifica una sèrie entre cometes que s'executa quan s'allibera una adreça. La sèrie hauria de tenir un %s. El %s és l'adreça IP que s'allibera en format de quartet amb punt. Això és vàlid a qualsevol nivell de contenidor.
appenddomain	appenddomain 0	No	No	Especifica si cal afegir el nom de domini 15 de l'opció definida al nom d'amfitrió suggerit pel client en el cas que el client no suggereixi també un nom de domini. Això és vàlid a qualsevol nivell de contenidor.
appenddomain	appenddomain no	No	No	Especifica si cal afegir el nom de domini 15 de l'opció definida al nom d'amfitrió suggerit pel client en el cas que el client no suggereixi també un nom de domini. Això és vàlid a qualsevol nivell de contenidor.
appenddomain	appenddomain false	No	No	Especifica si cal afegir el nom de domini 15 de l'opció definida al nom d'amfitrió suggerit pel client en el cas que el client no suggereixi també un nom de domini. Això és vàlid a qualsevol nivell de contenidor.
appenddomain	appenddomain 1	No	No	Especifica si cal afegir el nom de domini 15 de l'opció definida al nom d'amfitrió suggerit pel client en el cas que el client no suggereixi també un nom de domini. Això és vàlid a qualsevol nivell de contenidor.
appenddomain	appenddomain yes	No	No	Especifica si cal afegir el nom de domini 15 de l'opció definida al nom d'amfitrió suggerit pel client en el cas que el client no suggereixi també un nom de domini. Això és vàlid a qualsevol nivell de contenidor.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
appenddomain	appenddomain true	No	No	Especifica si cal afegir el nom de domini 15 de l'opció definida al nom d'amfitrió suggerit pel client en el cas que el client no suggereixi també un nom de domini. Això és vàlid a qualsevol nivell de contenidor.
canonical	canonical 0	No	0	Especifica que l'id del client és en format canònic. Això només és vàlid al contenidor de clients.
canonical	canonical no	No	0	Especifica que l'id del client és en format canònic. Això només és vàlid al contenidor de clients.
canonical	canonical false	No	0	Especifica que l'id del client és en format canònic. Això només és vàlid al contenidor de clients.
canonical	canonical 1	No	0	Especifica que l'id del client és en format canònic. Això només és vàlid al contenidor de clients.
canonical	canonical yes	No	0	Especifica que l'id del client és en format canònic. Això només és vàlid al contenidor de clients.
canonical	canonical true	No	0	Especifica que l'id del client és en format canònic. Això només és vàlid al contenidor de clients.
leaseTimeDefault	leaseTimeDefault *n unitat_temps*	No	86400 segons	Especifica el temps de lloguer per defecte dels clients. Això és vàlid a qualsevol nivell de contenidor. El paràmetre *unitat_temps* és opcional.
proxyarec	proxyarec never	No	usedhcpddnsplus	Especifica les opcions i els mètodes que cal utilitzar per actualitzar l'enregistrament A del DNS. `never` significa que no s'ha d'actualitzar mai l'enregistrament A. `usedhcpddns` significa utilitzar l'opció 81 si ho especifica el client. `usedhcpddnsplus` significa utilitzar l'opció 81 o bé la 12 i la 15, si així s'especifica. `always` significa dur a terme l'actualització de l'enregistrament A per a tots els clients. `XXXXprotected` modifica l'ordre **nsupdate** per assegurar-se que s'accepta el client. `standard` és un sinònim d'`always`. `protected` és un sinònim d'`alwaysprotected`. Això és vàlid a qualsevol nivell de contenidor.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
proxyarec	proxyarec usedhcpddns	No	usedhcpddnsplus	Especifica les opcions i els mètodes que cal utilitzar per actualitzar l'enregistrament A del DNS. `never` significa que no s'ha d'actualitzar mai l'enregistrament A. `usedhcpddns` significa utilitzar l'opció 81 si ho especifica el client. `usedhcpddnsplus` significa utilitzar l'opció 81 o bé la 12 i la 15, si així s'especifica. `always` significa dur a terme l'actualització de l'enregistrament A per a tots els clients. `XXXXprotected` modifica l'ordre **nsupdate** per assegurar-se que s'accepta el client. `standard` és un sinònim d'`always`. `protected` és un sinònim d'`alwaysprotected`. Això és vàlid a qualsevol nivell de contenidor.
proxyarec	proxyarec usedhcpddnsplus	No	usedhcpddnsplus	Especifica les opcions i els mètodes que cal utilitzar per actualitzar l'enregistrament A del DNS. `never` significa que no s'ha d'actualitzar mai l'enregistrament A. `usedhcpddns` significa utilitzar l'opció 81 si ho especifica el client. `usedhcpddnsplus` significa utilitzar l'opció 81 o bé la 12 i la 15, si així s'especifica. `always` significa dur a terme l'actualització de l'enregistrament A per a tots els clients. `XXXXprotected` modifica l'ordre **nsupdate** per assegurar-se que s'accepta el client. `standard` és un sinònim d'`always`. `protected` és un sinònim d'`alwaysprotected`. Això és vàlid a qualsevol nivell de contenidor.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
proxyarec	proxyarec always	No	usedhcpddnsplus	Especifica les opcions i els mètodes que cal utilitzar per actualitzar l'enregistrament A del DNS. `never` significa que no s'ha d'actualitzar mai l'enregistrament A. `usedhcpddns` significa utilitzar l'opció 81 si ho especifica el client. `usedhcpddnsplus` significa utilitzar l'opció 81 o bé la 12 i la 15, si així s'especifica. `always` significa dur a terme l'actualització de l'enregistrament A per a tots els clients. `XXXXprotected` modifica l'ordre **nsupdate** per assegurar-se que s'accepta el client. `standard` és un sinònim d'`always`. `protected` és un sinònim d'`alwaysprotected`. Això és vàlid a qualsevol nivell de contenidor.
proxyarec	proxyarec usedhcpddnsprotected	No	usedhcpddnsplus	Especifica les opcions i els mètodes que cal utilitzar per actualitzar l'enregistrament A del DNS. `never` significa que no s'ha d'actualitzar mai l'enregistrament A. `usedhcpddns` significa utilitzar l'opció 81 si ho especifica el client. `usedhcpddnsplus` significa utilitzar l'opció 81 o bé la 12 i la 15, si així s'especifica. `always` significa dur a terme l'actualització de l'enregistrament A per a tots els clients. `XXXXprotected` modifica l'ordre **nsupdate** per assegurar-se que s'accepta el client. `standard` és un sinònim d'`always`. `protected` és un sinònim d'`alwaysprotected`. Això és vàlid a qualsevol nivell de contenidor.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
proxyarec	proxyarec usedhcpddnsplusprotected	No	usedhcpddnsplus	Especifica les opcions i els mètodes que cal utilitzar per actualitzar l'enregistrament A del DNS. `never` significa que no s'ha d'actualitzar mai l'enregistrament A. `usedhcpddns` significa utilitzar l'opció 81 si ho especifica el client. `usedhcpddnsplus` significa utilitzar l'opció 81 o bé la 12 i la 15, si així s'especifica. `always` significa dur a terme l'actualització de l'enregistrament A per a tots els clients. `XXXXprotected` modifica l'ordre **nsupdate** per assegurar-se que s'accepta el client. `standard` és un sinònim d'`always`. `protected` és un sinònim d'`alwaysprotected`. Això és vàlid a qualsevol nivell de contenidor.
proxyarec	proxyarec alwaysprotected	No	usedhcpddnsplus	Especifica les opcions i els mètodes que cal utilitzar per actualitzar l'enregistrament A del DNS. `never` significa que no s'ha d'actualitzar mai l'enregistrament A. `usedhcpddns` significa utilitzar l'opció 81 si ho especifica el client. `usedhcpddnsplus` significa utilitzar l'opció 81 o bé la 12 i la 15, si així s'especifica. `always` significa dur a terme l'actualització de l'enregistrament A per a tots els clients. `XXXXprotected` modifica l'ordre **nsupdate** per assegurar-se que s'accepta el client. `standard` és un sinònim d'`always`. `protected` és un sinònim d'`alwaysprotected`. Això és vàlid a qualsevol nivell de contenidor.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
proxyarec	proxyarec standard	No	usedhcpddnsplus	Especifica les opcions i els mètodes que cal utilitzar per actualitzar l'enregistrament A del DNS. `never` significa que no s'ha d'actualitzar mai l'enregistrament A. `usedhcpddns` significa utilitzar l'opció 81 si ho especifica el client. `usedhcpddnsplus` significa utilitzar l'opció 81 o bé la 12 i la 15, si així s'especifica. `always` significa dur a terme l'actualització de l'enregistrament A per a tots els clients. `XXXXprotected` modifica l'ordre **nsupdate** per assegurar-se que s'accepta el client. `standard` és un sinònim d'`always`. `protected` és un sinònim d'`alwaysprotected`. Això és vàlid a qualsevol nivell de contenidor.
	proxyarec protected	No	usedhcpddnsplus	Especifica les opcions i els mètodes que cal utilitzar per actualitzar l'enregistrament A del DNS. `never` significa que no s'ha d'actualitzar mai l'enregistrament A. `usedhcpddns` significa utilitzar l'opció 81 si ho especifica el client. `usedhcpddnsplus` significa utilitzar l'opció 81 o bé la 12 i la 15, si així s'especifica. `always` significa dur a terme l'actualització de l'enregistrament A per a tots els clients. `XXXXprotected` modifica l'ordre **nsupdate** per assegurar-se que s'accepta el client. `standard` és un sinònim d'`always`. `protected` és un sinònim d'`alwaysprotected`. Això és vàlid a qualsevol nivell de contenidor.
releasednsA	releasednsA "*sèrie*"	No	Cap	Especifica la sèrie d'execució que cal utilitzar quan s'allibera una adreça. La sèrie s'utilitza per eliminar l'enregistrament A associat a l'adreça alliberada. Això és vàlid a qualsevol nivell de contenidor.
releasednsP	releasednsP "*sèrie*"	No	Cap	Especifica la sèrie d'execució que cal utilitzar quan s'allibera una adreça. La sèrie s'utilitza per eliminar l'enregistrament PTR associat a l'adreça alliberada. Això és vàlid a qualsevol nivell de contenidor.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
removedns	removedns "*sèrie*"	No	Cap	Especifica la sèrie d'execució que cal utilitzar quan s'allibera una adreça. La sèrie s'utilitza per eliminar l'enregistrament A i PTR associat a l'adreça alliberada. Això és vàlid a qualsevol nivell de contenidor. **Nota:** Això es desaprova a favor de les paraules clau **releasednsA** i **releasednsP**.
updatedns	updatedns "*sèrie*"	No	Cap	Especifica la sèrie d'execució que cal utilitzar quan es vincula una adreça. La sèrie s'utilitza per actualitzar els enregistraments A i PTR associats a l'adreça. Això és vàlid a qualsevol nivell de contenidor. **Nota:** Això es desaprova a favor de les paraules clau **updatednsA** i **updatednsP**.
updatednsA	updatednsA "*sèrie*"	No	Cap	Especifica la sèrie d'execució que cal utilitzar quan es vincula una adreça. La sèrie s'utilitza per actualitzar l'enregistrament A associat a l'adreça. Això és vàlid a qualsevol nivell de contenidor.
updatednsP	updatednsP "*sèrie*"	No	Cap	Especifica la sèrie d'execució que cal utilitzar quan es vincula una adreça. La sèrie s'utilitza per actualitzar l'enregistrament PTR associat a l'adreça. Això és vàlid a qualsevol nivell de contenidor.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
hostnamepolicy	hostnamepolicy suggested	No	per defecte	Especifica el nom d'amfitrió que cal tornar al client. La política per defecte consisteix a preferir el nom de domini i d'amfitrió definits als suggerits. Altres polítiques impliquen una adhesió estricta (per exemple: `defined` tornarà el nom definit o bé cap si no s'ha definit a la configuració). Així mateix, les polítiques que utilitzin el modificador `always` dictaran al servidor el retorn de l'opció de nom de l'amfitrió independentment de si el client ho ha sol•licitat mitjançant l'opció de llista de paràmetres. Tingueu en compte que el suggeriment d'un nom d'amfitrió també n'implica la sol•licitud i els noms d'amfitrió es poden suggerir mitjançant l'opció 81 o les opcions 12 i 15. Aquesta paraula clau és vàlida a qualsevol nivell de contenidor.
hostnamepolicy	hostnamepolicy resolved	No	per defecte	Especifica el nom d'amfitrió que cal tornar al client. La política per defecte consisteix a preferir el nom de domini i d'amfitrió definits als suggerits. Altres polítiques impliquen una adhesió estricta (per exemple: `defined` tornarà el nom definit o bé cap si no s'ha definit a la configuració). Així mateix, les polítiques que utilitzin el modificador `always` dictaran al servidor el retorn de l'opció de nom de l'amfitrió independentment de si el client ho ha sol•licitat mitjançant l'opció de llista de paràmetres. Tingueu en compte que el suggeriment d'un nom d'amfitrió també n'implica la sol•licitud i els noms d'amfitrió es poden suggerir mitjançant l'opció 81 o les opcions 12 i 15. Aquesta paraula clau és vàlida a qualsevol nivell de contenidor.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
hostnamepolicy	hostnamepolicy always_resolved	No	per defecte	Especifica el nom d'amfitrió que cal tornar al client. La política per defecte consisteix a preferir el nom de domini i d'amfitrió definits als suggerits. Altres polítiques impliquen una adhesió estricta (per exemple: `defined` tornarà el nom definit o bé cap si no s'ha definit a la configuració). Així mateix, les polítiques que utilitzin el modificador `always` dictaran al servidor el retorn de l'opció de nom de l'amfitrió independentment de si el client ho ha sol•licitat mitjançant l'opció de llista de paràmetres. Tingueu en compte que el suggeriment d'un nom d'amfitrió també n'implica la sol•licitud i els noms d'amfitrió es poden suggerir mitjançant l'opció 81 o les opcions 12 i 15. Aquesta paraula clau és vàlida a qualsevol nivell de contenidor.
hostnamepolicy	hostnamepolicy defined	No	per defecte	Especifica el nom d'amfitrió que cal tornar al client. La política per defecte consisteix a preferir el nom de domini i d'amfitrió definits als suggerits. Altres polítiques impliquen una adhesió estricta (per exemple: `defined` tornarà el nom definit o bé cap si no s'ha definit a la configuració). Així mateix, les polítiques que utilitzin el modificador `always` dictaran al servidor el retorn de l'opció de nom de l'amfitrió independentment de si el client ho ha sol•licitat mitjançant l'opció de llista de paràmetres. Tingueu en compte que el suggeriment d'un nom d'amfitrió també n'implica la sol•licitud i els noms d'amfitrió es poden suggerir mitjançant l'opció 81 o les opcions 12 i 15. Aquesta paraula clau és vàlida a qualsevol nivell de contenidor.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
hostnamepolicy	hostnamepolicy always_defined	No	per defecte	Especifica el nom d'amfitrió que cal tornar al client. La política per defecte consisteix a preferir el nom de domini i d'amfitrió definits als suggerits. Altres polítiques impliquen una adhesió estricta (per exemple: `defined` tornarà el nom definit o bé cap si no s'ha definit a la configuració). Així mateix, les polítiques que utilitzin el modificador `always` dictaran al servidor el retorn de l'opció de nom de l'amfitrió independentment de si el client ho ha sol•licitat mitjançant l'opció de llista de paràmetres. Tingueu en compte que el suggeriment d'un nom d'amfitrió també n'implica la sol•licitud i els noms d'amfitrió es poden suggerir mitjançant l'opció 81 o les opcions 12 i 15. Aquesta paraula clau és vàlida a qualsevol nivell de contenidor.
hostnamepolicy	hostnamepolicy default	No	per defecte	Especifica el nom d'amfitrió que cal tornar al client. La política per defecte consisteix a preferir el nom de domini i d'amfitrió definits als suggerits. Altres polítiques impliquen una adhesió estricta (per exemple: `defined` tornarà el nom definit o bé cap si no s'ha definit a la configuració). Així mateix, les polítiques que utilitzin el modificador `always` dictaran al servidor el retorn de l'opció de nom de l'amfitrió independentment de si el client ho ha sol•licitat mitjançant l'opció de llista de paràmetres. Tingueu en compte que el suggeriment d'un nom d'amfitrió també n'implica la sol•licitud i els noms d'amfitrió es poden suggerir mitjançant l'opció 81 o les opcions 12 i 15. Aquesta paraula clau és vàlida a qualsevol nivell de contenidor.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
bootfilepolicy	bootfilepolicy suggested	No	suggested	Especifica la preferència per retornar el nom de fitxer d'engegada a un client. `suggested` prefereix el nom de fitxer d'engegada suggerit pel client a qualsevol nom configurat pel servidor. `merge` afegeix el nom suggerit de client al directori d'inici configurat pel servidor. `defined` prefereix el nom definit a qualsevol nom de fitxer d'engegada suggerit. `always` retorna el nom definit independentment de si el client sol•licita l'opció de fitxer d'engegada mitjançant l'opció de llista de paràmetres.
bootfilepolicy	bootfilepolicy merge	No	suggested	Especifica la preferència per retornar el nom de fitxer d'engegada a un client. `suggested` prefereix el nom de fitxer d'engegada suggerit pel client a qualsevol nom configurat pel servidor. `merge` afegeix el nom suggerit de client al directori d'inici configurat pel servidor. `defined` prefereix el nom definit a qualsevol nom de fitxer d'engegada suggerit. `always` retorna el nom definit independentment de si el client sol•licita l'opció de fitxer d'engegada mitjançant l'opció de llista de paràmetres.
bootfilepolicy	bootfilepolicy defined	No	suggested	Especifica la preferència per retornar el nom de fitxer d'engegada a un client. `suggested` prefereix el nom de fitxer d'engegada suggerit pel client a qualsevol nom configurat pel servidor. `merge` afegeix el nom suggerit de client al directori d'inici configurat pel servidor. `defined` prefereix el nom definit a qualsevol nom de fitxer d'engegada suggerit. `always` retorna el nom definit independentment de si el client sol•licita l'opció de fitxer d'engegada mitjançant l'opció de llista de paràmetres.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
bootfilepolicy	bootfilepolicy always	No	suggested	Especifica la preferència per retornar el nom de fitxer d'engegada a un client. `suggested` prefereix el nom de fitxer d'engegada suggerit pel client a qualsevol nom configurat pel servidor. `merge` afegeix el nom suggerit de client al directori d'inici configurat pel servidor. `defined` prefereix el nom definit a qualsevol nom de fitxer d'engegada suggerit. `always` retorna el nom definit independentment de si el client sol•licita l'opció de fitxer d'engegada mitjançant l'opció de llista de paràmetres.
stealfromchildren	stealfromchildren true	No	No	Especifica si el contenidor superior, un cop se li hagin exhaurit les adreces, les hauria de "robar" dels contenidors subordinats. Això significa que si teniu una subxarxa amb classe definida amb un abast d'adreces, les adreces estan reservades pels clients que especifiquen la classe en qüestió. Si `stealfromchildren` és cert, aleshores les adreces es retiraran d'un subordinat per intentar satisfer la sol•licitud. El valor per defecte és no robar una adreça.
stealfromchildren	stealfromchildren 1	No	No	Especifica si el contenidor superior, un cop se li hagin exhaurit les adreces, les hauria de "robar" dels contenidors subordinats. Això significa que si teniu una subxarxa amb classe definida amb un abast d'adreces, les adreces estan reservades pels clients que especifiquen la classe en qüestió. Si `stealfromchildren` és cert, aleshores les adreces es retiraran d'un subordinat per intentar satisfer la sol•licitud. El valor per defecte és no robar una adreça.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
stealfromchildren	stealfromchildren sí	No	No	Especifica si el contenidor superior, un cop se li hagin exhaurit les adreces, les hauria de "robar" dels contenidors subordinats. Això significa que si teniu una subxarxa amb classe definida amb un abast d'adreces, les adreces estan reservades pels clients que especifiquen la classe en qüestió. Si `stealfromchildren` és cert, aleshores les adreces es retiraran d'un subordinat per intentar satisfer la sol•licitud. El valor per defecte és no robar una adreça.
stealfromchildren	stealfromchildren fals	No	No	Especifica si el contenidor superior, un cop se li hagin exhaurit les adreces, les hauria de "robar" dels contenidors subordinats. Això significa que si teniu una subxarxa amb classe definida amb un abast d'adreces, les adreces estan reservades pels clients que especifiquen la classe en qüestió. Si `stealfromchildren` és cert, aleshores les adreces es retiraran d'un subordinat per intentar satisfer la sol•licitud. El valor per defecte és no robar una adreça.
stealfromchildren	stealfromchildren 0	No	No	Especifica si el contenidor superior, un cop se li hagin exhaurit les adreces, les hauria de "robar" dels contenidors subordinats. Això significa que si teniu una subxarxa amb classe definida amb un abast d'adreces, les adreces estan reservades pels clients que especifiquen la classe en qüestió. Si `stealfromchildren` és cert, aleshores les adreces es retiraran d'un subordinat per intentar satisfer la sol•licitud. El valor per defecte és no robar una adreça.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
stealfromchildren	stealfromchildren no	No	No	Especifica si el contenidor superior, un cop se li hagin exhaurit les adreces, les hauria de "robar" dels contenidors subordinats. Això significa que si teniu una subxarxa amb classe definida amb un abast d'adreces, les adreces estan reservades pels clients que especifiquen la classe en qüestió. Si `stealfromchildren` és cert, aleshores les adreces es retiraran d'un subordinat per intentar satisfer la sol•licitud. El valor per defecte és no robar una adreça.
homedirectory	homedirectory *camí d'accés*	No	Cap	Especifica el directori d'inici que cal utilitzar a la secció de fitxer del paquet de resposta. Això es pot especificar a qualsevol nivell de contenidor. La política de fitxer d'engegada defineix la manera en què els elements especificats a la secció de fitxer del paquet d'entrada interactuen amb les sentències del directori d'inici i el fitxer d'engegada.
bootfile	bootfile *camí d'accés*	No	Cap	Especifica el fitxer d'engegada que cal utilitzar a la secció de fitxer del paquet de resposta. Això es pot especificar a qualsevol nivell de contenidor. La política de fitxer d'engegada defineix la manera en què els elements especificats a la secció de fitxer del paquet d'entrada interactuen amb les sentències del directori d'inici i el fitxer d'engegada.
pxebootfile	pxebootfile *arquitectura_sistema versió_major versió_menor nom_fitxer_engegada*	No	Cap	Especifica el fitxer d'engegada que cal donar a un client. Només s'utilitza quan el **dhcpsd** dóna suport als clients PXE (el **pxeservertype** és el **dhcp_pxe_binld**). L'analitzador del fitxer de configuració genera un error si el nombre de paràmetres després del `pxebootfile` és menor que quatre i ignora tots els paràmetres addicionals. El `pxebootfile` només es pot utilitzar dins un contenidor.

Paraula clau	Forma	Sub- contenidors	Valor per defecte	Significat
supportoption118	supportoption118 *no/sí*	No. Només es pot definir en un contenidor de subxarxes.	Cap	Aquesta paraula clau especifica si aquest contenidor dóna suport a l'opció 118. Sí significa que li dóna suport i No significa que no li dóna suport. Perquè es dugui a terme aquesta opció, també heu d'utilitzar la paraula clau **supportsubnetselection**.

Suggeriments de Gestió d'instal•lació de xarxa i DHCP

El concepte d'assignar dinàmicament adreces d'IP (Internet Protocol) és força nou. Els suggeriments següents proporcionen ajuda pel que fa a la interacció entre la Gestió d'instal•lació en xarxa (NIM) i el **DHCP**.

1. Quan configureu objectes a l'entorn NIM, utilitzeu noms d'amfitrió sempre que sigui possible. Això us permetrà utilitzar un servidor de noms dinàmic que actualitzi les adreces IP quan el nom d'amfitrió es converteixi en una adreça IP a l'entorn NIM.
2. Situeu el NIM master i el servidor **DHCP** al mateix sistema. El servidor **DHCP** té una opció a la sèrie DNS d'actualització que, si s'especifica al `NIM`, intenta mantenir els objectes NIM fora dels estats que necessiten adreces IP estàtiques quan aquestes adreces canvien.
3. Per als clients NIM, estabiu el període de lloguer per defecte al doble de temps que es tarda a instal•lar un client. D'aquesta manera, l'adreça IP llogada és vàlida durant la instal•lació. Després de la instal•lació, reinicieu el client. Segons el tipus d'instal•lació, s'iniciarà o s'haurà de configurar el **DHCP**.
4. El servidor `dhcpsd` hauria de ser el responsable de l'enregistrament DNS PTR i també de l'A. Quan el NIM torna a instal•lar la màquina, se suprimeix el fitxer que conté l'RSA i el client no pot actualitzar els enregistraments. El servidor actualitza els enregistraments del sistema. Per fer-ho, canvieu la línia `updatedns` del `/etc/dhcpcd.ini` a:

   ```
   updatedns "/usr/sbin/dhcpaction '%s' '%s' '%s' '%s' '%s' NONE NONIM"
   ```

   Al fitxer `/etc/dhcpsd.cnf`, canvieu la línia `updatedns` a:

   ```
   updatedns "/usr/sbin/dhcpaction '%s' '%s' '%s' '%s' '%s' BOTH NIM"
   ```

   Nota: Quan se situa un objecte NIM a l'estat pendent d'instal•lació BOS, pot ser que el servidor `dhcpsd` passi arguments diferents als suposats originalment. Minimitzeu el temps en què el client es troba en aquest estat pendent per evitar aquesta situació.

Gràcies a aquests suggeriments, l'entorn NIM treballa amb clients dinàmics.

Per obtenir més informació sobre la Gestió d'instal•lació de xarxa, consulteu l'apartat *AIX 5L Version 5.3 Network Installation Management Guide and Reference*.

Protocol de Configuració d'Amfitrió Dinàmic versió 6

El **Protocol de Configuració d'Amfitrió Dinàmic (DHCP)** proporciona un mètode per mantenir les configuracions de xarxa en una ubicació centralitzada. Aquest tema és específic del **DHCPv6**: totes les referències a "adreça IP" fan referència a les adreces IPv6 i totes les referències a "**DHCP**" fan referència a **DHCPv6** (a no ser que s'indiqui diversament).

Un servidor **DHCPv4** pot coexistir al mateix enllaç amb un servidor **DHCPv6**. Per obtenir una explicació en profunditat del protocol, vegeu l'RFC 3315.

El **DHCP** és un protocol de capa d'aplicació que permet a una màquina client de la xarxa obtenir adreces IP i altres paràmetres de configuració del servidor. Aquests paràmetres estan definits a *options*. Les

opcions s'obtenen mitjançant l'intercanvi de paquets entre un daemon del client i un altre del servidor. Aquests intercanvis de missatges són en forma de paquets **UDP**. Un client utilitza una adreça d'enllaç local, mitjançant l'ordre **autoconf6** o bé altres mètodes, per identificar la seva adreça d'origen al servidor. El servidor rep en una adreça de multidifusió d'àmbit d'enllaç reservada. Un agent de retransmissió permet que el client i el servidor es comuniquin si no es troben al mateix enllaç.

Aquest tema explica el reconeixement d'intercanvi de quatre missatges per a una sola interfície amb un IA_NA i una adreça per aquest IA_NA. Per obtenir una adreça IP, el daemon de client **DHCP** (**dhcpcd6**) envia un missatge de SOL•LICITUD a l'adreça **All_DHCP_Relay_Agents_and_Servers**, que el servidor rep i processa. (Es poden configurar diversos servidors a la xarxa per redundància.) Si hi ha una adreça lliure disponible per al client, es crea un missatge d'ANUNCI que s'envia al client. Aquest missatge conté una adreça IP i altres opcions apropiades per al client en qüestió. El client rep el missatge d'ANUNCI DHCP del servidor i l'emmagatzema mentre espera altres anuncis. Quan el client ha seleccionat el millor anunci, envia una PETICIÓ DHCP a l'adreça **All_DHCP_Relay_Agents_and_Servers** tot especificant l'anunci de servidor que desitja.

Tots els servidors **DHCP** configurats reben el missatge de PETICIÓ. Cadascun comprova si es tracta del servidor sol•licitat. El servidor no processa cap paquet amb un servidor DUID que no coincideixi amb el seu. El servidor sol•licitat marca l'adreça com a assignada i torna una RESPOSTA DHCP, moment en què es completa la transacció. El client té una adreça per al període de temps (valid-lifetime) designat pel servidor.

Quan caduca per a l'adreça la durada preferida, el client envia al servidor un paquet de RENOVACIÓ per estendre el temps de lloguer. Si el servidor desitja renovar l'adreça, envia una RESPOSTA DHCP. Si el client no obté una resposta del servidor al qual pertany la seva adreça corrent, fa una difusió múltiple d'un paquet de REVINCULACIÓ DHCP si, per exemple, el servidor s'ha traslladat d'una xarxa a una altra. Si el client no ha renovat l'adreça després de la durada vàlida, s'elimina l'adreça de la interfície i el procés torna a començar. Aquest cicle evita que s'assigni la mateixa adreça a diversos clients d'una xarxa.

Un client pot tenir diverses opcions IA_NA i cada IA_NA pot tenir diverses adreces. Així mateix, un client pot tenir diverses opcions IA_TA, cadascuna de les quals pot tenir també diverses adreces:

- **Identity association for non-temporary addresses (IA_NA)**: IA que porta adreces assignades que no són adreces temporals
- **Identity association for temporary addresses (IA_TA)**: IA que porta adreces temporals (vegeu l'RFC 3041).
- **DUID**: Un identificador únic **DHCP** d'un participant **DHCP**; cada client i servidor **DHCP** té un únic DUID que es manté al llarg de les reengegades.

El servidor **DHCP** assigna adreces basades en claus. Quatre claus comuns són **class**, **vendor**, **client ID** i **inoption**. El servidor utilitza aquestes claus per assignar una adreça i el conjunt d'opcions de configuració que es tornen al client.

class La clau **class** la pot configurar completament el client. Pot especificar una adreça i opcions. Aquesta clau es pot utilitzar per denotar la funció de màquina a la xarxa o bé per descriure com s'agrupen les màquines amb propòsits administratius. Per exemple, pot ser que l'administrador de la xarxa vulgui crear una classe Netbios que contingui opcions per als clients NetBIOS o una classe comptabilitat que representi a les màquines del departament de Comptabilitat que necessiten accedir a una determinada impressora.

vendor
La clau **vendor** ajuda a identificar el client mitjançant la plataforma de maquinari i de programari.

client ID
La clau **client ID** identifica el client mitjançant el DUID. L'ID de client està especificat al fitxer duid del daemon **dhcpcd**. El servidor també pot utilitzar l'ID de client per passar opcions a un client específic o prohibir que un client en concret rebi cap paràmetre.

Inoption
La clau **inoption** identifica el client mitjançant l'opció sol•licitada pel client.

Aquestes claus es poden utilitzar tant individualment com en combinacions. Si el client proporciona diverses claus i es poden assignar diverses adreces, només se'n selecciona una i l'opció establerta es deriva primerament de la clau seleccionada.

Cal un agent de retransmissió per tal que la difusió múltiple del client abandoni la xarxa local. Els agents de retransmissió actuen com a agents de reenviament dels paquets **DHCP**.

Servidor DHCPv6

El servidor **DHCPv6** té tres components principals.

El servidor **DHCP** es troba segmentat en tres components principals: una base de dades, un motor de protocol i un conjunt de fils de servei. Cada component té la seva pròpia informació de configuració.

Base de dades DHCPv6:

La base de dades `db_filev6.dhcpo` s'utilitza per fer un seguiment dels clients i de les adreces i per al control d'accés.

Les opcions també s'emmagatzemen a la base de dades per a la recuperació i lliurament als clients. La base de dades s'implementa com un objecte carregable dinàmicament.

La base de dades s'actualitza i verifica per coherència mitjançant la informació del fitxer de configuració. La base de dades també conté les agrupacions d'adreces i d'opcions

El fitxer d'emmagatzematge principal i la còpia de seguretat són fitxers ASCII. El format dels fitxers d'emmagatzematge principal de base de dades és el següent:

Nota: No editeu manualment aquests fitxers.

```
DB6-1.0
Client-Info {
duid 1-0006085b68e20004ace491d3
state 7
authinfo {
    protocol 2
    algorithm 1
    rdm 0
    replay 1206567640
}
  Interface 0 {
    Inoptions {
    interface-id "en1"
    policies 2
    maxopcode 16
    numiana 1
      Ianalist {
      option 3 40 00000001000000320000005000050018deaddeadaaaaaaaa0000000000000006000000064000000c8
      }
    numiata 0
      Optiontable {
      option 6 10 00030004001700180237
      option 8 2 e659
      option 15 14 000369626d000373756e00026870
      option 16 18 000004d200073078313131313131000369626d
      }
    }
    Ianarec {
    IAID 1
    t1 50
```

```
    t2 80
      Addrec {
      Address dead:dead:aaaa:aaaa::6
      state 3
      starttime  1087592918
      preferred-lifetime 100
      valid-lifetime 200
      }
    }
  }
}
```

La primera línia és un identificador de versió del fitxer `DB6-1.0`. Les línies següents són de definició d'enregistrament del client. El servidor llegeix des de la segona línia fins al final del fitxer. (Els paràmetres entre cometes s'han d'incloure entre cometes).

duid És l'ID que el client utilitza per representar-se al servidor.

Interface
Un client pot tenir diverses interfícies. Si un client té una sola interfície i crea missatges de **SOL•LICITUD** individuals per a cada IA_NA o IA_TA, el fitxer contindrà diverses interfícies per a aquest client.

Inoptions
Les opcions d'entrada del client.

policies
Senyalador per identificar la difusió individual, reconfig-option i rapid-commit.

maxopcode
El codi d'opció més gran.

numiana
El nombre d'IA_NAs d'aquesta interfície.

Ianalist
La llista d'opcions IA_NA d'entrada del client.

numiata
Nombre d'IA_TAs d'aquesta interfície.

Optiontable
La llista d'opcions sol•licitades pel client a excepció de les opcions IA_NA i IA_TA.

Ianarec
El contenidor d'enregistraments IA_NA desat des de la base de dades del servidor.

IAID L'ID de la IA_NA.

t1 El percentatge de durada preferida d'aquesta IA_NA.

t2 El percentatge de durada vàlida d'aquesta IA_NA

Addrec
El contenidor d'enregistraments d'adreça de la base de dades del servidor

Address
Adreça donada al client per a aquest enregistrament d'adreces.

state Estat actual del client. El motor de protocol **DHCP** conté el conjunt permès i els estats es mantenen a la base de dades **DHCP**. El nombre a la vora de **state** en representa el valor. Els estats poden ser:

(1) LLIURE
Representa les adreces disponibles per a l'ús. En general, els clients no tenen aquest estat a no ser que no tinguin assignada cap adreça. Les ordres **dadmin** i **lssrc** informen sobre aquest estat com a `Lliure`.

(2) VINCULAT
Indica que el client i l'adreça estan enllaçats i que s'ha assignat aquesta adreça al client durant un determinat període de temps. Les ordres **dadmin** i **lssrc** informen sobre aquest estat com a `Llogat`.

(3) CADUCAT
Indica que el client i l'adreça estan enllaçats, però només per motius d'informació, d'una manera semblant a les adreces alliberades. No obstant això, l'estat de caducat representa els clients que es deixen caducar els lloguers. Una adreça caducada es pot utilitzar i es torna a assignar quan cap de les adreces lliures està disponible i abans que es tornin a assignar les adreces alliberades. Les ordres **dadmin** i **lssrc** informen sobre aquest estat com a `Caducat`.

(4) ALLIBERAT
Indica que el client i l'adreça estan enllaçats només per motius d'informació. El protocol **DHCP** aconsella que els servidors **DHCP** mantinguin la informació dels clients per a futures consultes (sobretot per intentar donar la mateixa adreça al client al qual ja se li havia assignat anteriorment). Aquest estat indica que el client ha alliberat l'adreça. Els altres clients poden utilitzar l'adreça si no n'hi ha cap més de disponible. Les ordres **dadmin** i **lssrc** informen sobre aquest estat com a `Alliberat`.

(5) RESERVAT
Indica que el client i l'adreça estan enllaçats, però de manera suau. El client ha enviat un missatge de descobriment **DHCP** i el servidor **DHCP** ha respost, però el client encara no ha respost amb una sol•licitud **DHCP** per a l'adreça. Les ordres **dadmin** i **lssrc** informen sobre aquest estat com a `Reservat`.

(6) ERRONI
Representa una adreça que s'utilitza a la xarxa, però que el servidor **DHCP** no ha distribuït. Aquest estat també representa les adreces que els clients han rebutjat. Aquest estat no fa referència als clients. L'ordre **dadmin** informa sobre aquest estat com a `Used` i l'ordre **lssrc**, com a `Erroni`.

Temps d'inici
El temps en què aquesta adreça es va lliurar, representat en segons des de l'1 de gener del 2000

Durada-preferida
Nombre de segons abans que calgui renovar aquesta adreça.

Durada-vàlida
Nombre de segons abans que aquesta adreça sigui no vàlida i ja no es pugui utilitzar més.

protocol
El protocol d'autenticació que utilitza el client:

(1) RETARDAT
El client utilitza l'autenticació retardada.

(2) RECONFIGURAR LA CLAU
El client utilitza l'autenticació per reconfigurar la clau.

algorisme
L'algorisme d'autenticació que utilitza el client.

(1) HMAC-MD5
El client utilitza l'algorisme MD5 en clau per crear el resum del missatge.

rdm El mètode de detecció de reproducció que utilitza el client:

(0) Comptador que augmenta de forma monòtona
El client utilitza un comptador que augmenta de forma monòtona per modificar el valor de reproducció.

reproducció
El valor actual del campo de reproducció.

La sintaxi dels fitxers de punt de comprovació no està especificada. Si cau el servidor o bé heu d'aturar el sistema i no podeu tancar la base de dades amb normalitat, el servidor pot processar els fitxers de punt de comprovació i de còpia de seguretat per tornar a construir una base de dades vàlida. Quan el servidor cau, es perden els clients que no estan enregistrats al fitxer de punt de comprovació. Correntment, no es produeixen desaments intermitents quan es processa un client. Els fitxers de valors per defecte són:

/etc/dhcpv6/db_file6.cr
Operació de base de dades normal

/etc/dhcpv6/db_file6.crbk
Fa una còpia de seguretat per a la base de dades

Operacions de diversos fils del DHCP:

La darrera part del servidor **DHCP** és un conjunt d'operacions que s'utilitzen per mantenir el funcionament.

Atès que el **DHCP** és un servidor amb fils, aquestes operacions realment estan configurades com a fils que de tant en tant realitzen certes tasques per assegurar-se que tot està enllaçat correctament.

fil principal
Aquest fil gestiona senyals. Per exemple,
- Un SIGHUP (-1) causa una renovació de totes les bases de dades del fitxer de configuració.
- Un SIGTERM (-15) causarà que el servidor s'aturi correctament.
- Un SIGUSR1 (-30) causarà que el servidor buidi la base de dades de configuració.

fil src Aquest fil gestiona les sol•licituds SRC (com ara **startsrc**, **stopsrc**, **lssrc**, **traceson** i **refresh**).

fil dadmin
Aquest fil opera interactivament amb el programa de client **dadmin** i el servidor **DHCP**. L'eina **dadmin** es pot utilitzar per obtenir l'estat i per modificar la base de dades per evitar l'edició manual dels fitxers de la base de dades. Amb l'addició dels fils **dadmin** i **src**, el servidor pot gestionar sol•licituds de servei i seguir gestionant sol•licituds de client.

fil de deixalles
Aquest fil executa temporitzadors que netegen periòdicament la base de dades, la desen, depuren els clients que no tenen adreces, i eliminen les adreces reservades que han estat en estat reservat durant massa temps. Tots aquestes temporitzadors es poden configurar.

processadors de paquets
Cadascun d'ells pot gestionar una sol•licitud d'un client **DHCPv6**. El nombre de processadors de paquets necessaris depèn, en certa manera, de la càrrega i la màquina. Aquest nombre es pot configurar; el valor per defecte és 1. El nombre màxim de fils de paquets és 50.

fils d'enregistrament
En un sistema on s'enregistren quantitats significatives de dades als fitxers de registre, el nombre de fils d'inici de sessió pot augmentar-se a més del valor per defecte (1) fins al màxim (50).

fil de gestor de taules
Aquest fil garanteix que el daemon **dhcpsdv6** no processa els paquets duplicats.

fils de procés
Aquests fils processen els paquets del client **DHCPv6**.

fil de reconfiguració

Aquest fil gestiona la reconfiguració de client quan el servidor s'actualitza(amb l'ordre `dadmin -x 6 -i`, per exemple).

Configuració del DHCPv6

Per defecte, el servidor **DHCP** es configura mitjançant la lectura del fitxer `/etc/dhcpv6/dhcpsdv6.cnf`, el qual especifica la base de dades inicial d'opcions i adreces.

EThe serveservidor s'inicia a partir d'ordres SRC. Si el **dhcpsdv6** s'ha d'iniciar a través de reengegades, afegiu una entrada al fitxer `/etc/rc.tcpip`.

Normalment, la configuració del servidor **DHCP** és la part més complexa pel que fa a l'ús del **DHCP** a la xarxa. Primerament, decidiu les xarxes en què voleu tenir els clients **DHCP**. Cada subxarxa de la xarxa representa una agrupació d'adreces que el servidor **DHCP** ha d'afegir a la seva base de dades. Per exemple:

```
subnet dead:dead:aaaa:: 48 {
        option 23 dead::beef beef:aaaa::bbbb:c aaaa:bbbb::cccc  #nameserver list
        option 24 austin.ibm.com ibm.com                        # domain list
 }
```

L'exemple anterior mostra una subxarxa, la `dead:dead:aaaa::`, amb un prefix de 48 bits. Totes les adreces d'aquesta subxarxa, de la `dead:dead:aaaa::1` a la `dead:dead:aaaa:ffff:ffff:ffff:ffff:ff7f`, es troben a l'agrupació. Opcionalment, es pot especificar un abast al final de la línia abans de '{', o bé es pot incloure al contenidor de subxarxes un abast o una sentència d'exclusió.

Els comentaris comencen amb el signe #. El servidor **DHCP** obvia el text des del # inicial fins al final de la línia. El servidor utilitza cada línia d'opció per indicar al client el que ha de fer.

Si el servidor no entén la manera d'analitzar una opció, utilitza mètodes per defecte per enviar l'opció al client. Això també permet al servidor **DHCP** enviar opcions d'indrets específics no definides pel RFC, però que poden ser utilitzades per certs clients o configuracions de clients.

Fitxer de configuració DHCPv6:

El fitxer de configuració té una secció d'adreces i una altra de definició d'opcions. Aquestes seccions utilitzen contenidors per retenir opcions, modificadors i, potencialment, altres contenidors.

Un contenidor (un mètode per agrupar opcions) utilitza un identificador per classificar els clients en grups. Els tipus de contenidor són **subnet**, **class**, **vendor**, **inoption** i **client**. Actualment, no hi ha un contenidor genèric que l'usuari pugui definir. L'identificador només defineix el client perquè se'l pugui seguir si, per exemple, es desplaça entre subxarxes. Es pot utilitzar més d'un tipus de contenidor per definir l'accés del client.

Les opcions són identificadors que es tornen al client, com ara l'adreça DNS o els noms de domini.

Després de seleccionar els modificadors, el següent element que cal configurar és l'inici de sessió. Els paràmetres d'inici de sessió s'especifiquen en un contenidor com la base de dades, però la paraula clau del contenidor és **logging_info**. Quan s'aprèn a configurar el **DHCP**, és aconsellable posar l'inici de sessió al nivell superior. Així mateix, és millor especificar la configuració d'inici de sessió abans que qualsevol altra dada del fitxer de configuració per assegurar-se que els errors de configuració s'enregistren després que s'hagi inicialitzat el subsistema d'inici de sessió. Utilitzeu la paraula clau **logitem** per habilitar un nivell d'inici de sessió o elimineu la paraula clau **logitem** per inhabilitar un nivell d'inici de sessió. Altres paraules clau per a l'inici de sessió permeten especificar el nom de fitxer de registre, la grandària del fitxer i el nombre de fitxers de registre giratoris.

Contenidors DHCPv6:

Quan el servidor **DHCP** rep una sol•licitud, s'analitza el paquet i les claus d'identificació determinen els contenidors, les opcions i les adreces que cal extreure.

Cada tipus de contenidor utilitza una opció diferent per identificar un client:

- El contenidor **subnet** utilitza el camp **hintlist** o l'adreça d'interfície de la interfície receptora per determinar la subxarxa a la qual pertany el client.
- El contenidor **class** utilitza el valor de l'opció 15 (OPTION_USER_CLASS Identifier).
- El **vendor** utilitza el valor de l'opció 16 (OPTION_VENDOR_CLASS).
- El contenidor **client** utilitza l'opció 1 (OPTION_CLIENTID) del DUID del client DHCP.
- El contenidor **inoption** coincideix amb l'opció sol•licitada del client.

A excepció de les subxarxes, cada contenidor permet l'especificació del valor amb el qual coincideix, incloses les coincidències d'expressió regular.

També hi ha un contenidor implícit, el contenidor global. Les opcions i els modificadors estan situats al contenidor global a no ser que estiguin alterats temporalment o denegats. La major part dels contenidors es poden col•locar a dins d'altres contenidors que impliquen un àmbit de visibilitat. Tant pot ser que els contenidors tinguin abasts d'adreces associats com no. Les subxarxes tenen, per naturalesa, abasts associats.

Les normes bàsiques dels contenidors i subcontenidors són les següents:

- Només els contenidors de subxarxes són vàlids a nivell global.
- Les subxarxes no es poden col•locar dins d'altres contenidors.
- Els contenidors restringits no poden tenir contenidors regulars del mateix tipus. (Per exemple, un contenidor amb una opció que només permet una classe de Comptabilitat no pot incloure un contenidor amb una opció que permeti totes les classes que comencen amb la lletra `a`.)
- Els contenidors de clients restringits no poden tenir subcontenidors.
- Els contenidors inoption no poden tenir subcontenidors

Segons aquestes normes, podeu generar una jerarquia de contenidors que segmenti les opcions en grups per a clients específics o grups de clients.

Si un client coincideix amb diversos contenidors, el servidor **DHCP** passa la sol•licitud a la base de dades i es genera una llista de contenidors. La llista es presenta per ordre de profunditat i de prioritat. La prioritat es defineix com una jerarquia implícita als contenidors. Els contenidors estrictes tenen una prioritat major que els contenidors regulars. Clients, classes, proveïdors i subxarxes estan classificats, per aquest ordre, i dins el tipus de contenidor segons la profunditat. Això genera una llista ordenada de més específic a menys específic. Per exemple:

```
Subxarxa 1
    --Classe 1
    --Client 1
Subxarxa 2
    --Classe 1
    ----Proveïdor 1
    ----Client 1
    --Client 1
```

L'exemple mostra dues subxarxes, la `Subxarxa 1` i la `Subxarxa 2`. Hi ha un nom de classe, `Classe 1`, un nom de proveïdor, `Proveïdor 1` i un nom de client `Client 1`. La `Classe 1` i el `Client 1` estan definits en diversos llocs. Com que es troben en contenidors diferents, pot ser que tinguin el mateix nom, però que

els valors al seu interior siguin diferents. Si el `Client 1` envia un missatge al servidor **DHCP** des de la `Subxarxa 1` amb la `Classe 1` especificada a la llista d'opcions, el servidor **DHCP** generarà el següent camí d'accés del contenidor:

```
Subxarxa 1, Classe 1, Client 1
```

El contenidor més específic és l'últim de la llista. Per obtenir una adreça, s'examina la llista en jerarquia invertida per trobar la primera adreça disponible. Seguidament, la llista s'examina en jerarquia cap endavant per obtenir les opcions. Les opcions alteren temporalment els valors precedents a no ser que hi hagi una opció denegar present al contenidor. Així mateix, com que la `Classe 1` i el `Client 1` són a la `Subxarxa 1`, s'ordenen segons la prioritat de contenidor. Si el mateix client és a la Subxarxa 2 i envia el mateix missatge, la llista de contenidor que es genera és:

```
Subxarxa 2, Classe 1, Client 1 (a nivell de la Subxarxa 2), Client 1 (a nivell de la Classe 1)
```

Primer es fa una llista de la `Subxarxa 2`, després de la `Classe 1`, seguidament del `Client 1` a nivell de la `Subxarxa 2` (perquè aquesta sentència de client només es troba un nivell per sota de la jerarquia). La jerarquia implica que un client que coincideix amb la primera sentència de client és menys específic que el client que coincideix amb el `Client 1` de la `Classe 1` a la `Subxarxa 2`.

La prioritat dels contenidors no substitueix la prioritat seleccionada per profunditat dins la jerarquia. Per exemple, si el mateix client executa el mateix missatge i especifica un identificador de proveïdor, la llista de contenidor és:

```
Subxarxa 2,Classe 1,Proveïdor 1,Client 1(a nivell de la Subxarxa 2),Client 1(a nivell de la Classe 1)
```

La prioritat de contenidor millora el rendiment de cerca ja que segueix el concepte general segons el qual els contenidors de clients són la manera més específica de definir un o més clients. El contenidor de classes reté menys adreces específiques que un contenidor de clients; el de proveïdors és encara menys específic i el de subxarxes, el menys específic de tots.

Adreces i abasts d'adreces DHCPv6:

Qualsevol tipus de contenidor pot tenir associats abasts d'adreces; les subxarxes han de tenir abasts d'adreces associats.

Cada abast d'un contenidor ha de ser un subconjunt de l'abast i no s'ha de superposar amb els abasts dels altres contenidors. Per exemple, si una classe es troba definida en una subxarxa i té un abast, aquest abast ha de ser un subconjunt de l'abast de la subxarxa. De la mateixa manera, l'abast d'aquest contenidor de classes no es pot superposar amb cap altre abast del seu nivell.

Els abasts poden expressar-se a la línia del contenidor i modificar-se per abast, així com excloure sentències per permetre conjunts d'adreces desunits associats a un contenidor. Si teniu disponibles les deu adreces principals i les segones deu adreces d'una subxarxa, la subxarxa pot especificar aquestes adreces per abast a la clàusula de la subxarxa per reduir tant l'ús de la memòria com el risc de col•lisió d'adreces amb altres clients fora dels abasts especificats.

Després de seleccionar una adreça, s'elimina de la llista qualsevol contenidor subseqüent de la llista que contingui abasts d'adreces juntament amb els seus subordinats. Les opcions específiques de xarxa dels contenidors eliminats no són vàlides si no s'utilitza una adreça des d'aquell contenidor.

Opcions del fitxer de configuració DHCPv6:

Després d'haver netejat la llista per determinar les adreces, es genera un conjunt d'opcions per al client.

En aquest procés de selecció, les opcions sobreescriuen les opcions seleccionades prèviament a no ser aparegui un denegar; en aquest cas, l'opció denegada s'elimina de la llista que s'està enviant al client. Aquest mètode permet l'herència dels contenidors superiors per reduir la quantitat de dades que cal especificar.

Opcions específiques del servidor DHCPv6:

El darrer conjunt de paràmetres que s'han d'especificar són opcions específiques del servidor que permeten a l'usuari controlar el nombre de processadors de paquets, la freqüència d'execució dels fils de recollida de deixalles, etc.

Per exemple, dues opcions específiques del servidor són:

reservedTime
: Indica quant de temps una adreça roman en l'estat reservat després d'enviar un anunci al client **DHCP**.

reservedTimeInterval
: Indica la freqüència amb què el servidor **DHCP** escaneja les adreces per veure si n'hi ha cap que hagi estat en l'estat reservat més temps del que s'indica a *reservedTime*.

Aquestes opcions són útils si teniu diversos clients que difonen missatges de sol•licitud i que, o bé no difonen el seu missatge de sol•licitud, o bé el seu missatge de sol•licitud es perd a la xarxa. L'ús d'aquestes opcions evita que les adreces estiguin reservades de forma indefinida per a un client que no respecta els estàndards.

Un altra opció especialment útil é *SaveInterval*, que indica la freqüència dels desaments.

Fitxer /etc/dhcpv6/dhcpsdv6.cnf:

El servidor **DHCPv6** es configura mitjançant l'edició del fitxer `/etc/dhcpv6/dhcpsdv6.cnf`.

Les paraules clau són sensibles a les majúscules i minúscules. Quan es llista un '{' , ha de ser a la mateixa línia de la paraula clau. Podeu trobar una configuració de mostra al `/usr/samples/tcpip/dhcpv6`.

A continuació, us presentem la descripció del fitxer `/etc/dhcpv6/dhcpsdv6.cnf`. En aquest fitxer, es permeten les stanzes següents:

- Inici de sessió
- Paraules clau globals
- Sentències de contenidors no imbricats
- Sentències de contenidors imbricats
- Opcions
- Opcions comuns

Inici de sessió DHCPv6:

Les paraules clau del servidor **DHCPv6** que es descriuen aquí són per a les entrades de la stanza d'inici de sessió.

Aquesta stanza no és necessària, però si hi és, ha d'estar situada a la part superior del fitxer de configuració. Té el format següent:

```
logging_info { opcions_log }
```

Els valors *opcions_log* poden ser els següents:

Taula 63. Paraules clau, valors i descripcions de les entrades de la stanza d'inici de sessió.

Paraula clau	Valor	Descripció
logFileSize	*núm*	Especifica la grandària del fitxer de registre. El valor *núm* és la grandària màxima del fitxer de registre en quilooctets. El fitxer de registre es gira un cop ha aconseguit aquesta grandària. Si la `logFileSize` no està especificada, s'assumeix una grandària infinita.
logFileName	"*nom_fitxer*"	Especifica el nom del fitxer de registre. El valor *nom_fitxer* serà el nom del fitxer de registre. El nom de fitxer per defecte i la ubicació és `/var/tmp/dhcpsdv6.log`.
numLogFiles	*núm*	Especifica el nombre de fitxers de registre per rotació de fitxer. El valor per defecte és 0.
logItem	*tipus*	Especifica els tipus d'inici de sessió desitjats. Són vàlids els tipus següents: **SYSERR** Error del sistema, a la interfície de la plataforma. **OBJERR** Error d'objecte, entre objectes del procés. **PROTERR** Error de protocol, entre el client i el servidor. **WARNING** Avís, cal que l'usuari hi presti atenció. **EVENT** Incidència del procés. **ACTION** Acció empresa pel procés. **INFO** Informació que pot ser útil. **ACNTING** Qui ha estat servit i quan. **TRACE** Flux de codis, per a la depuració.

Paraules clau globals DHCPv6:

Els valors de paraula clau descrits aquí són per a entrades de la stanza de paraules clau globals.

Les paraules clau globals només són vàlides fora d'un contenidor. Es permeten els valors següents:

Taula 64. Paraules clau, valors i descripcions de les entrades de la stanza de paraules clau globals.

Paraula clau	Valor	Descripció
UsedIpAddressExpiredInterval	`num [`*`unitats`*`]`	Especifica la freqüència amb la qual les adreces situades a l'estat `ERRONI` es recobren i es tornen a provar per validar-les. Si una unitat no està establerta, el valor per defecte del sistema s'estableix en segons. El valor per defecte és -1.
leaseExpiredInterval	`num [`*`unitats`*`]`	Especifica la freqüència amb la qual les adreces de l'estat `VINCULAT` es comproven per veure si han caducat. Si l'adreça ha caducat, l'estat passa a `CADUCAT`. Si una unitat no està establerta, el valor per defecte del sistema s'estableix en segons. El valor per defecte és 900 segons.
reservedTime	`num [`*`unitats`*`]`	Especifica la freqüència amb la qual les adreces haurien de mantenir-se en estat `RESERVAT` abans de recobrar-se a l'estat `LLIURE`. Si una unitat no està establerta, el valor per defecte del sistema s'estableix en segons. El valor per defecte és -1.

Taula 64. Paraules clau, valors i descripcions de les entrades de la stanza de paraules clau globals. (continuació)

Paraula clau	Valor	Descripció
reservedTimeInterval	num [*unitats*]	Especifica la freqüència amb la qual les adreces de l'estat RESERVAT es comproven per veure si s'han de recobrar a l'estat LLIURE. Sense una unitat establerta, el valor per defecte del sistema s'estableix en segons. El valor per defecte és 900 segons.
saveInterval	num [*unitats*]	Especifica la freqüència amb la qual el servidor **DHCP** hauria d'imposar un desament de les bases de dades obertes. Per als servidors molt carregats, hauria de ser 60 o 120 segons. Si una unitat no està establerta, el valor per defecte del sistema s'estableix en segons. El valor per defecte és 3600 segons.
clientpruneintv	num [*unitats*]	Especifica la freqüència amb la qual el servidor **DHCP** fa que les bases de dades eliminin clients que no estan associats a cap adreça (a l'estat UNKNOWN). Això redueix l'ús de memòria del servidor **DHCP**. Sense una unitat establerta, el valor per defecte del sistema s'estableix en segons. El valor per defecte és 3600 segons.
numprocessthreads	num	Especifica el nombre de fils de processadors de paquet que cal crear. Un com a mínim. Cadascun d'ells gestiona un client. Per defecte, és 30.
numpacketthreads	num	Especifica el nombre de fils de paquet que cal crear. El mínim és d'1, però està establert en 5 per defecte.
numloggingthreads	num	Especifica el nombre de fils d'inici de sessió. El valor per defecte és 1.
numduidbuckets	num	Utilitzat pel gestor de taules, té una correlació directa amb el **numprocessthreads**. Per defecte, està establert en 53.
numclientbuckets	num	Quantitat de receptacles que s'utilitzaran per emmagatzemar els enregistraments de client. Per defecte, és 1021.
ignoreinterfacelist	*interfície* [*interfície*]	Llista d'interfícies que cal obviar. Pot ser una sola interfície o bé diverses.
backupfile	"*nom_fitxer*"	Fitxer que cal utilitzar per a les còpies de seguretat de base de dades. El fitxer de valor per defecte és /etc/dhcpv6/db_file6.crbk
checkpointfile	"*nom_fitxer*"	Especifica els fitxers de punt de comprovació de la base de dades. El primer fitxer de punt de comprovació és el camí d'accés. El segon fitxer de punt de comprovació és el camí d'accés amb el darrer caràcter substituït per un 2. Per tant, el fitxer de punt de comprovació no hauria d'acabar en 2.
clientrecorddb	"*nom_fitxer*"	Especifica el fitxer de desament de la base de dades. El fitxer conté tots els enregistraments de client que el servidor **DHCP** ha revisat. El fitxer de valor per defecte és **/etc/dhcpv6/db_file6.cr**
duid	idtype *valor* [*valor*]	Utilitzat per identificar el servidor. Es permeten els valors següents: • duid 1 *interfície* • duid 2 *interfície* • duid 3 enterprise number *identificador* • duid number 0x*dígit_hexadecimal*
preference-number	num	Permet que el clients identifiquin el servidor del qual prefereixen obtenir informació. Com més alt és el valor, hi ha més possibilitats que el client utilitzi aquest servidor per als seus serveis. El valor màxim i per defecte és 255.
unicast-enable	*policy*	Política de difusió individual del servidor, permet que el servidor es comuniqui mitjançant la difusió individual. Per defecte, està activat.
tablemgr-policy	*política*	Permet que el servidor tingui un gestor de taules per gestionar millor els clients d'entrada. Per defecte, està activat.

Taula 64. Paraules clau, valors i descripcions de les entrades de la stanza de paraules clau globals. (continuació)

Paraula clau	Valor	Descripció
auth	*policy*	Permet admetre l'autenticació retardada al servidor. Es desactiva per defecte.
auth-keyfile	"*filename*"	El fitxer que conté les claus d'autenticació retardada per al clients. El fitxer per defecte és **/etc/dhcpv6/dhcpsdv6.keys**.

Sentències de contenidors no imbricats DHCPv6:

La paraula clau **subnet** del servidor **DHCPv6** és per a les entrades de les sentències de contenidors no imbricats.

Les sentències de contenidors no imbricats només poden existir com a part de les paraules clau globals.

Taula 65. Paraules clau, valors i descripcions de les entrades de sentències de contenidors no imbricats.

Element	Descripció	
subnet	*id_subxarxa longitud_prefix* [*abast*] {OPTIONS}	Especifica la subxarxa que cal utilitzar. L'*id_subxarxa* ha de ser una adreça IPv6. La *longitud_prefix* ha de ser un enter positiu menor de 128.

Sentències de contenidors imbricats DHCPv6:

Les sentències de contenidors imbricats només poden existir com a opció dins una subxarxa.

Tots els contenidors poden tenir altres contenidors imbricats a no ser que s'indiqui diversament. La profunditat màxima d'imbricació és de set, inclosos la subxarxa i el contenidor global (només hi pot haver cinc contenidors imbricats sota un contenidor de subxarxes).

Els contenidors de Proveïdors i d'Inoption no poden tenir altres contenidors imbricats.

Taula 66. Paraules clau, valors i descripcions de les entrades de sentències de contenidors imbricats.

Paraula clau	Valor	Descripció
class	*nom* [*abast*] {OPTIONS|COMMON OPTIONS }	Contenidor de classes. El valor *nom* és una sèrie, sèries separades per espais, una expressió regular, un hexadecimal 0x*dígit_hexadecimal*, 0x*dígit_hexadecimal*
vendor	*nom* [*abast*] {OPTIONS|COMMON OPTIONS }	Contenidor de proveïdors. El valor *nom* és una sèrie, sèries separades per espais, una expressió regular, un hexadecimal 0x*dígit_hexadecimal*, 0x*dígit_hexadecimal*
client	<*id* | 0 0xhexdigit | regular expression> <ip | *abast* | none | any> {OPTIONA|COMMON OPTIONS }	Contenidor de clients. *id*- 1-hexdigit, 2-hexdigit, 3-hexdigit <ip|range|none|any> - adreça IP que cal donar als clients que coincideixen amb l'ID
inoption	*codi_e clau_per_aparellar* [*abast*] { OPTIONS|COMMON OPTIONS }	Contenidor Inoption *codi_e* - codi o número d'opció d'entrada que el client ha d'especificar *clau_per_aparellar* - Les dades d'opció que cal fer coincidir.

Opcions del fitxer DHCPv6:

Les opcions del fitxer `cnf` descrites aquí per a **DHCPv6** només poden existir en un contenidor.

Taula 67. Paraules clau, valors i descripcions de les entrades de la stanza d'opcions.

Paraula clau	Valor	Descripció
exclude	*abast*	Abast IP que cal excloure de l'abast actual, utilitzat sovint quan un abast no està especificat com a part de la sentència de contenidor
exclude	`ip`	Adreça IP que cal excloure de l'abast actual
range	*abast*	Abast IP per estendre l'abast actual, utilitzat sovint quan un abast no està especificat com a part de la sentència de contenidor
range	`ip`	Adreça IP que cal afegir, utilitzada per estendre l'abast
stealfromchildren	*política*	Roba una adreça dels contenidors subordinats si s'han exhaurit totes les adreces. Es desactiva per defecte.
stealfrompeer	*política*	Roba adreces de contenidors similars si s'han exhaurit totes les adreces. Es desactiva per defecte.
stealfromparent	*política*	Roba adreces de contenidors superiors si s'han exhaurit totes les adreces. Es desactiva per defecte.
balance-option	`{ balance-policy | <option | option option ...> }`	Equilibra el contenidor d'opcions, les opcions especificades en aquest contenidor es donaran al client segons la política. Aquesta paraula clau només pot existir sota el contenidor de subxarxes.
balance-policy	`b_policy`	El valor b_policy pot ser `fill` o `rotate`. El valor per defecte és `rotate`.
fill-count	`num`	El nombre de vegades que una opció s'anunciarà abans de lliurar la següent instància de la mateixa opció
interface-id	"*interfície*"	Només es pot llistar sota la subxarxa. A les sol•licituds de clients rebudes en aquesta interfície se'ls permetrà obtenir adreces.

Opcions comuns del DHCPv6:

Aquestes paraules clau són opcions comuns del **DHCPv6**.

Pot ser que es trobin dins els contenidors o bé a la secció global:

Taula 68. Paraules clau, valors i descripcions d'opcions comuns.

Paraula clau	Valor	Descripció
reconfig-policy	*policy*	Permet al servidor enviar un missatge de reconfiguració al client. No s'estableix per defecte i es considera desactivat.
rapid-commit	*policy*	Permet que el servidor realitzi una confirmació ràpida del contenidor o que l'estableixi globalment. No s'estableix per defecte i es considera desactivat.
prefered-lifetime	`num [`*units*`]`	Durada preferida de l'IANA o IATA. El valor per defecte és 43200 segons.
valid-lifetime	`num [`*units*`]`	Durada vàlida de l'IANA o IATA. El valor per defecte és 86400 segons.
rebind	`num`	Percentatge 0-100 de temps de revinculació de l'adreça. El valor per defecte és un 80 per cent.
renew	`num`	Percentatge 0-100 de temps de renovació de l'adreça. El valor per defecte és un 50 per cent.
unicast-option	`policy`	Permet als contenidors oferir un intercanvi de missatges mitjançant la difusió individual; es pot utilitzar per activar i desactivar contenidors i subxarxes individuals fins i tot si la política de servidor és diferent. No s'estableix per defecte i es considera desactivat.

Taula 68. Paraules clau, valors i descripcions d'opcions comuns. (continuació)

Paraula clau	Valor	Descripció
option	num <string|stings| hex>	Per a la llista d'opcions, consulteu l'apartat "Opcions conegudes de fitxer del servidor DHCPv6".
change-optiontable	optiontable	Només permesa en un contenidor de proveïdors.

Opcions conegudes de fitxer del servidor DHCPv6:

En aquest apartat es descriuen les opcions de fitxer conegudes del servidor **DHCPv6**.

Les opcions següents són les opcions conegudes de fitxer del servidor **DHCPv6**. Les opcions que tenen un "No" a la columna **Es pot especificar** no es poden especificar al fitxer de configuració; si estan especificades, s'ignoren.

Número d'opció	Tipus de dades per defecte	Es pot especificar?	Descripció
1	Cap	No	Demana
2	Cap	No	Anuncia
3	Cap	No	Sol•licita
4	Cap	No	Confirma
5	Cap	No	Adreça
6	Cap	No	Sol•licitud d'opció
7	número	No	El número de preferència del servidor
8	Cap	No	Temps transcorregut
9	Cap	No	Missatge de retransmissió
11	Cap	No	Auth
12	Sèrie ASCII sí, no, cert, fals	Sí	Difusió individual
13	Cap	No	Estat
14	Sèrie ASCII sí, no, cert, fals	Sí	COnfirmació ràpida
15	Cap	No	Classe User
16	Cap	No	Classe Vendor
17	Cap	No	Opció Vendor
18	Cap	No	ID d'interfície
19	Cap	No	Missatge de reconfiguració
20	Sèrie ASCII sí, no, cert, fals	Sí	Accepta reconfiguració
23	Adreces IPv6 separades per un espai	Sí	Servidors DNS
24	Sèrie ASCII	Sí	Llista de dominis

Valors dels paràmetres DHCPv6:

Aquests valors es poden utilitzar per als paràmetres **DHCPv6**.

unitats: segon, segons, minut, minuts, hora, hores, dia, dies, setmana, setmanes, mes, mesos, any, anys

interfície: en0, en1, tr0

identificador: nombres o caràcters

política: sí, no, cert, fals

abast: ipv6addresss-ipv6addresss

expressió regular: "!epression to match$", "!epression to match^"

Exemple de fitxer /etc/dhcpv6/dhcpsdv6.cnf:

L'exemple de fitxer `/etc/dhcpv6/dhcpsdv6.cnf` que es mostra a continuació permet entreveure els continguts del fitxer.

```
logging_info{
        logFileSize 4000
        logItem     SYSERR
        logItem     PROTERR
        logItem     WARNING
        logItem     EVENT
        logItem     ACTION
        logItem     INFO
        logItem     ACNTING
        logItem     TRACE
        numLogFiles     3
        logFileName "/var/tmp/dhcpsdv6.log"
}
duid 1 en0
numprocessthreads 10
numpacketthreads  5
preference-number 255
reconfig-policy no
rapid-commit  no
unicast-option    yes
leaseExpiredInterval  3000 seconds
unicast-enable          yes
saveInterval            60 seconds
reservedTimeInterval    8000 seconds
reservedTime            10000 seconds
clientpruneintv         20  seconds

subnet bbbb:aaaa:: 40 bbbb:aaaa::0004-bbbb:aaaa::000f {
        balance-option {
               option 23 dead::beef
               option 23 beef::aaaa
               option 24 yahoo.com
        }

subnet dead:dead:aaaa:: 48 dead:dead:aaaa:aaaa::0006-dead:dead:aaaa:aaaa::000a {
        interface-id "en1"
        preferred-lifetime      100 seconds
        valid-lifetime          200 seconds
        rapid-commit  yes
        option 23 dead::beef beef:aaaa::bbbb:c aaaa:bbbb::cccc
        option 24 ibm.com austin.ibm.com
}
```

Configuració de clients DHCPv6

El fitxer `/etc/dhcpv6/dhcpc6.cnf` s'utilitza per configurar els clients **DHCPv6**.

Les directives que es poden especificar en aquest fitxer estan incloses aquí. Si el **dhcpcd6** s'ha d'iniciar a través de reengegades, afegiu una entrada al fitxer `/etc/rc.tcpip`.

Paraules clau d'inici de sessió:

En aquest apartat es descriuen les paraules clau d'inici de sessió vàlides del servidor **DHCPv6**.

Són vàlides les paraules clau següents:

Taula 69. Paraules clau i descripcions de les paraules clau d'inici de sessió.

Paraula clau	Descripció
log-file-name	Camí d'accés i nom de fitxer del fitxer de registre més recent. Els noms de fitxer menys recents tenen el número 1 a (n-1) afegit al nom de fitxer; com més gran és el nombre, menys recent és el fitxer.
log-file-size	Especifica la grandària màxima d'un fitxer de registre en KB. Quan la grandària del fitxer de registre més recent arriba a aquest valor, se li canvia el nom i es crea un nou fitxer.
log-file-num	Especifica el nombre màxim de fitxers de registre mantinguts quan la grandària del fitxer de registre més recent arriba al valor **log-file-size** i es canvia el nom del fitxer per generar-ne un de nou.
log-item	Especifica els elements d'enregistrament que s'han d'enregistrar. **SYSERR** Error de sistema **OBJERR** Error d'objecte **PROTERR** Error de protocol **WARNING** Avís **EVENT** Incidència produïda **ACTION** Acció empresa pel procés **INFO** Informació addicional **ACNTING** Qui ha estat servit i quan **TRACE** Flux de codis, depuració.

Paraules clau DUID:

Els valors de paraula clau següents són per a entrades DUID.

El format de les entrades DUID és el següent:

```
duid  <duid_type> <value>  <value> ...
```

El tipus de DUID pot ser una paraula clau o un nombre i queda espai per a altres tipus de DUID que es defineixin en un futur. Hi ha tres tipus de DUID definits actualment pel RFC 3315 :

Taula 70. Paraules clau i valors de les entrades DUID.

Paraula clau	Descripció
LLT	Tipus DUID-LLT (valor 1)
LL	DUID-LL (valor 2)
EN	Tipus DUID-EN (valor 3)

El format específic de les entrades DUID depèn de la paraula clau utilitzada.

```
duid  LLT    <interface name>
duid  LL     <interface name>
duid  EN     <enterprise number>  <enterprise identifier>
duid  <number>  <hex data (prefixed with '0x')
```

Paraula clau Information-only:

La paraula clau information-only està en format `info-only` *`nom d'interfície`*.

A continuació, trobeu la paraula clau information-only:

Taula 71. Paraula clau i descripció de la paraula clau information-only.

Paraula clau	Descripció
`info-only` *`nom d'interfície`*	Aquesta paraula clau especifica el nom de la interfície per a la qual el client només ha d'obtenir informació de configuració, i no adreces, del servidor.

Renovació de lloguer i paraules clau de revinculació:

La renovació de lloguer i les paraules clau de revinculació que es descriuen en aquest apartat són per al servidor **DHCPv6**.

Taula 72. Paraules clau i descripcions per la renovació de lloguer i paraules clau de revinculació

Paraules clau	Descripció
`rebind-time` *`valor`*	En cas que el client no aconsegueixi renovar el lloguer (perquè el servidor no respon), el rebind-time especifica l'hora a la qual el client contacta els altres servidors per revincular el lloguer.
`renew-time` *`valor`*	El renew-time especifica l'hora en què el client contacta el servidor del qual el client ha obtingut la informació de lloguer, per tal de renovar-lo.

Paraules clau de la retransmissió de sol•licitud:

Les paraules clau de la retransmissió de sol•licitut inclouen **solicit-maxcount** i **solicit-timeout**.

Taula 73. Paraules clau i descripcions de les paraules clau de la retransmissió de sol•licitud.

Paraules clau	Descripcions
solicit-maxcount	La paraula clau solicit-maxcount especifica el nombre de missatges de sol•licitud que el client envia al servidor abans de rebre una resposta per part del servidor.
solicit-timeout	La paraula clau solicit-timeout especifica el temps fins el qual el client intenta enviar el missatge de sol•licitud al servidor abans de rebre una resposta per part del servidor.

Paraules clau d'opcions:

Si les paraules clau d'opcions apareixen fora de les stanzas d'"interfície", aleshores es consideren globals. Aquestes opcions són aplicables a totes les interfícies. Si les paraules clau d'opcions apareixen dins de les stanzas d'"interfície", només són aplicables a la interfície en qüestió.

La stanza d'opcions segueix aquest format:

```
option <keyword | option code>
option <keyword | option code> exec "exec string"
option <keyword | option code> { option specific parameters }
option <keyword | option code> { option specific parameters } exec "exec string"
```

Un codi d'opció es pot especificar mitjançant el codi d'opció enregistrada IANA. No obstant això, algunes opcions també es poden especificar mitjançant les paraules clau que es mostren seguidament:

Paraula clau	Codi d'opció
ia-na	3
ia-ta	4
request-option	6
rapid-commit	14
user-class	15
vendor-class	16
vendor-opts	17
reconf-accept	20
dns-servers	23
domain-list	24

A continuació, vegeu una explicació addicional de cada paraula clau:

Paraula clau	Finalitat, format i paràmetres
ia-na	**Finalitat** Especifica l'opció 3. Si està especificada, el client sol•licita adreces no temporals del servidor. **Format** `option ia-na [ { paràmetres } ] [ exec "exec string" ]` **Paràmetres** L'opció **ia-na** agafa els següents paràmetres: ia-id *valor* renew-time *valor* rebind-time *valor* Aquests paràmetres especifiquen els valors preferits de l'usuari i són opcionals. El *valor* especificat pot ser un nombre decimal o un nombre hexadecimal amb el prefix '0x'
ia-ta	**Finalitat** Especifica l'opció 4. Si està especificada, el client sol•licita adreces temporals del servidor. **Format** `option ia-ta [ { paràmetres } ] [ exec "exec string" ]` **Paràmetres** L'opció **ia-ta** agafa els següents paràmetres: ia-id *valor* Aquest paràmetre especifica els valors preferits de l'usuari i és opcional. El *valor* especificat pot ser un nombre decimal o un nombre hexadecimal amb el prefix '0x'
request-option	**Finalitat** Especifica l'opció 6. Si està especificada, el client sol•licita una llista d'opcions del servidor. **Format** `option request-option { paràmetres } [ exec "exec string" ]` **Paràmetres** L'opció **request-option** agafa una llista de codis d'opcions (en decimals) separada per espais com a argument
rapid-commit	**Finalitat** Especifica l'opció 14. Si està especificada, el client indica que està preparat per dur a terme l'intercanvi de missatges de sol•licitud-resposta. **Format** `option rapid-commit [exec "exec string"]` **Paràmetres** No agafa cap paràmetre que no sigui la sentència exec opcional

Paraula clau	Finalitat, format i paràmetres
user-class	**Finalitat** Especifica l'opció 15. Si està especificada, el client indica el tipus o categoria d'usuari o les aplicacions que representa. **Format** `option user-class { paràmetres } [ exec "exec string" ]` **Paràmetres** L'opció **user-class** agafa una o més instàncies de les dades de classe d'usuari. Cada instància de dades de classe d'usuari és una sèrie entre cometes o no de longitud arbitrària. Si una sèrie conté un espai en blanc, s'ha de posar entre cometes. Es requereixen els paràmetres. El format del paràmetre és: class *valor* class *valor* on *valor* és una sèrie entre cometes o no.
vendor-class	**Finalitat** Especifica l'opció 16. Si està especificada, el client indica el proveïdor que va fabricar el maquinari que està utilitzant el client. **Format** option vendor-class { *paràmetres* } [exec "exec string"] **Paràmetres** L'opció **vendor-class** agafa el nombre enregistrat d'Empresa del proveïdor i una instància o més de dades de classe de proveïdor. Cada instància de dades de classe de proveïdor és una sèrie entre cometes o no de longitud arbitrària, que descriu alguna característica de la configuració de maquinari del client. Els paràmetres *no* són opcionals. El format és: vendor-id *valor* class *valor* class *valor* on *valor* és una sèrie entre cometes o no.
vendor-opts	**Finalitat** Especifica l'opció 17. Si està especificada, el client indica la informació específica de proveïdor al servidor. **Format** `option vendor-opts <nombre_empresa> { paràmetres } [ exec "exec string" ]]` **Paràmetres** L'opció **vendor-opts** agafa el nombre enregistrat d'Empresa del proveïdor i una instància o més de dades d'opció de proveïdor. Cada instància de dades d'opció de proveïdor és un codi d'opció de proveïdor seguit d'unes dades d'opció en format de sèrie o hexadecimal. Els paràmetres *no* són opcionals. El format és: vendor-id *valor* option *codi_op dades_opció* option *codi_op dades_opció* on *dades_opció* és una sèrie entre cometes o no o bé una sèrie hexadecimal (amb el prefix '0x')
reconf-accept	**Finalitat** Especifica l'opció 20. Si està especificada, el client indica al servidor si el client desitja acceptar un missatge de reconfiguració del servidor. **Format** `option reconf-accept [ { exec "exec string" } ]` **Paràmetres** L'opció **reconf-accept** no agafa cap paràmetre específic d'opció llevat de la sentència exec.
dns-servers	**Finalitat** Especifica l'opció 23. Si està especificada, el client indica al servidor el conjunt preferit de servidors DNS. **Format** `option dns-servers [ { paràmetres } ] [ exec "exec string" ]` **Paràmetres** L'opció **dns-servers** agafa una llista d'adreces IPv6 com a argument separada per espais/línies.

Paraula clau	Finalitat, format i paràmetres
domain-list	**Finalitat** Especifica l'opció 24. Si està especificada, el client indica la llista de domini preferida. **Format** `option domain-list [ { paràmetres } ] [ exec "exec string" ]` **Paràmetres** L'opció **domain-list** agafa una llista de sèries de nom de domini separada per espais/línies.

Paraules clau d'interfície:

La paraula clau d'interfície està en format `interface <nom d'interfície> [ { option declaration/s } ]`.

Taula 74. Paraula clau i descripció de les paraules clau d'interfície.

Paraules clau	Descripcions
`interface <nom d'interfície> [ { option declaration/s } ]`	La sentència d'interfície pren una declaració d'opció o més com a arguments. Aquestes opcions, especificades dins d'una stanza d'interfície són específiques de la interfície, a diferència de les opcions declarades fora de la stanza d'interfície, que s'apliquen a totes les interfícies.

```
interface  en1  {
                          option ia-na {
            ia-id  01
            renew-time 0x40
            rebind-time 0x60
 }

  option  request-option  { 3 23 24 }

       option  user-class {
          class ibm
               class "userclassA and B"
               class "userclassB"
       }

      option  vendor-class {
            vendor-id 1234
               class "vendorclassA"
               class "vendorclassB"
      }

      option  vendor-opts {
          vendor-id 2343
                 option 89       vendoroption89
                 option 90       vendoroption90
      }

 option reconf-accept
```

Agent DHCP Relay

El fitxer `/etc/dhcprd.cnf` és el fitxer de configuració de l'agent de retransmissió **DHCP** i **BOOTP**. A continuació s'expliquen el format del fitxer i les instruccions i paraules clau permeses.

Les instruccions s'especifiquen amb el format següent:

<paraula_clau> <valor1> ... <valorN>

L'agent de retransmissió iniciat o reiniciat utilitza la presència i els valors d'aquests paràmetres.

Aquest conjunt de paràmetres especifica els fitxers de registre que mantindrà aquest servidor. Cada paràmetre s'identifica amb una paraula clau i va seguit pel seu valor.

Paraula clau	Valor	Definició
numLogFiles	0 a *n*	Nombre de fitxers de registre. Si s'especifica un 0, no es mantindrà cap fitxer de registre i no es mostrarà cap missatge d'enregistrament enlloc. *n* és el nombre màxim de fitxers de registre mantinguts mentre la grandària del fitxer de registre més recent aconsegueix la seva grandària màxima i es crea un nou fitxer de registre.
logFileSize	En KB	Grandària màxima d'un fitxer de registre. Quan la grandària del fitxer de registre més recent aconsegueix aquest valor, se li canvia el nom i es crea un nou fitxer de registre.
logFileName	camí d'accés de fitxer	Nom del fitxer de registre més recent. Els fitxers de registre menys recents tenen el número de l'1 a l'(*n* - 1) afegit a llurs noms; com més gran és el número, menys recent és el fitxer.
logItem	Un element que s'enregistrarà.	**SYSERR** Error del sistema, a la interfície de la plataforma. **OBJERR** Error d'objecte, entre els objectes del procés. **PROTERR** Error de protocol, entre client i servidor. **WARNING** Avís, que mereix l'atenció de l'usuari. **EVENT** Incidència ocorreguda al procés. **ACTION** Acció realitzada pel procés. **INFO** Informació que pot ser útil. **ACNTING** A qui es va servir i quan. **TRACE** Flux de codi, per a la depuració.

Per exemple, un fitxer `/etc/dhcprd.cnf` pot tenir les entrades següents:

```
numLogFiles  4
logFileSize  1000
logFileName    /usr/tmp/dhcprd.log
logItem     SYSERR
logItem     OBJERR
logItem     PROTERR
logItem     WARNING
logItem     EVENT
logItem     ACTION
logItem     INFO
logItem     ACNTING
logItem     TRACE
```

Paraula clau	Valor	Definició
relay	**IPv4**, **IPv6** o **ALL**	Especifica el mode de retransmissió de paquets. Si s'especifica **IPv4**, l'agent de retransmissió només actua com l'agent de retransmissió **DHCPv4**. Aquest és el mode per defecte de l'agent de retransmissió. Si s'especifica **IPv6**, l'agent de retransmissió només actua com l'agent de retransmissió **DHCPv6**. Si s'especifica **ALL**, l'agent de retransmissió actua com l'agent de retransmissió **DHCPv4** i **DHCPv6**.
servidor	Adreça IP	Especifica l'adreça IP d'un servidor **BOOTP** o **DHCP**. El paquet es reenviarà als servidors llistats en aquest fitxer.
server6	Adreça IPv6	Especifica l'adreça IPv6 del servidor **DHCPv6**. El paquet es reenviarà als servidors llistats aquí.
option6	*<codi_opció> <dades_opció>*	Especifica les opcions de l'agent de retransmissió **DHCPv6**. La paraula clau només és vàlida si el mode de retransmissió està establert en IPv6. El valor *codi_opció* s'especifica com un nombre decimal. El valor *dades_opció* s'especifica com una sèrie entre cometes o sense, o en format hexadecimal (amb el prefix `0x`).
single-site		Especifica que el dispositiu en el qual s'executa l'agent de retransmissió pertany només a un lloc.

Proxy PXE del daemon DHCP

El Proxy PXE del servidor **DHCP** es comporta de forma semblant a un servidor **DHCP** ja que està pendent del trànsit ordinari del client **DHCP** i respon a determinades sol•licituds del client. No obstant això, a diferència del servidor **DHCP**, el Proxy PXE del servidor **DHCP** no administra adreces de xarxa i només respon a clients que s'identifiquen com a clients PXE.

Les respostes del Proxy PXE del servidor **DHCP** contenen el mecanisme pel qual el client localitza els servidors d'engegada o les adreces de xarxa i descripcions dels servidors d'engegada compatibles suportats.

L'ús d'un Proxy PXE del servidor **DHCP** a més d'un servidor **DHCP** proporciona tres funcions clau. Primer, podeu separar l'administració de les adreces de xarxa de l'administració de les imatges d'engegada. Amb l'ús de dos processos diferents al mateix sistema, podeu configurar la informació d'engegada gestionada pel Proxy PXE del servidor **DHCP** sense pertorbar ni necessitar l'accés a la configuració del servidor **DHCP**. En segon lloc, podeu definir múltiples servidors d'engegada i deixar que el client PXE seleccioni un servidor determinat durant l'engegada. Cada servidor d'engegada pot, per exemple, oferir un tipus diferent de sistema operatiu o configuració del sistema. Finalment, l'ús del servidor proxy ofereix la capacitat de configurar el client PXE per utilitzar l'adreçament IP de difusió múltiple per descobrir la ubicació dels servidors d'engegada compatibles.

El Proxy PXE del servidor **DHCP** es pot configurar per executar-se al mateix sistema on s'està executant el servidor **DHCP** o bé en un sistema diferent. També es pot configurar per executar-se al mateix sistema on s'està executant el daemon de servidor d'engegada o bé en un sistema diferent.

Components del servidor DHCP Proxy PXE

Hi ha tres components del servidor PXED.

El servidor PXED es troba segmentat en tres parts principals: una base de dades, un motor de protocol i un conjunt de fils de servei, i cada part té la seva pròpia informació de configuració.

Base de dades PXED:

La base de dades `db_file.dhcpo` s'utilitza per generar les opcions que cal enviar al client quan aquest envia un paquet de PETICIÓ.

Les opcions que la base de dades torna depenen del tipus de servidor que s'ha seleccionat. Això s'estableix mitjançant la paraula clau **pxeservertype** al fitxer `pxed.cnf`.

La base de dades s'actualitza i verifica per coherència mitjançant la informació del fitxer de configuració.

Motor de protocol PXED:

El motor de protocol utilitza la base de dades per determinar la informació que caldria retornar al client.

El motor de protocol PXED es basa en l'Intel Preboot Execution Environment (PXE) Specification Version 2.1 i encara és compatible amb l'Intel PXE Specification Version 1.1.

Operacions de diversos fils del PXED:

La darrera part del servidor PXED és un conjunt d'operacions que s'utilitzen per mantenir el funcionament. Atès que el PXED és un servidor amb fils, aquestes operacions realment estan configurades com a fils que de tant en tant realitzen certes tasques per assegurar-se que tot està enllaçat correctament.

El primer fil, el *principal*, gestiona les sol•licituds SRC (com ara **startsrc**, **stopsrc**, **lssrc**, **traceson** i **refresh**). Aquest fil coordina també totes les operacions que afecten tots els fils i gestiona els senyals. Per exemple,

- Un SIGHUP (-1) provoca una renovació de totes les bases de dades del fitxer de configuració.
- Un SIGTERM (-15) fa que el servidor s'aturi correctament.

L'altre fil processa els paquets. Segons el tipus de servidor, hi pot haver un o dos fils. Un fil està pendent del port 67 i el segon, del port 4011. Cadascun d'ells pot gestionar la sol•licitud d'un client.

Configuració del servidor PXED

Per defecte, el servidor PXED es configura mitjançant la lectura del fitxer `/etc/pxed.cnf`, el qual especifica la base de dades inicial d'adreces i opcions del servidor.

El servidor s'inicia des la SMIT o mitjançant ordres SRC.

La configuració del servidor PXED és normalment la part més complexa pel que fa a l'ús del PXED a la xarxa. Primerament, decidiu quines xarxes cal que tinguin clients PXE. A l'exemple següent es configura el daemon **pxed** per tal que s'executi a la mateixa màquina que el servidor DHCP:

```
pxeservertype       proxy_del_servidor_dhcp

subnet default
{
    vendor pxe
    {
        option    6      2       # Inhabilitar descobriment de servidor d'engegada de difusió múltiple
        option    8      1   2     9.3.4.5    9.3.4.6   2    1    9.3.149.29
                                 # L'opció anterior dóna la llista de servidors d'engegada
        option    9      0       "Servidor d'arrencada PXE" \
                                 1       "Servidor d'engegada Microsoft Windows NT"  \
```

```
                        2       "Servidor d'engegada DOS/UNDI"
        option    10    20    "segons abans d'autoseleccionar el 1r element del menú d'engegada"
     }
}
```

Les subopcions del contenidor de proveïdors només s'envien als clients PXE si l'adreça IP del client es troba a l'abast d'adreces IP de la subxarxa (per exemple, de 9.3.149.0 a 9.3.149.255).

A l'exemple següent es configura el daemon **pxed** per tal que s'executi en una màquina diferent del servidor **DHCP**:

```
subnet default
{
    vendor pxe
    {
        option    6      10      # El nom del fitxer d'engegada es troba al paquet d'oferta pxed
                                 # inicial del client.
        option    8      1   2     9.3.4.5    9.3.4.6   2    1    9.3.149.29
                                 # L'opció anterior dóna la llista de servidors d'engegada
        option    9      0       "Servidor d'arrencada PXE" \
                         1       "Servidor d'engegada Microsoft Windows NT"  \
                         2       "Servidor d'engegada DOS/UNDI"
        option    10    20    "segons abans d'autoseleccionar el 1r element del menú d'engegada"
        bootstrapserver          9.3.148.65
        pxebootfile    1    2    1   window.one
        pxebootfile    2    2    1   linux.one
        pxebootfile    1    2    1   hello.one
        client 6 10005a8ad14d any
        {
           pxebootfile    1    2    1   aix.one
           pxebootfile    2    2    1   window.one
        }
    }

Vendor pxeserver
{
    option     7     224.234.202.202
}
```

La paraula clau **pxeservertype** no està establerta al fitxer de configuració, per la qual cosa es pren el valor per defecte, que és **pdhcp_only**. Això significa que el servidor PXED s'executa en una màquina diferent del servidor **DHCP**. Amb aquesta configuració, el servidor PXED està pendent de dos ports (67 i 4011) per als paquets BINLD de sol•licitud/informació dels clients. L'opció 7 s'envia al servidor BINLD quan el servidor PXED rep un paquet de sol•licitud/informació al port 67 de part del BINLD i l'opció 60 està establerta en el servidor PXED.

La clàusula de base de dades `db_file` indica el mètode de base de dades que cal utilitzar per processar aquesta part del fitxer de configuració. Els comentaris comencen amb el signe #. El servidor PXED obvia des del # al final de la línia. El servidor utilitza cada línia d'`opció` per indicar al client el que ha de fer."Subopcions del contenidor de proveïdors del PXE" a la pàgina 303 descriu les opcions conegudes i suportades actualment. Consulteu l'apartat "Sintaxi de fitxer de servidor PXED per al funcionament general del servidor" a la pàgina 305 sobre els mètodes per especificar opcions que el servidor no coneix.

Fitxer de configuració PXED:

El fitxer de configuració té una secció d'adreça i una secció de definició d'opcions que es basen en el concepte de contenidors que retenen opcions, modificadors i, potencialment, altres contenidors.

Un *contenidor* (que és, bàsicament, un mètode per agrupar opcions) utilitza un identificador per classificar els clients en grups. Els tipus de contenidor són els de subxarxes, classes, proveïdors i clients.

Actualment, no hi ha un contenidor genèric que l'usuari pugui definir. L'identificador només defineix el client perquè se'l pugui seguir si, per exemple, es desplaça entre subxarxes. Es pot utilitzar més d'un tipus de contenidor per definir l'accés del client.

Les *Opcions* són identificadors que es tornen al client, com ara la passarel•la per defecte i l'adreça DNS.

Contenidors PXED:

Quan el servidor **DHCP** rep una sol•licitud, s'analitza el paquet i les claus d'identificació determinen els contenidors, les opcions i les adreces que cal extreure.

L'exemple de l'apartat Configuració del servidor PXED mostra un contenidor de subxarxes. La clau d'identificació és la posició del client a la xarxa. Si el client és d'aquesta xarxa, cau en aquest contenidor.

Cada tipus de contenidor utilitza una opció diferent per identificar un client:

- El contenidor de subxarxes utilitza el camp `giaddr` o l'adreça d'interfície de la interfície receptora per determinar la subxarxa de la qual procedeix el client.
- El contenidor de classes utilitza el valor de l'opció 77 (Identificador de classes d'indret d'usuari).
- El proveïdor utilitza el valor de l'opció 60 (Identificador de classes de proveïdor).
- El contenidor de clients utilitza l'opció 61 (Identificador de clients) per als clients PXE i el camp `chaddr` del paquet **BOOTP** per als clients **BOOTP**.

A excepció de les subxarxes, cada contenidor permet l'especificació del valor amb el qual coincidirà, incloses les coincidències d'expressió regular.

També hi ha un contenidor implícit, el contenidor *global*. Les opcions i els modificadors del contenidor global s'apliquen a tots els contenidors, a no ser que estiguin alterats temporalment o denegats. La major part dels contenidors es poden col•locar a dins d'altres contenidors que impliquen un àmbit de visibilitat. Tant pot ser que els contenidors tinguin abasts d'adreces associats com no. Les subxarxes tenen, per naturalesa, abasts associats.

Les normes bàsiques dels contenidors i subcontenidors són les següents:

- Tots els contenidors són vàlids a nivell global.
- Les subxarxes no es poden col•locar mai dins d'altres contenidors.
- Els contenidors restringits no poden tenir contenidors regulars del mateix tipus. (Per exemple, un contenidor amb una opció que només permet una classe de `Comptabilitat` no pot incloure un contenidor amb una opció que permeti totes les classes que comencen amb la lletra "a". Això no és permès.)
- Els contenidors de clients restringits no poden tenir subcontenidors.

Segons aquestes normes, podeu generar una jerarquia de contenidors que segmenti les opcions en grups per a clients específics o grups de clients.

Si un client coincideix amb diversos contenidors, com es distribueixen les opcions i les adreces? El servidor **DHCP** rep els missatges, passa la sol•licitud a la base de dades (`db_file`, en aquest cas) i es genera una llista de contenidors. La llista es presenta per ordre de profunditat i de prioritat. La prioritat es defineix com una jerarquia implícita dels contenidors. Els contenidors estrictes tenen una prioritat major que els contenidors regulars. Els clients, les classes, els proveïdors i finalment les subxarxes es classifiquen per aquest ordre i dins el tipus de contenidor segons la profunditat. Això genera una llista ordenada de més específic a menys específic. Per exemple:

```
Subxarxa 1
--Classe 1
--Client 1
Subxarxa 2
```

```
--Classe 1
----Proveïdor 1
----Client 1
--Client 1
```

L'exemple anterior mostra dues subxarxes, `Subxarxa 1` i `Subxarxa 2`. Hi ha un nom de classe, `Classe 1`, un nom de proveïdor, `Proveïdor 1` i un nome de client, `Client 1`. `Classe 1` i `Client 1` estan definits a diferents llocs. Com que es troben en contenidors diferents, pot ser que tinguin el mateix nom, però que els valors al seu interior siguin diferents. Si el `Client 1` envia un missatge al servidor **DHCP** des de la `Subxarxa 1` amb la `Classe 1` especificada a la llista d'opcions, el servidor **DHCP** generarà el següent camí d'accés del contenidor:

`Subxarxa 1, Classe 1, Client 1`

El contenidor més específic és l'últim de la llista. Per obtenir una adreça, s'examina la llista en jerarquia invertida per trobar la primera adreça disponible. Seguidament, la llista s'examina en jerarquia cap endavant per obtenir les opcions. Les opcions alteren temporalment els valors precedents a no ser que hi hagi una opció **deny** al contenidor. Així mateix, com que la `Classe 1` i el `Client 1` són a la `Subxarxa 1`, s'ordenen segons la prioritat de contenidor. Si el mateix client és a la `Subxarxa 2` i envia el mateix missatge, la llista de contenidor que es genera és:

`Subxarxa 2, Classe 1, Client 1` (al nivell de la `Subxarxa 2`), `Client 1` (al nivell de la `Classe 1`)

Primer es fa una llista de la `Subxarxa 2`, després de la `Classe 1`, seguidament del `Client 1` a nivell de la `Subxarxa 2` (perquè aquesta sentència de client només es troba un nivell per sota de la jerarquia). La jerarquia implica que un client que coincideix amb la primera sentència de client és menys específic que el client que coincideix amb el `Client 1` de la `Classe 1` a la `Subxarxa 2`.

La prioritat dels contenidors no substitueix la prioritat seleccionada per profunditat dins la jerarquia. Per exemple, si el mateix client executa el mateix missatge i especifica un identificador de proveïdor, la llista de contenidor és:

`Subxarxa 2, Classe 1, Proveïdor 1, Client 1` (al nivell de la `Subxarxa 2`), `Client 1` (al nivell de la `Classe 1`)

La prioritat de contenidor millora el rendiment de cerca ja que segueix el concepte general segons el qual els contenidors de clients són la manera més específica de definir un o més clients. El contenidor de classes reté menys adreces específiques que un contenidor de clients; el de proveïdors és encara menys específic i el de subxarxes, el menys específic de tots.

Adreces i abasts d'adreces PXED:

Qualsevol tipus de contenidor pot tenir associats abasts d'adreces; les subxarxes els han de tenir. Cada abast d'un contenidor ha de ser un subconjunt de l'abast del contenidor superior i no s'ha de superposar amb els altres abasts.

Per exemple, si una classe es troba definida en una subxarxa i té un abast, aquest abast ha de ser un subconjunt de l'abast de la subxarxa. De la mateixa manera, l'abast d'aquest contenidor de classes no es pot superposar amb cap altre abast del seu nivell.

Els abasts poden expressar-se a la línia del contenidor i modificar-se per abast, així com excloure sentències per permetre conjunts d'adreces desunits associats a un contenidor. Per tant, si teniu disponibles les deu adreces principals i les segones deu adreces d'una subxarxa, la subxarxa pot especificar aquestes adreces per abast a la clàusula de la subxarxa per reduir tant l'ús de la memòria com el risc de col•lisió d'adreces amb altres clients fora dels abasts especificats.

Després de seleccionar una adreça, s'elimina de la llista qualsevol contenidor subseqüent de la llista que contingui abasts d'adreces juntament amb els seus subordinats. El motiu és que les opcions específiques de xarxa en els contenidors eliminats no són vàlides si no s'utilitza una adreça des d'aquell contenidor.

Opcions del fitxer de configuració PXED:

Després d'haver netejat la llista per determinar les adreces, es genera un conjunt d'opcions per al client.

En aquest procés de selecció, les opcions sobreescriuen les opcions seleccionades prèviament a no ser aparegui un *denegar*; en aquest cas, l'opció denegada s'elimina de la llista que s'està enviant al client. Aquest mètode permet l'herència dels contenidors superiors per reduir la quantitat de dades que cal especificar.

Inici de sessió PXED:

Els paràmetres d'inici de sessió s'especifiquen en un contenidor com la base de dades, però la paraula clau del contenidor és **logging_info**.

Quan s'aprèn a configurar el PXED, és aconsellable posar l'inici de sessió al nivell superior. Així mateix, és millor especificar la configuració d'inici de sessió abans que qualsevol altra dada del fitxer de configuració per assegurar-se que els errors de configuració s'enregistrin després que s'hagi inicialitzat el subsistema d'inici de sessió. Utilitzeu la paraula clau **logitem** per habilitar un nivell d'inici de sessió o elimineu la paraula clau **logitem** per inhabilitar un nivell d'inici de sessió. Altres paraules clau per a l'inici de sessió permeten especificar el nom de fitxer de registre, la grandària del fitxer i el nombre de fitxers de registre giratoris.

Consideracions de rendiment del PXED:

És important entendre que determinades paraules clau de configuració i l'estructura del fitxer de configuració tenen un efecte en l'ús de la memòria i el rendiment del servidor PXED.

Primerament, es pot evitar l'ús excessiu de la memòria si entenem el model d'herència d'opcions dels contenidors superiors als subordinats. En un entorn que no dóna suport als clients que no figuren a la llista, l'administrador ha de mostrar explícitament a la llista cada client del fitxer. Quan es realitza una llista d'opcions per a qualsevol client específic, el servidor utilitza més memòria per emmagatzemar aquest arbre de configuració que quan les opcions s'hereten d'un contenidor superior (per exemple, la subxarxa, la xarxa o els contenidors globals). Per tant, l'administrador hauria de comprovar si hi ha opcions repetides al nivell de client en el fitxer de configuració i, si es així, determinar si aquestes opcions es poden especificar al contenidor superior i compartir per tot el grup de clients.

Així mateix, quan s'utilitzen les entrades **logItem** INFO i TRACE, s'enregistren nombrosos missatges durant el processament de cada missatge d'un client PXE. Afegir una línia al fitxer de registre pot ser una operació costosa; per tant, limitar la quantitat d'inicis de sessió millora el rendiment del servidor PXED. Quan se sospita la possibilitat d'un error amb el servidor PXED, es pot tornar a habilitar dinàmicament l'inici de sessió mitjançant l'ordre SRC **traceson**.

Subopcions del contenidor de proveïdors del PXE

Quan es dóna suport a un client PXE, el servidor **DHCP** passa l'opció següent al servidor BINLD que BINLD utilitza per configurar-se a si mateix:

Núm. opció	Tipus de dades per defecte	Es pot especificar?	Descripció
6	Nombre decimal	Sí	PXE_DISCOVERY_CONTROL. Límit 0-16. És un camp de bits. El bit 0 és el bit menys important. **bit 0** Si s'estableix, inhabilita el descobriment de difusió. **bit 1** Si s'estableix, inhabilita el descobriment de difusió múltiple. **bit 2** Si s'estableix, només utilitza/accepta servidors a PXE_BOOT_ SERVERS. **bit 3** Si s'estableix, i hi ha un nom de fitxer d'engegada al paquet d'oferta PXED inicial, baixa el fitxer d'engegada (no hi ha sol•licitud/menú/descobriment del servidor d'engegada). **bit 4-7** Ha de ser 0. Si aquesta opció no s'especifica, el client pressuposa que tots els bits són iguals a 0.
7	Un quartet amb punts	Sí	Adreça IP de difusió múltiple. Adreça IP de difusió múltiple de descobriment del servidor d'engegada. Els servidors d'engegada capaços del descobriment de difusió múltiple han d'estar pendents d'aquesta adreça de multidifusió. Aquesta opció és necessària si no s'estableix el bit d'inhabilitació del descobriment de difusió múltiple (bit 1) a l'opció PXE_DISCOVERY_ CONTROL.
8	*Tipus de servidor d'engegada(0-65535)*	Sí	PXE_BOOT_SERVERS *Recompte d'adreces IP (0-256)* **Tipus 0** Servidor d'engegada Microsoft Windows *Adreça IP...Adreça IP* NT *Tipus de servidor d'engegada Adreça IP* **Tipus 1** Servidor d'engegada Intel LCM *recompte Adreça IP ...* **Tipus 3** Servidor d'engegada DOS/UNDI *Adreça IP* **Tipus 4** Servidor d'engegada NEC ESMPRO **Tipus 5** Servidor d'engegada IBM WSoD **Tipus 6** Servidor d'engegada IBM LCCM **Tipus 7** Servidor d'engegada CA Unicenter TNG. **Tipus 8** Servidor d'engegada HP OpenView. **Tipus 9 a 32767** Reservats **Tipus 32768 a 65534** Ús del proveïdor **Tipus 65535** Servidor de prova PXE API. Si *Recompte d'adreces IP* és zero per a un tipus de servidor, el client pot acceptar les ofertes de qualsevol servidor d'engegada d'aquell tipus. Els servidors d'engegada no responen a les sol•licituds de descobriment de tipus que no suporten.
9	*Tipus de servidor d'engegada (0-65535)*	Sí	PXE_BOOT_MENU *"descripció"* L'"ordre" d'engegada del servidor d'engegada va implícit amb el tipus. *"descripció"...ordre de menú*.

Núm. opció	Tipus de dades per defecte	Es pot especificar?	Descripció
10	*Temps d'espera en segons (0-255)*	Sí	PXE_MENU_PROMPT *"sol•licitud"* El temps d'espera és el nombre de segons que cal esperar abans de seleccionar automàticament el primer element de menú d'engegada. Al sistema client, la sol•licitud es visualitza seguida del nombre de segons que queden abans que se seleccioni automàticament el primer element del menú d'engegada. Si es fa clic a la tecla F8 al sistema client, es mostra un menú. Si es proporciona aquesta opció al client, el menú es visualitza sense sol•licitud ni temps d'espera. Si el temps d'espera és 0, se seleccionarà automàticament el primer element del menú. Si el temps d'espera és 255, es mostraran el menú i la sol•licitud sense selecció automàtica ni temps d'espera.

Sintaxi de fitxer de servidor PXED per al funcionament general del servidor

Les paraules clau de fitxer de servidor PXED del servidor **DHCPv6** que es descriuen aquí fan referència al funcionament general del servidor. S'identifiquen les formes, els subcontenidors, els valors per defecte i els significats.

Nota: Les Unitats de temps (*unitats_temps*) que es mostren a la taula següent són opcionals i representen un modificador de l'hora actual. La unitat de temps per defecte és els minuts. Són valors vàlids els segons (1), els minuts (60), les hores (3600), els dies (86400), les setmanes (604800), els mesos (2392000) i els anys (31536000). El nombre que apareix entre parèntesis és un multiplicador aplicat al valor específic *n* per expressar el valor en segons.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
database	database *tipus db*	Sí	Cap	El contenidor primari que reté les definicions de les agrupacions d'adreces, les opcions i les sentències d'accés de client. El *tipus db* és el nom d'un mòdul que es carrega per processar aquesta part del fitxer. L'únic valor disponible actualment és el **db_file**.
logging_info	logging_info	Sí	Cap	El contenidor d'inici de sessió primari que defineix els paràmetres d'inici de sessió.
logitem	logitem NONE	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies
logitem	logitem SYSERR	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies
logitem	logitem OBJERR	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies
logitem	logitem PROTOCOL	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies
logitem	logitem PROTERR	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies
logitem	logitem WARN	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
logitem	logitem WARNING	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies
logitem	logitem CONFIG	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies
logitem	logitem EVENT	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies
logitem	logitem PARSEERR	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies
logitem	logitem ACTION	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies
logitem	logitem ACNTING	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies
logitem	logitem STAT	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies
logitem	logitem TRACE	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies
logitem	logitem RTRACE	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies
logitem	logitem START	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies
numLogFiles	numLogFiles *n*	No	0	Especifica el nombre de fitxers de registre que cal crear. L'enregistrament gira quan s'emplena el primer. *n* és el nombre de fitxers que cal crear.
logFileSize	logFileSize *n*	No	0	Especifica la grandària de cada fitxer de registre en unitats de 1024 octets.
logFileName	logFileName *camí d'accés*	No	Cap	Especifica el camí d'accés al primer fitxer de registre. El fitxer de registre original s'anomena *nom_fitxer* o *nom_fitxer.extensió*. El *nom_fitxer* ha de tenir vuit caràcters com a màxim. Quan es gira un fitxer, es canvia de nom començant amb la base *nom_fitxer* i, a continuació, afegint un nombre o substituint l'extensió per un nombre. Per exemple, si el nom de fitxer original és `fitxer`, el nom de fitxer girat esdevé `fitxer01`. Si el nom de fitxer original és `fitxer.log`, esdevé `fitxer.01`.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
pxeservertype	pxeservertype *tipus_servidor*	No	només_dhcp	Indica el tipus de servidor **dhcpsd** de què es tracta. El *tipus_servidor* pot ser **proxy_on_dhcp_server**. Això vol dir que el PXED s'està executant a la mateixa màquina que el servidor **DHCP** i està pendent de rebre les sol•licituds de client PXE només al port 4011, o bé el valor per defecte de **pdhcp_only**, la qual cosa vol dir que el PXED s'està executant en una màquina separada i ha d'estar pendent de rebre els paquets de client als ports 67 i 4011.

Sintaxi de fitxer del servidor PXED per a la base de dades db_file

A continuació es descriu la sintaxi de fitxer del servidor PXED per a la base de dades`db_file`. S'identifiquen les formes, els subcontenidors, els valors per defecte i els significats.

Nota:

1. Les Unitats de temps (*unitats_temps*) que es mostren a la taula següent són opcionals i representen un modificador de l'hora actual. La unitat de temps per defecte és els minuts. Són valors vàlids els segons (1), els minuts (60), les hores (3600), els dies (86400), les setmanes (604800), els mesos (2392000) i els anys (31536000). El nombre que apareix entre parèntesis és un multiplicador aplicat al valor específic *n* per expressar el valor en segons.
2. Pot ser que els elements que s'especifiquen en un contenidor s'alterin temporalment dins un subcontenidor. Per exemple, podríeu definir globalment els clients **BOOTP**, però permetre els clients **BOOTP** en una subxarxa determinada tot especificant la paraula clau supportBootp en ambdós contenidors.
3. Els contenidors de clients, classes i proveïdors permeten un suport d'expressió regular. Per als de classes i proveïdors, una sèrie entre cometes. El primer caràcter després de les cometes és un signe d'admiració (!) que indica que la resta de la sèrie s'ha de tractar com una expressió regular. El contenidor de clients permet les expressions regulars tant al camp **tipus maquinari** com al camp **adreça maquinari**. S'utilitza una sèrie simple per representar ambdós camps amb el format següent:

   ```
   decimal_number-data
   ```

   Si el nombre_decimal és el zero, aleshores la dada és una sèrie ASCII. Si és qualsevol altre nombre, la dada és en dígits hexadecimals.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
subnet	subnet default	Sí	Cap	Especifica una subxarxa que no té cap abast. El servidor només utilitza la subxarxa quan respon a un paquet d'INFORMACIÓ del client.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
subnet	subnet *id_subxarxa màscara de xarxa*			Especifica una subxarxa i una agrupació d'adreces. Es pressuposa que totes les adreces són a l'agrupació a no ser que s'especifiqui un abast en la línia o que les adreces es modifiquin posteriorment al contenidor mitjançant un abast o una sentència d'exclusió. L'abast opcional és un parell d'adreces IP en format de quartet amb punt separades per un guió. Es pot especificar una etiqueta opcional i la prioritat. Les subxarxes virtuals les utilitzen per identificar i ordenar les subxarxes de la subxarxa virtual. Dos punts separen l'etiqueta de la prioritat. Aquests contenidors només es permeten a nivell de contenidor de base de dades o global.
subnet	subnet *id_subxarxa màscara de xarxa abast*			Especifica una subxarxa i una agrupació d'adreces. Es pressuposa que totes les adreces són a l'agrupació a no ser que s'especifiqui un abast en la línia o que les adreces es modifiquin posteriorment al contenidor mitjançant un abast o una sentència d'exclusió. L'abast opcional és un parell d'adreces IP en format de quartet amb punt separades per un guió. Es pot especificar una etiqueta opcional i la prioritat. Les subxarxes virtuals les utilitzen per identificar i ordenar les subxarxes de la subxarxa virtual. Dos punts separen l'etiqueta de la prioritat. Aquests contenidors només es permeten a nivell de contenidor de base de dades o global.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
subnet	subnet *id_subxarxa màscara de xarxa etiqueta*:*prioritat*			Especifica una subxarxa i una agrupació d'adreces. Es pressuposa que totes les adreces són a l'agrupació a no ser que s'especifiqui un abast en la línia o que les adreces es modifiquin posteriorment al contenidor mitjançant un abast o una sentència d'exclusió. L'abast opcional és un parell d'adreces IP en format de quartet amb punt separades per un guió. Es pot especificar una etiqueta opcional i la prioritat. Les subxarxes virtuals les utilitzen per identificar i ordenar les subxarxes de la subxarxa virtual. Dos punts separen l'etiqueta de la prioritat. Aquests contenidors només es permeten a nivell de contenidor de base de dades o global.
subnet	subnet *id_subxarxa màscara de xarxa abast etiqueta*:*prioritat*			Especifica una subxarxa i una agrupació d'adreces. Es pressuposa que totes les adreces són a l'agrupació a no ser que s'especifiqui un abast en la línia o que les adreces es modifiquin posteriorment al contenidor mitjançant un abast o una sentència d'exclusió. L'abast opcional és un parell d'adreces IP en format de quartet amb punt separades per un guió. Es pot especificar una etiqueta opcional i la prioritat. Les subxarxes virtuals les utilitzen per identificar i ordenar les subxarxes de la subxarxa virtual. Dos punts separen l'etiqueta de la prioritat. Aquests contenidors només es permeten a nivell de contenidor de base de dades o global.
subnet	subnet *id_subxarxa abast*	Sí	Cap	Especifica una subxarxa que va en un contenidor de xarxa. Defineix un abast d'adreces que és tota la subxarxa a no ser que s'especifiqui la part d'abast opcional. La màscara de xarxa associada a la subxarxa s'agafa del contenidor de xarxa circumdant. **Nota:** Aquest mètode es desaprova a favor de les altres formes de subxarxa.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
option	option *nombre dades* ...	No	Cap	Especifica una opció per enviar-la a un client o, en cas que s'hagi denegat, una opció que eviti l'enviament al client. La clàusula opcional `* denega` significa que totes les opcions que no s'especifiquin al contenidor actual no es retornaran al client. L'opció *nombre*deny només denega l'opció especificada. *nombre* és un enter de 8 bits sense signe. *dades* és específic de l'opció (consulteu més amunt) o bé es pot especificar com a sèrie entre cometes (que indiqui el text ASCII) o 0x*dígits_hexadecimals* o hex"*dígits_hexadecimals*" o hex "*dígits_hexadecimals*". Si l'opció es troba en un contenidor de proveïdors, s'encapsularà amb altres opcions en una opció 43.
option	option *nombre*deny	No	Cap	Especifica una opció per enviar-la a un client o, en cas que s'hagi denegat, una opció que eviti l'enviament al client. La clàusula opcional `* denega` significa que totes les opcions que no s'especifiquin al contenidor actual no es retornaran al client. L'opció *nombre*deny només denega l'opció especificada. *nombre* és un enter de 8 bits sense signe. *dades* és específic de l'opció (consulteu més amunt) o bé es pot especificar com a sèrie entre cometes (que indiqui el text ASCII) o 0x*dígits_hexadecimals* o hex"*dígits_hexadecimals*" o hex "*dígits_hexadecimals*". Si l'opció es troba en un contenidor de proveïdors, s'encapsularà amb altres opcions en una opció 43.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
option	option * deny	No	Cap	Especifica una opció per enviar-la a un client o, en cas que s'hagi denegat, una opció que eviti l'enviament al client. La clàusula opcional `* denega` significa que totes les opcions que no s'especifiquin al contenidor actual no es retornaran al client. L'opció *nombre*deny només denega l'opció especificada. *nombre* és un enter de 8 bits sense signe. *dades* és específic de l'opció (consulteu més amunt) o bé es pot especificar com a sèrie entre cometes (que indiqui el text ASCII) o 0x*dígits_hexadecimals* o hex"*dígits_hexadecimals*" o hex "*dígits_hexadecimals*". Si l'opció es troba en un contenidor de proveïdors, s'encapsularà amb altres opcions en una opció 43.
exclude	exclude *una adreça IP*	No	Cap	Modifica l'abast al contenidor on hi ha la sentència d'exclusió. Als nivells de contenidor de base de dades o global, la sentència d'exclusió no és vàlida. Aquesta sentència elimina de l'abast actual del contenidor l'adreça o abast especificats. La sentència d'exclusió us permet crear abasts no contigus per a les subxarxes o altres contenidors.
exclude	exclude *quartet_amb punt-quartet_amb punt*	No	Cap	Modifica l'abast al contenidor on hi ha la sentència d'exclusió. Als nivells de contenidor de base de dades o global, la sentència d'exclusió no és vàlida. Aquesta sentència elimina de l'abast actual del contenidor l'adreça o abast especificats. La sentència d'exclusió us permet crear abasts no contigus per a les subxarxes o altres contenidors.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
range	range *adreça_IP*	No	Cap	Modifica l'abast del contenidor on hi ha la sentència d'abast. Als nivells de contenidor de base de dades o global, la sentència d'abast no és vàlida. Si l'abast és el primer del contenidor que no especifica un abast a la línia de definició del contenidor, aleshores l'abast per al contenidor esdevé l'abast especificat per la sentència d'abast. S'afegeix a l'abast actual qualsevol sentència d'abast després del primer abast o totes les sentències d'abast per a un contenidor que especifiqui abasts a la definició. Amb la sentència d'abast, es pot afegir a l'abast una sola adreça o bé un grup d'adreces. L'abast ha d'encaixar dins la definició de contenidor de subxarxes.
range	range *quartet_amb punt-quartet_amb punt*	No	Cap	Modifica l'abast del contenidor on hi ha la sentència d'abast. Als nivells de contenidor de base de dades o global, la sentència d'abast no és vàlida. Si l'abast és el primer del contenidor que no especifica un abast a la línia de definició del contenidor, aleshores l'abast per al contenidor esdevé l'abast especificat per la sentència d'abast. S'afegeix a l'abast actual qualsevol sentència d'abast després del primer abast o totes les sentències d'abast per a un contenidor que especifiqui abasts a la definició. Amb la sentència d'abast, es pot afegir a l'abast una sola adreça o bé un grup d'adreces. L'abast ha d'encaixar dins la definició de contenidor de subxarxes.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
client	client *tipus maquinari adreça maquinari* NONE	Sí	Cap	Especifica un contenidor de clients que denega al client especificat per l'*adreça maquinari* i el *tipus maquinari* l'obtenció d'una adreça. Si el *tipus maquinari* és igual a 0, llavors l'*adreça maquinari* és una sèrie ASCII. Altrament, el *tipus maquinari* és el tipus de maquinari per al client i l'*adreça maquinari* és l'adreça de maquinari del client. Si l'*adreça maquinari* és una sèrie, s'accepten els caràcters de cometes al voltant de la sèrie. Si l'*adreça maquinari* és una sèrie hexadecimal, llavors l'adreça es pot especificar amb 0x*dígits_hexadecimals* o hex *dígits*. L'*abast* fa que el client especificat mitjançant l'*adreça maquinari* i el *tipus maquinari* obtingui una adreça de l'*abast*. Per coincidir amb diversos clients, han de ser expressions regulars.
client	client *tipus maquinari adreça maquinari* ANY	Sí	Cap	Especifica un contenidor de clients que denega al client especificat per l'*adreça maquinari* i el *tipus maquinari* l'obtenció d'una adreça. Si el *tipus maquinari* és igual a 0, llavors l'*adreça maquinari* és una sèrie ASCII. Altrament, el *tipus maquinari* és el tipus de maquinari per al client i l'*adreça maquinari* és l'adreça de maquinari del client. Si l'*adreça maquinari* és una sèrie, s'accepten els caràcters de cometes al voltant de la sèrie. Si l'*adreça maquinari* és una sèrie hexadecimal, llavors l'adreça es pot especificar amb 0x*dígits_hexadecimals* o hex *dígits*. L'*abast* fa que el client especificat mitjançant l'*adreça maquinari* i el *tipus maquinari* obtingui una adreça de l'*abast*. Per coincidir amb diversos clients, han de ser expressions regulars.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
client	client *tipus maquinari adreça maquinari quartet_amb punt*	Sí	Cap	Especifica un contenidor de clients que denega al client especificat per l'*adreça maquinari* i el *tipus maquinari* l'obtenció d'una adreça. Si el *tipus maquinari* és igual a 0, llavors l'*adreça maquinari* és una sèrie ASCII. Altrament, el *tipus maquinari* és el tipus de maquinari per al client i l'*adreça maquinari* és l'adreça de maquinari del client. Si l'*adreça maquinari* és una sèrie, s'accepten els caràcters de cometes al voltant de la sèrie. Si l'*adreça maquinari* és una sèrie hexadecimal, llavors l'adreça es pot especificar amb 0x*dígits_hexadecimals* o hex *dígits*. L'*abast* fa que el client especificat mitjançant l'*adreça maquinari* i el *tipus maquinari* obtingui una adreça de l'*abast*. Per coincidir amb diversos clients, han de ser expressions regulars.
client	client *tipus maquinari adreça maquinari abast*	Sí	Cap	Especifica un contenidor de clients que denega al client especificat per l'*adreça maquinari* i el *tipus maquinari* l'obtenció d'una adreça. Si el *tipus maquinari* és igual a 0, llavors l'*adreça maquinari* és una sèrie ASCII. Altrament, el *tipus maquinari* és el tipus de maquinari per al client i l'*adreça maquinari* és l'adreça de maquinari del client. Si l'*adreça maquinari* és una sèrie, s'accepten els caràcters de cometes al voltant de la sèrie. Si l'*adreça maquinari* és una sèrie hexadecimal, llavors l'adreça es pot especificar amb 0x*dígits_hexadecimals* o hex *dígits*. L'*abast* fa que el client especificat mitjançant l'*adreça maquinari* i el *tipus maquinari* obtingui una adreça de l'*abast*. Per coincidir amb diversos clients, han de ser expressions regulars.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
class	class *sèrie*	Sí	Cap	Especifica un contenidor de classes amb la *sèrie* de nom. La sèrie pot estar entre cometes o no. Si està entre cometes, les cometes s'eliminen abans de la comparació. Les cometes són necessàries en les sèries amb espais o tabuladors. Aquest contenidor és vàlid a qualsevol nivell. Es pot especificar un abast per indicar un conjunt d'adreces que es lliuren a un client amb aquesta classe. L'abast és només una adreça IP de quartet amb punt o bé dues adreces IP de quartet amb punt separades per un guió.
class	class *sèrie abast*	Sí	Cap	Especifica un contenidor de classes amb la *sèrie* de nom. La sèrie pot estar entre cometes o no. Si està entre cometes, les cometes s'eliminen abans de la comparació. Les cometes són necessàries en les sèries amb espais o tabuladors. Aquest contenidor és vàlid a qualsevol nivell. Es pot especificar un abast per indicar un conjunt d'adreces que es lliuren a un client amb aquesta classe. L'abast és només una adreça IP de quartet amb punt o bé dues adreces IP de quartet amb punt separades per un guió.
xarxa	network *id_xarxa màscara de xarxa*	Sí	Cap	Especifica una xarxa ID que utilitza informació de classe (per exemple, 9.3.149.0 amb una màscara de xarxa de 255.255.255.0 seria la xarxa 9.0.0.0 255.255.255.0). Aquesta versió del contenidor de xarxa s'utilitza per retenir subxarxes amb la mateixa xarxa ID i màscara de xarxa. Quan es proporciona un abast, totes les adreces de l'abast es troben a l'agrupació. L'abast ha de ser a la xarxa de l'ID de xarxa, que utilitza l'adreçament complet de classe. Això només és vàlid al nivell de contenidor global o de base de dades. **Nota:** La paraula clau de xarxa es desaprova a favor del contenidor de subxarxes.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
xarxa	network *id_xarxa*	Sí	Cap	Especifica una xarxa ID que utilitza informació de classe (per exemple, 9.3.149.0 amb una màscara de xarxa de 255.255.255.0 seria la xarxa 9.0.0.0 255.255.255.0). Aquesta versió del contenidor de xarxa s'utilitza per retenir subxarxes amb la mateixa xarxa ID i màscara de xarxa. Quan es proporciona un abast, totes les adreces de l'abast es troben a l'agrupació. L'abast ha de ser a la xarxa de l'ID de xarxa, que utilitza l'adreçament complet de classe. Això només és vàlid al nivell de contenidor global o de base de dades. **Nota:** La paraula clau de xarxa es desaprova a favor del contenidor de subxarxes.
xarxa	network *id de xarxa abast*	Sí	Cap	Especifica una xarxa ID que utilitza informació de classe (per exemple, 9.3.149.0 amb una màscara de xarxa de 255.255.255.0 seria la xarxa 9.0.0.0 255.255.255.0). Aquesta versió del contenidor de xarxa s'utilitza per retenir subxarxes amb la mateixa xarxa ID i màscara de xarxa. Quan es proporciona un abast, totes les adreces de l'abast es troben a l'agrupació. L'abast ha de ser a la xarxa de l'ID de xarxa, que utilitza l'adreçament complet de classe. Això només és vàlid al nivell de contenidor global o de base de dades. **Nota:** La paraula clau de xarxa es desaprova a favor del contenidor de subxarxes.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
vendor	vendor *id_proveïdor*	Sí	Cap	Especifica un contenidor de proveïdors. Els contenidors de proveïdors s'utilitzen per tornar l'opció 43 al client. L'id de proveïdor pot especificar-se en una sèrie entre cometes o en una sèrie binària en forma de 0x*dígits_hexadecimals* o hex"*dígits*". Després de l'id de proveïdor hi pot haver un abast opcional. L'abast s'especifica amb dos quartets amb punt separats per un guió. Després de l'abast opcional, es pot especificar una sèrie ASCII o una sèrie hexadecimal opcional com a primera part de l'opció 43. Si les opcions són al contenidor, s'afegeixen a les dades de l'opció 43. Un cop s'hagin processat totes les opcions, s'afegeix a les dades una Opció de llista de Final de llista. Per retornar les opcions fora d'una opció 43, utilitzeu un client d'expressió regular que coincideixi amb tots els clients per especificar opcions normals per retornar basades en l'ID de proveïdor.
vendor	vendor *id_proveïdor* hex""			Especifica un contenidor de proveïdors. Els contenidors de proveïdors s'utilitzen per tornar l'opció 43 al client. L'id de proveïdor pot especificar-se en una sèrie entre cometes o en una sèrie binària en forma de 0x*dígits_hexadecimals* o hex"*dígits*". Després de l'id de proveïdor hi pot haver un abast opcional. L'abast s'especifica amb dos quartets amb punt separats per un guió. Després de l'abast opcional, es pot especificar una sèrie ASCII o una sèrie hexadecimal opcional com a primera part de l'opció 43. Si les opcions són al contenidor, s'afegeixen a les dades de l'opció 43. Un cop s'hagin processat totes les opcions, s'afegeix a les dades una Opció de llista de Final de llista. Per retornar les opcions fora d'una opció 43, utilitzeu un client d'expressió regular que coincideixi amb tots els clients per especificar opcions normals per retornar basades en l'ID de proveïdor.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
vendor	vendor *id_proveïdor* hex ""			Especifica un contenidor de proveïdors. Els contenidors de proveïdors s'utilitzen per tornar l'opció 43 al client. L'id de proveïdor pot especificar-se en una sèrie entre cometes o en una sèrie binària en forma de 0x*dígits_hexadecimals* o hex"*dígits*". Després de l'id de proveïdor hi pot haver un abast opcional. L'abast s'especifica amb dos quartets amb punt separats per un guió. Després de l'abast opcional, es pot especificar una sèrie ASCII o una sèrie hexadecimal opcional com a primera part de l'opció 43. Si les opcions són al contenidor, s'afegeixen a les dades de l'opció 43. Un cop s'hagin processat totes les opcions, s'afegeix a les dades una Opció de llista de Final de llista. Per retornar les opcions fora d'una opció 43, utilitzeu un client d'expressió regular que coincideixi amb tots els clients per especificar opcions normals per retornar basades en l'ID de proveïdor.
vendor	vendor *id_proveïdor* 0xdata			Especifica un contenidor de proveïdors. Els contenidors de proveïdors s'utilitzen per tornar l'opció 43 al client. L'id de proveïdor pot especificar-se en una sèrie entre cometes o en una sèrie binària en forma de 0x*dígits_hexadecimals* o hex"*dígits*". Després de l'id de proveïdor hi pot haver un abast opcional. L'abast s'especifica amb dos quartets amb punt separats per un guió. Després de l'abast opcional, es pot especificar una sèrie ASCII o una sèrie hexadecimal opcional com a primera part de l'opció 43. Si les opcions són al contenidor, s'afegeixen a les dades de l'opció 43. Un cop s'hagin processat totes les opcions, s'afegeix a les dades una Opció de llista de Final de llista. Per retornar les opcions fora d'una opció 43, utilitzeu un client d'expressió regular que coincideixi amb tots els clients per especificar opcions normals per retornar basades en l'ID de proveïdor.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
vendor	vendor *id_proveïdor* ""			Especifica un contenidor de proveïdors. Els contenidors de proveïdors s'utilitzen per tornar l'opció 43 al client. L'id de proveïdor pot especificar-se en una sèrie entre cometes o en una sèrie binària en forma de 0x*dígits_hexadecimals* o hex"*dígits*". Després de l'id de proveïdor hi pot haver un abast opcional. L'abast s'especifica amb dos quartets amb punt separats per un guió. Després de l'abast opcional, es pot especificar una sèrie ASCII o una sèrie hexadecimal opcional com a primera part de l'opció 43. Si les opcions són al contenidor, s'afegeixen a les dades de l'opció 43. Un cop s'hagin processat totes les opcions, s'afegeix a les dades una Opció de llista de Final de llista. Per retornar les opcions fora d'una opció 43, utilitzeu un client d'expressió regular que coincideixi amb tots els clients per especificar opcions normals per retornar basades en l'ID de proveïdor.
vendor	vendor *id_proveïdor abast*			Especifica un contenidor de proveïdors. Els contenidors de proveïdors s'utilitzen per tornar l'opció 43 al client. L'id de proveïdor pot especificar-se en una sèrie entre cometes o en una sèrie binària en forma de 0x*dígits_hexadecimals* o hex"*dígits*". Després de l'id de proveïdor hi pot haver un abast opcional. L'abast s'especifica amb dos quartets amb punt separats per un guió. Després de l'abast opcional, es pot especificar una sèrie ASCII o una sèrie hexadecimal opcional com a primera part de l'opció 43. Si les opcions són al contenidor, s'afegeixen a les dades de l'opció 43. Un cop s'hagin processat totes les opcions, s'afegeix a les dades una Opció de llista de Final de llista. Per retornar les opcions fora d'una opció 43, utilitzeu un client d'expressió regular que coincideixi amb tots els clients per especificar opcions normals per retornar basades en l'ID de proveïdor.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
vendor	vendor *id_proveïdor abast* hex""			Especifica un contenidor de proveïdors. Els contenidors de proveïdors s'utilitzen per tornar l'opció 43 al client. L'id de proveïdor pot especificar-se en una sèrie entre cometes o en una sèrie binària en forma de 0x*dígits_hexadecimals* o hex"*dígits*". Després de l'id de proveïdor hi pot haver un abast opcional. L'abast s'especifica amb dos quartets amb punt separats per un guió. Després de l'abast opcional, es pot especificar una sèrie ASCII o una sèrie hexadecimal opcional com a primera part de l'opció 43. Si les opcions són al contenidor, s'afegeixen a les dades de l'opció 43. Un cop s'hagin processat totes les opcions, s'afegeix a les dades una Opció de llista de Final de llista. Per retornar les opcions fora d'una opció 43, utilitzeu un client d'expressió regular que coincideixi amb tots els clients per especificar opcions normals per retornar basades en l'ID de proveïdor.
vendor	vendor *id_proveïdor abast* hex ""			Especifica un contenidor de proveïdors. Els contenidors de proveïdors s'utilitzen per tornar l'opció 43 al client. L'id de proveïdor pot especificar-se en una sèrie entre cometes o en una sèrie binària en forma de 0x*dígits_hexadecimals* o hex"*dígits*". Després de l'id de proveïdor hi pot haver un abast opcional. L'abast s'especifica amb dos quartets amb punt separats per un guió. Després de l'abast opcional, es pot especificar una sèrie ASCII o una sèrie hexadecimal opcional com a primera part de l'opció 43. Si les opcions són al contenidor, s'afegeixen a les dades de l'opció 43. Un cop s'hagin processat totes les opcions, s'afegeix a les dades una Opció de llista de Final de llista. Per retornar les opcions fora d'una opció 43, utilitzeu un client d'expressió regular que coincideixi amb tots els clients per especificar opcions normals per retornar basades en l'ID de proveïdor.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
vendor	vendor *id_proveïdor abast* 0xdata			Especifica un contenidor de proveïdors. Els contenidors de proveïdors s'utilitzen per tornar l'opció 43 al client. L'id de proveïdor pot especificar-se en una sèrie entre cometes o en una sèrie binària en forma de 0x*dígits_hexadecimals* o hex"*dígits*". Després de l'id de proveïdor hi pot haver un abast opcional. L'abast s'especifica amb dos quartets amb punt separats per un guió. Després de l'abast opcional, es pot especificar una sèrie ASCII o una sèrie hexadecimal opcional com a primera part de l'opció 43. Si les opcions són al contenidor, s'afegeixen a les dades de l'opció 43. Un cop s'hagin processat totes les opcions, s'afegeix a les dades una Opció de llista de Final de llista. Per retornar les opcions fora d'una opció 43, utilitzeu un client d'expressió regular que coincideixi amb tots els clients per especificar opcions normals per retornar basades en l'ID de proveïdor.
vendor	vendor *id_proveïdor abast* ""			Especifica un contenidor de proveïdors. Els contenidors de proveïdors s'utilitzen per tornar l'opció 43 al client. L'id de proveïdor pot especificar-se en una sèrie entre cometes o en una sèrie binària en forma de 0x*dígits_hexadecimals* o hex"*dígits*". Després de l'id de proveïdor hi pot haver un abast opcional. L'abast s'especifica amb dos quartets amb punt separats per un guió. Després de l'abast opcional, es pot especificar una sèrie ASCII o una sèrie hexadecimal opcional com a primera part de l'opció 43. Si les opcions són al contenidor, s'afegeixen a les dades de l'opció 43. Un cop s'hagin processat totes les opcions, s'afegeix a les dades una Opció de llista de Final de llista. Per retornar les opcions fora d'una opció 43, utilitzeu un client d'expressió regular que coincideixi amb tots els clients per especificar opcions normals per retornar basades en l'ID de proveïdor.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
inoption	inoption *nombre dades_opció*	Sí	Cap	Especifica un contenidor que cal fer coincidir amb qualsevol opció d'entrada arbitrària especificada pel client. El *nombre* especifica el nombre d'opció. *dades_opció* especifica la clau que cal fer coincidir per tal que se seleccioni aquest contenidor durant la selecció d'opció i d'adreça per al client. *dades_opció* s'especifica de forma esperada — amb una sèrie entre cometes, una adreça IP, un valor enter — en les opcions conegudes o bé es pot especificar opcionalment mitjançant una sèrie hexadecimal d'octets si la precedeixen els caràcters `0x`. Pel que fa a les opcions que el servidor no coneix, es pot especificar una sèrie hexadecimal d'octets de la mateixa manera. Addicionalment, *dades_opció* pot indicar una expressió regular que cal comparar amb la representació de sèrie de les dades d'opció del client. Les expressions regulars s'especifiquen en una sèrie entre cometes que comença amb `"!` (caràcter de cometes dobles seguit d'un signe d'exclamació). La forma en sèrie d'opcions menys conegudes pel servidor és una sèrie hexadecimal d'octets SENSE els caràcters `0x` al davant.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
inoption	inoption *nombre dades_opció abast*	Sí	Cap	Especifica un contenidor que cal fer coincidir amb qualsevol opció d'entrada arbitrària especificada pel client. El *nombre* especifica el nombre d'opció. *dades_opció* especifica la clau que cal fer coincidir per tal que se seleccioni aquest contenidor durant la selecció d'opció i d'adreça per al client. *dades_opció* s'especifica de forma esperada — amb una sèrie entre cometes, una adreça IP, un valor enter — en les opcions conegudes o bé es pot especificar opcionalment mitjançant una sèrie hexadecimal d'octets si la precedeixen els caràcters `0x`. Pel que fa a les opcions que el servidor no coneix, es pot especificar una sèrie hexadecimal d'octets de la mateixa manera. Addicionalment, *dades_opció* pot indicar una expressió regular que cal comparar amb la representació de sèrie de les dades d'opció del client. Les expressions regulars s'especifiquen en una sèrie entre cometes que comença amb `"!` (caràcter de cometes dobles seguit d'un signe d'exclamació). La forma en sèrie d'opcions menys conegudes pel servidor és una sèrie hexadecimal d'octets SENSE els caràcters `0x` al davant.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
virtual	virtual fill *id id* ...	No	Cap	Especifica una subxarxa virtual amb una política. `fill` significa utilitzar totes les adreces del contenidor abans d'anar al contenidor següent. `rotate` significa seleccionar una adreça de l'agrupació següent de la llista a cada sol•licitud. `sfill` i `srotate` són el mateix que `fill` i `rotate`, però es realitza una cerca per veure si el client coincideix amb els contenidors, els proveïdors o les classes de la subxarxa. Si es troba una coincidència que pot subministrar una adreça, s'agafa l'adreça d'aquest contenidor en lloc de seguir les normes. Hi pot haver tots els IDs que calgui. L'*id* és l'ID de subxarxa de la definició de subxarxa o l'etiqueta de la definició de subxarxa. L'etiqueta és necessària si hi ha diverses subxarxes amb el mateix id de subxarxa.
virtual	virtual sfill *id id* ...	No	Cap	Especifica una subxarxa virtual amb una política. `fill` significa utilitzar totes les adreces del contenidor abans d'anar al contenidor següent. `rotate` significa seleccionar una adreça de l'agrupació següent de la llista a cada sol•licitud. `sfill` i `srotate` són el mateix que `fill` i `rotate`, però es realitza una cerca per veure si el client coincideix amb els contenidors, els proveïdors o les classes de la subxarxa. Si es troba una coincidència que pot subministrar una adreça, s'agafa l'adreça d'aquest contenidor en lloc de seguir les normes. Hi pot haver tots els IDs que calgui. L'*id* és l'ID de subxarxa de la definició de subxarxa o l'etiqueta de la definició de subxarxa. L'etiqueta és necessària si hi ha diverses subxarxes amb el mateix id de subxarxa.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
virtual	virtual rotate *id id* ...	No	Cap	Especifica una subxarxa virtual amb una política. `fill` significa utilitzar totes les adreces del contenidor abans d'anar al contenidor següent. `rotate` significa seleccionar una adreça de l'agrupació següent de la llista a cada sol•licitud. `sfill` i `srotate` són el mateix que `fill` i `rotate`, però es realitza una cerca per veure si el client coincideix amb els contenidors, els proveïdors o les classes de la subxarxa. Si es troba una coincidència que pot subministrar una adreça, s'agafa l'adreça d'aquest contenidor en lloc de seguir les normes. Hi pot haver tots els IDs que calgui. L'*id* és l'ID de subxarxa de la definició de subxarxa o l'etiqueta de la definició de subxarxa. L'etiqueta és necessària si hi ha diverses subxarxes amb el mateix id de subxarxa.
virtual	virtual srotate *id id* ...	No	Cap	Especifica una subxarxa virtual amb una política. `fill` significa utilitzar totes les adreces del contenidor abans d'anar al contenidor següent. `rotate` significa seleccionar una adreça de l'agrupació següent de la llista a cada sol•licitud. `sfill` i `srotate` són el mateix que `fill` i `rotate`, però es realitza una cerca per veure si el client coincideix amb els contenidors, els proveïdors o les classes de la subxarxa. Si es troba una coincidència que pot subministrar una adreça, s'agafa l'adreça d'aquest contenidor en lloc de seguir les normes. Hi pot haver tots els IDs que calgui. L'*id* és l'ID de subxarxa de la definició de subxarxa o l'etiqueta de la definició de subxarxa. L'etiqueta és necessària si hi ha diverses subxarxes amb el mateix id de subxarxa.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
inorder:	inorder: *id id ...*	No	Cap	Especifica una subxarxa virtual amb unes normes d'emplenament. Això vol dir que s'han d'utilitzar totes les adreces del contenidor abans d'anar al següent. Hi pot haver tots els IDs que calgui. L'*id* és l'ID de subxarxa de la definició de subxarxa o l'etiqueta de la definició de subxarxa. L'etiqueta és necessària si hi ha diverses subxarxes amb el mateix ID de subxarxa.
balance:	balance: *id id ...*	No	Cap	Especifica una subxarxa virtual amb unes normes de rotació. Això vol dir que s'ha d'utilitzar l'adreça següent al contenidor següent. Hi pot haver tots els IDs que calgui. L'*id* és l'ID de subxarxa de la definició de subxarxa o l'etiqueta de la definició de subxarxa. L'etiqueta és necessària si hi ha diverses subxarxes amb el mateix ID de subxarxa.
bootstrapserver	bootstrapserver *adreça IP*	No	Cap	Especifica el servidor que els clients haurien d'utilitzar als fitxers **TFTP** després de rebre els paquets **BOOTP** o **DHCP**. Aquest valor emplena el camp **siaddr** del paquet. Això és vàlid a qualsevol nivell de contenidor.
giaddrfield	giaddrfield *adreça IP*	No	Cap	Especifica el camp giaddr per als paquets de resposta. **Nota:** Aquesta especificació no es permet als protocols **BOOTP** i **DHCP**, però alguns clients demanen que el camp **giaddr** sigui la passarel•la per defecte de la xarxa. A causa d'aquest conflicte potencial, el **giaddrfield** només s'hauria d'utilitzar dins d'un contenidor de clients, tot i que pot funcionar a qualsevol nivell.
bootfile	bootfile *camí d'accés*	No	Cap	Especifica el fitxer d'engegada que cal utilitzar a la secció de fitxer del paquet de resposta. Això es pot especificar a qualsevol nivell de contenidor. La política de fitxer d'engegada defineix la manera en què els elements especificats a la secció de fitxer del paquet d'entrada interactuen amb les sentències del directori d'inici i el fitxer d'engegada.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
pxebootfile	pxebootfile *System Arch MajorVer MinorVer Bootfilename*	No	Cap	Especifica el fitxer d'engegada que cal donar a un client. L'analitzador del fitxer de configuració genera un error si el nombre de paràmetres després de la paraula clau és menor que 4 i en prescindeix si és major que 4. Aquesta paraula clau només es pot utilitzar en un contenidor.

Si voleu detalls sobre altres opcions, consulteu l'apartat "Opcions conegudes de fitxer del servidor DHCP" a la pàgina 221 i "Subopció de contenidor de proveïdors PXE" a la pàgina 223.

Boot Image Negotiation Layer daemon

El servidor BINLD (Boot Image Negotiation Layer daemon) és la tercera fase de contacte per als clients PXE (preboot execution environment).

Després de comunicar-se amb el servidor DHCP per obtenir una adreça IP i amb el Proxy PXE del servidor DHCP per obtenir la ubicació del servidor d'engegada, es contacta el servidor d'engegada per aconseguir el nom de fitxer i la ubicació des de la qual descarregar la imatge d'engegada. El client PXE pot retornar per comunicar-se amb el servidor d'engegada diverses vegades durant l'engegada si el client requereix diversos fitxers en el procés d'engegada.

La fase final de l'engegada de xarxa PXE consisteix a descarregar la imatge d'engegada que ha proporcionat el servidor d'engegada. El servidor d'engegada proporciona al client PXE la ubicació del servidor TFTP i del nom de fitxer que cal descarregar.

Components del servidor BINLD

Aquí es presenten els tres components principals del servidor BINLD.

El servidor BINLD es troba segmentat en tres parts principals: una base de dades, un motor de protocol i un conjunt de fils de servei, i cada part té la seva pròpia informació de configuració.

Base de dades BINLD:

La base de dades `db_file.dhcpo` s'utilitza per generar les opcions que responen a un paquet de PETICIÓ del client.

Les opcions que la base de dades retorna depenen del tipus de servidor que s'ha seleccionat. Les opcions s'estableixen mitjançant la paraula clau **pxeservertype** al fitxer `binld.cnf`.

La base de dades s'actualitza i verifica per coherència mitjançant la informació del fitxer de configuració.

Motor de protocol BINLD:

El motor de protocol utilitza la base de dades per determinar la informació que caldria retornar al client.

El motor de protocol PXED es basa en l'Intel Preboot Execution Environment (PXE) Specification Version 2.1, però encara és compatible amb el PXE Intel PXE Specification Version 1.1.

Operacions de diversos fils del BINLD:

La darrera part del servidor BINLD és un conjunt d'operacions que s'utilitzen per mantenir el funcionament.

Atès que el BINLD és un servidor amb fils, aquestes operacions realment estan configurades com a fils que de tant en tant realitzen certes tasques per assegurar-se que tot està enllaçat correctament.

El primer fil, el *principal*, gestiona les sol•licituds SRC (com ara les **startsrc**, **stopsrc**, **lssrc**, **traceson** i **refresh**). Aquest fil coordina també totes les operacions que afecten tots els fils i gestiona els senyals. Per exemple,

- Un SIGHUP (-1) provoca una renovació de totes les bases de dades del fitxer de configuració.
- Un SIGTERM (-15) fa que el servidor s'aturi correctament.

L'altre fil processa els paquets. Segons el tipus de servidor, hi pot haver un o dos fils. Un fil està pendent del port 67 i el segon, del port 4011. Cadascun d'ells pot gestionar la sol•licitud d'un client.

Configuració del BINLD

Per defecte, el servidor BINLD es configura mitjançant la lectura del fitxer `/etc/binld.cnf`, el qual especifica la base de dades inicial d'adreces i opcions del servidor.

El servidor s'inicia des la SMIT o mitjançant ordres SRC.

La configuració del servidor BINLD és normalment la part més complexa pel que fa a l'ús del BINLD a la xarxa. Primerament, decidiu quines xarxes cal que tinguin clients PXE. A l'exemple següent es configura un servidor BINLD per tal que s'executi a la mateixa màquina que el servidor DHCP:

```
pxeservertype       binld_on_dhcp_server

subnet default
{
    vendor pxe
    {
                bootstrapserver  9.3.149.6      #TFTP server IP address
                pxebootfile   1   2   1   window.one   1   0
                pxebootfile   2   2   1   linux.one    2   3
                pxebootfile   1   2   1   hello.one    3   4
                client 6 10005a8ad14d any
                {
                   pxebootfile   1   2   1   aix.one     5   6
                   pxebootfile   2   2   1   window.one  6   7
        }
     }
}
```

Amb aquesta configuració, el servidor BINLD està pendent dels paquets de difusió individual dels clients al port 4011 i dels Paquets de difusió múltiple al port 4011 si el BINLD obté l'Adreça de multidifusió del dhcpsd/pxed. El servidor BINLD respon als paquets de PETICIÓ/INFORMACIÓ dels clients amb el nom del fitxer d'engegada i l'adreça IP del servidor TFTP. Si el BINLD no troba el fitxer d'engegada amb una Capa coincident especificada pel client, intenta trobar un fitxer d'engegada per a la capa següent. El BINLD no respon si no hi ha cap fitxer d'engegada que coincideixi amb els requisits del client (*Tipus*, *SystemArch*, *Versió_major*, *Versió_menor*, i *Capa*).

A l'exemple següent es configura el BINLD per tal que s'executi en una altra màquina (és a dir, el DHCP / PXED no s'executa a la mateixa màquina).

```
subnet 9.3.149.0 255.255.255.0
{

     vendor pxe
     {

     bootstrapserver        9.3.149.6      # TFTP server ip address.
     pxebootfile    1    2    1   window.one    1   0
     pxebootfile    2    2    1   linux.one     2   3
     pxebootfile    1    2    1   hello.one     3   4
     client 6 10005a8ad14d any
```

```
        {
        pxebootfile    1    2    1   aix.one      5   6
        pxebootfile    2    2    1   window.one   6   7
        }
      }
}
```

En aquest exemple, no s'ha configurat el *tipus_servidor_pxe*, de manera que el tipus de servidor per defecte és **binld_only**. El servidor BINLD està pendent dels paquets de difusió individual dels clients al port 4011, dels paquets de difusió individual broadcast & al port 67 i dels paquets de difusió múltiple al port 4011 si el BINLD obté l'Adreça de multidifusió del dhcpsd/pxed. El nom del fitxer d'engegada i l'adreça IP del servidor TFTP només s'envien a un client PXE si l'adreça IP del client es troba a l'abast d'adreces IP de la subxarxa (de 9.3.149.0 a 9.3.149.255).

A l'exemple següent es configura el BINLD per tal que s'executi a la mateixa màquina que el servidor PXED:

```
pxeservertype       binld_on_proxy_server
subnet default
{
     vendor
     {
     bootstrapserver        9.3.149.6          # TFTP server ip address.
     pxebootfile    1    2    1   window.one    1    0
     pxebootfile    2    2    1   linux.one     2    3
     pxebootfile    1    2    1   hello.one     3    4
     client 6 10005a8ad14d any
       {
       pxebootfile    1    2    1   aix.one     5   6
       pxebootfile    2    2    1   window.one  6   7
       }
     }
}
```

En aquesta configuració, el servidor BINLD només està pendent dels paquets de difusió múltiple al port 4011 si el BINLD obté l'Adreça de multidifusió del dhcpsd/pxed. Si no rep cap adreça de multidifusió, el BINLD surt i s'enregistra un missatge d'error al fitxer de registre.

La clàusula de base de dades `db_file` indica el mètode de base de dades que cal utilitzar per processar aquesta part del fitxer de configuració. Els comentaris comencen amb el signe #. El servidor PXED els obvia del # al final de la línia. El servidor utilitza cada línia d'`opció` per indicar al client el que ha de fer."Subopcions del contenidor de proveïdors del PXE" a la pàgina 303 descriu les subopcions conegudes i suportades actualment. Consulteu l'apartat "Sintaxi de fitxer del servidor BINLD per al funcionament general del servidor" a la pàgina 332 sobre els mètodes per especificar opcions que el servidor no coneix.

Fitxer de configuració BINLD:

El fitxer de configuració té una secció d'adreça i una secció de definició d'opcions que es basen en el concepte de contenidors que retenen opcions, modificadors i, potencialment, altres contenidors.

Un *contenidor* (que és, bàsicament, un mètode per agrupar opcions) utilitza un identificador per classificar els clients en grups. Els tipus de contenidor són els de subxarxes, classes, proveïdors i clients. Actualment, no hi ha un contenidor genèric que l'usuari pugui definir. L'identificador només defineix el client perquè se'l pugui seguir si, per exemple, es desplaça entre subxarxes. Es pot utilitzar més d'un tipus de contenidor per definir l'accés del client.

Les *Opcions* són identificadors que es tornen al client, com ara la passarel•la per defecte i l'adreça DNS.

Contenidors BINLD:

Quan el servidor DHCP rep una sol•licitud, s'analitza el paquet i les claus d'identificació determinen els contenidors, les opcions i les adreces que cal extreure.

El darrer exemple de la configuració BINLD mostra un contenidor de subxarxes. La clau d'identificació és la posició del client a la xarxa. Si el client és d'aquesta xarxa, cau en aquest contenidor.

Cada tipus de contenidor utilitza una opció diferent per identificar un client:

- El contenidor de subxarxes utilitza el camp giaddr o l'adreça d'interfície de la interfície receptora per determinar la subxarxa de la qual procedeix el client.
- El contenidor de classes utilitza el valor de l'opció 77 (Identificador de classes d'indret d'usuari).
- El proveïdor utilitza el valor de l'opció 60 (Identificador de classes de proveïdor).
- El contenidor de clients utilitza l'opció 61 (Identificador de clients) per als clients PXED i el camp chaddr del paquet BOOTP per als clients BOOTP.

A excepció de les subxarxes, cada contenidor permet l'especificació del valor amb el qual coincideix, incloses les coincidències d'expressió regular.

També hi ha un contenidor implícit, el contenidor *global*. Les opcions i els modificadors situats al contenidor global s'apliquen a tots els contenidors, a no ser que estiguin alterats temporalment o denegats. La major part dels contenidors es poden col•locar a dins d'altres contenidors que impliquen un àmbit de visibilitat. Tant pot ser que els contenidors tinguin abasts d'adreces associats com no. Les subxarxes tenen, per naturalesa, abasts associats.

Les normes bàsiques dels contenidors i subcontenidors són les següents:

- Tots els contenidors són vàlids a nivell global.
- Les subxarxes no es poden col•locar mai dins d'altres contenidors.
- Els contenidors restringits no poden tenir contenidors regulars del mateix tipus. (Per exemple, un contenidor amb una opció que només permet una classe de `Comptabilitat` no pot incloure un contenidor amb una opció que permeti totes les classes que comencen amb la lletra "a". Això no és permès.)
- Els contenidors de clients restringits no poden tenir subcontenidors.

Segons aquestes normes, podeu generar una jerarquia de contenidors que segmenti les opcions en grups per a clients específics o grups de clients.

Si un client coincideix amb diversos contenidors, com es distribueixen les opcions i les adreces? El servidor DHCP rep els missatges, passa la sol•licitud a la base de dades (`db_file` en aquest cas) i es genera una llista de contenidors. La llista es presenta per ordre de profunditat i de prioritat. La prioritat es defineix com una jerarquia implícita als contenidors. Els contenidors estrictes tenen una prioritat major que els contenidors regulars. Els clients, les classes, els proveïdors i finalment les subxarxes es classifiquen per aquest ordre i dins el tipus de contenidor segons la profunditat. Això genera una llista ordenada de més específic a menys específic. Per exemple:

```
Subxarxa 1
--Classe 1
--Client 1
Subxarxa 2
--Classe 1
----Proveïdor 1
----Client 1
--Client 1
```

L'exemple mostra dues subxarxes, la `Subxarxa 1` i la `Subxarxa 2`. Hi ha un nom de classe, `Classe 1`, un nom de proveïdor, `Proveïdor 1` i un nom de client `Client 1`. La `Classe 1` i el `Client 1` estan definits en

diversos llocs. Com que es troben en contenidors diferents, pot ser que tinguin el mateix nom, però que els valors al seu interior siguin diferents. Si el `Client 1` envia un missatge al servidor DHCP des de la `Subxarxa 1` amb la `Classe 1` especificada a la llista d'opcions, el servidor DHCP generarà el següent camí d'accés del contenidor:

`Subxarxa 1, Classe 1, Client 1`

El contenidor més específic és l'últim de la llista. Per obtenir una adreça, s'examina la llista en jerarquia invertida per trobar la primera adreça disponible. Seguidament, la llista s'examina en jerarquia cap endavant per obtenir les opcions. Les opcions alteren temporalment els valors precedents a no ser que hi hagi una opció *deny* al contenidor. Així mateix, com que la `Classe 1` i el `Client 1` són a la `Subxarxa 1`, s'ordenen segons la prioritat de contenidor. Si el mateix client és a la `Subxarxa 2` i envia el mateix missatge, la llista de contenidor que es genera és:

`Subxarxa 2, Classe 1, Client 1` (al nivell de la `Subxarxa 2`), `Client 1` (al nivell de la `Classe 1`)

Primer es fa una llista de la `Subxarxa 2`, després de la `Classe 1`, seguidament del `Client 1` al nivell de la `Subxarxa 2` (perquè aquesta sentència de client només es troba un nivell sota la jerarquia). La jerarquia implica que un client que coincideix amb la primera sentència de client és menys específic que el client que coincideix amb el `Client 1` de la `Classe 1` a la `Subxarxa 2`.

La prioritat dels contenidors no substitueix la prioritat seleccionada per profunditat dins la jerarquia. Per exemple, si el mateix client executa el mateix missatge i especifica un identificador de proveïdor, la llista de contenidor és:

`Subxarxa 2, Classe 1, Proveïdor 1, Client 1` (al nivell de la `Subxarxa 2`), `Client 1` (al nivell de la `Classe 1`)

La prioritat de contenidor millora el rendiment de cerca ja que segueix el concepte general segons el qual els contenidors de clients són la manera més específica de definir un o més clients. El contenidor de classes reté menys adreces específiques que un contenidor de clients; el de proveïdors és encara menys específic i el de subxarxes, el menys específic de tots.

Adreces i abasts d'adreces BINLD:

Qualsevol tipus de contenidor pot tenir associats abasts d'adreces; les subxarxes han de tenir un abast d'adreces associat.

Cada abast d'un contenidor ha de ser un subconjunt de l'abast del contenidor superior i no s'ha de superposar amb els altres abasts. Per exemple, si una classe es troba definida en una subxarxa i té un abast, aquest abast ha de ser un subconjunt de l'abast de la subxarxa. De la mateixa manera, l'abast d'aquest contenidor de classes no es pot superposar amb cap altre abast del seu nivell.

Els abasts poden expressar-se a la línia del contenidor i modificar-se per abast, així com excloure sentències per permetre conjunts d'adreces desunits associats a un contenidor. Per tant, si teniu disponibles les deu adreces principals i les segones deu adreces d'una subxarxa, la subxarxa pot especificar aquestes adreces per abast a la clàusula de la subxarxa per reduir tant l'ús de la memòria com el risc de col•lisió d'adreces amb altres clients fora dels abasts especificats.

Un cop s'ha seleccionat una adreça, qualsevol contenidor subseqüent de la llista que contingui abasts d'adreces s'elimina de la llista juntament amb els seus subordinats. El motiu és que les opcions específiques de xarxa en els contenidors eliminats no són vàlides si no s'utilitza una adreça des d'aquell contenidor.

Opcions del fitxer de configuració BINLD:

Després d'haver netejat la llista per determinar les adreces, es genera un conjunt d'opcions per al client.

En aquest procés de selecció, les opcions sobreescriuen les opcions seleccionades prèviament a no ser aparegui un *deny*; en aquest cas, l'opció denegada s'elimina de la llista que s'està enviant al client. Aquest mètode permet l'herència dels contenidors superiors per reduir la quantitat de dades que cal especificar.

Inici de sessió BINLD:

Els paràmetres d'inici de sessió s'especifiquen en un contenidor com la base de dades, però la paraula clau del contenidor és **logging_info**.

Quan s'aprèn a configurar el PXED, és aconsellable posar l'inici de sessió al nivell superior. Així mateix, és millor especificar la configuració d'inici de sessió abans que qualsevol altra dada del fitxer de configuració per assegurar-se que els errors de configuració s'enregistrin després que s'hagi inicialitzat el subsistema d'inici de sessió. Utilitzeu la paraula clau **logitem** per abilitar un nivell d'inici de sessió o elimineu la paraula clau **logitem** per inhabilitar un nivell d'inici de sessió. Altres paraules clau per a l'inici de sessió permeten especificar el nom de fitxer de registre, la grandària del fitxer i el nombre de fitxers de registre rotatius.

Consideracions de rendiment del BINLD:

És important entendre que determinades paraules clau de configuració i l'estructura del fitxer de configuració tenen un efecte en l'ús de la memòria i el rendiment del servidor PXED.

Primerament, es pot evitar l'ús excessiu de la memòria si entenem el model d'herència d'opcions dels contenidors superiors als subordinats. En un entorn que no dóna suport als clients que no figuren a la llista, l'administrador ha de mostrar explícitament a la llista cada client del fitxer. Quan es realitza una llista d'opcions per a qualsevol client específic, el servidor utilitza més memòria per emmagatzemar aquest arbre de configuració que quan les opcions s'hereten d'un contenidor superior (per exemple, la subxarxa, la xarxa o els contenidors globals). Per tant, l'administrador hauria de comprovar si hi ha opcions repetides al nivell de client en el fitxer de configuració i, si es així, determinar si aquestes opcions es poden especificar al contenidor superior i compartir per tot el grup de clients.

Així mateix, quan s'utilitzen les entrades **logItem** INFO i TRACE, s'enregistren nombrosos missatges durant el processament de cada missatge d'un client PXE. Afegir una línia al fitxer de registre pot ser una operació costosa; per tant, limitar la quantitat d'inicis de sessió millora el rendiment del servidor PXED. Quan se sospita la possibilitat d'un error amb el servidor PXED, es pot tornar a habilitar dinàmicament l'inici de sessió mitjançant l'ordre SRC traceson.

Sintaxi de fitxer del servidor BINLD per al funcionament general del servidor

A continuació es descriu la sintaxi de fitxer del servidor BINLD per al funcionament general del servidor. S'identifiquen les formes, subcontenidors, els valors per defecte i els significats.

Nota: Les Unitats de temps (*unitats_temps*) que es mostren a la taula següent són opcionals i representen un modificador de l'hora actual. La unitat de temps per defecte és els minuts. Són valors vàlids els segons (1), els minuts (60), les hores (3600), els dies (86400), les setmanes (604800), els mesos (2392000) i els anys (31536000). El nombre que apareix entre parèntesis és un multiplicador aplicat al valor específic *n* per expressar el valor en segons.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
base de dades	base de dades*tipus base de dades*	Sí	Cap	El contenidor primari que reté les definicions de les agrupacions d'adreces, les opcions i les sentències d'accés de client. El *tipus base de dades* és el nom d'un mòdul que es carrega per processar aquesta part del fitxer. L'únic valor disponible actualment és el **db_file**.
logging_info	logging_info	Sí	Cap	El contenidor d'inici de sessió primari que defineix els paràmetres d'inici de sessió.
logitem	logitem NONE	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies.
logitem	logitem SYSERR	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies.
logitem	logitem OBJERR	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies.
logitem	logitem PROTOCOL	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies.
logitem	logitem PROTERR	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies.
logitem	logitem WARN	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies.
logitem	logitem WARNING	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies.
logitem	logitem CONFIG	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies.
logitem	logitem EVENT	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies.
logitem	logitem PARSEERR	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies.
logitem	logitem ACTION	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies.
logitem	logitem ACNTING	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies.
logitem	logitem STAT	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies.
logitem	logitem TRACE	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies.
logitem	logitem RTRACE	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies.
logitem	logitem START	No	Tots prenen per defecte no habilitat.	Habilita el nivell d'inici de sessió. Es permeten diverses línies.
numLogFiles	numLogFiles *n*	No	0	Especifica el nombre de fitxers de registre que cal crear. L'enregistrament gira quan s'emplena el primer. *n* és el nombre de fitxers que cal crear.
logFileSize	logFileSize *n*	No	0	Especifica la grandària de cada fitxer de registre en unitats de 1024 octets.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
logFileName	logFileName *camí d'accés*	No	Cap	Especifica el camí d'accés al primer fitxer de registre. El fitxer de registre original s'anomena *nom_fitxer* o *nom_fitxer.extensió*. Quan es gira un fitxer, es canvia de nom començant amb la base *nom_fitxer* i, a continuació, afegint un nombre o substituint l'extensió per un nombre. Per exemple, si el nom de fitxer original és `fitxer`, el nom de fitxer girat esdevé `fitxer01`. Si el nom de fitxer original és `fitxer.log`, esdevé `fitxer.01`.
pxeservertype	pxeservertype *tipus_servidor*	No	només_dhcp	Indica el tipus de servidor dhcpsd de què es tracta. El *tipus_servidor* pot ser un dels següents **binld_on_dhcp_server** Això vol dir que el **BINLD** s'està executant a la mateixa màquina que el servidor DHCP i està pendent de la sol•licitud del Client PXE del port 4011 i l'Adreça de multidifusió si es rep del DHCP / PXED. **binld_on_proxy_server** Això vol dir que el **BINLD** s'està executant a la mateixa màquina que el servidor PXED i està pendent de la sol•licitud del Client PXE en una Adreça de multidifusió si es rep del DHCP / PXED. El valor per defecte és **binld_only**, la qual cosa vol dir que el BINLD s'està executant en una altra màquina i ha d'estar pendent dels paquets de client del port 67 , 4011 i Adreça de multidifusió si es reben del DHCP / PXED.
dhcp_or_proxy _address	dhcp_or_proxy_address *adreça IP*	No	Cap	Proporciona l'adreça IP del servidor dhcp o pxed on el servidor BINLD pot enviar un paquet de difusió individual de tipus PETICIÓ/INFORMACIÓ per rebre l'Adreça de multidifusió. Aquesta paraula clau només es defineix quan el dhcp o el pxed estan en una subxarxa diferent del BINLD.

Sintaxi de fitxer del servidor BINLD per a la base de dades db_file

A continuació es descriu la sintaxi de fitxer del servidor BINLD per a la base de dades`db_file`. S'identifiquen les formes, els subcontenidors, els valors per defecte i els significats.

Nota:

1. Les Unitats de temps (*unitats_temps*) que es mostren a la taula següent són opcionals i representen un modificador de l'hora actual. La unitat de temps per defecte és els minuts. Són valors vàlids els segons (1), els minuts (60), les hores (3600), els dies (86400), les setmanes (604800), els mesos (2392000) i els anys (31536000). El nombre que apareix entre parèntesis és un multiplicador aplicat al valor específic *n* per expressar el valor en segons.

2. Pot ser que els elements que s'especifiquen en un contenidor s'alterin temporalment dins un subcontenidor. Per exemple, podríeu definir globalment els clients BOOTP, però permetre els clients BOOTP en una subxarxa determinada tot especificant la paraula clau supportBootp en ambdós contenidors.
3. Els contenidors de clients, classes i proveïdors permeten un suport d'expressió regular. Per als de classes i proveïdors, una sèrie entre cometes. El primer caràcter després de les cometes és un signe d'admiració(!) que indica que la resta de la sèrie s'ha de tractar com una expressió regular. El contenidor de clients permet les expressions regulars tant al camp hwtype com al hwaddr. S'utilitza una sèrie simple per representar ambdós camps amb el format següent:

   ```
   decimal_number-data
   ```

   Si el nombre_decimal és el zero, aleshores la dada és una sèrie ASCII. Si és qualsevol altre nombre, la dada és en dígits hex.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
subnet	subnet default	Sí	Cap	Especifica una subxarxa que no té cap abast. Un servidor utilitza la subxarxa només quan respon a un paquet d'INFORMACIÓ del client i l'adreça del client no té cap altre contenidor de subxarxes coincident.
subnet	subnet*id de subxarxa màscara de xarxa*	Sí	Cap	Especifica una subxarxa i una agrupació d'adreces. Es pressuposa que totes les adreces són a l'agrupació a no ser que s'especifiqui un abast en la línia o que les adreces es modifiquin posteriorment al contenidor mitjançant un abast o una sentència d'exclusió. L'abast opcional és un parell d'adreces IP en format de quartet amb punt separades per un guió. Es pot especificar una etiqueta opcional i la prioritat. Les subxarxes virtuals les utilitzen per identificar i ordenar les subxarxes de la subxarxa virtual. Dos punts separen l'etiqueta de la prioritat. Aquests contenidors només es permeten a nivell de contenidor de base de dades o global.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
subnet	subnet *id de subxarxa màscara de xarxa abast*	Sí	Cap	Especifica una subxarxa i una agrupació d'adreces. Es pressuposa que totes les adreces són a l'agrupació a no ser que s'especifiqui un abast en la línia o que les adreces es modifiquin posteriorment al contenidor mitjançant un abast o una sentència d'exclusió. L'abast opcional és un parell d'adreces IP en format de quartet amb punt separades per un guió. Es pot especificar una etiqueta opcional i la prioritat. Les subxarxes virtuals les utilitzen per identificar i ordenar les subxarxes de la subxarxa virtual. Dos punts separen l'etiqueta de la prioritat. Aquests contenidors només es permeten a nivell de contenidor de base de dades o global.
subnet	subnet *id de subxarxa màscara de xarxa etiqueta:prioritat*	Sí	Cap	Especifica una subxarxa i una agrupació d'adreces. Es pressuposa que totes les adreces són a l'agrupació a no ser que s'especifiqui un abast en la línia o que les adreces es modifiquin posteriorment al contenidor mitjançant un abast o una sentència d'exclusió. L'abast opcional és un parell d'adreces IP en format de quartet amb punt separades per un guió. Es pot especificar una etiqueta opcional i la prioritat. Les subxarxes virtuals les utilitzen per identificar i ordenar les subxarxes de la subxarxa virtual. Dos punts separen l'etiqueta de la prioritat. Aquests contenidors només es permeten a nivell de contenidor de base de dades o global.
subnet	subnet *id de subxarxa màscara de xarxa abast etiqueta:prioritat*			Especifica una subxarxa i una agrupació d'adreces. Es pressuposa que totes les adreces són a l'agrupació a no ser que s'especifiqui un abast en la línia o que les adreces es modifiquin posteriorment al contenidor mitjançant un abast o una sentència d'exclusió. L'abast opcional és un parell d'adreces IP en format de quartet amb punt separades per un guió. Es pot especificar una etiqueta opcional i la prioritat. Les subxarxes virtuals les utilitzen per identificar i ordenar les subxarxes de la subxarxa virtual. Dos punts separen l'etiqueta de la prioritat. Aquests contenidors només es permeten a nivell de contenidor de base de dades o global.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
subnet	subnet *id de subxarxa abast*	Sí	Cap	Especifica una subxarxa que va en un contenidor de xarxa. Defineix un abast d'adreces que és tota la subxarxa a no ser que s'especifiqui la part d'abast opcional. La màscara de xarxa associada a la subxarxa s'agafa del contenidor de xarxa circumdant. **Nota:** Aquest mètode es desaprova a favor d'altres formes de subxarxa
option	option *nombre dades* ...	No	Cap	Especifica una opció per enviar-la a un client o, en cas que s'hagi denegat, una opció que eviti l'enviament al client. L'opció * **deny** la clàusula significa que totes les opcions que no s'especifiquin al contenidor actual no es retornaran al client. L'opció *nombre*deny només denega l'opció especificada. *nombre* és un enter de 8 bits sense signe. *dades* és específic de l'opció (consulteu més amunt) o bé es pot especificar com a sèrie entre cometes (que indiqui el text ASCII) o 0x*dígits_hexadecimals* o hex"*dígits_hexadecimals*" o hex "*dígits_hexadecimals*". Si l'opció es troba en un contenidor de proveïdors, s'encapsularà amb altres opcions en una opció 43.
option	option *nombre*deny	No	Cap	Especifica una opció per enviar-la a un client o, en cas que s'hagi denegat, una opció que eviti l'enviament al client. L'opció * **deny** la clàusula significa que totes les opcions que no s'especifiquin al contenidor actual no es retornaran al client. L'opció *nombre*deny només denega l'opció especificada. *nombre* és un enter de 8 bits sense signe. *dades* és específic de l'opció (consulteu més amunt) o bé es pot especificar com a sèrie entre cometes (que indiqui el text ASCII) o 0x*dígits_hexadecimals* o hex"*dígits_hexadecimals*" o hex "*dígits_hexadecimals*". Si l'opció es troba en un contenidor de proveïdors, s'encapsularà amb altres opcions en una opció 43.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
option	option * deny	No	Cap	Especifica una opció per enviar-la a un client o, en cas que s'hagi denegat, una opció que eviti l'enviament al client. L'opció *** deny** la clàusula significa que totes les opcions que no s'especifiquin al contenidor actual no es retornaran al client. L'opció *nombre*deny només denega l'opció especificada. *nombre* és un enter de 8 bits sense signe. *dades* és específic de l'opció (consulteu més amunt) o bé es pot especificar com a sèrie entre cometes (que indiqui el text ASCII) o 0x*dígits_hexadecimals* o hex"*dígits_hexadecimals*" o hex "*dígits_hexadecimals*". Si l'opció es troba en un contenidor de proveïdors, s'encapsularà amb altres opcions en una opció 43.
exclude	exclude *una adreça IP*	No	Cap	Modifica l'abast al contenidor on hi ha la sentència d'exclusió. Als nivells de contenidor de base de dades o global, la sentència d'exclusió no és vàlida. Aquesta sentència elimina de l'abast actual del contenidor l'adreça o abast especificats. La sentència d'exclusió us permet crear abasts no contigus per a les subxarxes o altres contenidors.
exclude	exclude *quartet_amb_punt-quartet_amb_punt*	No	Cap	Modifica l'abast al contenidor on hi ha la sentència d'exclusió. Als nivells de contenidor de base de dades o global, la sentència d'exclusió no és vàlida. Aquesta sentència elimina de l'abast actual del contenidor l'adreça o abast especificats. La sentència d'exclusió us permet crear abasts no contigus per a les subxarxes o altres contenidors.
range	range *adreça_IP*	No	Cap	Modifica l'abast al contenidor on hi ha la sentència d'abast. Als nivells de contenidor de base de dades o global, la sentència d'abast no és vàlida. Si l'abast és el primer del contenidor que no especifica un abast a la línia de definició del contenidor, aleshores l'abast per al contenidor esdevé l'abast especificat per la sentència d'abast. S'afegeixen a l'abast actual qualsevol sentència d'abast després del primer abast o totes les sentències d'abast per a un contenidor que especifiqui abasts a la definició. Amb la sentència d'abast, es poden afegir a l'abast una sola adreça o bé un grup d'adreces. L'abast ha d'encaixar dins la definició de contenidor de subxarxes.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
range	range *quartet_amb_punt-quartet_amb_punt*	No	Cap	Modifica l'abast al contenidor on hi ha la sentència d'abast. Als nivells de contenidor de base de dades o global, la sentència d'abast no és vàlida. Si l'abast és el primer del contenidor que no especifica un abast a la línia de definició del contenidor, aleshores l'abast per al contenidor esdevé l'abast especificat per la sentència d'abast. S'afegeixen a l'abast actual qualsevol sentència d'abast després del primer abast o totes les sentències d'abast per a un contenidor que especifiqui abasts a la definició. Amb la sentència d'abast, es poden afegir a l'abast una sola adreça o bé un grup d'adreces. L'abast ha d'encaixar dins la definició de contenidor de subxarxes.
client	client *tipus maquinari adreça maquinari* NONE			Especifica un contenidor de clients que denega al client especificat per l'*adreça maquinari* i el *tipus maquinari* l'obtenció d'una adreça. Si el *tipus maquinari* és igual a 0, llavors l'*adreça maquinari* és una sèrie ASCII. Altrament, el *tipus maquinari* és el tipus de maquinari per al client i l'*adreça maquinari* és l'adreça de maquinari del client. Si l'*adreça maquinari* és una sèrie, s'accepten els caràcters de cometes al voltant de la sèrie. Si l'*adreça maquinari* és una sèrie hexadecimal, llavors l'adreça es pot especificar amb 0x*dígits_hexadecimals* o hex *dígits*. L'*abast* fa que el client especificat mitjançant l'*adreça maquinari* i el *tipus maquinari* obtingui una adreça de l'*abast*. Per coincidir amb diversos clients, han de ser expressions regulars.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
client	client *tipus maquinari adreça maquinari* ANY			Especifica un contenidor de clients que denega al client especificat per l'*adreça maquinari* i el *tipus maquinari* l'obtenció d'una adreça. Si el *tipus maquinari* és igual a 0, llavors l'*adreça maquinari* és una sèrie ASCII. Altrament, el *tipus maquinari* és el tipus de maquinari per al client i l'*adreça maquinari* és l'adreça de maquinari del client. Si l'*adreça maquinari* és una sèrie, s'accepten els caràcters de cometes al voltant de la sèrie. Si l'*adreça maquinari* és una sèrie hexadecimal, llavors l'adreça es pot especificar amb 0x*dígits_hexadecimals* o hex *dígits*. L'*abast* fa que el client especificat mitjançant l'*adreça maquinari* i el *tipus maquinari* obtingui una adreça de l'*abast*. Per coincidir amb diversos clients, han de ser expressions regulars.
client	client *tipus maquinari adreça maquinari quartet_amb punt*			Especifica un contenidor de clients que denega al client especificat per l'*adreça maquinari* i el *tipus maquinari* l'obtenció d'una adreça. Si el *tipus maquinari* és igual a 0, llavors l'*adreça maquinari* és una sèrie ASCII. Altrament, el *tipus maquinari* és el tipus de maquinari per al client i l'*adreça maquinari* és l'adreça de maquinari del client. Si l'*adreça maquinari* és una sèrie, s'accepten els caràcters de cometes al voltant de la sèrie. Si l'*adreça maquinari* és una sèrie hexadecimal, llavors l'adreça es pot especificar amb 0x*dígits_hexadecimals* o hex *dígits*. L'*abast* fa que el client especificat mitjançant l'*adreça maquinari* i el *tipus maquinari* obtingui una adreça de l'*abast*. Per coincidir amb diversos clients, han de ser expressions regulars.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
client	client *tipus maquinari adreça maquinari abast*			Especifica un contenidor de clients que denega al client especificat per l'*adreça maquinari* i el *tipus maquinari* l'obtenció d'una adreça. Si el *tipus maquinari* és igual a 0, llavors l'*adreça maquinari* és una sèrie ASCII. Altrament, el *tipus maquinari* és el tipus de maquinari per al client i l'*adreça maquinari* és l'adreça de maquinari del client. Si l'*adreça maquinari* és una sèrie, s'accepten els caràcters de cometes al voltant de la sèrie. Si l'*adreça maquinari* és una sèrie hexadecimal, llavors l'adreça es pot especificar amb 0x*dígits_hexadecimals* o hex *dígits*. L'*abast* fa que el client especificat mitjançant l'*adreça maquinari* i el *tipus maquinari* obtingui una adreça de l'*abast*. Per coincidir amb diversos clients, han de ser expressions regulars.
class	class *sèrie*	Sí	Cap	Especifica un contenidor de classes amb la *sèrie* de nom. La sèrie pot estar entre cometes o no. Si està entre cometes, les cometes s'eliminen abans de la comparació. Les cometes són necessàries en les sèries amb espais o tabuladors. Aquest contenidor és vàlid a qualsevol nivell. Es pot especificar un abast per indicar un conjunt d'adreces que es lliuren a un client amb aquesta classe. L'abast és només una adreça IP de quartet amb punt o bé dues adreces IP de quartet amb punt separades per un guió.
class	class *sèrie abast*	Sí	Cap	Especifica un contenidor de classes amb la *sèrie* de nom. La sèrie pot estar entre cometes o no. Si està entre cometes, les cometes s'eliminen abans de la comparació. Les cometes són necessàries en les sèries amb espais o tabuladors. Aquest contenidor és vàlid a qualsevol nivell. Es pot especificar un abast per indicar un conjunt d'adreces que es lliuren a un client amb aquesta classe. L'abast és només una adreça IP de quartet amb punt o bé dues adreces IP de quartet amb punt separades per un guió.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
network	network *id de xarxa màscara de xarxa*	Sí	Cap	Especifica una xarxa ID que utilitza informació de classe (per exemple, 9.3.149.0 amb una màscara de xarxa de 255.255.255.0 seria la xarxa 9.0.0.0 255.255.255.0). Aquesta versió del contenidor de xarxa s'utilitza per retenir subxarxes amb la mateixa xarxa ID i màscara de xarxa. Quan es proporciona un abast, totes les adreces de l'abast es troben a l'agrupació. L'abast ha de ser a la xarxa de l'ID de xarxa, que utilitza l'adreçament complet de classe. Això només és vàlid al nivell de contenidor global o de base de dades. **Nota:** La paraula clau de xarxa es desaprova a favor del contenidor de subxarxes.
network	network *id de xarxa*	Sí	Cap	Especifica una xarxa ID que utilitza informació de classe (per exemple, 9.3.149.0 amb una màscara de xarxa de 255.255.255.0 seria la xarxa 9.0.0.0 255.255.255.0). Aquesta versió del contenidor de xarxa s'utilitza per retenir subxarxes amb la mateixa xarxa ID i màscara de xarxa. Quan es proporciona un abast, totes les adreces de l'abast es troben a l'agrupació. L'abast ha de ser a la xarxa de l'ID de xarxa, que utilitza l'adreçament complet de classe. Això només és vàlid al nivell de contenidor global o de base de dades. **Nota:** La paraula clau de xarxa es desaprova a favor del contenidor de subxarxes.
network	network *id de xarxa abast*			Especifica una xarxa ID que utilitza informació de classe (per exemple, 9.3.149.0 amb una màscara de xarxa de 255.255.255.0 seria la xarxa 9.0.0.0 255.255.255.0). Aquesta versió del contenidor de xarxa s'utilitza per retenir subxarxes amb la mateixa xarxa ID i màscara de xarxa. Quan es proporciona un abast, totes les adreces de l'abast es troben a l'agrupació. L'abast ha de ser a la xarxa de l'ID de xarxa, que utilitza l'adreçament complet de classe. Això només és vàlid al nivell de contenidor global o de base de dades. **Nota:** La paraula clau de xarxa es desaprova a favor del contenidor de subxarxes.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
vendor	vendor *id_proveïdor*	Sí	Cap	Especifica un contenidor de proveïdors. Els contenidors de proveïdors s'utilitzen per tornar l'opció 43 al client. L'id de proveïdor pot especificar-se en una sèrie entre cometes o en una sèrie binària en forma de 0x*dígits_hexadecimals* o hex"*dígits*". Després de l'id de proveïdor hi pot haver un abast opcional. L'abast s'especifica amb dos quartets amb punt separats per un guió. Després de l'abast opcional, es pot especificar una sèrie ASCII o una sèrie hexadecimal opcional com a primera part de l'opció 43. Si les opcions són al contenidor, s'afegeixen a les dades de l'opció 43. Un cop s'hagin processat totes les opcions, s'afegeix a les dades una Opció de llista de Final de llista. Per retornar les opcions fora d'una opció 43, utilitzeu un client d'expressió regular que coincideixi amb tots els clients per especificar opcions normals per retornar basades en l'ID de proveïdor. El **pxe** després de la paraula clau **proveïdor** crea un contenidor de proveïdors per al PXEClient. El **pxeserver** després de la paraula clau **proveïdor** crea un contenidor de proveïdors per al PXEServer.
vendor	vendor *id_proveïdor* hex""	Sí	Cap	Especifica un contenidor de proveïdors. Els contenidors de proveïdors s'utilitzen per tornar l'opció 43 al client. L'id de proveïdor pot especificar-se en una sèrie entre cometes o en una sèrie binària en forma de 0x*dígits_hexadecimals* o hex"*dígits*". Després de l'id de proveïdor hi pot haver un abast opcional. L'abast s'especifica amb dos quartets amb punt separats per un guió. Després de l'abast opcional, es pot especificar una sèrie ASCII o una sèrie hexadecimal opcional com a primera part de l'opció 43. Si les opcions són al contenidor, s'afegeixen a les dades de l'opció 43. Un cop s'hagin processat totes les opcions, s'afegeix a les dades una Opció de llista de Final de llista. Per retornar les opcions fora d'una opció 43, utilitzeu un client d'expressió regular que coincideixi amb tots els clients per especificar opcions normals per retornar basades en l'ID de proveïdor. El **pxe** després de la paraula clau **proveïdor** crea un contenidor de proveïdors per al PXEClient. El **pxeserver** després de la paraula clau **proveïdor** crea un contenidor de proveïdors per al PXEServer.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
vendor	vendor *id_proveïdor* hex ""	Sí	Cap	Especifica un contenidor de proveïdors. Els contenidors de proveïdors s'utilitzen per tornar l'opció 43 al client. L'id de proveïdor pot especificar-se en una sèrie entre cometes o en una sèrie binària en forma de 0x*dígits_hexadecimals* o hex"*dígits*". Després de l'id de proveïdor hi pot haver un abast opcional. L'abast s'especifica amb dos quartets amb punt separats per un guió. Després de l'abast opcional, es pot especificar una sèrie ASCII o una sèrie hexadecimal opcional com a primera part de l'opció 43. Si les opcions són al contenidor, s'afegeixen a les dades de l'opció 43. Un cop s'hagin processat totes les opcions, s'afegeix a les dades una Opció de llista de Final de llista. Per retornar les opcions fora d'una opció 43, utilitzeu un client d'expressió regular que coincideixi amb tots els clients per especificar opcions normals per retornar basades en l'ID de proveïdor. El **pxe** després de la paraula clau **proveïdor** crea un contenidor de proveïdors per al PXEClient. El **pxeserver** després de la paraula clau **proveïdor** crea un contenidor de proveïdors per al PXEServer.
vendor	vendor *id_proveïdor* 0xdata	Sí	Cap	Especifica un contenidor de proveïdors. Els contenidors de proveïdors s'utilitzen per tornar l'opció 43 al client. L'id de proveïdor pot especificar-se en una sèrie entre cometes o en una sèrie binària en forma de 0x*dígits_hexadecimals* o hex"*dígits*". Després de l'id de proveïdor hi pot haver un abast opcional. L'abast s'especifica amb dos quartets amb punt separats per un guió. Després de l'abast opcional, es pot especificar una sèrie ASCII o una sèrie hexadecimal opcional com a primera part de l'opció 43. Si les opcions són al contenidor, s'afegeixen a les dades de l'opció 43. Un cop s'hagin processat totes les opcions, s'afegeix a les dades una Opció de llista de Final de llista. Per retornar les opcions fora d'una opció 43, utilitzeu un client d'expressió regular que coincideixi amb tots els clients per especificar opcions normals per retornar basades en l'ID de proveïdor. El **pxe** després de la paraula clau **proveïdor** crea un contenidor de proveïdors per al PXEClient. El **pxeserver** després de la paraula clau **proveïdor** crea un contenidor de proveïdors per al PXEServer.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
vendor	vendor *id_proveïdor* ""	Sí	Cap	Especifica un contenidor de proveïdors. Els contenidors de proveïdors s'utilitzen per tornar l'opció 43 al client. L'id de proveïdor pot especificar-se en una sèrie entre cometes o en una sèrie binària en forma de 0x*dígits_hexadecimals* o hex"*dígits*". Després de l'id de proveïdor hi pot haver un abast opcional. L'abast s'especifica amb dos quartets amb punt separats per un guió. Després de l'abast opcional, es pot especificar una sèrie ASCII o una sèrie hexadecimal opcional com a primera part de l'opció 43. Si les opcions són al contenidor, s'afegeixen a les dades de l'opció 43. Un cop s'hagin processat totes les opcions, s'afegeix a les dades una Opció de llista de Final de llista. Per retornar les opcions fora d'una opció 43, utilitzeu un client d'expressió regular que coincideixi amb tots els clients per especificar opcions normals per retornar basades en l'ID de proveïdor. El **pxe** després de la paraula clau **proveïdor** crea un contenidor de proveïdors per al PXEClient. El **pxeserver** després de la paraula clau **proveïdor** crea un contenidor de proveïdors per al PXEServer.
vendor	vendor *id_proveïdor abast*	Sí	Cap	Especifica un contenidor de proveïdors. Els contenidors de proveïdors s'utilitzen per tornar l'opció 43 al client. L'id de proveïdor pot especificar-se en una sèrie entre cometes o en una sèrie binària en forma de 0x*dígits_hexadecimals* o hex"*dígits*". Després de l'id de proveïdor hi pot haver un abast opcional. L'abast s'especifica amb dos quartets amb punt separats per un guió. Després de l'abast opcional, es pot especificar una sèrie ASCII o una sèrie hexadecimal opcional com a primera part de l'opció 43. Si les opcions són al contenidor, s'afegeixen a les dades de l'opció 43. Un cop s'hagin processat totes les opcions, s'afegeix a les dades una Opció de llista de Final de llista. Per retornar les opcions fora d'una opció 43, utilitzeu un client d'expressió regular que coincideixi amb tots els clients per especificar opcions normals per retornar basades en l'ID de proveïdor. El **pxe** després de la paraula clau **proveïdor** crea un contenidor de proveïdors per al PXEClient. El **pxeserver** després de la paraula clau **proveïdor** crea un contenidor de proveïdors per al PXEServer.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
vendor	vendor *id_proveïdor abast* hex""	Sí	Cap	Especifica un contenidor de proveïdors. Els contenidors de proveïdors s'utilitzen per tornar l'opció 43 al client. L'id de proveïdor pot especificar-se en una sèrie entre cometes o en una sèrie binària en forma de 0x*dígits_hexadecimals* o hex"*dígits*". Després de l'id de proveïdor hi pot haver un abast opcional. L'abast s'especifica amb dos quartets amb punt separats per un guió. Després de l'abast opcional, es pot especificar una sèrie ASCII o una sèrie hexadecimal opcional com a primera part de l'opció 43. Si les opcions són al contenidor, s'afegeixen a les dades de l'opció 43. Un cop s'hagin processat totes les opcions, s'afegeix a les dades una Opció de llista de Final de llista. Per retornar les opcions fora d'una opció 43, utilitzeu un client d'expressió regular que coincideixi amb tots els clients per especificar opcions normals per retornar basades en l'ID de proveïdor. El **pxe** després de la paraula clau **proveïdor** crea un contenidor de proveïdors per al PXEClient. El **pxeserver** després de la paraula clau **proveïdor** crea un contenidor de proveïdors per al PXEServer.
vendor	vendor *id_proveïdor abast* hex ""	Sí	Cap	Especifica un contenidor de proveïdors. Els contenidors de proveïdors s'utilitzen per tornar l'opció 43 al client. L'id de proveïdor pot especificar-se en una sèrie entre cometes o en una sèrie binària en forma de 0x*dígits_hexadecimals* o hex"*dígits*". Després de l'id de proveïdor hi pot haver un abast opcional. L'abast s'especifica amb dos quartets amb punt separats per un guió. Després de l'abast opcional, es pot especificar una sèrie ASCII o una sèrie hexadecimal opcional com a primera part de l'opció 43. Si les opcions són al contenidor, s'afegeixen a les dades de l'opció 43. Un cop s'hagin processat totes les opcions, s'afegeix a les dades una Opció de llista de Final de llista. Per retornar les opcions fora d'una opció 43, utilitzeu un client d'expressió regular que coincideixi amb tots els clients per especificar opcions normals per retornar basades en l'ID de proveïdor. El **pxe** després de la paraula clau **proveïdor** crea un contenidor de proveïdors per al PXEClient. El **pxeserver** després de la paraula clau **proveïdor** crea un contenidor de proveïdors per al PXEServer.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
vendor	vendor *id_proveïdor abast* 0xdata	Sí	Cap	Especifica un contenidor de proveïdors. Els contenidors de proveïdors s'utilitzen per tornar l'opció 43 al client. L'id de proveïdor pot especificar-se en una sèrie entre cometes o en una sèrie binària en forma de 0x*dígits_hexadecimals* o hex"*dígits*". Després de l'id de proveïdor hi pot haver un abast opcional. L'abast s'especifica amb dos quartets amb punt separats per un guió. Després de l'abast opcional, es pot especificar una sèrie ASCII o una sèrie hexadecimal opcional com a primera part de l'opció 43. Si les opcions són al contenidor, s'afegeixen a les dades de l'opció 43. Un cop s'hagin processat totes les opcions, s'afegeix a les dades una Opció de llista de Final de llista. Per retornar les opcions fora d'una opció 43, utilitzeu un client d'expressió regular que coincideixi amb tots els clients per especificar opcions normals per retornar basades en l'ID de proveïdor. El **pxe** després de la paraula clau **proveïdor** crea un contenidor de proveïdors per al PXEClient. El **pxeserver** després de la paraula clau **proveïdor** crea un contenidor de proveïdors per al PXEServer.
vendor	vendor *id_proveïdor abast* ""	Sí	Cap	Especifica un contenidor de proveïdors. Els contenidors de proveïdors s'utilitzen per tornar l'opció 43 al client. L'id de proveïdor pot especificar-se en una sèrie entre cometes o en una sèrie binària en forma de 0x*dígits_hexadecimals* o hex"*dígits*". Després de l'id de proveïdor hi pot haver un abast opcional. L'abast s'especifica amb dos quartets amb punt separats per un guió. Després de l'abast opcional, es pot especificar una sèrie ASCII o una sèrie hexadecimal opcional com a primera part de l'opció 43. Si les opcions són al contenidor, s'afegeixen a les dades de l'opció 43. Un cop s'hagin processat totes les opcions, s'afegeix a les dades una Opció de llista de Final de llista. Per retornar les opcions fora d'una opció 43, utilitzeu un client d'expressió regular que coincideixi amb tots els clients per especificar opcions normals per retornar basades en l'ID de proveïdor. El **pxe** després de la paraula clau **proveïdor** crea un contenidor de proveïdors per al PXEClient. El **pxeserver** després de la paraula clau **proveïdor** crea un contenidor de proveïdors per al PXEServer.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
vendor	vendor pxe	Sí	Cap	Especifica un contenidor de proveïdors. Els contenidors de proveïdors s'utilitzen per tornar l'opció 43 al client. L'id de proveïdor pot especificar-se en una sèrie entre cometes o en una sèrie binària en forma de 0x*dígits_hexadecimals* o hex"*dígits*". Després de l'id de proveïdor hi pot haver un abast opcional. L'abast s'especifica amb dos quartets amb punt separats per un guió. Després de l'abast opcional, es pot especificar una sèrie ASCII o una sèrie hexadecimal opcional com a primera part de l'opció 43. Si les opcions són al contenidor, s'afegeixen a les dades de l'opció 43. Un cop s'hagin processat totes les opcions, s'afegeix a les dades una Opció de llista de Final de llista. Per retornar les opcions fora d'una opció 43, utilitzeu un client d'expressió regular que coincideixi amb tots els clients per especificar opcions normals per retornar basades en l'ID de proveïdor. El **pxe** després de la paraula clau **proveïdor** crea un contenidor de proveïdors per al PXEClient. El **pxeserver** després de la paraula clau **proveïdor** crea un contenidor de proveïdors per al PXEServer.
vendor	vendor pxeserver	Sí	Cap	Especifica un contenidor de proveïdors. Els contenidors de proveïdors s'utilitzen per tornar l'opció 43 al client. L'id de proveïdor pot especificar-se en una sèrie entre cometes o en una sèrie binària en forma de 0x*dígits_hexadecimals* o hex"*dígits*". Després de l'id de proveïdor hi pot haver un abast opcional. L'abast s'especifica amb dos quartets amb punt separats per un guió. Després de l'abast opcional, es pot especificar una sèrie ASCII o una sèrie hexadecimal opcional com a primera part de l'opció 43. Si les opcions són al contenidor, s'afegeixen a les dades de l'opció 43. Un cop s'hagin processat totes les opcions, s'afegeix a les dades una Opció de llista de Final de llista. Per retornar les opcions fora d'una opció 43, utilitzeu un client d'expressió regular que coincideixi amb tots els clients per especificar opcions normals per retornar basades en l'ID de proveïdor. El **pxe** després de la paraula clau **proveïdor** crea un contenidor de proveïdors per al PXEClient. El **pxeserver** després de la paraula clau **proveïdor** crea un contenidor de proveïdors per al PXEServer.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
inoption	inoption *nombre dades_opció*	Sí	Cap	Especifica un contenidor que cal fer coincidir amb qualsevol opció d'entrada arbitrària especificada pel client. El *nombre* especifica el nombre d'opció. *dades_opció* especifica la clau que cal fer coincidir per tal que se seleccioni aquest contenidor durant la selecció d'opció i d'adreça per al client. *dades_opció* s'especifica de forma esperada — amb una sèrie entre cometes, una adreça IP, un valor enter — en les opcions conegudes o bé es pot especificar opcionalment mitjançant una sèrie hexadecimal d'octets si la precedeixen els caràcters `0x`. Pel que fa a les opcions que el servidor no coneix, es pot especificar una sèrie hexadecimal d'octets de la mateixa manera. Addicionalment, *dades_opció* pot indicar una expressió regular que cal comparar amb la representació de sèrie de les dades d'opció del client. Les expressions regulars s'especifiquen en una sèrie entre cometes que comença amb `"!` (caràcter de cometes dobles seguit d'un signe d'exclamació). La forma en sèrie d'opcions menys conegudes pel servidor és una sèrie hexadecimal d'octets SENSE els caràcters `0x` al davant.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
inoption	inoption *nombre dades_opció abast*	Sí	Cap	Especifica un contenidor que cal fer coincidir amb qualsevol opció d'entrada arbitrària especificada pel client. El *nombre* especifica el nombre d'opció. *dades_opció* especifica la clau que cal fer coincidir per tal que se seleccioni aquest contenidor durant la selecció d'opció i d'adreça per al client. *dades_opció* s'especifica de forma esperada — amb una sèrie entre cometes, una adreça IP, un valor enter — en les opcions conegudes o bé es pot especificar opcionalment mitjançant una sèrie hexadecimal d'octets si la precedeixen els caràcters `0x`. Pel que fa a les opcions que el servidor no coneix, es pot especificar una sèrie hexadecimal d'octets de la mateixa manera. Addicionalment, *dades_opció* pot indicar una expressió regular que cal comparar amb la representació de sèrie de les dades d'opció del client. Les expressions regulars s'especifiquen en una sèrie entre cometes que comença amb `"!` (caràcter de cometes dobles seguit d'un signe d'exclamació). La forma en sèrie d'opcions menys conegudes pel servidor és una sèrie hexadecimal d'octets SENSE els caràcters `0x` al davant.
virtual	virtual fill *id id* ...	No	Cap	Especifica una subxarxa virtual amb una política. `fill` significa utilitzar totes les adreces del contenidor abans d'anar al contenidor següent. `rotate` significa seleccionar una adreça de l'agrupació següent de la llista a cada sol•licitud. `sfill` i `srotate` són el mateix que `fill` i `rotate`, però es realitza una cerca per veure si el client coincideix amb els contenidors, els proveïdors o les classes de la subxarxa. Si es troba una coincidència que pot subministrar una adreça, s'agafa l'adreça d'aquest contenidor en lloc de seguir les normes. Hi pot haver tots els IDs que calgui. L'*id* és l'ID de subxarxa de la definició de subxarxa o l'etiqueta de la definició de subxarxa. L'etiqueta és necessària si hi ha diverses subxarxes amb el mateix id de subxarxa.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
virtual	virtual sfill *id id* ...	No	Cap	Especifica una subxarxa virtual amb una política. `fill` significa utilitzar totes les adreces del contenidor abans d'anar al contenidor següent. `rotate` significa seleccionar una adreça de l'agrupació següent de la llista a cada sol•licitud. `sfill` i `srotate` són el mateix que `fill` i `rotate`, però es realitza una cerca per veure si el client coincideix amb els contenidors, els proveïdors o les classes de la subxarxa. Si es troba una coincidència que pot subministrar una adreça, s'agafa l'adreça d'aquest contenidor en lloc de seguir les normes. Hi pot haver tots els IDs que calgui. L'*id* és l'ID de subxarxa de la definició de subxarxa o l'etiqueta de la definició de subxarxa. L'etiqueta és necessària si hi ha diverses subxarxes amb el mateix id de subxarxa.
virtual	virtual rotate *id id* ...	No	Cap	Especifica una subxarxa virtual amb una política. `fill` significa utilitzar totes les adreces del contenidor abans d'anar al contenidor següent. `rotate` significa seleccionar una adreça de l'agrupació següent de la llista a cada sol•licitud. `sfill` i `srotate` són el mateix que `fill` i `rotate`, però es realitza una cerca per veure si el client coincideix amb els contenidors, els proveïdors o les classes de la subxarxa. Si es troba una coincidència que pot subministrar una adreça, s'agafa l'adreça d'aquest contenidor en lloc de seguir les normes. Hi pot haver tots els IDs que calgui. L'*id* és l'ID de subxarxa de la definició de subxarxa o l'etiqueta de la definició de subxarxa. L'etiqueta és necessària si hi ha diverses subxarxes amb el mateix id de subxarxa.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
virtual	virtual srotate *id id* ...	No	Cap	Especifica una subxarxa virtual amb una política. `fill` significa utilitzar totes les adreces del contenidor abans d'anar al contenidor següent. `rotate` significa seleccionar una adreça de l'agrupació següent de la llista a cada sol•licitud. `sfill` i `srotate` són el mateix que `fill` i `rotate`, però es realitza una cerca per veure si el client coincideix amb els contenidors, els proveïdors o les classes de la subxarxa. Si es troba una coincidència que pot subministrar una adreça, s'agafa l'adreça d'aquest contenidor en lloc de seguir les normes. Hi pot haver tots els IDs que calgui. L'*id* és l'ID de subxarxa de la definició de subxarxa o l'etiqueta de la definició de subxarxa. L'etiqueta és necessària si hi ha diverses subxarxes amb el mateix id de subxarxa.
virtual		No	Cap	Especifica una subxarxa virtual amb una política. `fill` significa utilitzar totes les adreces del contenidor abans d'anar al contenidor següent. `rotate` significa seleccionar una adreça de l'agrupació següent de la llista a cada sol•licitud. `sfill` i `srotate` són el mateix que `fill` i `rotate`, però es realitza una cerca per veure si el client coincideix amb els contenidors, els proveïdors o les classes de la subxarxa. Si es troba una coincidència que pot subministrar una adreça, s'agafa l'adreça d'aquest contenidor en lloc de seguir les normes. Hi pot haver tots els IDs que calgui. L'*id* és l'ID de subxarxa de la definició de subxarxa o l'etiqueta de la definició de subxarxa. L'etiqueta és necessària si hi ha diverses subxarxes amb el mateix id de subxarxa.
inorder:	inorder: *id id* ...	No	Cap	Especifica una subxarxa virtual amb unes normes d'emplenament. Això vol dir que s'han d'utilitzar totes les adreces del contenidor abans d'anar al següent. Hi pot haver tots els IDs que calgui. L'*id* és l'ID de subxarxa de la definició de subxarxa o l'etiqueta de la definició de subxarxa. L'etiqueta és necessària si hi ha diverses subxarxes amb el mateix ID de subxarxa.

Paraula clau	Forma	Sub- contenidors?	Valor per defecte	Significat
balance:	balance: *id id ...*	No	Cap	Especifica una subxarxa virtual amb unes normes de rotació. Això vol dir que s'ha d'utilitzar l'adreça següent al contenidor següent. Hi pot haver tots els IDs que calgui. L'*id* és l'ID de subxarxa de la definició de subxarxa o l'etiqueta de la definició de subxarxa. L'etiqueta és necessària si hi ha diverses subxarxes amb el mateix ID de subxarxa.
bootstrapserver	bootstrapserver *adreça IP*	No	Cap	Especifica el servidor que els clients haurien d'utilitzar als fitxers TFTP després de rebre els paquets BOOTP o DHCP. Aquest valor emplena el camp **siaddr** del paquet. Això és vàlid a qualsevol nivell de contenidor.
giaddrfield	giaddrfield *adreça IP*	No	Cap	Especifica el giaddrfield per als paquets de resposta. **Nota:** Aquesta especificació no es permet als protocols BOOTP i DHCP, però alguns clients demanen que el camp **giaddr** sigui la passarel•la per defecte per a la xarxa. A causa d'aquest conflicte potencial, el giaddrfield només s'hauria d'utilitzar dins d'un contenidor de clients, tot i que pot funcionar a qualsevol nivell.
bootfile	bootfile *camí d'accés*	No	Cap	Especifica el fitxer d'engegada que cal utilitzar a la secció de fitxer del paquet de resposta. Això es pot especificar a qualsevol nivell de contenidor. La política de fitxer d'engegada defineix la manera que els elements especificats a la secció de fitxer del paquet d'entrada interactuen amb les sentències del directori d'inici i el fitxer d'engegada.
pxebootfile	pxebootfile *SystemArch Versió_major Versió_menor Nom_fitxer_engegada Tipus Capa*	No	Cap	Especifica el fitxer d'engegada que cal donar a un client PXE. L'analitzador del fitxer de configuració genera un error si el nombre de paràmetres després de la paraula clau és menor que 4, en prescindeix si és major que 7 i si n'hi ha 4 pressuposa el valor del Tipus = 0 i la Capa = 0. Aquesta paraula clau només es pot utilitzar en un contenidor.

Si voleu detalls sobre altres opcions, consulteu l'apartat "Opcions conegudes de fitxer del servidor DHCP" a la pàgina 221 i "Subopcions del contenidor de proveïdors del PXE" a la pàgina 303.

Daemons TCP/IP

Els daemons (també coneguts com a *servidors*) són processos que s'executen contínuament en segon pla i duen a terme funcions que altres processos requereixen. El **Transmission Control Protocol/Internet Protocol (TCP/IP)** proporciona daemons per implementar certes funcions al sistema operatiu.

Aquests daemons són processos de fons que s'executen sense interrompre altres processos (a no ser que això formi part de la funció del daemon).

Els daemons s'invoquen mitjançant ordres a nivell de gestió del sistema, mitjançant altres daemons o seqüències d'intèrpret d'ordres. També podeu controlar els daemons amb el daemon **inetd**, la seqüència d'intèrpret d'ordres **rc.tcpip** i el Controlador de recursos del sistema (SRC).

Subsistemes i subservidors

Un *subsistema* és un daemon, o servidor, controlat pel SRC. Un *subservidor* és un daemon controlat per un subsistema. (Les ordres i els noms daemon es denoten normalment per una **d** al final del nom.)

Les categories de subsistema i de subservidor s'exclouen mútuament. És a dir, no es fa una llista de daemons com a subsistema i subservidor alhora. L'únic subsistema **TCP/IP** que controla altres daemons és el daemon **inetd**. Tots els subservidors **TCP/IP** són també subservidors **inetd**.

Per obtenir una llista dels daemons **TCP/IP**, consulteu l'apartat "Daemons TCP/IP" a la pàgina 431.

Control de recursos del sistema

Entre altres funcions, l'SRC us permet iniciar daemons, aturar-os i traçar llur activitat. A més, l'SRC proporciona la capacitat d'agrupar daemons en subsistemes i subservidors.

El Control de recursos del sistema és una eina dissenyada per ajudar-vos en el control de daemons. L'SRC permet el control més enllà dels senyaladors i paràmetres disponibles amb cada ordre de daemon.

Per obtenir més informació sobre el Controlador de recursos del sistema, consulteu l'apartat System Resource Controller de la publicació *Operating system and device management*.

Per obtenir una llista de les ordres SRC, consulteu l'apartat "Ordres SRC" a la pàgina 429.

Configuració del daemon inetd

Dueu a terme aquests passos per configurar el daemon **inetd** del **TCP/IP**.

Per configurar el daemon **inetd**:

1. Especifiqueu el subservidors que s'invocaran afegint un daemon **inetd**.
2. Especifiqueu les característiques de reinici tot canviant les característiques del daemon **inetd**.

Taula 75. Configuració de les tasques del daemon inetd

Tasca	Camí d'accés ràpid de la SMIT	Ordre o fitxer
Inici del Daemon **inetd**	`smit mkinetd`	**startsrc -s inetd**
Canvi de les característiques de reinici del Daemon **inetd**	`smit chinetd` o `smit lsinetd`	
Aturada del Daemon **inetd**	`smit rminetd`	**stopsrc -s inetd**
Llista de tots els subservidors **inetd**	`smit inetdconf`	
Afegiment d'un subservidor **inetd**[1]	`smit mkinetdconf`	edita el `/etc/inetd.conf` i executa el **refresh -s inetd** o el **kill -1** *inetdPID*[2]
Canvi/mostra de les característiques d'un subservidor **inetd**	`smit inetdconf`	edita el `/etc/inetd.conf` i executa el **refresh -s inetd** o el **kill -1** *inetdPID*[2]
Eliminació d'un subservidor **inetd**	`smit rminetd`	edita el `/etc/inetd.conf` i executa el **refresh -s inetd** o el **kill -1** *inetdPID*[2]

Nota:

1. Afegir un subservidor **inetd** configura el daemon **inetd** de manera que invoca el subservidor quan cal.
2. Les ordres **refresh** i **kill** informen al daemon **inetd** dels canvis del fitxer de configuració.

Serveis de xarxa de client

Els Serveis de xarxa de client (accessibles mitjançant el camí d'accés ràpid de la SMIT, `smit clientnet`) es refereixen als protocols del **TCP/IP** disponibles que el sistema operatiu pot utilitzar.

Cada protocol (o servei) es coneix pel número de port que utilitza a la xarxa, i d'aquí ve el terme *port conegut*. Per facilitar la tasca als programadors, els números de port es poden expressar tant amb noms com amb nombres. Per exemple, el protocol de correu del **TCP/IP** utilitza el port 25 i se'l coneix amb el nom **smtp**. Si es fa una llista (sense comentaris) d'un protocol al fitxer `/etc/services`, aleshores un amfitrió pot utilitzar aquest protocol.

Per defecte, tots els protocols del **TCP/IP** es defineixen al fitxer `/etc/services`. No cal que configureu aquest fitxer. Si escriviu els vostres propis programes de client/servidor, és probable que vulgueu afegir el servei al fitxer `/etc/services` i reservar un número de port i un nom específics per al servei. Si decidiu afegir el servei al `/etc/services`, tingueu en compte que els números de port del 0 al 1024 estan reservats per a ús del sistema.

Taula 76. Tasques dels serveis de xarxa de client

Tasca	Camí d'accés ràpid de la SMIT	Ordre o fitxer
Llista de tots els serveis	`smit lsservices`	visualitza `/etc/services`
Afegiment d'un servei	`smit mkservices`	edita `/etc/services`
Canvi/mostra de les característiques d'un servei	`smit chservices`	edita `/etc/services`
Eliminació d'un servei	`smit rmservices`	edita `/etc/services`

Serveis de xarxa del servidor

Els serveis de xarxa del servidor inclouen el control de l'accés remot, l'inici o aturada del **TCP/IP** i la gestió del programa de control de dispositiu **pty** tal i com es mostra en aquesta taula.

El programa de control de dispositiu **pty** està instal•lat automàticament amb el sistema. Per defecte, està configurat per donar suport a 16 enllaços simbòlics d'estil BSD i el sistema el pot utilitzar en el moment d'engegar.

Taula 77. Tasques dels serveis de xarxa del servidor

Tasca	Camí d'accés ràpid de la SMIT	Ordre o fitxer
Control de l'accés remot		Consulteu l'apartat "Accés a l'execució d'ordres remotes" i "Usuaris del Programa de transferència de fitxers restringit" de *Security*.
Inici, reinici o aturada dels subsistemes TCP/IP	`smit otherserv`	Consulteu l'apartat "Control de recursos del sistema" a la pàgina 354.
Canvi/mostra de les característiques del programa de control de dispositiu pty	`smit chgpty`	**chdev -l pty0 -P -a num=***X* on *X* oscil•la entre 0 i 64
Inhabilitació del programa de control de dispositiu pty per a l'ús	`smit pty` i seleccioneu **Elimina el PTY; Conserva la definició**	Cap ordre o fitxer relacionats.
Habilitació del programa de control de dispositiu pty per a l'ús	`smit pty` i seleccioneu **Configura el PTY definit**	Cap ordre o fitxer relacionats.
Generació d'un informe d'errors	`smit errpt`	Cap ordre o fitxer relacionats.
Traça del pty	`smit trace`	Cap ordre o fitxer relacionats.

Encaminament TCP/IP

Un *camí* defineix un camí d'accés per enviar paquets a través de la xarxa d'Internet a una adreça en una altra xarxa.

Un camí no defineix el camí d'accés complet, sinó només el segment de camí d'accés des d'un amfitrió a una passarel•la que pot reenviar paquets a una destinació (o des d'una passarel•la a una altra). Hi ha cinc tipus de camins:

Element	Descripció
camí d'amfitrió	Defineix una passarel•la que pot reenviar paquets a un amfitrió específic en una altra xarxa.
camí de xarxa	Defineix una passarel•la que pot reenviar paquets a qualsevol dels amfitrions d'una xarxa específica.
camí per defecte	Defineix una passarel•la per utilitzar-la quan no s'ha definit altrament cap camí de xarxa o d'amfitrió a una destinació.
camí de bucle de retorn	Camí per defecte per a tots els paquets enviats a les adreces de xarxa local. L'IP del camí de bucle de retorn sempre és 127.0.0.1.
camí de difusió	Camí per defecte per a tots els paquets de difusió general. S'assignen automàticament dos camins de difusió a cada subxarxa en què la xarxa té un IP (un a l'adreça de subxarxa i un a l'adreça de difusió de la subxarxa).

Els camins es defineixen a la *taula d'encaminament* de kernel. Les definicions de camins inclouen informació sobre les xarxes accessibles des de l'amfitrió local i sobre les passarel•les que es poden utilitzar per accedir a xarxes remotes. Quan una passarel•la rep un datagrama, comprova les taules d'encaminament per esbrinar a on ha d'enviar el datagrama la següent vegada pel camí d'accés de la destinació.

Podey afegir múltiples camins per a la mateixa destinació a la taula d'encaminament del kernel. Una cerca d'encaminament avalua tots els camins que coincideixen amb la sol•licitud i tria el camí amb la mètrica de distància més baixa. Si hi ha diversos camins coincidents amb una distància igual, la cerca tria el camí més específic. Si ambdós criteris són iguals en diversos camins, les cerques d'encaminament alternen les opcions dels camins coincidents.

Encaminament estàtic i dinàmic

Al **TCP/IP**, l'encaminament pot ser de dos tipus: *estàtic* o *dinàmic*.

Amb l'encaminament estàtic, manteniu la taula d'encaminament de forma manual mitjançant l'ordre **route**. L'encaminament estàtic és pràctic per a una sola xarxa que es comunica amb una o dues altres xarxes. No obstant això, a mesura que la vostra xarxa comenci a comunicar-se amb més xarxes, el nombre de passarel•les augmentarà, així com la quantitat de temps i d'esforç necessaris per mantenir la taula d'encaminament de forma manual.

Amb l'encaminament dinàmic, els daemons actualitzen la taula d'encaminament de forma automàtica. Els daemons d'encaminament reben contínuament informació difosa per altres daemons d'encaminament i, per tant, actualitzen contínuament la taula d'encaminament.

El **TCP/IP** proporciona dos daemons per utilitzar-los en l'encaminament dinàmic, els daemons **routed** i **gated**. El daemon **gated** dóna suport simultàniament als protocols d'encaminament **Routing Information Protocol (RIP)**, **Routing Information Protocol Next Generation (RIPng)**, **Exterior Gateway Protocol (EGP)**, **Border Gateway Protocol (BGP)** i **BGP4+**, **Defense Communications Network Local-Network Protocol (HELLO)**, **Open Shortest Path First (OSPF)**, **Intermediate System to Intermediate System (IS-IS)** i **Internet Control Message Protocol (ICMP i ICMPv6)/Descobriment d'encaminaments**. A més, el daemon **gated** dóna suport al **Simple Network Management Protocol (SNMP)**. El daemon **routed** només dóna suport al **Routing Information Protocol**.

Els daemons d'encaminament poden operar en una de les dues modalitats, *passiva* o *activa*, depenent de les opcions que utilitzeu quan inicieu els daemons. En la modalitat activa, ambdós daemons d'encaminament difonen informació d'encaminament de forma periòdica sobre la seva xarxa local a les passarel•les i amfitrions, i reben informació d'encaminament de part d'amfitrions i passarel•les. En la modalitat passiva, els daemons d'encaminament reben informació d'encaminament de part d'amfitrions i passarel•les, però no intenten mantenir actualitzades les passarel•les remotes (no anuncien la seva pròpia informació d'encaminament).

Aquests dos tipus d'encaminament es poden utilitzar no només per a les passarel•les, sinó també per a altres amfitrions d'una xarxa. L'encaminament estàtic funciona igual per a les passarel•les que per a altres amfitrions. No obstant això, quan s'executin en un amfitrió que no és una passarel•la, cal executar els daemons d'encaminament dinàmic en la modalitat passiva (sense informació).

Passarel•les d'encaminament TCP/IP

Les passarel•les són un tipus d'encaminador. Els *encaminadors* connecten dos o més xarxes i proporcionen la funció d'encaminament. Alguns encaminadors, per exemple, encaminen al nivell de la interfície de xarxa o al nivell físic. Tanmateix, les *passarel•les*, encaminen al nivell de xarxa.

Les passarel•les reben datagrames IP d'altres passarel•les o amfitrions per lliurar-les als amfitrions de la xarxa local, i encaminen datagrames IP d'una xarxa a una altra. Per exemple, una passarel•la que connecta dues xarxes Token-Ring té dues targetes adaptadores Token-Ring, cadascuna amb la seva interfície de xarxa Token-Ring. Per passar informació, la passarel•la rep datagrames a través d'una interfície de xarxa i els envia a través d'una altra interfície de xarxa. Les passarel•les verifiquen periòdicament les seves connexions de xarxa a través de missatges d'estat de la interfície.

Les passarel•les encaminen paquets d'acord amb la xarxa de destinació, no d'acord amb l'amfitrió de destinació. És a dir, no és necessari que una màquina de passarel•la efectuï un seguiment de cada possible destinació d'amfitrió d'un paquet. En comptes d'això, una passarel•la encamina paquets d'acord amb la xarxa de l'amfitrió de destinació. La xarxa de destinació, aleshores, s'encarrega d'enviar el paquet a l'amfitrió de destinació. Així, una típica màquina de passarel•la només requereix una capacitat d'emmagatzematge en disc limitada (si cal) i una capacitat de memòria principal limitada.

La distància que ha de recórrer un missatge des de l'amfitrió originari fins a l'amfitrió de destinació depèn del nombre de *salts de passarel•la* que ha de fer. Una passarel•la es troba a zero salts d'una xarxa a la qual està connectada directament, a un salt d'una xarxa a la qual pot accedir a través d'una passarel•la, i així successivament. La distància del missatge normalment s'expressa en el nombre de salts de passarel•la necessaris, o *recomptes de salts* (també anomenat *mètrica*).

Passarel•les d'encaminament interiors i exteriors:

Les passarel•les interiors són passarel•les que pertanyen al mateix sistema autònom. Es comuniquen entre si mitjançant el **Routing Information Protocol (RIP)**, el **Routing Information Protocol Next Generation (RIPng)**, el protocol **Intermediate System to Intermediate System**, el protocol **Open Shortest Path First (OSPF)**, o el **Protocol HELLO (HELLO)**. Les passarel•les exteriors pertanyen a sistemes autònoms diferents. Utilitzen l'**Exterior Gateway Protocol (EGP)**, el **Border Gateway Protocol (BGP)**, o el **BGP4+**.

Per exemple, tingueu presents dos sistemes autònoms. El primer és de totes les xarxes administrades per l'empresa Widget. El segon és de totes les xarxes administrades per l'empresa Gadget. L'empresa Widget té una màquina, que es diu poma, que és la passarel•la de Widget a Internet. L'empresa Gadget té una màquina, que es diu taronja, que és la passarel•la de Gadget a Internet. Ambdues empreses tenen diverses xarxes diferents internes de les empreses. Les passarel•les que connecten les xarxes internes són passarel•les interiors. Però les màquines poma i taronja són passarel•les exteriors.

Cada passarel•la exterior no es comunica amb cadascuna de les altres passarel•les exteriors. En comptes d'això, la passarel•la exterior adquireix un conjunt de veïns (altres passarel•les exteriors) amb qui sí es comunica. Aquests veïns no estan definits per proximitat geogràfica, sinó per les seves comunicacions establertes entre si. Els passarel•les de veïnatge, al seu torn, tenen altres veïns de passarel•la exterior. En aquest sentit, les taules d'encaminament de les passarel•les exteriors s'actualitzen i la informació d'encaminament es propaga entre les passarel•les exteriors.

La informació d'encaminament s'envia en una parella, (X,D), on la lletra X és una xarxa i la lletra D és una distància que reflecteix el cost per arribar a la xarxa especificada. Cada passarel•la anuncia les xarxes a les quals pot accedir i els costs d'accedir-hi. La passarel•la receptora calcula els camins d'accés més curts

a les altres passarel•les i passa aquesta informació als seus veïns. Així, cada passarel•la exterior està rebent contínuament informació d'encaminament, actualitzant la seva taula d'encaminament i passant aquesta informació als seus veïns exteriors.

Protocols de passarel•la:

Totes les passarel•les, siguin interiors o exteriors, utilitzen protocols per comunicar-se entre si. A continuació, us oferim unes breus descripcions dels protocols de passarel•la **TCP/IP** d'ús més freqüent:

Protocol HELLO (HELLO)
El **HELLO** és un protocol que utilitzen les passarel•les interiors per comunicar-se entre si. El **HELLO** calcula el camí d'accés més curt a altres xarxes determinant el camí d'accés que té el mínim temps de retard.

Protocol d'informació d'encaminament (RIP)
El **Protocol d'informació d'encaminament** és un protocol que utilitzen les passarel•les interiors per comunicar-se entre si. Igual que el **Protocol HELLO**, el **RIP** calcula el camí d'accés més curt a altres xarxes. A diferència del **HELLO**, el **RIP** estima la distància no per temps de retard, sinó per recompte de salts. Com que el daemon **gated** emmagatzema totes les mètriques internament com a retards de temps, converteix els recomptes de salts del **RIP** en retards de temps.

Routing Information Protocol Next Generation
El **RIPng** és el protocol **RIP** millorat per donar suport a l'**IPv6**.

Open Shortest Path First (OSPF)
L'**OPSF** és un protocol que utilitzen les passarel•les interiors per comunicar-se entre si. És un protocol d'estat d'enllaç que està millor adaptat que el **RIP** per a les xarxes complexes amb molts encaminadors. Proporciona un encaminament de múltiples camins d'accés d'igual cost.

Exterior Gateway Protocol (EGP)
Les passarel•les exteriors poden utilitzar el **Exterior Gateway Protocol** per comunicar-se entre si. L'**EGP** no calcula el camí d'accés més curt a altres xarxes. En comptes d'això, simplement indica si es pot accedir o no a una determinada xarxa.

Border Gateway Protocol (BGP)
Les passarel•les exteriors poden utilitzar aquest protocol per comunicar-se entre si. Intercanvia informació d'accessibilitat entre sistemes autònoms, però proporciona més funcions que l'**EGP**. El **BGP** utilitza atributs de camí d'accés per proporcionar més informació sobre cada camí com a ajuda a l'hora de seleccionar el millor camí.

Border Gateway Protocol 4+
El **BGP4+** és el protocol **BGP** versió 4, que dóna suport a l'**IPv6** i té altres millores sobre les versions anteriors del protocol.

Intermediate System to Intermediate System (IS-IS)
Les passarel•les interiors utilitzen el protocol **IS-IS** per comunicar-se entre si. És un protocol d'estat d'enllaç que pot encaminar paquets IP i ISO/CLNP i, igual que l'**OSPF**, utilitza un algorisme de "primer el camí d'accés més curt" per determinar els camins.

Consideracions sobre les passarel•les

Realitzeu aquestes accions abans de configurar la passarel•la.

Abans de configurar les passarel•les de la xarxa, primer heu de fer el següent:

1. Considereu el nombre de passarel•les que utilitzareu. El nombre de passarel•les que haureu de configurar dependrà:
   - Del nombre de xarxes que voleu connectar.
   - De com voleu connectar les xarxes.
   - Del nivell d'activitat a les xarxes connectades.

Per exemple, suposeu que tots els usuaris de la Xarxa 1, Xarxa 2, i Xarxa 3 necessiten comunicar-se entre si.

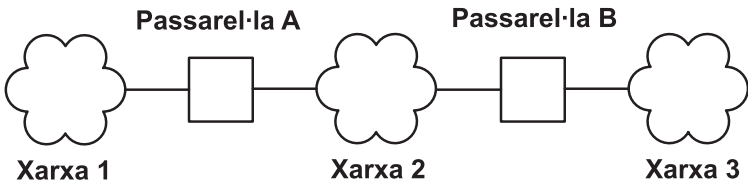


Figura 24. Configuració de passarel•la simple

Aquesta il•lustració conté tres núvols de xarxa numerats un, dos i tres. Les xarxes una i dues estan connectades amb la passarel•la A.Les xarxes dues i tres estan connectades amb la passarel•la B.

Per connectar la Xarxa 1 directament a la Xarxa 2, hauríeu d'utilitzar una passarel•la senzilla (Passarel•la A). Per connectar la Xarxa 2 directament a la Xarxa 3, hauríeu d'utilitzar una altra passarel•la (Passarel•la B). Ara, si suposem que estan definits els camins adequats, tots els usuaris de les tres xarxes es poden comunicar.

No obstant això, si la Xarxa 2 està molt ocupada, la comunicació entre la Xarxa 1 i la Xarxa 3 pot patir retards inacceptables. A més, si la major part de la comunicació entre xarxes té lloc entre la Xarxa 1 i la Xarxa 3, és possible que vulgueu connectar la Xarxa 1 directament a la Xarxa 3. Per fer això, podríeu utilitzar un parell addicional de passarel•les, la Passarel•la C (a la Xarxa 1) i la Passarel•la D (a la Xarxa 3), amb una connexió directa entre aquestes dues passarel•les addicionals. Tanmateix, això pot ser una solució ineficaç, ja que una passarel•la pot connectar més de dues xarxes.

Una solució més eficaç seria connectar la Passarel•la A a la Passarel•la B directament, així com a la Xarxa 2. Això requeriria un segon adaptador de xarxa tant a la Passarel•la A com a la Passarel•la B. En general, el nombre de xarxes que connecteu a través d'una sola passarel•la està limitat pel nombre de targetes adaptadores de xarxa a les quals pot donar suport la màquina de passarel•la.

2. Decidiu el tipus d'encaminament que voleu utilitzar.

   Si la vostra xarxa és petita i la seva configuració no canvia gairebé mai, probablement voleu utilitzar un encaminament estàtic. Però si teniu una xarxa gran la configuració de la qual canvia sovint, probablement voleu utilitzar un encaminament dinàmic. Podeu decidir utilitzar una combinació d'encaminament estàtic i dinàmic. És a dir, és possible que vulgueu proporcionar definicions estàtiques a uns quants camins específics, mentre permeteu que els daemons actualitzin altres camins. Els encaminaments estàtics que creeu no s'anuncien a les altres passarel•les i els daemons d'encaminament no els actualitzen.

3. Si feu servir un encaminament dinàmic, trieu el daemon d'encaminament d'acord amb el tipus de passarel•la que necessiteu i els protocols als quals ha de donar suport la vostra passarel•la. Si la passarel•la és una passarel•la interior i només necessita donar suport al **RIP**, trieu el daemon **routed**. Si la passarel•la ha de donar suport a algun altre protocol, o si és una passarel•la exterior, trieu el daemon **gated**.

   Nota: Es poden produir resultats imprevisibles si s'executen els daemons **gated** i **routed** simultàniament al mateix amfitrió.

Configuració d'una passarel•la

Per configurar una màquina perquè actuï com una passarel•la, utilitzeu aquestes instruccions.

Perquè estigui més clar, aquest procediment pressuposa que la màquina de passarel•la connecta dues xarxes i que ja ha estat configurada mínimament en una de les xarxes.

1. Instal•leu i configureu el segon adaptador de xarxa, si encara no ho heu fet. (Consulteu els apartats “Instal•lació d'un adaptador de xarxa” a la pàgina 161 i “Configuració i gestió d'adaptadors” a la pàgina 161.)

2. Trieu una adreça IP per a la segona interfície de xarxa i, a continuació, configureu la interfície de xarxa seguint les instruccions de l'apartat “Gestió de la interfície de xarxa” a la pàgina 167.
3. Afegiu un camí a la segona xarxa.
4. Per utilitzar una màquina com un encaminador d'internetwork en xarxes **TCP/IP**, escriviu:
   ```
   no -o ipforwarding=1
   ```

La màquina de passarel•la ara pot accedir a les dues xarxes a les quals està connectada directament.

1. Si voleu utilitzar un encaminament estàtic per comunicar amb amfitrions o xarxes més enllà d'aquestes dues xarxes, afegiu els camins que vulgueu.
2. Si voleu utilitzar un encaminament dinàmic, seguiu les instruccions dels apartats “Configuració del daemon routed” a la pàgina 362 o “Configuració del daemon gated” a la pàgina 363. Si la vostra internetwork és per accedir a Internet, també hauríeu de seguir les instruccions de l'apartat “Números de sistema autònom” a la pàgina 365.

Taula 78. Tasques de la configuració de passarel•les

Tasca	Camí d'accés ràpid de la SMIT	Fitxer d'ordres
Visualització de la taula d'encaminament	`smit lsroute`	**netstat -rn**[1]
Addició d'un encaminament estàtic	`smit mkroute`	**route add** *destinació passarel•la*[2]
Eliminació d'un encaminament estàtic	`smit rmroute`	**route delete** *destinació passarel•la*[2]
Llançament de la taula d'encaminament	`smit fshrttbl`	**route flush**

Nota:

1. La taula està dividida en columnes per adreça de destinació, adreça de passarel•la, senyaladors, recompte de referència (recompte de salts), i interfície de xarxa. (Per obtenir una descripció detallada de cadascuna d'aquestes columnes, vegeu l'ordre **netstat** a la publicació *Commands Reference, Volume 4*.) Si les trames no arriben a la seva destinació i les taules d'encaminament indiquen el camí correcte, és possible que existeixi alguna o algunes de les condicions següents:
   - La xarxa falla.
   - L'amfitrió remot o la passarel•la falla.
   - L'amfitrió remot o la passarel•la no està activat o no està a punt per rebre trames.
   - L'amfitrió remot no té cap camí de tornada a la xarxa d'origen.
2. El valor *destinació* és l'adreça de decimal amb punt o el nom simbòlic de la xarxa o l'amfitrió de destinació, i el valor *passarel•la* és l'adreça de decimal amb punt o el nom simbòlic de la passarel•la. (Un camí per defecte especifica 0 com la destinació.)

Restriccions d'ús dels camins

Es poden restringir els camins de forma que només els puguin utilitzar alguns usuaris. Les restriccions es basen en els ID de grup primari dels usuaris.

Mitjançant l'ordre **route**, podeu especificar una llista de fins a 32 ID de grup que podran o no utilitzar un camí. Si la llista és de grups permesos, tot usuari que pertanyi a un grup de la llista podrà utilitzar el camí. Si la llista és de grups no permesos, només els usuaris que no pertanyin a cap dels grups de la llista podran utilitzar el camí. L'usuari root pot utilitzar qualsevol camí.

Els grups també es poden associar amb una interfície mitjançant l'ordre **ifconfig**. En aquest cas, un paquet reenviable pot utilitzar qualsevol camí permès per als grups associats amb la seva interfície d'entrada.

Si hi ha dos o més camins cap a la mateixa destinació, qualsevol readreçament ICMP que es rebi per a aquesta destinació s'ignorarà i no es realitzarà el descobriment de la MTU del camí d'accés en aquests camins.

Detecció de passarel•les en desús

Es pot configurar un amfitrió perquè detecti si una passarel•la que està utilitzant es troba inactiva i, en conseqüència, poder ajustar la seva taula d'encaminament.

Si l'opció de xarxa **-passive_dgd** és 1, la detecció de passarel•les en desús passives s'habilita per a tot el sistema. Si no es rep cap resposta per a **dgd_packets_lost** sol•licituds **ARP** consecutives a una passarel•la, aquesta passarel•la es pressuposa inactiva i les mètriques de distància (també anomenades *recompte de salts* o *cost*) de tots els camins que utilitzen aquesta passarel•la s'augmenten al màxim valor possible. Després que hagin passat **dgd_retry_time** minuts, els costs del camí es restauren als seus valors configurats per l'usuari. L'amfitrió també actua en funció de la fallada de les connexions **TCP**. Si es perden **dgd_packets_lost** paquets **TCP** consecutius, l'entrada de l'**ARP** per a la passarel•la en ús se suprimeix i la connexió **TCP** intenta el següent camí millor. La propera vegada que s'utilitzi la passarel•la, tindran lloc les accions anteriors si la passarel•la realment està inactiva. Es poden configurar els paràmetres **passive_dgd**, **dgd_packets_lost** i **dgd_retry_time** mitjançant l'ordre **no**.

Els amfitrions també es poden configurar per utilitzar la detecció de passarel•les en desús actives sobre una base per camí amb el senyalador **-active_dgd** de l'ordre **route**. La detecció de passarel•les en desús actives efectua un ping en totes les passarel•les utilitzades pels camins per als quals està habilitada cada **dgd_ping_time** segons. Si no es rep cap resposta per part d'una passarel•la, se li efectua un ping més ràpidament fins a **dgd_packets_lost** vegades. Si es continua sense rebre cap resposta, s'augmenten els costs de tots els camins que utilitzen aquesta passarel•la. Es continua fent ping a la passarel•la i, si al final es rep una resposta, els costs dels camins es restauraran als valors configurats per l'usuari. El paràmetre **dgd_ping_time** es pot configurar mitjançant l'ordre **no**.

La detecció de passarel•les en desús és més útil per als amfitrios que utilitzen un encaminament estàtic que els que n'utilitzen un de dinàmic. La detecció de passarel•les en desús passives provoquen problemes de menor rendiment i es recomana utilitzar-la en qualsevol xarxa que tingui passarel•les redundants. No obstant això, la detecció de passarel•les en desús passives es realitza només sobre una base del millor esforç. Alguns protocols, com ara l'**UDP**, no proporcionen cap retroacció a l'amfitrió si la transmissió de dades falla, i en aquest cas la detecció de passarel•les en desús passives no pot dur a terme cap acció.

La detecció de passarel•les en desús actives és més útil quan un amfitrió ha de descobrir immediatament quan queda inactiva una passarel•la. Com que consulta a cada passarel•la per a la qual està habilitada cada pocs segons, hi ha una mica d'excés d'utilització de la xarxa associada a aquest ús. La detecció de passarel•les en desús actives es recomana només per a amfitrions que proporcionen serveis bàsics i en xarxes amb un nombre limitat d'amfitrions.

Nota: La detecció de passarel•les en desús i els protocols d'encaminament utilitzats pels dimonis **gated** i **routed** realitzen una funció similar descobrint canvis en la configuració de xarxa i ajustant la taula d'encaminament en conseqüència. No obstant això, utilitzen mecanismes diferents per fer-ho i, si s'executen alhora, poden entrar en conflicte entre si. Per aquest motiu, la detecció de passarel•les en desús no s'ha d'utilitzar en sistemes que executen els dimonis**gated** o **routed**.

Quan la detecció de passarel•les en desús detecta que la ruta primària torna a estar en línia i el paràmetre **dgd_flush_cached_route** està habilitat, les rutes actuals emmagatzemades en memòria cau de totes les connexión s'eliminen. Les rutes de totes les connexions actives actuals es validen una altra vegada per trobar el millor camí per enviar dades. Es pot configurar el paràmetre **dgd_flush_cached_route** mitjançant l'ordre **no**. Per defecte, el paràmetre **dgd_flush_cached_route** està deshabilitat.

Nota: El paràmetre **dgd_flush_cached_route** només ha d'habilitar-se en entorns de xarxa estables. Altrament, podríen haver-hi problemes de rendiment greus a causa d'encaminadors erronis o inestables, els quals poden causar detecció de passarel•les en desús per actualitzar freqüentment les taules d'encaminament. La neteja freqüent de rutes emmagatzemades en memòria cau també pot ser car.

Clonatge de camins

El clonatge de camins permet que es creï un camí d'amfitrió per a cada amfitrió amb què es comunica un sistema.

Quan s'està a punt d'enviar el trànsit de xarxa, es realitza una cerca de la taula d'encaminament per cercar un camí fins aquell amfitrió. Si es troba un camí d'amfitrió específic, s'utilitzarà. Si no es troba cap camí d'amfitrió específic, es pot cercar un camí de xarxa o el camí per defecte. Si el camí que es troba té establert el senyalador de clonatge, 'c', es crearà un camí d'amfitrió per a la destinació mitjançant la passarel•la del camí que s'està clonant. Les cerques subseqüents a la taula d'encaminament per a aquesta destinació cercaran el camí de l'amfitrió clonat. Els camins clonats tenen establerts el senyalador 'W'. Aquests camins esgotaran el temps d'espera i se suprimiran de la taula d'encaminament si no s'utilitzen durant els minuts que indica *caducitat_camí*. Podeu modificar *caducitat_camí* mitjançant l'ordre **no**.

La característica de clonatge de camins s'utilitza principalment amb el protocol de descobriment de la MTU del camí d'accés de l'AIX per permetre que efectuï un seguiment de la informació de la MTU del camí d'accés per a cada destinació amb què es comuniqui. Si les opcions de xarxa **tcp_pmtu_discover** o **udp_pmtu_discover** (que s'estableixen amb l'ordre **no**) són 1, el senyalador de clonatge s'activa per a tots els camins de xarxa del sistema. El descobriment de la MTU del camí d'accés està habilitat per defecte.

Nota: Per afegir manualment una entrada de ruta clonada, podeu manipular la taula de ruta amb l'ordre **route**.

Informació relacionada:

ordre de ruta

Extracció dinàmica d'un camí

Si utilitzeu el daemon **routed**, *no* se substituirà un camí suprimit per informació RIP d'entrada (perquè s'utilitza l'ioctl).

Si utilitzeu el daemon **gated** i no s'utilitza el senyalador **-n**, el camí suprimit manualment *sí* que se substituirà pel camí tal com s'ha descobert en la informació RIP d'entrada.

Configuració del daemon routed

Seguiu aquests passos per configurar el daemon **routed**.

Per configurar el daemon **routed**:

1. Elimineu el símbol de comentari (#) i modifiqueu la clàusula del routed a la seqüència de l'intèrpret d'ordres `/etc/rc.tcpip`. Així s'inicia automàticament el daemon **routed** amb cada engegada del sistema.
   - Especifiqueu si voleu que la passarel•la s'executi en modalitat activa (senyalador **-s**) o passiva (senyalador **-q**).
   - Especifiqueu si voleu el traçat de paquets activat o desactivat (senyalador **-t**). El traçat de paquets també es pot activar després que ja s'hagi iniciat el daemon **routed** utilitzant l'ordre **kill** per enviar un senyal **SIGUSR1** al daemon. Aquest senyal també es pot utilitzar per incrementar el nivell de traçat en quatre nivells. A més, el traçat de paquets es pot desactivar mentre el daemon **routed** es troba en execució utilitzant l'ordre **kill** per enviar un senyal **SIGUSR2** al daemon. Per obtenir més informació, vegeu el daemon **routed** i l'ordre **kill**.
   - Especifiqueu si voleu la depuració activada o desactivada (senyalador **-d**). Si utilitzeu aquest senyalador, especifiqueu a quin fitxer de registre voleu tenir emmagatzemada la informació de depuració, o bé trieu que es dirigeixi a la pantalla de la consola.
   - Especifiqueu si esteu executant el daemon **routed** en una passarel•la (senyalador **-g**).

     Nota: Un amfitrió que no sigui una passarel•la pot executar el daemon **routed**, però cal executar-lo en modalitat passiva.

2. Identifiqueu les xarxes conegudes llistant-les al fitxer /etc/networks. Per obtenir més informació, consulteu l'apartat Networks File Format for TCP/IP de la publicació *Files Reference*. Hi ha un fitxer networks de mostra ubicat al directori /usr/samples/tcpip.
3. Configureu els camins al fitxer /etc/gateways per a les passarel•les conegudes que no estan directament connectades a la vostra xarxa. Consulteu l'apartat Gateways File Format for TCP/IP de la publicació *Files Reference* per obtenir exemples detallats de les entrades del fitxer /etc/gateways. Hi ha un fitxer gateways de mostra ubicat al directori /usr/samples/tcpip.

Atenció: No executeu el daemon **routed** i el daemon **gated** a la mateixa màquina. Poden produir-se resultats imprevisibles.

Configuració del daemon gated

En la configuració del daemon **gated**, heu de decidir quins protocols de passarel•la són els més adequats per al vostre sistema.

Per configurar el daemon **gated**:

1. Decidiu quins protocols de passarel•la són els més adequats per al vostre sistema. Les opcions de protocol d'encaminament són l'**EGP**, el **BGP**, el **RIP**, el **RIPng**, el **HELLO**, l'**OSPF**, l'**ICMP/Descobriment d'encaminaments**, i l'**IS-IS**. També podeu utilitzar l'**SNMP**, un protocol que us permet canviar o mostrar informació de gestió d'un element de xarxa des d'un amfitrió remot.

   Nota: Utilitzeu l'**EGP**, el **BGP** or el **BGP4**+ per anunciar adreces de xarxes d'un sistema autònom a les passarel•les d'altres sistemes autònoms. Si esteu a Internet, cal utilitzar l'**EGP**, el **BGP** o el **BGP4+** per anunciar l'accessibilitat de la xarxa al sistema de passarel•la core. Utilitzeu els protocols d'encaminament interiors per anunciar la informació d'accessibilitat dins d'un sistema autònom.
2. Identifiqueu les xarxes conegudes llistant-les al fitxer /etc/networks. Per obtenir més informació, consulteu l'apartat Networks File Format for TCP/IP de la publicació *Files Reference*. Hi ha un fitxer networks de mostra ubicat al directori /usr/samples/tcpip.
3. Editeu el fitxer /etc/gated.conf per reflectir la configuració desitjada del daemon **gated**.

   Nota: La versió de **gated** a l'AIX 4.3.2 i superior és 3.5.9. La sintaxi del fitxer /etc/gated.conf ha canviat. Els exemples que es proporcionen més avall són per a la versió 3.5.9 de **gated**. Per configurar el fitxer /etc/gated.conf per a versions anteriors a l'AIX 4.3.2, utilitzeu la sintaxi proporcionada al mateix fitxer /etc/gated.conf.

   a. Especifiqueu el nivell de sortida de traça que voleu. Si es necessita la traça abans d'analitzar el fitxer gated.conf, utilitzeu el senyalador **-t** per activar la traça quan s'iniciï el daemon. Per obtenir més informació, vegeu el daemon gated a la publicació *Commands Reference, Volume 2*.
   b. Especifiqueu els protocols d'encaminament que voleu utilitzar. Cada protocol té la seva pròpia sentència de protocol. Elimineu els símbols de comentari (#) i modifiqueu les sentències corresponents als protocols que voleu utilitzar.
      - Si utilitzeu l'**EGP**:
        - Configureu la clàusula autonomoussystem de l'**EGP**. Aconseguiu un número de sistema autònom de part de l'autorització d'Internet si esteu a Internet, o si no, assigneu un número de sistema autònom tenint en consideració els números de sistema autònom dels altres sistemes de la xarxa.
        - Establiu la sentència de l'**EGP** en yes.
        - Configureu la clàusula group per a cada sistema autònom.
        - Configureu una clàusula neighbor per a cada veïnatge d'aquest sistema autònom. Per exemple:

```
autonomoussystem 283 ;

egp yes {
        group maxup 1 {
             neighbor nogendefault 192.9.201.1 ;
```

```
                neighbor nogendefault 192.9.201.2 ;
        } ;
        group {
                neighbor 192.10.201.1 ;
                neighbor 192.10.201.2 ;
        } ;
} ;
```

- Si utilitzeu el **RIP** o el **HELLO**:
  - Estabiu la sentència del **RIP** o del **HELLO** en yes.
  - Especifiqueu nobroadcast a la sentència del **RIP** o del **HELLO** si voleu que la passarel•la només accepti informació d'encaminament, i no enviï informació. O bé especifiqueu broadcast a la sentència del **RIP** o del **HELLO** si voleu que la passarel•la enviï i accepti informació d'encaminament.
  - Si voleu que la passarel•la enviï directament a les passarel•les d'origen, utilitzeu la sentència sourcegateways. Especifiqueu un nom de passarel•la o una adreça d'Internet en decimal amb punt a la clàusula sourcegateways. Per exemple:

    ```
    # Enviar directament a passarel•les específiques

    rip/hello yes {
              sourcegateways
                    101.25.32.1
                    101.25.32.2 ;
    } ;
    ```

    L'exemple següent mostra la stanza del **RIP**/**HELLO** al fitxer gated.conf d'una màquina que no envia paquets **RIP**, i no rep paquets **RIP** a la seva interfície tr0.

    ```
    rip/hello nobroadcast {
             interface tr0 noripin ;
    } ;
    ```

- Si utilitzeu el **BGP**:
  - Configureu la clàusula autonomoussystem del **BGP**. Aconseguiu un número de sistema autònom de part de l'autorització d'Internet si esteu a Internet, o si no, assigneu un número de sistema autònom tenint en consideració els números de sistema autònom dels altres sistemes de la xarxa.
  - Estabiu la sentència del **BGP** en yes.
  - Configureu una clàusula peer per a cada veïnatge d'aquest sistema autònom. Per exemple:

    ```
    # Realitzar totes les operacions BGP

    bgp yes {
            peer 192.9.201.1 ;
    } ;
    ```

- Si utilitzeu l'**SNMP**:
  - Estabiu la sentència de l'**SNMP** en yes.

    ```
    snmp yes ;
    ```

Configuració del daemon gated per executar l'IPv6:

Utilitzeu aquest procediment per configurar el daemon **gated** per executar l'**Internet Protocol versió 6 (IPv6)**.

Per configurar el daemon **gated** perquè s'executi amb l'**Internet Protocol versió 6 (IPv6)**, assegureu-vos primer que el vostre sistema s'hagi configurat per a l'**IPv6** i l'encaminament de l'**IPv6**:

1. Executeu **autoconf6** per configurar automàticament les vostres interfícies per a l'**IPv6**.
2. Configureu adreces locals de lloc per a cada interfície **IPv6** on voleu utilitzar l'encaminament de l'**IPv6** mitjançant l'ordre següent:

   ```
   ifconfig interfície inet6 fec0:n::adreça/64 alias
   ```

en què

interfície
És el nom de la interfície, com ara `tr0` o `en0`.

n És un nombre decimal; per exemple, `11`

adreça És la part de l'adreça d'interfície **IPv6** que segueix els dobles dos punts; per exemple, amb l'adreça **IPv6** `fe80::204:acff:fe86:298d`, l'entrada de l'*adreça* seria `204:acff:fe86:298d`.

Nota: Podeu utilitzar l'ordre **netstat -i** per veure què és la vostra adreça **IPv6** per a cada interfície configurada.

Si el Token Ring `tr0` té una adreça **IPv6** de `fe80::204:acff:fe86:298d`, executeu l'ordre següent:

```
ifconfig tr0 inet6 fec0:13::204:acff:fe86:298d/64 alias
```

3. Activeu el reenviament d'**IPv6** amb l'ordre següent:

   ```
   no -o ip6forwarding=1
   ```

4. Inicieu **ndpd-router** amb l'ordre següent:

   ```
   ndpd-router -g
   ```

   Consulteu **ndpd-router** a *Commands Reference, Volume 4* per determinar els senyaladors que cal utilitzar per la configuració de la xarxa.

   Iniciar **ndpd-router** permet que el sistema actuï com un encaminador per al **Protocol de descobriment de veïnatge**. Els encaminadors del **Protocol de descobriment de veïnatge** informen als amfitrions de descobriment de veïnatge amb informació d'encaminament de manera que els amfitrions puguin encaminar paquets **IPv6**.

   Els amfitrions de la xarxa que vulgueu que formin part de la xarxa **IPv6** han d'executar **ndpd-host**. Els amfitrions de la xarxa que executen **ndpd-host** es reconeixeran com a part d'una xarxa **IPv6** i utilitzaran el **Protocol de descobriment de veïnatge**, que els permet determinar i supervisar adreces de capa d'enllaç tant per permetre l'encaminament de veïnatge com per cercar encaminadors de veïnatge per reenviar paquets.

   Consulteu **ndpd-router** i **ndpd-host** in *Commands Reference, Volume 4* o llegiu RFC 1970, *Neighbor Discovery* per obtenir més informació.

5. A continuació, configureu el daemon **gated**:
   a. Decidiu quins protocols de passarel•la **IPv6** són els més adequats per al vostre sistema. Les opcions de protocols d'encaminament **IPv6** són el **Border Gateway Protocol** millorat per a l'**IPv6** (**BGP4+**) i el **Routing Information Protocol Next Generation** (**RIPng**).
   b. Editeu el fitxer `/etc/gated.conf` per reflectir la configuració desitjada del daemon **gated**.

      Nota: L'AIX 4.3.2 i posterior executen **gated** versió 3.5.9. La sintaxi del fitxer `gated.conf` ha canviat lleugerament de les versions anteriors. Llegiu la documentació de `gated.conf` a a *Files Reference* o utilitzeu el fitxer d'exemple subministrat al directori `/usr/sample/tcpip` per veure la sintaxi correcta.

      Quan configureu el **BGP4+** o el **RIPng**, utilitzeu adreces **IPv6** on la sintaxi especifiqui una adreça IP.

      Nota: Per defecte, el **RIPng** difon de forma múltiple els seus paquets.

Un cop modificat el fitxer `/etc/gated.conf`, es pot iniciar el daemon **gated**.

Números de sistema autònom

Si utilitzeu l'**EGP** o el **BGP**, hauríeu d'obtenir un *número de sistema autònom* oficial per a la vostra passarel•la.

Per obtenir un número de sistema autònom oficial, poseu-vos en contacte amb el NIC a l'adreça d'Internet següent:

INFO@INTERNIC.NET

IPv6 mòbil

L'**IPv6** mòbil proporciona suport de mobilitat per a l'**IPv6**. Permet mantenir la mateixa adreça d'Internet a tot el món i permet que les aplicacions que utilitzen aquesta adreça mantinguin les connexions de la capa superior i de transport quan es canvien les ubicacions. Permet la mobilitat en suports d'emmagatzematge homogenis i heterogenis.

Per exemple, l'**IPv6** mòbil facilita el moviment de nodes des d'un segment Ethernet a una cel•la LAN sense fil mentre l'adreça IP del node mòbil roman sense canvis.

A l'**IPv6** mòbil, cada node mòbil s'identifica amb dues adreces IP: l'adreça d'inici i l'adreça d'atenció. L'adreça d'inici és una adreça IP permanent que identifica el node mòbil independentment de la seva ubicació. L'adreça d'atenció canvia a cada nou punt d'adjunció i proporciona informació sobre la situació actual del node mòbil. Quan un node mòbil arriba a una xarxa visitada, cal que adquireixi una adreça d'atenció, que s'utilitzarà mentre el node mòbil estigui en aquesta ubicació de la xarxa visitada. Pot utilitzar els mètodes del descobriment de veïnatge de l'**IPv6** per obtenir l'adreça d'atenció (consulteu l'apartat "Descobriment de veïnatge/autoconfiguració d'adreces sense estat" a la pàgina 126). És possible tant l'autoconfiguració sense estat com amb estat. També es pot configurar manualment l'adreça d'atenció. La forma d'adquisició de l'adreça d'atenció és irrellevant per a l'**IPv6** mòbil.

Com a mínim hi ha d'haver un agent d'inici configurat a la xarxa domèstica, i el node mòbil ha d'estar configurat per saber l'adreça IP del seu agent d'inici. El node mòbil envia a l'agent d'inici un paquet que conté una actualització de vinculació. L'agent d'inici rep el paquet i fa una associació entre l'adreça d'inici al node mòbil i l'adreça d'atenció rebuda. L'agent d'inici respon amb un paquet que conté un reconeixement de vinculació.

L'agent d'inici manté una memòria cau de vinculació que conté associacions entre les adreces d'inici i les adreces d'atenció dels nodes mòbils als quals presta servei. L'agent d'inici interceptarà els paquets destinats a l'adreça d'inici i els reenviarà als nodes mòbils. Aleshores, un node mòbil enviarà una actualització de vinculació al node corresponsal informant-lo de la seva adreça d'atenció, i el node corresponsal crearà una entrada de memòria cau de vinculació per poder enviar el trànsit futur directament al node mòbil a la seva adreça d'atenció.

El suport de mobilitat de l'AIX proporciona les funcions bàsiques següents:

Com a node d'**Agent d'inici**:

- Mantenir una entrada a la seva memòria cau de vinculació per a cada node mòbil al qual presta servei.
- Interceptar paquets adreçats a un node mòbil al qual està prestant servei actualment com l'agent d'inici, a l'enllaç d'inici d'aquest node mòbil, mentre el node mòbil es troba fora de casa.
- Encapsular aquests paquets interceptats per transmetre'ls a través d'un túnel a l'adreça d'atenció primària del node mòbil indicada a la seva vinculació a la memòria cau de vinculació de l'agent d'inici.
- Tornar una opció de reconeixement de vinculació en resposta a l'opció d'actualització de vinculació rebuda amb el conjunt de bits de reconeixement.
- Processar la detecció d'adreces duplicades a l'adreça d'atenció del node mòbil per garantir que les adreces de l'**IPv6** són exclusives.
- Donar suport al descobriment dinàmic d'adreces de l'agent d'inici per assistir als nodes mòbils en el descobriment de les adreces dels agents d'inici.
- Donar suport a la recepció de sol•licitud de prefix mòbil i l'enviament d'anunci de prefix mòbil.

Com a node de **Corresponsal estacionari**:

- Processar una opció d'adreça d'inici rebuda a qualsevol paquet de l'**IPv6**.

- Processar una opció d'actualització de vinculació rebuda en un paquet i tornar una opció de reconeixement de vinculació si el bit de reconeixement (A) s'estableix a l'actualització de vinculació rebuda.
- Mantenir una memòria cau de vinculació de les vinculacions rebudes a les actualitzacions de vinculació acceptades.
- Enviar paquets mitjançant una capçalera d'encaminament quan hi ha una entrada de memòria cau de vinculació per a un node mòbil que conté l'adreça d'atenció actual del node mòbil.

Com a node d'**Encaminador** en una xarxa visitada pel node mòbil:
- Enviar una opció d'interval d'anunci als anuncis d'encaminador per ajudar a la detecció de moviment dels nodes mòbils. Es pot configurar amb el paràmetre **-m** al daemon **ndpd-router**.
- Donar suport a l'enviament d'anuncis d'encaminador de difusió múltiple no sol•licitats a la velocitat més ràpida descrita a l'RFC 2461. Es pot configurar amb els paràmetres **-m** i **-D** al daemon **ndpd-router**.
- Enviar una opció d'informació de l'agent d'inici (preferència i temps de vida de l'agent d'inici) als anuncis d'encaminador per ajudar als nodes mòbils a triar el seu agent d'inici. Es pot configurar amb el paràmetre **-H** al daemon **ndpd-router**.

Seguretat de l'IPv6 mòbil

Els missatges d'actualització de vinculació i de reconeixement de vinculació intercanviats entre el node mòbil i l'agent d'inici han d'estar protegits per la Seguretat IP mitjançant la protecció d'ESP (Encapsulating Security Payload) amb un algorisme d'autenticació de càrrega no NULL.

Per obtenir més informació sobre seguretat IP, consulteu l'apartat *Security*.

L'establiment de vinculació entre el node mòbil i el node corresponsal es protegeix mitjançant el procediment de capacitat d'encaminament de retorn. En aquest procediment, els missatges que s'intercanvien entre el node de l'agent d'inici i els nodes mòbils també estan protegits per la Seguretat IP mitjançant l'ESP. Com que els missatges d'actualització de vinculació i de reconeixement de vinculació intercanviats entre un node corresponsal i un node mòbil estan protegits pel procediment de capacitat d'encaminament de retorn, no hi ha cap requisit de Seguretat IP per als corresponsals. Però, si un corresponsal utilitza la Seguretat IP per restringir el seu accés, els missatges amb el protocol MH (135) han d'estar permesos.

Es poden definir túnels manualment o mitjançant l'IKE com a emissor de resposta (només està suportat el mode agressiu). Com a mínim, es definiran els següents túnels de Seguretat IP a l'agent d'inici mitjançant la capçalera ESP:
- un túnel en modalitat de transport amb el protocol MH (135) entre l'adreça IP de l'agent d'inici i l'adreça d'inici de cada node mòbil susceptible de ser enregistrat en aquest agent d'inici.
- un túnel en modalitat de túnel amb el protocol MH (135) entre qualsevol adreça IP i l'adreça d'inici de cada node mòbil susceptible de ser enregistrat en aquest agent d'inici.

Cal definir els túnels corresponents en els nodes mòbils.

Nota: Els missatges d'actualització de vinculació i de reconeixement de vinculació s'envien mitjançant una capçalera de mobilitat i han d'estar protegits per la Seguretat IP mitjançant la protecció d'ESP.

En les implementacions anteriors de l'IPv6 mòbil a l'AIX, es proporcionava suport per als nodes mòbils mitjançant paquets d'opció de destinació per enviar missatges d'actualització de vinculació. Aquests missatges podien estar protegits amb la Seguretat IP mitjançant una capçalera d'autenticació.

Perquè un agent d'inici o un node corresponsal accepti aquests missatges d'actualització de vinculació mitjançant una opció de destinació, editeu el fitxer `/etc/rc.mobip6` i habiliteu la variable **Enable_Draft13_Mobile** abans d'iniciar l'**IPv6** mòbil. En aquest cas, si utilitzeu la Seguretat IP per

protegir els missatges d'actualització de vinculació, heu de definir els túnels IKE o manuals en modalitat de transport al protocol 60, que protegirà els missatges de reconeixement i d'actualització de vinculació.

Perquè un agent d'inici o un node corresponsal accepti els missatges d'actualització de vinculació no protegits per la Seguretat IP, editeu el fitxer `/etc/rc.mobip6` i inhabiliteu la variable **Check_IPsec**. Aquest mètode no és recomanable perquè presenta una vulnerabilitat de seguretat significativa per la capacitat d'afectar l'encaminament de paquets adreçats a un node mòbil.

Configuració de l'IPv6 mòbil

Aquí s'introdueix la informació sobre la configuració de l'**IPv6** mòbil. Per utilitzar l'**IPv6** mòbil, primer heu d'instal•lar el catàleg de fitxers `bos.net.mobip6.rte`.

Per obtenir informació sobre la instal•lació de catàlegs de fitxers, consulteu l'apartat Installing optional software products and service updates de la publicació *Installation and migration*

Inici de l'IPv6 mòbil com a agent d'inici:

Utilitzeu aquest procediment per iniciar l'**IPv6** mòbil com a agent d'inici.

1. Definiu túnels IKE (fases 1 i 2) com a emissors de resposta mitjançant el protocol **ESP** o l'associació de Seguretat IP ESP manual entre l'adreça IP de l'agent d'inici i l'adreça d'inici de cada mòbil amb el qual es pot comunicar el corresponsal.
2. Habiliteu el sistema com un node corresponsal i agent d'inici de l'**IPv6** mòbil. A la línia d'ordres, escriviu `smit enable_mobip6_home_agent`.
3. Seleccioneu quan voleu tenir-ho habilitat.

Inici de l'IPv6 mòbil com a corresponsal:

Utilitzeu aquest procediment per iniciar l'IPv6 mòbil com a corresponsal.

1. Definiu túnels IKE (fases 1 i 2) com a emissors de resposta mitjançant el protocol **ESP** o l'associació de Seguretat IP ESP manual entre l'adreça IP de l'agent d'inici i l'adreça d'inici de cada mòbil amb el qual es pot comunicar el corresponsal.
2. Habiliteu el sistema com un node corresponsal de l'**IPv6** mòbil. A la línia d'ordres, escriviu `smit enable_mobip6_correspondent`.
3. Seleccioneu quan voleu tenir-ho habilitat.

Inici de l'IPv6 mòbil com a encaminador:

Utilitzeu aquest procediment per iniciar l'**IPv6** mòbil com a encaminador.

Executeu l'ordre següent per facilitar la detecció de moviment:

```
ndpd-router -m
```

Aturada de l'IPv6 mòbil:

Utilitzeu aquest procediment per aturar l'**IPv6** mòbil.

1. Escriviu `smit disable_mobip6` a la línia d'ordres.
2. Seleccioneu quan voleu que s'aturi l'**IPv6** mòbil.
3. Seleccioneu si voleu aturar el daemon **ndpd-router**.
4. Seleccioneu si voleu inhabilitar el reenviament de l'**IPv6**.

Resolució de problemes de l'IPv6 mòbil

Utilitzeu l'ordre **mobip6ctrl -b** per solucionar els problemes de l'**IPv6** mòbil.

1. Per obtenir els estats de vinculació executeu el següent:

```
mobip6ctrl -b
```

2. Consulteu l'apartat "Resolució de problemes del TCP/IP" a la pàgina 419 per obtenir informació sobre l'ús dels programes d'utilitat de resolució de problemes del **TCP/IP**.

Adreça IP virtual

Una adreça IP virtual elimina la dependència d'un amfitrió de les interfícies de xarxa individuals.

Els paquets d'entrada s'envien a l'adreça VIPA del sistema, però tots els paquets es desplacen a través de les interfícies de xarxa reals.

Anteriorment, si una interfície fallava, es perdien totes les connexions a aquella interfície. Amb una VIPA al vostre sistema i protocols d'encaminament dins la xarxa que proporcionin un reencaminament automàtic, el restabliment després de les fallades es produeix sense interrupció de les connexions d'usuari existents que utilitzen la interfície virtual perquè els paquets puguin arribar a través d'una altra interfície física. Els sistemes que executen una VIPA estan molt més disponibles perquè les caigudes d'adaptador ja no afecten les connexions actives. Com que hi ha diversos adaptadors físics per portar el trànsit IP del sistema, la càrrega general no es concentra en un sol adaptador i la subxarxa associada.

La funció VIPA de l'AIX és transparent per a l'equip de la xarxa. No es necessita cap equip de xarxa especial ni cap altre maquinari. Per implementar una VIPA, cal que tingueu els elements següents:

- dos o més interfícies IP existents de qualsevol tipus físic en diferents subxarxes que es connectin a la la xarxa corporativa
- protocols d'encaminament IP en execució amb la xarxa corporativa

Configuració d'una VIPA

Una VIPA es configura, igual que qualsevol interfície de xarxa IP, a la SMIT. A més, podeu especificar un grup d'interfícies mentre configureu una VIPA.

Quan es configura d'aquesta manera, per a totes les connexions de sortida iniciades per l'amfitrió de la VIPA a través d'aquestes interfície, que estan dissenyades per utilitzar una VIPA, l'adreça virtual passa a ser l'adreça d'origen ubicada a la capçalera de paquet **TCP/IP** dels paquets de sortida.

1. Per a una VIPA de l'IPv4, escriviu `smit mkinetvi` a la línia d'ordres. Per a una VIPA de l'IPv6, escriviu `smit mkinetvi6` a la línia d'ordres.
2. Empleneu tots els camps obligatoris. Per obtenir informació addicional, consulteu "Entorn VIPA de mostra" a la pàgina 370. Premeu Intro.

Addició d'un adaptador a una VIPA

Utilitzeu aquest procediment per afegir un adaptador a una adreça IP virtual (VIPA).

Per afegir un adaptador a la vostra interfície VIPA, seguiu aquests passos:

1. Escriviu `smit chvi` a la línia d'ordres.
2. Seleccioneu la VIPA a la qual voleu afegir un adaptador i feu clic a Intro.
3. Especifiqueu l'adaptador que voleu afegir al camp **Nom(s) d'interfície**.
4. Escriviu `AFEGIR` al camp **AFEGIR/ELIMINAR interfície(s)** i feu clic a Intro.

Eliminació d'un adaptador d'una VIPA

Utilitzeu aquest procediment per eliminar un adaptador d'una adreça IP virtual (VIPA).

Per eliminar un adaptador d'una VIPA, seguiu aquests passos:

1. Escriviu `smit chvi` a la línia d'ordres.
2. Seleccioneu la VIPA de la qual voleu eliminar un adaptador i feu clic a Intro.
3. Especifiqueu l'adaptador que voleu eliminar al camp **Nom(s) d'interfície**.
4. Escriviu `ELIMINAR` al camp **AFEGIR/ELIMINAR interfície(s)** i feu clic a Intro.

Entorn VIPA de mostra

L'entorn VIPA de mostra següent amb connexions Ethernet implica un sistema amb una adreça IP virtual i dues connexions físiques.

Un sistema té una adreça IP virtual, `vi0`, de `10.68.6.1`, i dues connexions físiques, `en1` amb l'adreça IP `10.68.1.1` i `en5` amb l'adreça IP `10.68.5.1`. En aquest exemple, ambdues connexions físiques són Ethernet, però tota mescla d'interfícies IP, com ara Token-Ring o FDDI, estaria suportada mentre les subxarxes estiguessin connectades al final a la xarxa corporativa més gran i mentre els encaminadors corporatius les coneguessin.

L'execució de l'ordre **lsattr -El vi0** genera els resultats següents:

```
netaddr          10.68.6.1      N/D                                          Cert
state            activat             Interfície de xarxa Ethernet estàndard         Cert
netmask          255.255.255.0  Grandària màxima de paquet IP per a aquest dispositiu      Cert
netaddr6                        Grandària màxima de paquet IP per a xarxes remotes Cert
alias6                          Adreça d'Internet                             Cert
prefixlen                       Estat d'interfície actual                     Cert
alias4                          Encapsulació de nivell d'enllaç de cua          Cert
interface_names  en1,en5        Interfícies que usen l'adreça virtual         Cert
```

L'execució de l'ordre **ifconfig vi0** genera els resultats següents:

```
vi0: flags=84000041<UP,RUNNING,64BIT>
       inet 10.68.6.1 netmask 0xffffff00
       iflist : en1 en5
```

L'execució de l'ordre **netstat -rn** genera els resultats següents:

```
Taules d'encaminament
Destinació       Passarel•la       Senyaladors     Refs    Ús    Si     Grups exp PMTU

Arbre de camí per a la família de protocols 2 (Internet):
default           10.68.1.2      UG        3      1055   en1     -   -
10.68.1/24        10.68.1.1      U         0      665    en1     -   -
10.68.5/24        10.68.5.1      U         0      1216   en5     -   -
127/8             127.0.0.1      U         4      236    lo0     -   -
10.68.6.1         127.0.0.1      UH        0      0      lo0     -   -
```

Els paquets de sortida que no tenen establerta cap adreça d'origen i que estan encaminats a través de les interfícies `en1` i `en5` tindran l'adreça d'origen establerta en l'adreça virtual (`10.68.6.1`). Els paquets d'entrada estan encaminats a l'adreça VIPA (`10.68.6.1`) anunciada a la xarxa. Com que `vi0` és virtual (és a dir, no està associada a cap dispositiu) no hauria de tenir cap entrada a la taula d'encaminament de tot el sistema visualitzada mitjançant l'ordre **netstat -rn**. Això significa que no s'afegeix cap camí d'interfície quan la interfície es configura a la SMIT.

Si una de les interfícies físiques, una adjunció de xarxa o un camí d'accés de xarxa falla, els protocols de xarxa encaminen a l'altra interfície física del mateix sistema. Si un sistema remot fa un telnet a l'adreça `vi0`, els paquets adreçats a `vi0` poden arribar mitjançant `en1` o `en5`. Si `en1` està desactivada, per exemple, els paquets encara poden arribar per `en5`. Tingueu present que els protocols d'encaminament poden trigar en propagar els camins.

Quan s'utilitza la VIPA, els sistemes finals i els encaminadors intermediaris han de poder encaminar els paquets destinats per a la VIPA (`vi0`) a una de les interfícies físiques (`en1` o `en5`).

VIPA versus àlies

El concepte de VIPA és semblant al dels àlies IP excepte en que les adreces no estan associades amb una interfície de maquinari.

La VIPA ofereix diversos avantatges que no tenen els àlies IP:

- La VIPA ofereix un dispositiu virtual que es pot activar i desactivar independentment sense afectar les interfícies físiques.
- Les adreces VIPA es poden canviar mentre que els àlies només es poden afegir o suprimir.

Accés mitjançant l'adreça IP dels adaptadors reals

Després d'implementar una VIPA les interfícies individuals encara són accessibles per a altres sistemes. No obstant això, utilitzar les adreces IP reals per a sessions ping i telnet esquiva l'avantatge d'una comunicació independent dels adaptador físics. La VIPA oculta els errors d'adaptadors físics als clients remots. L'ús de les adreces reals reintrodueix la dependència dels adaptador físics.

Si el sistema remot contacta amb el sistema VIPA mitjançant l'adreça VIPA o si una aplicació del sistema VIPA inicia la comunicació amb un altre sistema, l'adreça VIPA s'utilitzarà com l'adreça IP d'origen del paquet. No obstant això, si el sistema remot inicia la sessió mitjançant l'adreça IP de la interfície real, aquesta adreça IP real serà l'adreça IP d'origen en els paquets de resposta. Hi ha una excepció. Per a les aplicacions que es vinculen a una interfície IP determinada, els paquets de sortida portaran l'adreça d'origen de la interfície a la qual estan vinculats.

VIPA i protocols d'encaminament

El daemon gated s'ha modificat per a la VIPA de forma que no afegeixi el camí d'interfície ni enviï anuncis a les interfícies virtuals.

El protocol **OSPF**, suportat pel gated, anunciarà la interfície virtual als encaminadors adjacents. Els altres amfitrions de la xarxa podran dialogar amb l'amfitrió VIPA a través de l'encaminador del primer salt.

Adreces VIPA múltiples

Es poden configurar interfícies virtuals múltiples. Les interfícies VIPA múltiples serien útils, per exemple, si els encaminadors de xarxa poguessin donar un tracte preferencial als paquets enviats a o des de certes adreces VIPA.

O bé, podeu utilitzar interfícies VIPA múltiples si vinculen aplicacions a una interfície VIPA específica. Per exemple, per executar múltiples servidors web per a múltiples empreses en una sola màquina, podeu configurar el següent:

- vi0 200.1.1.1 www.empresaA.com
- vi1 200.1.1.2 www.empresaB.com
- vi2 200.1.1.3 www.empresaC.com

EtherChannel i acumulació d'enllaços IEEE 802.3ad

L'EtherChannel i l'acumulació d'enllaços IEEE 802.3ad són tecnologies d'acumulació de ports d'una xarxa que permeten acumular junts diversos adaptadors Ethernet perquè formin un sol dispositiu pseudo-Ethernet.

Per exemple, `ent0` i `ent1` es poden acumular en un adaptador EtherChannel anomenat `en3` i la interfície `en3` es configuraria aleshores amb una adreça IP. El sistema considera aquests adaptadors agregats com un adaptador. Per tant, l'IP es configura a través d'ells com si es tractés d'un adaptador Ethernet qualsevol. D'altra banda, tots els adaptadors de l'EtherChannel o de l'acumulació d'enllaços tindran la mateixa adreça de maquinari (MAC), per tant, els sistemes remots els tractaran com si fossin un sol adaptador. Tant l'EtherChannel com l'acumulació d'enllaços IEEE 802.3ad requereixen suport per commutadors perquè aquestes dues tecnologies saben bé quins port de commutador han de tractar com un de sol.

Nota: El controlador d'EtherChannel assigna una adreça de control d'accés al medi (MAC) no vàlida, `02:00:00:00:00:00`, al port del canal inactiu de la configuració de l'adaptador Ethernet amfitrió (HEA). Aquesta adreça MAC no vàlida s'assigna quan es crea l'EtherChannel o quan els ports del HEA s'afegeixen al canal inactiu en temps d'execució. Durant la migració després d'un error o el restabliment

de l'EtherChannel, l'adreça MAC no vàlida s'intercanvia amb l'adreça MAC vàlida, i l'adreça MAC vàlida s'intercanvia amb l'adreça MAC no vàlida en temps d'execució.

El principal avantatge de l'EtherChannel i de l'acumulació d'enllaços IEEE 802.3ad és que tenen l'amplada de banda de xarxa de tots els adaptadors en una sola xarxa. Si un adaptador falla, el trànsit de la xarxa s'envia automàticament al següent adaptador disponible sense que ocasioni cap trastorn en les connexions d'usuari existents. L'adaptador tornarà a prestar servei automàticament a l'EtherChannel o a l'acumulació d'enllaços quan es recuperi.

Hi ha algunes diferències entre l'EtherChannel i l'acumulació d'enllaços IEEE 802.3ad. Considereu les diferències llistades a Taula 79 per determinar quina tecnologia best s'adapta millor les vostres necessitats.

Taula 79. Diferències entre EtherChannel i acumulació d'enllaços IEEE 802.3ad

EtherChannel	Acumulació d'enllaços IEEE 802.3ad
Requereix una configuració de commutadors.	Requereix una configuració de commutadors per intercanvi de LACPDU (unitats de dades del protocol de control d'acumulacions d'enllaços).
Els batecs no s'intercanvien entre el port del commutador i el port del sistema adjacent.	Els batecs (LACPDU) s'intercanvien at the interval en un interval que es defineix als estàndards de l'IEEE 802.3ad. Els batecs proporcionen protecció addicional en cas d'error.

La funcionalitat del Dynamic Adapter Membership està disponible a l'AIX. Podeu utilitzar aquesta funcionalitat per afegir o eliminar adaptadors d'un EtherChannel sense cap mena d'interrupció a les connexions dels usuaris.

Conceptes relacionats:

"Dynamic Adapter Membership" a la pàgina 383
Abans de l'AIX 5L Versió 5.2 amb el paquet de manteniment recomanat 5200-03, per poder afegir i eliminar un adaptador d'un EtherChannel, primer calia desconnectar-ne la interfície i interrompre temporalment tot el trànsit d'usuaris. Per tal de superar aquesta limitació, s'ha afegit el DAM (Dynamic Adapter Membership) a l'AIX 5L Versió 5.2 amb el paquet de manteniment recomanat 5200-03.

"EtherChannel"
Els adaptadors que pertanyen a un EtherChannel han d'estar connectats al mateix commutador habilitat per a utilitzar EtherChannel. Si els adaptadors estan connectats a commutadors diferents, han d'apilar-se i actuar com a un únic commutador.

"Configuració d'acumulacions d'enllaços IEEE" a la pàgina 386
L'IEEE 802.3ad és una forma estàndard de dur a terme una acumulació d'enllaços. El concepte és que funciona igual que l'EtherChannel en els diferents adaptadors Ethernet que s'hagin afegir a un sol adaptador virtual, proporcionant així una major amplada de banda i millor protecció contra els errors.

"Casos d'interoperabilitat" a la pàgina 390
Tingueu en compte els següents casos d'interoperabilitat quan configureu l'EtherChannel o amb l'acumulació d'enllaços IEEE 802.3ad.

EtherChannel

Els adaptadors que pertanyen a un EtherChannel han d'estar connectats al mateix commutador habilitat per a utilitzar EtherChannel. Si els adaptadors estan connectats a commutadors diferents, han d'apilar-se i actuar com a un únic commutador.

Heu de configurar manualment aquest commutador per tractar els ports que pertanyen a l'EtherChannel com un enllaç agregat. És possible que la documentació del vostre commutador faci referència a aquesta possibilitat com a *acumulació d'enllaços* o *trunking*.

Perquè l'EtherChannel funcioni correctament, el mecanisme de sondeig d'enllaços que verifica periòdicament l'estat de l'enllaç ha de estar habilitat a cada adaptador abans que es crei l'Etherchannel. El trànsit es distribueix a través dels adaptadors de la forma estàndard (en què l'adaptador a través del qual s'envien els paquets es tria en funció d'un algorisme) o segons una base de rotació de valors (en què els

paquets s'envien uniformement a través de tots els adaptadors). El trànsit d'entrada es distribueix segons la configuració del commutador i no la controla la modalitat de funcionament de l'EtherChannel.

Podeu configurar diversos EtherChannel per sistema. Si tots els enllaços d'un Etherchannel estan connectats a un commutador únic i si el commutador es desconnecta o falla, es perd tot l'Etherchannel.Per solucionar aquest problema, existeix l'opció d'una còpia de seguretat, la qual manté el servei actiu quan l'EtherChannel falla. L'adaptador de còpia de seguretat i l'adaptador de l'EtherChannel han d'estar connectats a commutadors de xarxa diferents perquè aquesta configuració funcioni correctament. Si tots els adaptadors de l'EtherChannel fallessin, s'utilitzaria l'adaptador de còpia de seguretat per enviar i rebre tot el trànsit. Quan es restaura un enllaç de l'EtherChannel, el servei torna a l'EtherChannel.

Per exemple, es poden configurar els `ent0` i `ent1` com a adaptadors d'EtherChannel principals, i l'`ent2` com a adaptador de còpia de seguretat i crear un Etherchannel anomenat `en3`. De manera ideal, l'`ent0` i l'`ent1` estan connectats al mateix commutador habilitat per a l'EtherChannel i l'`ent2` està connectat a un commutador diferent. En aquest exemple, tot el trànsit enviat a través de l'`en3` (la interfície de l'Etherchannel) s'envia a través de l'`ent0` o l'`ent1` per defecte (depèn de l'esquema de distribució del paquet de l'EtherChannel), mentre que l'`ent2` roman inactiu. Si en qualsevol moment tant l'`ent0` com `ent1` fallen, tot el trànsit s'envia a través de l'adaptador de còpia de seguretat `ent2`. Quan es recupera l'`ent0` o l'`ent1`, es tornen a utilitzar per a tot el trànsit.

La Còpia de seguretat de la interfície de la xarxa, una modalitat d'operació disponible per a l'EtherChannel, protegeix contra un determinat punt d'error de la xarxa. No es requereix cap programari especial per utilitzar la Còpia de seguretat de la interfície de la xarxa, però l'adaptador de còpia de seguretat ha d'estar connectat a un commutador diferent per garantir la fiabilitat màxima. En la modalitat de Còpia de seguretat de la interfície de la xarxa, només s'utilitza de forma activa un adaptador cada vegada pel trànsit de xarxa. L'Ethernet prova l'adaptador que està actualment actiu i, si es vol, el camí d'accés de la xarxa per un node especificat per l'usuari. Quan es detecta una anomalia, s'utilitzarà el següent adaptador per tot el trànsit. La Còpia de seguretat de la interfície de la xarxa proporciona les funcions de detecció i migració després d'un error sense que hi hagi cap trastorn en les connexions d'usuaris. La Còpia de seguretat de la interfície de la xarxa va ser implementada originalment com a una modalitat en el menú del System Management Interface Tool (SMIT) de l'EtherChannel. L'adaptador de còpia de seguretat proporciona la funció equivalent, de manera que aquesta modalitat va ser eliminada del menú de l'SMIT. Per configurar la Còpia de seguretat de la interfície de la xarxa, consulteu l'apartat “Configuració de còpia de seguretat de la interfície de la xarxa” a la pàgina 378.

Consideracions sobre la configuració de l'EtherChannel

Consulteu aquesta llista de recomanacions abans de configurar l'EtherChannel.

- Podeu tenir fins a vuit adaptadors principals Ethernet i fins a vuit adaptadors Ethernet de còpia de seguretat per EtherChannel.
- Podeu configurar múltiples EtherChannels en un mateix sistema però cada EtherChannel constitueix una interfície Ethernet addicional. És possible que calgui augmentar l'opció **ifsize** de l'ordre **no** perquè inclogui no només les interfícies d'Ethernet per cada adaptador si no també tots els EtherChannels que s'hagin configurat. En l'AIX 5.2 i versions anteriors, el valor per defecte de **ifsize** és de vuit. El valor per defecte és 256.
- Podeu utilitzar qualsevol adaptador Ethernet que tingui suport en un EtherChannel (consulteu l'apartat “Adaptadors admesos” a la pàgina 391). No obstant això, els adaptadors Ethernet han d'estar connectats a un commutador que doni suport a EtherChannel. Consulteu la documentació que s'adjunta amb el commutador per tal de determinar si dóna suport a l'EtherChannel (la documentació del vostre commutador pot fer referència a aquesta funció anomenant-la també acumulació d'enllaços o trunking).
- Tots els adaptadors de l'EtherChannel han d'estar configurats a la mateixa velocitat (100 Mbps, per exemple) i han de ser dúplex complet.

- El sistema no pot accedir als adaptadors utilitzats a l'EtherChannel després de configurar l'EtherChannel. Per modificar els atributs, com ara la velocitat dels suports, les grandàries de la cua de transmissió o de recepció, etcètera, heu de fer-ho abans d'incloure'ls a l'EtherChannel.
- Els adaptadors que tingueu pensat utilitzar amb l'EtherChannel no han de tenir adreça IP configurada abans d'iniciar aquest procediment. Quan configureu un EtherChannel amb adaptadors que s'hagin configurat anteriorment amb una adreça IP, assegureu-vos que les interfícies tinguin l'estat `detach`. Els adaptadors que s'han d'afegir a l'EtherChannel no poden tenir configurades les interfícies en l'estat `up` a l'ODM (Object Data Manager), això passaria si les adreces IP d'haguessin configurat utilitzant la SMIT. Si ho estiguessin hi podria haver problemes a l'hora d'iniciar l'EtherChannel quan es reengegués la màquina perquè la interfície subjacent s'ha configurat abans que l'EtherChannel amb la informació que ha trobat a l'ODM. A més, quan es configura l'EtherChannel, troba que ja s'està utilitzant un dels adaptadors. Per canviar-ho, abans de crear l'EtherChannel, escriviu `smitty chinet`, seleccioneu cadascuna de les interfícies dels adaptadors que s'han d'incloure a l'EtherChannel, i canvieu-ne el valor **state** per `detach`. D'aquesta manera us assegureu que quan es reengegui la màquina, es podrà configurar l'EtherChannel sense errors.

  Per obtenir més informació sobre l'ODM, consulteu l'apartat Object Data Manager (ODM) de la publicació *General Programming Concepts: Writing and Debugging Programs*.
- Si aneu a utilitzar adaptadors Ethernet 10/100 en l'EtherChannel per les versions d'AIX anteriors a la versió AIX 5L Versió 5.2 amb el paquet de manteniment recomanat 5200-03, potser haureu d'habilitar el sondeig d'enllaços en aquests adaptadors abans d'afegir-los a l'EtherChannel. Escriviu `smitty chgenet` a la línia d'ordres. Canvieu el valor **Habilitar sondeig d'enllaços** a `sí` i feu clic a Intro.

  Nota: En l'AIX 5L Versió 5.2 amb el paquet de manteniment recomanat 5200-03 i versions posteriors, no cal habilitar el mecanisme de sondeig d'enllaços. El sondejador d'enllaços s'iniciarà automàticament.
- Si teniu pensat utilitzar trames jumbo, és possible que hagueu d'habilitar aquesta funció en cada adaptador abans de crear l'EtherChannel i el propi EtherChannel. Escriviu `smitty chgenet` a la línia d'ordres. Canvieu el valor **Habilitar trames jumbo** a `sí` i feu clic a Intro. Feu-ho en cada adaptador pel que vulgueu habilitar trames jumbo. Les trames jumbo s'habiliten més tard al propi EtherChannel.

  Nota: L'habilitació de les trames jumbo en cada adaptador subjacent no és necessària quan està habilitada l'opció en el propi EtherChannel. La funció s'habilitarà automàticament si establir l'atribut **Habilitar trames jumbo** en `yes`.
- Els nivells AIX 5.3 i AIX 6.1 admeten les configuracions següents pels adaptadors HEA (Host Ethernet Adpaters).
  - S'admet l'agregació d'enllaços entre el port HEA dedicat i l'adaptador PCI/PCI-E tant per l'agregació manual com per l'agregació LACP.
  - La configuració EtherChannel que inclou el suport HEA no dedicat, EtherChannel amb adaptador de còpia de seguretat com a PCI/PCI-E o Ethernet virtual.

    Nota: Per a un port HEA no dedicat en una configuració EtherChannel, s'aplicaran les limitacions sobre l'agregació d'enllaços.
- AIX Versió 6.1 amb el nivell de tecnologia 6100-06 i versions posteriors admeten EtherChannel en commutadors apilats.
- No es dóna suport a l'engegada de xarxa o instal•lació de xarxa sobre EtherChannel en el client de Gestió d'instal•lació en xarxa (NIM).

Configuració d'un EtherChannel

Utilitzeu aquest procediment per configurar un EtherChannel.

1. Escriviu `smitty etherchannel` a la línia d'ordres.
2. Seleccioneu **Afegir un EtherChannel / Agregació d'enllaç** de la llista i feu clic a Intro.
3. Seleccioneu els adaptadors Ethernet principals que vulgueu al vostre EtherChannel i feu clic a Intro. Si penseu utilitzar la còpia de seguretat d'EtherChannel, no seleccioneu l'adaptador que penseu utilitzar per la còpia de seguretat en aquest moment.

Nota: El camp **Adaptadors de xarxa disponibles** mostra tots els adaptadors Ethernet. Si seleccioneu un adaptador Ethernet que ja s'està fent servir (com a interfície definida), obtindreu un missatge d'error. Primer heu de desconnectar aquesta interfície si voleu fer-la servir.

4. Escriviu la informació en els camps segons les directrius següents:
   - **Adaptador superior:** Proporciona informació d'un dispositiu superior d'EtherChannel (per exemple, quan un EtherChannel pertany a un adaptador Ethernet compartit). Aquest camp mostra un valor de `NONE` si l'EtherChannel no es troba en cap altre adaptador (valor per defecte). Si l'EtherChannel es troba en algun altre adaptador, aquest camp mostrarà el nom de l'adaptador superior (per exemple, `ent6`). Aquest camp només és informatiu i no es pot modificar. L'opció de l'adaptador superior està disponible en l'AIX 5.3 i posteriors versions.
   - **EtherChannel / Adaptadors d'agregació d'enllaços:** Hauríeu de veure tots els adaptadors principals que esteu utilitzant al vostre EtherChannel. Heu seleccionat aquests adaptadors al pas anterior.
   - **Habilitar adreça alternativa:** Aquest camp és opcional. Si establiu aquest camp en `sí` permetreu especificar una adreça MAC que vulgueu que l'EtherChannel utilitzi. Si establiu aquesta opció en `no`, l'EtherChannel utilitzarà l'adreça MAC del primer adaptador.
   - **Adreça alternativa:** Si establiu el camp **Habilitar adreça alternativa** en `sí`, especifiqueu l'adreça MAC que vulgueu utilitzar aquí. L'adreça que especifiqueu ha de començar per `0x` i ha de ser una adreça hexadecimal de 12 dígits (per exemple, 0x001122334455).
   - **Habilitar trames Ethernet jumbo:** Aquest camp és opcional. Per utilitzar-lo, el vostre commutador ha de suportar trames jumbo. Aquesta opció només funcionarà amb la interfície Ethernet estàndard (en) i no amb una interfície IEEE 802.3 (et). Establiu aquesta opció en `sí` si la voleu activar.
   - **Modalitat:** Podeu triar una de les modalitats següents:
     - **estàndard**: En aquesta modalitat l'EtherChannel utilitza un algorisme per seleccionar l'adaptador al que enviarà els paquets. L'algorisme consta d'un valor de dades, dividint-lo pel nombre d'adaptadors de l'EtherChannel i utilitzant la resta (l'operador de mòduls) per identificar l'enllaç de sortida. El valor Modalitat de dispersió determina quins valors de dades alimenten aquest algorisme (consulteu l'atribut Modalitat de dispersió si voleu una explicació de les diferents modalitats de dispersió). Per exemple, si la Modalitat de dispersió és `estàndard`, utilitzarà l'adreça IP de destinació del paquet. Si és 10.10.10.11 i hi ha 2 adaptadors a l'EtherChannel, (1 / 2) = 0 amb resta d'1, per tant, s'utilitza el segon adaptador (els adaptadors van numerats començant pel 0). Els adaptadors s'enumeren segons l'ordre en què es llisten al menú de la SMIT. Aquesta és la modalitat de l'operació per defecte.
     - **rotació_valors**: En aquesta modalitat l'EtherChannel rotarà a través dels adaptadors, donant a cada adaptador un paquet abans de repetir. Els paquets es poden enviar en ordres força diferents respecte a com les ha donat l'EtherChannel, però sempre s'aprofitarà al màxim l'amplada de banda. Seria una combinació no vàlida triar aquesta modalitat amb una Modalitat de dispersió que no fos `per defecte`. Si trieu la modalitat modalitat de rotació de valors, deixeu el valor de la Modalitat de dispersió com `per defecte`.
     - **netif_backup**: Per tal d'habilitar la modalitat Mode de còpia de seguretat d'interfície de xarxa, podeu configurar un o més adaptadors a l'EtherChannel principal o a l'EtherChannel de còpia de seguretat. Per obtenir més informació, consulteu l'apartat "Configuració de la còpia de seguretat d'interficie de xarxa" a la pàgina 379.
     - **8023ad**: Aquesta opció permet utilitzar el protocol de control d'agregació d'enllaços (LACP) d'IEEE 802.3ad per dur a terme una agregació automàtica d'enllaços. Pe obtenir més informació sobre aquesta funció, consulteu l'apartat "Configuració d'acumulacions d'enllaços IEEE" a la pàgina 386.
   - **Interval IEEE 802.3ad**: Podeu triar un d'aquests valors:
     - **long**: valor per defecte de l'interval. Si se selecciona, l'EtherChannel sol•licitarà els paquets LACP del seu associat en el valor d'interval llarg tal com ho especifica el protocol
     - **short**: si se selecciona, l'EtherChannel sol•licitarà els paquets LACP del seu associat en el valor d'interval curt tal com ho especifica el protocol.

Nota: El valor de l'interval només s'utilitza quan l'EtherChannel funciona en el mode IEEE 802.3ad. Altrament, el valor es passa per alt.

Nota: L'AIX admet la sol•licitud d'interval llarg i curt del seu associat.

- **Modalitat de dispersió**: Trieu una de les següents modalitats de dispersió que determinarà el valor de les dades que utilitzarà l'algorisme per determinar l'adaptador de sortida:
  - **per defecte**: L'adreça IP de destinació del paquet s'utilitza per determinar l'adaptador de sortida. Pel trànsit no IP (com ara ARP), el darrer octet de l'adreça MAC de destinació s'utilitza per fer el càlcul. Aquesta modalitat garanteix que els paquets s'enviïn a través de l'EtherChannel en l'ordre en què s'han rebut però pot ser que no faci un ús total de l'amplada de banda.
  - **port_src**: El valor del port UDP o TCP d'origen del paquet s'utilitza per determinar l'adaptador de sortida. Si el paquet no és trànsit UDP o TCP, s'utilitzarà el darrer octet de l'adreça IP de destinació. Si el paquet no és trànsit IP, s'utilitzarà el darrer octet de l'adreça MAC de destinació.
  - **port_dst**: El valor del port UDP o TCP de destinació del paquet s'utilitza per determinar l'adaptador de sortida. Si el paquet no és trànsit UDP o TCP, s'utilitzarà el darrer octet de l'adreça IP de destinació. Si el paquet no és trànsit IP, s'utilitzarà el darrer octet de l'adreça MAC de destinació.
  - **port_dst_ src**: Els valors UDP o TCP d'origen i de destinació s'utilitzen per determinar l'adaptador de sortida (específicament, s'afegeixen els ports d'origen i de destinació i després es divideixen en dos abans d'alimentar l'algorisme). Si el paquet no és trànsit UDP o TCP, s'utilitzarà el darrer octet de l'adreça IP de destinació. Si el paquet no és trànsit IP, s'utilitzarà el darrer octet de l'adreça MAC de destinació. Aquesta modalitat pot oferir una bona distribució dels paquets en moltes situacions, tant per clients com per servidors.

  Nota: Seria una combinació no vàlida triar una Modalitat de dispersió que no fos `per defecte` amb una modalitat de `rotació_valors`.

  Per aprendre més sobre la distribució i l'equilibri de càrrega de paquets, consulteu l'apartat "Opcions de l'equilibri de càrrega EtherChannel" a la pàgina 380.
- **Adaptador de còpia de seguretat** Aquest camp és opcional. Escriviu una llista d'adaptadors que vulgueu utilitzar com a còpia de seguretat d'EtherChannel.
- **Adreça d'Internet per una acció ping:** Aquest camp és opcional i només tindrà efecte si executeu la modalitat **Còpia de seguretat de l'interfície de la xarxa** o si teniu un o més adaptadors e l'EtherChannel i un o més adaptadors de la llista de còpia de seguretat. L'EtherChannel emet una ordre ping a l'adreça IP o al nom de l'amfitrió que especifiqueu. Si l'EtherChannel no aconsegueix dur a terme l'acció ping en aquesta adreça la quantitat de vegades que s'hagi especificat al camp **Nombre de reintents** i en els temps especificats al camp **Temps d'espera de reintent**, l'EtherChannel commuta als altres adaptadors de la llista de còpia de seguretat.
- **Nombre de reintents:** Escriviu el nombre d'anomalies en la resposta de l'acció ping que es permeten abans que l'EtherChannel commuti l'adaptador. El valor per defecte és tres. Aquest camp és opcional i només és vàlid si heu definit una **Adreça d'Internet per una acció ping**.
- **Temps d'espera de reintent:** Escriviu el nombre de segons entre les vegades en què l'EtherChannel emetrà una acció ping a l'**Adreça d'Internet per una acció ping**. El valor per defecte és un segon. Aquest camp és opcional i només és vàlid si heu definit una **Adreça d'Internet per una acció ping**.

5. Premeu Intro després de canviar els camps que vulgueu per crear l'EtherChannel.
6. Configureu l'IP a través del dispositiu d'EtherChannel que acabeu de crear escrivint `smitty chinet` a la línia d'ordres.
7. Seleccioneu de la llista la nova interfície d'EtherChannel.
8. Empleneu tots els camps necessaris i i feu clic a Intro.

Si voleu informació sobre altres tasques que es poden dur a terme després de configurar l'EtherChannel, consulteu l'apartat "Llistat dels EtherChannels o de les acumulacions d'enllaços" a la pàgina 382.

Opcions de restabliment i migració després d'un error

Les funcions de restabliment i migració després d'un error estan disponibles per l'EtherChannel o l'acumulació d'enllaços d'IEEE 802.3ad.

Amb aquestes funcions hi ha disponibles les millores següents:

- la pèrdua de paquets es pot evitar durant el restabliment
- les migracions després d'un error es poden definir perquè s'esdevinguin de forma simultània
- el restabliment automàtic es pot desactivar de manera que l'adaptador de còpia de seguretat continua funcionant
- les acumulacions d'enllaços es poden forçar perquè la es faci còpia de seguretat de la migració després d'un error del canal principal o a la inversa.

Restabliment sense pèrdues:

La funció de restabliment sense pèrdues garanteix que el restabliment de l'adaptador de còpia de seguretat pels valors del canal principal perdrà el mínim de paquets possible.

Abans de dur a terme un restabliment sense pèrdues, l'EtherChannel o IEEE 802.3ad farà un restabliment pels valors del canal principal en el mateix moment en què ha detectat el restabliment d'un dels adaptadors principals. En alguns casos, el commutador de l'adaptador no tindrà l'estat que tenia quan va enviar o rebre dades, i alguns paquets es perdran immediatament després del restabliment.

Amb el restabliment sense pèrdues, l'adaptador EtherChannel o IEEE 802.3ad restableix els valors del canal principal només quan ha pogut rebre realment trànsit de correu. D'aquesta manera es garanteix que el port del commutador s'inicialitzi completament i que no es perdin paquets.

Migració sense pèrdues després d'un error:

La funció de migració sense pèrdues després d'un error modifica el funcionament de la funció de restabliment sense pèrdues.

Quan els errors de ping provoquen una migració després d'un error, per defecte, es durà a terme un restabliment sense pèrdues. Això implica un període d'espera fins que el commutador de l'adaptador inactiu rebi trànsit de correu abans d'inicialitzar la migració després d'un error. No obstant això, si l'atribut **noloss_failover** s'estableix a `no`, la migració després d'un error de l'acció ping es produirà immediatament.

Recuperació automàtica:

Després d'una migració després d'un error des del canal primari a l'adaptador de còpia de seguretat, l'EtherChannel o l'IEEE 802.3ad Link Aggregation inicia automàticament una recuperació al canal primari que ha fallat quan almenys un dels seus adaptadors es recupera.

Aquesta opció de recuperació no s'admet en la modalitat IEEE 802.3ad i la migració després d'un error a l'adaptador de còpia de seguretat és a causa de l'error del Protocol de control d'acumulació d'enllaços (LACP). L'error del LACP apareix quan tots els adaptadors del canal primari no reben les unitats de dades LACP dintre del temps d'espera. El temps d'espera es determina per l'estàndard IEEE, el qual es basa en el interval que es configura en el mode 802.3ad.

Aquest comportament per defecte es pot modificar establint l'atribut **auto_recovery** en `no`. D'aquesta manera, l'EtherChannel o l'IEEE 802.3ad Link Aggregation segueix funcionant a l'adaptador de còpia de seguretat després de la migració després d'un error. Les operacions a l'adaptador de còpia de seguretat continuen fins que es produeix una de les següents incidències:

- S'ha forçat una migració després d'un error.
- L'adaptador de còpia de seguretat ha fallat.

- Es detecta un error de ping a l'adaptador de còpia de seguretat

Migracions després d'un error forçades:

L'EtherChannel o l'acumulació d'enllaços IEEE 802.3ad es poden forçar perquè facin una migració després d'un error del canal principal a l'adaptador de còpia de seguretat o de l'adaptador de còpia de seguretat al canal principal.

Les migracions després d'un error forçades només funcionen si hi ha definit un adaptador de còpia de seguretat i si el canal inactiu està definit i en execució. Per exemple, per forçar una migració després d'un error del canal principal a l'adaptador de còpia de seguretat, l'adaptador de còpia de seguretat ha d'estar en execució.

Per utilitzar aquesta funció, escriviu `smitty etherchannel` i seleccioneu l'opció **Forçar una migració després d'un error a un EtherChannel / Acumulació d'enllaços** que apareix per pantalla. A continuació, seleccioneu l'EtherChannel i l'acumulació d'enllaços IEEE 802.3ad en què s'ha de forçar la migració després d'un error.

Configuració de còpia de seguretat de la interfície de la xarxa

La còpia de seguretat de la interfície de la xarxa protegeix contra un determinat punt d'error de la xarxa proporcionant funcions de detecció d'errors i migració després d'un error sense que hi hagi cap trastorn en les connexions d'usuaris. Quan es treballa en aquesta modalitat, només hi ha un adaptador actiu en cada ocasió.

Si falla l'adaptador actiu, s'utilitzarà pel trànsit un altre adaptador de l'EtherChannel. Quan es treballa en la modalitat de còpia de seguretat de la interfície de la xarxa, no és necessari connectar-se als commutadors habilitats per l'EtherChannel.

La configuració de la còpia de seguretat de la interfície de la xarxa és més efectiva quan els adaptadors es connecten a diferents commutadors de xarxa, ja que així s'obté més redundància que si es connectessin tots els adaptadors a un sol commutador. Quan faci connexions a diferents commutadors, asseguri's que hi hagi connexió entre els commutadors. D'aquesta manera la funció de migració després d'un error passa d'un adaptador a un altre garantint que hi hagi sempre un camí per l'adaptador que estigui actiu.

Es dona prioritat a l'adaptador configurat a l'EtherChannel primari per sobre de l'adaptador de còpia de seguretat. L'adaptador primari s'utilitzarà sempre que sigui funcional. Això contrasta amb el comportament de la modalitat de còpia de seguretat de la interfície de la xarxa en versions anteriors, en què l'adaptador de còpia de seguretat s'utilitzava fins que fallava, independentment de si s'havia recuperat ja l'adaptador principal.

Per exemple, `ent0` es podria configurar com adaptador principal i `ent2` com adaptador de còpia de seguretat, creant un EtherChannel anomenat `ent3`. Idealment, `ent0` i `ent2` es connectarien a dos commutadors diferents. En aquest exemple, tot el trànsit enviat a través d'`ent3` (la interfície d'EtherChannel) s'envia a través d'`ent0` per defecte, sempre que `ent2` estigui desocupat. Si en algun moment fallés l'`ent0`, tot el trànsit s'envia a través de l'adaptador de còpia de seguretat, `ent2`. Quan l'`ent0` es recupera, es torna a utilitzar per tot el trànsit.

Ara és possible configurar l'EtherChannel per detectar un error d'enllaços i la falta d'accés a la xarxa per múltiples EtherChannels amb un adaptador de còpia de seguretat. Per fer-ho, utilitzeu l'atribut **netaddr** per especificar l'adreça IP o el nom de l'amfitrió d'un amfitrió remot on sempre hi ha connectivitat. L'EtherChannel periòdicament emetrà una ordre ping a aquest amfitrió per determinar si encara hi ha un camí d'accés a la xarxa. Si no es respon a un nombre especificat d'intents, l'EtherChannel farà una migració després d'un error cap a l'altra adaptador per veure si hi ha un camí d'accés de xarxa a l'amfitrió remot que passi a través de l'altre adaptador. En aquesta configuració, cada adaptador ha d'estar connectat a un commutador diferent i, a més, ha de tenir també un camí diferent a l'amfitrió al quan s'emeti l'ordre ping.

Aquesta funció ping està disponible per un o més EtherChannels amb un adaptador de còpia de seguretat. No obstant això, si es produeix una migració després d'un error a causa de les accions ping sense resposta de l'adaptador principal, l'adaptador de còpia de seguretat continua essent el canal actiu mentre estigui en funcionament. No hi ha manera de saber, mentre es treballi amb l'adaptador de còpia de seguretat, si es pot arribar a l'amfitrió al que s'emet l'ordre ping des de l'adaptador principal. Per tal d'evitar que la migració després d'un error vagi i vingui entre l'adaptador principal i el de còpia de seguretat, es continua treballant en el de còpia de seguretat (a menys que les ordres ping quedin també sense resposta a l'adaptador de còpia de seguretat, o si el propi adaptador de còpia de seguretat falla, en aquest cas la migració després d'un error es produirà en l'adaptador principal). No obstant això, si la migració després d'un error es produís per una anomalia a l'adaptador principal (no perquè les ordres ping no tinguin resposta), aleshores l'EtherChannel tornarà a l'adaptador principal tan aviat com torni a estar actiu,com sempre.

Per configurar la còpia de seguretat de la interfície de la xarxa a noves versions, consulteu l'apartat “Configuració de la còpia de seguretat d'interficie de xarxa”.

Configuració de la còpia de seguretat d'interficie de xarxa:

Utilitzeu aquest procediment per configurar una còpia de seguretat de la interfície de la xarxa a les versions més noves.

1. Amb autorització root, escriviu `smitty etherchannel` a la línia d'ordres.
2. Seleccioneu **Afegir un EtherChannel / Agregació d'enllaç** de la llista i feu clic a Intro.
3. Seleccioneu l'adaptador Ethernet principal i feu clic a Intro. És l'adaptador que s'utilitzarà fins que no falli.

   Nota: El camp **Adaptadors de xarxa disponibles** mostra tots els adaptadors Ethernet. Si seleccioneu un adaptador Ethernet que ja s'està utilitzant, obtindreu un missatge d'error i haureu de desconnectar aquesta interfície abans de poder utilitzar-la. Consulteu “Canvis a l'EtherChannel amb 5200-01 i anteriors” a la pàgina 385 per obtenir informació sobre com desconnectar una interfície.
4. Escriviu la informació en els camps següents segons les directrius que s'indiquen:
   - **Adaptador superior:** Aquest camp proporciona informació d'un dispositiu superior d'EtherChannel (per exemple, quan un EtherChannel pertany a un adaptador Ethernet compartit). Aquest camp mostra un valor de `NONE` si l'EtherChannel no es troba en cap altre adaptador (valor per defecte). Si l'EtherChannel es troba en algun altre adaptador, aquest camp mostrarà el nom de l'adaptador superior (per exemple, `ent6`). Aquest camp només és informatiu i no es pot modificar. L'opció de l'adaptador de còpies de seguretat està disponible en l'AIX.
   - **Adaptadors EtherChannel / Acumulació d'enllaços**: Hauríeu de veure l'adaptador principal que he seleccionat al pas anterior.
   - **Habilitar adreça alternativa**: Aquest camp és opcional. Si establiu aquest camp en `sí` permetreu especificar una adreça MAC que vulgueu que l'EtherChannel utilitzi. Si establiu aquesta opció en `no`, l'EtherChannel utilitzarà l'adreça MAC de l'adaptador principal.
   - **Adreça alternativa**: Si establiu el camp **Habilitar adreça alternativa** en `sí`, especifiqueu l'adreça MAC que vulgueu utilitzar aquí. L'adreça que especifiqueu ha de començar per `0x` i ha de ser una adreça hexadecimal de 12 dígits (per exemple, 0x001122334455).
   - **Habilitar trames Ethernet jumbo**: Aquest camp és opcional. Per utilitzar-lo, el vostre commutador ha de suportar trames jumbo. Aquesta opció només funciona amb la interfície Ethernet estàndard (en) i no amb una interfície IEEE 802.3 (et). Establiu aquesta opció en `sí` si la voleu utilitzar.
   - **Modalitat**: És irrellevant la modalitat de funcionament que trieu perquè només hi ha un adaptador a l'EtherChannel principal. Tots els paquets d'envien a través d'aquest adaptador fins que falli. No hi ha cap modalitat `netif_backup` perquè aquesta modalitat es pot emular utilitzant un adaptador de còpia de seguretat.

- **Modalitat de dispersió**: És irrellevant la modalitat de dispersió que trieu perquè només hi ha un adaptador a l'EtherChannel principal. Tots els paquets d'envien a través d'aquest adaptador fins que falli.
- **Adaptador de còpia de seguretat**: Escriviu una llista d'un o més adaptadors que voleu incloure en el grup de còpia de seguretat de l'EtherChannel. Després d'un esdeveniment de migració després d'un error degut a la pèrdua del grup de l'EtherChannel principal, s'utilitzen els adaptadors de còpia de seguretat fins que es recuperi el grup de l'EtherChannel principal.
- **Adreça d'Internet per acció Ping**: Aquest camp és opcional. L'EtherChannel emet una ordre ping a l'adreça IP o al nom de l'amfitrió que especifiqueu aquí. Si l'EtherChannel no aconsegueix dur a terme l'acció ping en aquesta adreça la quantitat de vegades que s'hagi especificat al camp **Nombre de reintents** i en els intervals especificats al camp **Temps d'espera de reintent**, l'EtherChannel commuta l'adaptador.
- **Nombre de reintents**: Escriviu el nombre d'anomalies en la resposta de l'acció ping que es permeten abans que l'EtherChannel commuti l'adaptador. El valor per defecte és tres. Aquest camp és opcional i només és vàlid si heu definit una **Adreça d'Internet per una acció ping**.
- **Temps d'espera de reintent**: Escriviu el nombre de segons entre les vegades en què l'EtherChannel emeti una acció ping a l'**Adreça d'Internet per una acció ping**. El valor per defecte és un segon. Aquest camp és opcional i només és vàlid si heu definit una **Adreça d'Internet per una acció ping**.

5. Premeu Intro després de canviar els camps que vulgueu per crear l'EtherChannel.
6. Configureu l'IP a través de la interfície que acabeu de crear escrivint `smitty chinet` a la línia d'ordres.
7. Seleccioneu de la llista la nova interfície d'EtherChannel.
8. Empleneu tots els camps necessaris i i feu clic a Intro.

Ara ja teniu configurada la còpia de seguretat de la vostra interfície de xarxa.

Opcions de l'equilibri de càrrega EtherChannel

Hi ha dos mètodes d'equilibri de càrrega per donar sortida al trànsit a EtherChannel, que són: rotació de valors, que dispesa el gràfic de sortida uniformement a tots els adaptadors d'EtherChannel; i estàndard, que selecciona l'adaptador utilitzant un algorisme.

El paràmetre de modalitat de dispersió (hash) determina el valor numèric que alimenta l'algorisme.

La taula següent resum les combinacions d'opcions d'equilibri de càrrega que s'ofereixen.

Taula 80. Les combinacions de modalitat i modalitat de dispersió i les distribucions de trànsit de sortida.

Modalitat	Modalitat de dispersió	Distribució del trànsit de sortida
estàndard o 8023ad	per defecte	El funcionament tradicional de l'AIX. L'algorisme de selecció d'adaptadors utilitza el darrer octet de l'adreça IP de destinació (pel trànsit de **TCP/IP**) o de l'adreça MAC (pel trànsit ARP i d'altres no IP). Aquesta modalitat acostuma a ser una bona opció inicial per un servidor que tingui una gran quantitat de clients.
estàndard o 8023ad	src_dst_port	El camí d'accés de l'adaptador de sortida se selecciona mitjançant un algorisme que utilitza els valors de port combinats TCP o UDP d'origen i destinació. Com que cada connexió é un port TCP o UDP exclusiu, les tres modalitats de dispersió que es basen en ports proporcionen més flexibilitat de distribució d'adaptadors quan hi ha diferents connexions TCP o UDP independents entre una parella d'adreces IP.

Taula 80. Les combinacions de modalitat i modalitat de dispersió i les distribucions de trànsit de sortida. (continuació)

Modalitat	Modalitat de dispersió	Distribució del trànsit de sortida
estàndard o 8023ad	src_port	L'algorisme de selecció d'adaptadors utilitza el valor de port TCP o UDP origen. En la sortida de l'ordre **netstat -an**, el port és el valor de sufix de l'adreça TCP/IP que hi ha a la columna `Local`.
estàndard o 8023ad	dst_port	El camí d'accés de l'adaptador de sortida se selecciona mitjançant l'algorisme que utilitza el valor de ports del sistema de destinació. En la sortida de l'ordre **netstat -an**, el sufix de l'adreça TCP/IP que hi ha a la columna `Foreign` és el valor del port de destinació TCP o UDP.
rotació de valors	per defecte	El trànsit de sortida es dispersa uniformement a tots els ports d'adaptadors d'EtherChannel. Aquesta modalitat és l'opció típica per dos amfitrions connectats de forma consecutiva (sense que hi hagi intervenció d'un commutador).

Distribució de rotació de valors:

Tot el trànsit de sortida es dispersa uniformement a través de tots els adaptadors de l'EtherChannel. Proporciona la millor optimització de l'amplada de banda pel sistema del servidor AIX. Mentre que la distribució de rotació de valors és la forma ideal d'utilitzar tots els enllaços d'igual manera, tingueu en compte que també introdueix el possibilitat de què hi hagi paquets anòmals en el sistema de recepció.

En general, la modalitat de rotació de valors és ideal per connexions de forma consecutiva que s'executen en trames jumbo. En aquest entorn, no hi ha cap commutador que hi intervingui, per tant, no pot passar que el processament en el commutador pugui alterar l'hora de lliurament del paquet, o el camí d'accés de l'adaptador. En camí d'accés de la xarxa del cable directe, els paquets es reben exactament igual com s'han enviat. Les trames jumbo (amb un MTU de 9000 octets) sempre proporcionen un millor rendiment de transferència de fitxers que els MTU de 1500 octets tradicionals. No obstant això, en aquest cas, afegeixen una altra avantatge. Aquests grans paquets triguen més estona a enviar-se per tant, és menys probable que l'amfitrió que els rep s'estigui interrompent constantment amb paquets anòmals.

La modalitat de rotació de valor es pot implementar en altres entorns però amb un risc superior que hi hagi paquets anòmals al sistema de recepció. Aquest risc és particularment elevat quan hi ha poques connexions TCP de de modalitat continua i de llarga duració. Quan hi ha moltes connexions d'aquest tipus entre una parella d'amfitrions, els paquets procedents de diferents connexions es podrien barrejar, disminuint així la possibilitat que hi hagi paquets per la mateixa connexió de arribin amb anomalies. Comproveu les estadístiques dels paquets anòmals a la secció `tcp` de la sortida de l'ordre **netstat -s**. Un valor que va augmentant constantment indica un possible problema en el trànsit que s'ha enviat a un EtherChannel.

Si els paquets anòmals són un problema en un sistema que ha d'utilitzar MTU d'Ethernet tradicional i s'ha de connectar a través d'un commutador, proveu diverses modalitats de dispersió que s'ofereix en l'operació de modalitat estàndard. Cada modalitat té una força en particular, però les modalitats per defecte i src_dst_port són els punts de partida lògics perquè tenen una aplicació més variada.

Algoritme estàndard o 802.3ad:

Hi ha avantatges a l'hora d'utilitzar l'algorisme estàndard de l'EtherChannel.

L'algorisme estàndard s'utilitza per agregacions d'enllaç estàndard i de l'estil 802.3ad. AIX divideix l'últim byte del "valor numèric" pel número d'adaptadors a EtherChannel i utilitza la resta per identificar l'enllaç de sortida. Si el que en queda és zero, se selecciona el primer adaptador de l'EtherChannel; un recordatori d'un significa que se selecciona el segon adaptador i així successivament (els adaptadors se seleccionen en l'ordre en què apareixen llistats a l'atribut **adapter_names**).

La selecció de la modalitat Hash determina el valor numèric emprat al càlcul. Per defecte, l'últim byte de l'adreça IP o MAC de destinació s'utilitza al càlcul. Amb tot, també es poden utilitzar els valors de port TCP o UDP d'origen i destinació. Aquestes alternatives permeten ajustar la distribució del trànsit de sortida pels adaptadors reals d'EtherChannel.

En la modalitat de dispersió per defecte, l'algorisme de selecció d'adaptadors s'aplica al darrer octet de l'adreça IP de destinació pel trànsit IP. Pel trànsit ARP i altres tipus de trànsit no IP, s'aplica la mateixa fórmula al darrer octet de l'adreça MAC de destinació. A menys que hi hagi un error en l'adaptador que provoqui una migració després d'un error, tot el trànsit entre una parella d'amfitrions que estan en la modalitat estàndard per defecte surt pel mateix adaptador. La modalitat hash per defecte pot ser ideal quan l'amfitrió local estableix connexions amb moltes adreces IP.

No obstant això, si l'amfitrió local estableix connexions llargues a unes quantes adreces IP, observareu que alguns adaptadors estan sotmesos a més càrrega que d'altres perquè tot el trànsit enviat a una destinació específica s'envia a través del mateix adaptador. Mentre que això garanteix que els paquets arribin a temps, és possible que no utilitzi l'amplada de banda de la forma més efectiva en tots els casos. Les modalitats de dispersió basades en ports encara envien paquets per ordre però permeten que els paquets que pertanyen a connexions UDP o TCP diferents, fins i tot si s'envien a la mateixa destinació, s'enviïn a través d'adaptadors diferents, és a dir, fent un millor ús de l'amplada de banda de tots els adaptadors.

En la modalitat de dispersió **src_dst_port**, s'afegeixen els valors de ports TCP o UDP d'origen i de destinació del paquet de sortida i després es divideixen en dos. El número enter resultant (sense decimals) es col•loca al logaritme estàndard. El trànsit TCP o UDP s'envia a l'adaptador seleccionat mitjançant l'algorisme estàndard i el valor de la modalitat hash seleccionat. Cap trànsit que no sigui TCP ni UDP tornarà a la modalitat hash; això vol dir que l'últim byte de l'adreça IP o MAC de destinació. L'opció de la modalitat de dispersió **src_dst_port** considera tant els valors de port TCP o UDP d'origen com de destinació. En aquesta modalitat, tots els paquets d'una connexió TCP o UDP s'envien a través d'un sol adaptador de manera que es garanteix que arribin per ordre però el trànsit continua dispersat perquè les connexions (fins i tot les que van al mateix amfitrió) es poden enviar a través de diferents adaptadors. Els resultats d'aquesta modalitat de dispersió no es bifurquen amb la direcció d'establiment de connexions perquè utilitza els valors de port TCP o UDP d'origen i de destinació.

En la modalitat de dispersió **src_port** s'utilitza el valor de port TCP o UDP d'origen del paquet de sortida. En la modalitat de dispersió **dst_port** s'utilitza el valor de port TCP or UDP de destinació del paquet de sortida. Utilitzeu les opcions de la modalitat de dispersió **src_port** o **dst_port** si els valors de port canvies d'una connexió a una altra i si l'opció **src_dst_port** no produeix una distribució desitjable.

Llistat dels EtherChannels o de les acumulacions d'enllaços

Utilitzeu aquest procediment per llistar els EtherChannels o les acumulacions d'enllaços.

1. En la línia d'ordres, escriviu `smitty etherchannel`.
2. Seleccioneu **Llistar tots els EtherChannels / totes les acumulacions d'enllaços** i feu clic a Intro.

Canvi de l'adreça alternativa

Per tal d'especificar una adreça MAC per l'EtherChannel o per l'acumulació d'enllaços, seguiu aquests passos.

1. Segons la versió de l'AIX que estigueu executant, pot ser que hagueu de desconnectar la interfície:
   - En l'AIX 5.2 amb 5200-01 i versions anteriors, escriviu `smitty chinet` i seleccioneu la interfície que pertanyi al vostre EtherChannel. Canvieu l'atribut de l'**estat actual** a **detach** i, a continuació, feu clic a Intro.

- A l'AIX 5L Versió 5.2 amb el paquet de manteniment recomanat 5200-03 i versions posteriors, podeu canviar l'adreça alternativa de l'EtherChannel sense desconnectar-ne la interfície.

2. En la línia d'ordres, escriviu `smitty etherchannel`.
3. Seleccioneu **Canviar / Mostrar característiques d'un EtherChannel** i feu clic a Intro.
4. Si teniu múltiples EtherChannels, seleccioneu l'EtherChannel pel que vulgueu crear una adreça alternativa.
5. Canvieu el valor d'**Habilitar adreça alternativa d'EtherChannel** a `yes`.
6. Escriviu l'adreça alternativa al camp **Adreça alternativa d'EtherChannel**. L'adreça ha de començar per `0x` i ha de ser una adreça hexadecimal de 12 dígits (per exemple, 0x001122334455).
7. Premeu Intro per finalitzar el procés.

   Nota: Si es canvia l'adreça MAC de l'EtherChannel durant el temps d'execució, es pot produir una pèrdua de connectivitat temporal. Això és així perquè cal restablir els adaptadors perquè coneguin la nova adreça de maquinari i alguns adaptadors poden trigar només segons en inicialitzar-se.

Dynamic Adapter Membership

Abans de l'AIX 5L Versió 5.2 amb el paquet de manteniment recomanat 5200-03, per poder afegir i eliminar un adaptador d'un EtherChannel, primer calia desconnectar-ne la interfície i interrompre temporalment tot el trànsit d'usuaris. Per tal de superar aquesta limitació, s'ha afegit el DAM (Dynamic Adapter Membership) a l'AIX 5L Versió 5.2 amb el paquet de manteniment recomanat 5200-03.

Així es permet que es puguin afegir i eliminar adaptadors d'un EtherChannel sense que hi hagi cap trastorn en les connexions d'usuaris. També es pot afegir o eliminar un adaptador de còpia de seguretat; inicialment es pot crear un EtherChannel sense adaptador de còpia de seguretat i se'n pot afegir un més endavant si es considera necessari.

No només es poden afegir o eliminar adaptador sense ocasionar cap trastor en les connexions d'usuaris, també es pot modificar la majoria d'atributs de l'EtherChannel en el temps d'execució. Per exemple, podeu començar a utilitzar la funció "ping" de la còpia de seguretat de la interfície de la xarxa mentre està utilitzant l'EtherChannel o canviar l'amfitrió remot en el qual s'està sotmetent l'ordre ping en qualsevol moment que es desitgi.

També podeu convertir un EtherChannel regular en una acumulació d'enllaços IEEE 802.3ad (o a la inversa). Això permet que els usuaris experimentin amb aquesta funció sense haver d'eliminar ni tornar a crear l'EtherChannel.

A més, amb el DAM, podeu triar si voleu crear un EtherChannel d'un adaptador. Un EtherChannel d'un adaptador funciona exactament igual que un adaptador regular. No obstant això, si aquest adaptador fallés, es podria substituir en el temps d'execució sense perdre mai la connectivitat. Per a fer-ho, afegiu un adaptador temporal a l'EtherChannel, wliminwu l'adaptador defectuós de l'EtherChannel, substituïu l'adaptador defectuós per un que utilitzi el sistema Hot Plug, afegiu l'adaptador nou a l'EtherChannel i, aleshores, elimineu l'adaptador temporal. Durant aquest procés mai notareu que es perdi connectivitat. No obstant això, si l'adaptador hagués treballat com a adaptador autònom, caldrà desconnectar-lo abans d'eliminar-lo utilitzant el sistema Hot Plug, i durant aquesta estona no hi hauria trànsit.

Com afegir, eliminar o canviar un adaptador en un EtherChannel o una acumulació d'enllaços

Hi ha dues maneres d'afegir, eliminar o canviar un adaptador en un EtherChannel o una acumulació d'enllaços

Un mètode requereix que la interfície de l'EtherChannel o de l'acumulació d'enllaços estigui desconnectada, mentre que l'altre no (utilitzant la Qualitat de membre d'adaptadors dinàmics que hi ha disponible a l'AIX 5L Versió 5.2 amb el paquet de manteniment recomanat 5200-03 i versions posteriors).

Canvis a l'EtherChannel utilitzant el Dynamic Adapter Membership:

Si feu canvis utilitzant el Dynamic Adapter Membership no caldrà que atureu tot el trànsit que surti de l'EtherChannel desconnectant-ne l'interfície.

Considereu el següent abans de continuar:

1. Quan afegiu un adaptador en el temps d'execució, observeu que hi ha diferents adaptadors Ethernet que donen suport a diferents possibilitats (per exemple, la possibilitat d'efectuar un descàrrega de suma de comprovació, per utilitzar segments privats, per fer enviaments grans, etcètera). Si s'utilitzen diferents tipus d'adaptadors al mateix EtherChannel, les possibilitats indicades a la cap de la interfície són les que admeten tots els adaptadors (per exemple, si tots els adaptadors menys un donen suport a la utilització de segments privats, l'EtherChannel indicarà que no dóna admet segments privats; si tots els adaptadors donen suport a enviaments grans, el canal indicarà que admet enviaments grans). Quan s'afegeix un adaptador a un EtherChannel durant el temps d'execució, assegureu-vos que al menys doni suport a les mateixes funcions que la resta d'adaptadors que ja hi ha a l'EtherChannel. Si heu intentat afegir un adaptador que no dóna suport a totes les funcions que admet l'EtherChannel, es produirà un error en l'acumulació. No obstant això, observeu que si es desconnecta la interfície de l'EtherChannel, podeu afegir un adaptador (independentment de les funcions que admeti) i quan la interfície es torni a activar, l'EtherChannel tornarà a mirar les funcions a les que dóna suport basant-se en la nova llista d'adaptadors.
2. Si no utilitzeu cap adreça alternativa i penseu suprimir l'adaptador, l'adreça MAC del qual es va utilitzar a l'EtherChannel (l'adreça MAC utilitzada a l'EtherChannel és "propietat" d'un dels adaptador), l'EtherChannel utilitzarà l'adreça MAC del següent adaptador disponible. En altres paraules, l'adaptador que esdevé el primer després de dur a terme la supressió, o l'adaptador de còpia de seguretat si és que se suprimeixen tots els adaptadors principals. Per exemple, si un EtherChannel té com adaptadors principals `ent0` i `ent1` i com adaptador de còpia de seguretat `ent2`, per defecte utilitzarà l'adreça MAC d'`ent0` (aleshores podrem dir que `ent0` és el "propietari" de l'adreça MAC). Si se suprimeix `ent0`, l'EtherChannel utilitzarà aleshores l'adreça MAC d'`ent1`. Si després se suprimeix `ent1`, l'EtherChannel utilitzarà l'adreça MAC d'`ent2`. Si més endavant es torna a afegir `ent0` a l'EtherChannel, es continuarà utilitzant l'adreça MAC d'`ent2` perquè `ent2` ara és el propietari de l'adreça MAC. Si seguidament se suprimeix `ent2` de l'EtherChannel, es començarà a utilitzar una altra vegada l'adreça MAC d'`ent0`.

   Quan se suprimeix l'adaptador del qual l'EtherChannel està fent servir l'adreça MAC es pot perdre temporalment la connectivitat perquè tots els adaptadors de l'EtherChannel s'hauran de restablir perquè coneguin la nova adreça de maquinari. Alguns adaptadors triguen segons en inicialitzar-se.

   Si l'EtherChannel utilitza una adreça alternativa (una adreça MAC que hàgiu especificat), continuarà utilitzant aquesta adreça MAC independentment dels adaptadors que s'afegeixin o que se suprimeixin. A més, això significa que no es produeix cap pèrdua temporal de connectivitat quan s'afegeixen o se suprimeixen adaptadors perquè cap d'ells és el "propietari" de l'adreça MAC de l'EtherChannel.
3. Ara es podran modificar gairebé tots els atributs de l'EtherChannel durant el temps d'execució. La única excepció és l'atribut **Habilitar trames Ethernet jumbo de gigabits**. Per modificar l'atribut **Habilitar trames Ethernet jumbo de gigabits** primer haureu de desconnectar la interfície de l'EtherChannel abans de fer cap intent de modificar-ne el valors.
4. Per a tots aquells atributs que no es puguin canviar durant el temps d'execució (fins ara només, **Habilitar trames Ethernet jumbo de gigabits**) hi ha un camp anomenat **Aplicar canvi només a DATABASE**. Si aquest atribut s'estableix en `yes`, es podrà canviar, durant el temps d'execució, el valor d'un atribut que normalment no es podia modificar durant el temps d'execució. Amb el camp **Aplicar canvi només a DATABASE** establert en `yes`, només es canviarà l'atribut a l'ODM i no es reflectirà a l'EtherChannel en execució fins que no es torni a carregar en memòria (desconnectant-ne la interfície, utilitzant les ordres `rmdev -l EtherChannel_device` i, a continuació, `mkdev -l EtherChannel_device`), o fins que no es torni a iniciar la màquina. Aquesta és una forma molt convenient si voleu garantir que l'atribut es modifiqui la propera vegada que es torni a engegar la màquina sense haver de trastornar l'execució de l'EtherChannel.

5. En una partició lògica, si elimineu un adaptador d'un EtherChannel, també heu d'eliminar el port de commutador associat de l'EtherChannel al commutador. En cas contrari, pot ser que es perdi la connexió si el commutador utilitza el mateix port de commutador per a la connexió.

Per fer els canvis a l'EtherChannel o a l'acumulació d'enllaços utilitzant el Dynamic Adapter Membership, seguiu aquests passos:

1. En la línia d'ordres, escriviu `smitty etherchannel`.
2. Seleccioneu **Canviar / Mostrar característiques d'un EtherChannel / Acumulació d'enllaços**.
3. Seleccioneu l'EtherChannel o Acumulació d'enllaços que vulgueu modificar.
4. Empleneu els camps necessaris segons les directrius següents:
   - Al camp **Afegir adaptador** o **Eliminar adaptador**, seleccioneu l'adaptador Ethernet que vulgueu afegir o eliminar.
   - Als camps **Afegir adaptador de còpia de seguretat** o **Eliminar adaptador de còpia de seguretat**, seleccioneu l'adaptador Ethernet que vulgueu comença o deixar d'utilitzar com a còpia de seguretat.
   - Gairebé tots els atributs EtherChannel es poden modificar durant el temps d'execució, excepte l'atribut **Habilitar trames Ethernet jumbo de gigabits**.
   - Per convertir un EtherChannel normal en una acumulació d'enllaços IEEE 802.3ad, canvieu l'atribut **Modalitat** per `8023ad`. Per convertir una acumulació d'enllaços IEEE 802.3ad en un EtherChannel, canvieu l'atribut **Modalitat** per `estàndard` o `rotació de valors`.
5. Empleneu les dades necessàries i feu clic a Intro.

Canvis a l'EtherChannel amb 5200-01 i anteriors:

Utilitzeu aquest procediment per desconnectar la interfície i fer canvis a un EtherChannel amb 5200-01 i anteriors.

1. Escriviu `smitty chinet` i seleccioneu la interfície que pertanyi al vostre EtherChannel. Canvieu l'atribut de l'**estat actual** a **detach** i, a continuació, feu clic a Intro.
2. En la línia d'ordres, escriviu `smitty etherchannel`.
3. Seleccioneu **Canviar / Mostrar característiques d'un EtherChannel / Acumulació d'enllaços** i feu clic a Intro.
4. Seleccioneu l'EtherChannel o Acumulació d'enllaços que vulgueu modificar.
5. Modifiqueu els atributs que vulgueu canviar al vostre EtherChannel o Acumulació d'enllaços i feu clic a Intro.
6. Empleneu els camps necessaris i feu clic a Intro.

Eliminació d'un EtherChannel o d'una acumulació d'enllaços:

Utilitzeu aquest procediment per eliminar un EtherChannel o acumulació d'enllaços.

1. Escriviu `smitty chinet` i seleccioneu la interfície que pertanyi al vostre EtherChannel. Canvieu l'atribut de l'**estat actual** a **detach** i, a continuació, feu clic a Intro.
2. En la línia d'ordres, escriviu `smitty etherchannel`.
3. Seleccioneu **Eliminar un EtherChannel** i feu clic a Intro.
4. Seleccioneu l'EtherChannel que vulgueu eliminar i feu clic a Intro.

Configuració o eliminació d'un adaptador de còpia de seguretat en un EtherChannel o Acumulació d'enllaços existent:

El procediment següent configura o elimina un adaptador de còpia de seguretat o un EtherChannel o Acumulació d'enllaços.

1. Escriviu `smitty chinet` i seleccioneu la interfície que pertanyi al vostre EtherChannel. Canvieu l'atribut de l'**estat actual** a **detach** i, a continuació, feu clic a Intro.

2. En la línia d'ordres, escriviu `smitty etherchannel`.
3. Seleccioneu **Canviar / Mostrar característiques d'un EtherChannel / Acumulació d'enllaços**.
4. Seleccioneu l'EtherChannel o l'Acumulació d'enllaços en el que vulgueu afegir o modificar un adaptador de còpia de seguretat.
5. Escriviu l'adaptador que vulgueu utilitzar com a adaptador de còpia de seguretat al camp **Adaptador de còpia de seguretat** o seleccioneu **NONE** si voleu deixar d'utilitzar l'adaptador de còpia de seguretat.

Configuració d'acumulacions d'enllaços IEEE

L'IEEE 802.3ad és una forma estàndard de dur a terme una acumulació d'enllaços. El concepte és que funciona igual que l'EtherChannel en els diferents adaptadors Ethernet que s'hagin afegir a un sol adaptador virtual, proporcionant així una major amplada de banda i millor protecció contra els errors.

Per exemple, `ent0` i `ent1` es poden afegir a una acumulació d'enllaços IEEE 802.3ad anomenada `ent3`; aleshores, la interfície `ent3` es configuraria amb una adreça IP. El sistema considera aquests adaptadors agregats com un adaptador. A més, l'IP es configura a través d'ells com si ho fes a través de qualsevol altre adaptador Ethernet.

L'IEEE 802.3ad requereix suport al commutador.

Els avantatges d'utilitzar l'acumulador d'enllaços IEEE 802.3ad en comptes de l'EtherChannel són que podeu utilitzar commutadors que donin suport a la normativa IEEE 802.3ad però no a l'EtherChannel i que proporciona protecció contra els errors de l'adaptador.

Quan es configura una acumulació IEEE 802.3ad, els LACPDU (unitats de dades del protocol de control d'acumulacions d'enllaços) s'intercanvien entre la màquina servidor (sistema amfitrió) i el commutador adjacent. Només el canal actiu, que pot ser tant el canal primari com l'adaptador de còpia de seguretat, intercanvia LACPDU amb el commutador adjacent.

Per tal d'acumular adaptadors (el que significa que el conmutador permet que estiguin a la mateixa acumulació) han de tenir la mateixa velocitat de línia (per exemple, tots han de ser de 100 Mbps o tots d'1 Gbps) i han de ser tots dúplex complet. Si intenteu ajuntar adaptadors de velocitat de línia diferents o modalitats de dúplex diferents, la creació de l'acumulació al sistema AIX serà correcta però pot ser que el commutador no acumuli els adaptadors junts. Si el commutador no acumula correctament els adaptadors junts, podria passar que noteu una davallada el rendiment de la xarxa. Per obtenir informació sobre com determinar si l'acumulació en un commutador ha resultat satisfactòria, consulteu l'apartat “Resolució de problemes amb l'acumulació d'enllaços IEEE 802.3ad” a la pàgina 388.

Segons l'especificació de l'IEEE 802.3ad, els paquets enviats a la mateixa adreça IP s'envien a través del mateix adaptador. Per tant, quan es treballa en la modalitat `802.3ad`, els paquets sempre es distribueixen de la manera estàndard, mai de la manera de rotació de valors.

La funció de l'adaptador de còpia de seguretat està disponible per a acumulacions d'enllaços d'IEEE 802.3ad tal com a l'EtherChannel. L'adaptador de còpia de seguretat també compleix amb la IEEE 802.3ad LACP. El port del commutador connectat a l'adaptador de còpia de seguretat també té l'IEEE 802.3ad habilitat.

Nota: Els passos per habilitar la utilització de l'IEEE 802.3ad varien segons el commutador. Heu de consultar la documentació del vostre commutador per tal de determinar quins passos inicial, si n'hi ha, s'han de dur a terme per tal d'habilitar l'LACP al commutador.

Si voleu informació sobre com configurar una acumulació d'IEEE 802.3ad, consulteu l'apartat “Configuració de l'acumulació d'enllaços d'IEEE 802.3ad” a la pàgina 387.

Considereu el següent abans de configurar una acumulació d'enllaços d'IEEE 802.3ad:

- Tot i que oficialment no se'n dóna suport, la implementació a l'AIX de l'IEEE 802.3ad permet que l'acumulació d'enllaços contingui adaptadors de diferents velocitats de línia. No obstant això, només heu d'acumular adaptadors que s'hagin establert a la mateixa velocitat de línia i que estiguin establerts a dúplex complet. Això ajuda a evitar possibles problemes de configuració de l'acumulació d'enllaços al commutador. Per obtenir més informació sobre tipus d'acumulació permeses pel vostre commutador, consulteu la documentació del vostre commutador.
- Si utilitzeu adaptadors d'Ethernet 10/100 a l'acumulador d'enllaços, heu d'habilitar el sondejador d'enllaços en els adaptadors abans d'afegir-los a l'acumulador. Escriviu `smitty chgenet` a la línia d'ordres. Canvieu el valor **Habilitar sondeig d'enllaços** a `sí` i feu clic a Intro. Realitzeu aquesta acció per cada adaptador Ethernet 10/100 que afegiu a l'acumulador d'enllaços.

  Nota: En l'AIX 5L Versió 5.2 amb el paquet de manteniment recomanat 5200-03 i versions posteriors, no cal habilitar el mecanisme de sondeig d'enllaços. El sondeig d'enllaços s'inicia automàticament.

Configuració de l'acumulació d'enllaços d'IEEE 802.3ad:

Seguiu aquests passos per configurar una acumulació d'enllaços d'IEEE 802.3ad

1. Escriviu `smitty etherchannel` a la línia d'ordres.
2. Seleccioneu **Afegir un EtherChannel / Agregació d'enllaç** de la llista i feu clic a Intro.
3. Seleccioneu els adaptadors Ethernet principals que vulgueu a la vostra acumulació d'enllaços i feu clic a Intro. Si penseu utilitzar un adaptador de còpia de seguretat, no seleccioneu l'adaptador que penseu utilitzar per la còpia de seguretat en aquest moment.

   Nota: L'opció **Adaptadors de xarxa disponibles** mostra tots els adaptador Ethernet. Si seleccioneu un adaptador Ethernet que ja s'està fent servir (com a interfície definida), obtindreu un missatge d'error. Primer heu de desconnectar aquestes interfícies si voleu fer-les servir.
4. Escriviu la informació en els camps segons les directrius següents:
   - **Adaptador superior:** Proporciona informació d'un dispositiu superior d'EtherChannel (per exemple, quan un EtherChannel pertany a un adaptador Ethernet compartit). Aquest camp mostra un valor de `NONE` si l'EtherChannel no es troba en cap altre adaptador (valor per defecte). Si l'EtherChannel es troba en algun altre adaptador, aquest camp mostrarà el nom de l'adaptador superior (per exemple, `ent6`). Aquest camp només és informatiu i no es pot modificar. L'opció de l'adaptador superior està disponible en l'AIX 5.3 i posteriors versions.
   - **EtherChannel / Adaptadors d'agregació d'enllaços:** Hauríeu de veure tots els adaptadors principals que esteu utilitzant a la vostra acumulació d'enllaços. Heu seleccionat aquests adaptadors al pas anterior.
   - **Habilitar adreça alternativa:** Aquest camp és opcional. Si establiu aquest camp en `sí` permetreu especificar una adreça MAC que vulgueu que utilitzi l'acumulació d'enllaços. Si establiu aquesta opció en `no`, l'acumulació d'enllaços utilitzarà l'adreça MAC del primer adaptador.
   - **Adreça alternativa:** Si establiu el camp **Habilitar adreça alternativa** en `sí`, especifiqueu l'adreça MAC que vulgueu utilitzar aquí. L'adreça que especifiqueu ha de començar per `0x` i ha de ser una adreça hexadecimal de 12 dígits (per exemple, 0x001122334455).
   - **Habilitar trames Ethernet jumbo:** Aquest camp és opcional. Per utilitzar-lo, el vostre commutador ha de suportar trames jumbo. Aquesta opció només funciona amb la interfície Ethernet estàndard (en) i no amb una interfície IEEE 802.3 (et). Establiu aquesta opció en `sí` si la voleu activar.
   - **Modalitat:** Escriviu `8023ad`.
   - **Modalitat de dispersió**: Podeu triar una de les següents modalitats de dispersió, que determina el valor de les dades que utilitzarà l'algorisme per determinar l'adaptador de sortida:
     - **per defecte**: En aquesta modalitat de dispersió, s'utilitzarà la destinació de l'adreça IP del paquet per determinar l'adaptador de sortida. Pel trànsit no IP (com ara ARP), el darrer octet de l'adreça MAC de destinació s'utilitza per fer el càlcul. Aquesta modalitat garantirà que els paquets s'enviïn a través de l'EtherChannel en l'ordre en què s'han rebut però pot ser que no faci un ús total de l'amplada de banda.

– **port_src**: El valor del port UDP o TCP d'origen del paquet s'utilitza per determinar l'adaptador de sortida. Si el paquet no és trànsit UDP o TCP, s'utilitzarà el darrer octet de l'adreça IP de destinació. Si el paquet no és trànsit IP, s'utilitzarà el darrer octet de l'adreça MAC de destinació.
– **port_dst**: El valor del port UDP o TCP de destinació del paquet s'utilitza per determinar l'adaptador de sortida. Si el paquet no és trànsit UDP o TCP, s'utilitzarà el darrer octet de l'adreça IP de destinació. Si el paquet no és trànsit IP, s'utilitzarà el darrer octet de l'adreça MAC de destinació.
– **port_dst_ src**: Els valors UDP o TCP d'origen i de destinació s'utilitzen per determinar l'adaptador de sortida (específicament, s'afegeixen els ports d'origen i de destinació i després es divideixen en dos abans d'alimentar l'algorisme). Si el paquet no és trànsit UDP o TCP, s'utilitzarà el darrer octet de l'adreça IP de destinació. Si el paquet no és trànsit IP, s'utilitzarà el darrer octet de l'adreça MAC de destinació. Aquesta modalitat pot oferir una bona distribució dels paquets en moltes situacions, tant per clients com per servidors.

Per aprendre més sobre la distribució i l'equilibri de càrrega de paquets, consulteu l'apartat "Opcions de l'equilibri de càrrega EtherChannel" a la pàgina 380.

- **Adaptador de còpia de seguretat** Aquest camp és opcional. Escriviu l'adaptador que vulgueu utilitzar com a còpia de seguretat.
- **Adreça d'Internet per una acció ping:** Aquest camps és opcional i només estarà disponible si disposeu d'un o més adaptadors a l'acumulació principal i a l'adaptador de còpia de seguretat. L'acumulació d'enllaços emet una acció ping a l'adreça IP o al nom d'amfitrió que especifiqueu aquí. Si l'acumulació d'enllaços no aconsegueix dur a terme l'acció ping en aquesta adreça la quantitat de vegades que s'hagi especificat al camp **Nombre de reintents** i en els intervals especificats al camp **Temps d'espera de reintent**, l'acumulació d'enllaços commuta els adaptadors.
- **Nombre de reintents:** Escriviu el nombre d'anomalies en la resposta de l'acció ping que es permeten abans que l'acumulació d'enllaços commuti l'adaptador. El valor per defecte és tres. Aquest camp és opcional i només és vàlid si heu definit una **Adreça d'Internet per una acció ping**.
- **Temps d'espera de reintent:** Escriviu el nombre de segons entre les vegades en què l'acumulació d'enllaços emet una acció ping a l'**Adreça d'Internet per una acció ping**. El valor per defecte és un segon. Aquest camp és opcional i només és vàlid si heu definit una **Adreça d'Internet per una acció ping**.

5. Premeu Intro després de canviar els camps que vulgueu per crear l'acumulació d'enllaços.
6. Configureu l'IP a través del dispositiu d'acumulació d'enllaços que acabeu de crear escrivint `smitty chinet` a la línia d'ordres.
7. Seleccioneu de la llista la nova interfície d'acumulació d'enllaços.
8. Empleneu tots els camps necessaris i i feu clic a Intro.

Resolució de problemes amb l'acumulació d'enllaços IEEE 802.3ad:

Utilitzeu l'ordre **entstat** per resoldre problemes que tingueu amb l'acumulació d'enllaços IEEE 802.3ad

Si esteu tenint problemes amb l'acumulació d'enllaços IEEE 802.3ad, utilitzeu l'ordre següent per verificar la modalitat de funcionament de l'acumulació d'enllaços:

```
entstat -d dispositiu
```

en què *dispositiu* és el dispositiu de l'acumulació d'enllaços.

Així també determineu de forma òptima l'estat del progrés del LACP segons els LACPDU rebuts del commutador. Els següents valors d'estat són possibles:

- `Inactiu`: No s'ha iniciat els LACP. És l'estat quan una acumulació d'enllaços encara no s'ha configurat, perquè encara no se li ha assignat una adreça IP o perquè s'ha desconnectat la seva interfície.

- `Negociant`: El LACP està en progrés però el commutador encara acumulat els adaptadors. Si l'acumulació d'enllaços roman en aquest estat més d'un minut, verifiqueu que s'hagi configurat correctament el commutador. Per exemple, hauríeu de verificar si s'ha habilitat el LACP en els ports.
- `Agregat`: El LACP ha resultat satisfactori i el commutador ha acumulat els adaptadors junts.
- `Error`: El LACP ha fallat. Algunes de les possibles causes són que els adaptadors de l'acumulació estan establerts en diferents velocitats de línia o en modalitat dúplex o que estan connectats a diferents commutadors. Comproveu la configuració dels adaptadors.

  A més, alguns commutadors permeten acumular només ports continus i poden tenir una limitació en el nombre d'adaptadors que es poden acumular. Consulteu la documentació del commutador per determinar les limitacions que pugui tenir el commutador i, a continuació, verifiqueu la configuració del commutador.

Nota: L'estat de l'acumulació d'enllaços és un valor de diagnòstic i no afecta la part de configuració de l'AIX. Aquest valor d'estat s'ha lliurat fent un intnt òptim. Per tal de depurar els possibles problemes d'acumulacions, és millor verificar la configuració del commutador.

Les estadístiques següents d'acumulació d'enllaços IEEE 802.3ad representen l'estat del LACP en cada port de l'acumulació.

Es mostren tant per l'Actor (l'acumulació d'enllaços IEEE 802.3ad) com per l'Associat (el port del commutador).

```
Prioritat del sistema:  el valor de prioritat per aquest sistema.
Sistema: el valor que identifica de forma exclusiva aquest sistema.
Clau operativa: el valor que denota quins ports es poden
        acumular junt
Prioritat de port: el valor de prioritat per aquest port
Port: el valor exclusiu que identifica aquest port a l'acumulació
Estat:
        Activitat LACP: Activa o Passiva - si s'inicia sempre
                l'enviament dels LACPDU o només com a resposta d'un altre
                LACPDU: l'acumulació d'enllaços IEEE 802.3ad funcionarà
                sempre en modalitat Activa.
        Temps d'espera del LACP: Llarg o Curt - temps
                per esperar abans d'enviar els LACPDU: l'acumulació d'enllaços
                IEEE 802.3ad sempre utilitzarà el temps d'espera més llarg.
        Acumulació: Individual o Acumulable - si aquest port
                por dur a terme una acumulació amb altres ports o si només pot
                formar una acumulació amb ell mateix: el port en una
                acumulació d'enllaços IEEE 802.3ad d'un sol adaptador es
                marcarà com Individual, o Acumulable si hi ha més d'un
                port.
        Sincronització: IN_SYNC o OUT_OF_SYNC - si l'acumulació
                ha determinat si ha aconseguit la sincronització
                amb l'associat.
        Recopilació: Habilitada o Inhabilitada - si l'acumulació d'enllaços
                IEEE 802.3ad està recopilant (rebent) paquets.
        Distribució: Habilitada o Inhabilitada - si l'acumulació d'enllaços
                IEEE 802.3ad està distribuint (enviant) paquets.
        Per defecte: Cert o Fals - si l'acumulació d'enllaços
                IEEE 802.3ad està utilitzant els valor per defecte per la
                informació de l'associat.
        Caducat: Cert o Fals - si l'acumulació d'enllaços IEEE 802.3ad
                ha funcionat en modalitat caducada.
```

Les estadístiques següents es mostren tant port per port com per acumulats:

`LACPDU rebuts:` els paquets LACPDU rebuts.
`LACPDU transmesos:` els paquets LACPDU enviats.
`PDU de marcador rebuts:` els PDU de marcador rebuts.
`PDU de marcador transmesos:` els PDU de marcador enviats:
aquesta versió del protocol no implementa el protocol de marcador, per tant, aquestes estadístiques sempre seran zero.
`PDU de resposta del marcador rebuts:` els PDU de marcador rebuts.
`PDU de resposta del marcador transmesos:` els PDU de resposta del marcador enviats:
aquesta versió del protocol no implementa el protocol de marcador, per tant, aquestes estadístiques sempre seran zero.
`PDU desconeguts rebuts:` els PDU rebuts de tipus desconegut.
`PDU no permesos rebuts:` els PDU rebuts de tipus conegut però que estan malformats o que tenen un longitud imprevista o que tenen un subtipus desconegut.

Casos d'interoperabilitat

Tingueu en compte els següents casos d'interoperabilitat quan configureu l'EtherChannel o amb l'acumulació d'enllaços IEEE 802.3ad.

Després de la taula trobareu una explicació addicional de cada cas.

Taula 81. Diferents combinacions de configuració de l'AIX i dels commutadors i els resultats que s'obtindrien amb cada combinació.

Modalitat EtherChannel	Configuració dels commutadors	Resultat
8023ad	IEEE 802.3ad LACP	OK - L'AIX inicia els LACPDU, que desencadenen l'acumulació d'enllaços IEEE 802.3ad al commutador.
estàndard o rotació de valors	EtherChannel	OK - Presenta el comportament tradicional d'EtherChannel.
8023ad	EtherChannel	No desitjable - No es pot afegir cap commutador ni AIX. L'AIX inicia LACPDUs, però el commutador els ignora i no envia LACPDU a l'AIX. Com que falten LACPDU, l'AIX no distribueix els paquets a l'enllaç/port. Com a conseqüència, es perd connectivitat de xarxa.
estàndard o rotació de valors	IEEE 802.3ad LACP	No desitjable - No es pot afegir cap commutador. El resultat pot venir d'un rendiment escàs perquè el commutador trasllada l'adreça MAC entre els ports dels commutadors

A continuació hi trobareu una breu descripció de cada combinació de configuració:

- 8023ad amb EtherChannel:

  En aquest cas, l'AIX enviarà els LACPDU, però quedaran sense resposta perquè el commutador funciona com un EtherChannel. Com que falten LACPDU, AIX no utilitzarà l'enllaç/port per a la distribució de paquets. Com a conseqüència, es perdrà connectivitat de xarxa.

  Nota: En aquest cas, l'ordre `entstat -d` sempre informarà que l'estat de l'agregació s'està negociant. A més a més, a la sortida d'entstat, la secció IEEE 802.3ad Port Statistics mostrarà que la **Distribució** està inhabilitada per a **Actor**.
- estàndard o rotació de valors amb EtherChannel:

  Aquesta és la configuració EtherChannel més habitual.
- estàndard o rotació de valors amb IEEE 802.3ad LACP:

Aquesta configuració no és vàlida. Si el commutador utilitza LACP per crear una acumulació, l'acumulació no s'arribarà a produir mai perquè l'AIX mai respondrà els LACPDU. Perquè funcioni correctament, cal establir `8023ad` a l'AIX.

Adaptadors admesos

L'EtherChannel i l'acumulació d'enllaços IEEE 802.3ad reben suport en els adaptadors Ethernet IBM Power Systems Peripheral Component Interconnect-X (PCI-X) i PCI Express (PCIe).

Hi ha les següents observacions addicionals:

- Adaptador Ethernet d'E/S virtual

  Els adaptadors Ethernet d'E/S Virtual només estan admesos en dos possibles configuracions d'EtherChannel:

  – Un adaptador Ethernet d'E/S Virtual com a principal, un adaptador Ethernet d'E/S Virtual com a còpia de seguretat. En aquesta configuració, l'atribut **Adreça Internet per funció ping** ha d'estar habilitada perquè l'EtherChannel pugui detectar errors de connectivitat remota. Per al Servidor d'E/S virtual (VIOS) 2.2.3.0, o posterior, i l'AIX Versió 7.1 amb Nivell de tecnologia 3 o posterior, podeu utilitzar la característica d'estat de l'enllaç de pujada Ethernet virtual per detectar un error del VIOS o del Adaptador d'Ethernet compartit (SEA) definint l'atribut **`poll_uplink`** del dispositiu Ethernet virtual a `yes`.

  – Un adaptador Ethernet físic admès com a principal, un adaptador Ethernet d'E/S Virtual com a còpia de seguretat. En aquesta configuració, l'atribut **Adreça Internet per funció ping** ha d'estar habilitada perquè l'EtherChannel pugui detectar errors de connectivitat remota.

- Adaptador Ethernet d'amfitrió (HEA)

  Els ports lògics HEA reben suport EtherChannel si tots els adaptadors de l'EtherChannel són ports lògics HEA. Per al port HEA dedicat, l'agregació d'enllaços amb l'adaptador PCI/PCI-E està admesa. A més a més, també s'admet un adaptador PCI/PCI-E i Ethernet virtual com a adaptador de reserva (si l'adaptador principal conté HEA).

  Si utilitzeu diversos ports lògics HEA com a adaptadors principals a un EtherChannel, els ports físics associats amb els ports lògics HEA també s'hauran de col•locar en un EtherChannel del commutador Ethernet. En conseqüència, totes les particions que utilitzin els ports lògics HEA per anar als mateixos ports físics HEA també s'hauran de col•locar a un EtherChannel.

  Per exemple, suposeu que la partició 1 està configurada de la manera següent:

  – Un port HEA lògic del port HEA físic 0

  – Un port HEA lògic del port HEA físic 1

  – Un EtherChannel creat mitjançant els ports HEA lògics anomenats anteriorment

  Si una altra partició del mateix sistema ha de fer servir un port HEA lògic del port HEA físic 0 del port HEA físic 1, haureu de crear un EtherChannel per la partició per als dos ports HEA lògics, de manera similar a la configuració de la partició 1. Si intenteu utilitzar qualsevol dels ports HEA lògics com a ports independents a altres particions, és possible que es produeixin problemes de connectivitat degut a que és possible que els paquets no es lliurin al port HEA lògic adient.

  La restricció no existeix si s'utilitzen ports HEA lògics a la configuració de la còpia de seguretat de la interfície de xarxa (1 principal 1 còpia de seguretat), donat que els ports HEA físics no necessiten cap configuració específica al commutador Ethernet.

  Nota: Si els ports lògics dels ports HEA físics estan configurats com a part de l'agregació LACP (802.3ad), aleshores aquests ports físics han de ser exclusius de l'LPAR. L'HMC no impedeix que els ports s'assignin a altres LPAR, però no n'admet la configuració.

- Fibre Channel sobre adaptadors de xarxa Ethernet convergits

  L'agregació d'un enllaç entre un port compartit (un port que s'utilitza pel trànsit Ethernet i pel canal de fibra) i altres adaptadors admesos només s'admet si el commutador està connectat al port compartit i admet l'agregació de l'enllaç sense tenir cap impacte al trànsit del canal de fibra.

- Adaptadors de virtualització E/S d'arrel única (SR-IOV)

L'agregació d'enllaços amb pots lògics SR-IOV es pot adreçar mitjançant un dels mètodes següents:

- Agregació d'enllaços IEEE 802.3ad, també coneguda com Protocol de control d'agregació d'enllaços (Link Aggregation Control Protocol - LACP)
- Recolzament de seguretat d'interfícies de xarxa (Network Interface Backup - NIB)
- Ambdós (LACP i NIB)

Per aplicacions de xarxa on és necessària l'amplada de banda de més d'un sol port, es pot utilitzar l'agregació d'enllaços IEEE 802.3ad per agregar diversos ports lògics SR-IOV. Un port lògic SR-IOV agregat mitjançant l'agregació d'enllaços IEEE 802.3ad ha d'ésser l'únic port lògic configurat per al port físic. És possible que diversos ports lògics SR-IOV configurats per al mateix port físic, on un dels ports lògics està configurat per formar part d'una configuració d'agregació d'enllaços IEEE 802.3ad, no siguin gestionats correctament pel commutador perquè més d'un soci LACP s'estigui comunicant a través del port físic. Per evitar la configuració d'un segon port lògic SR-IOV al mateix port físic que el port lògic on hi ha una configuració d'agregació d'enllaços IEEE 802.3ad, el valor de capacitat del port lògic s'ha de definir en 100 (100%) quan es configuri el port lògic.

Per aplicacions de xarxa on és necessària l'amplada de banda de menys d'un sol port juntament amb protecció contra un error de xarxa, els ports lògics SR-IOV poden ser part d'una configuració NIB. Quan es configura un port lògic SR-IOV com a adaptador primari o de còpia de seguretat en una configuració NIB, el port físic es pot compartir amb altres ports lògics SR-IOV. En aquesta configuració, l'atribut **Adreça Internet per fer ping** es pot habilitar per detectar errors de connectivitat remota. Els ports lògics SR-IOV poden ser l'adaptador primari o de còpia de seguretat per a un altre port lògic SR-IOV, un adaptador Ethernet virtual o un port d'adaptador físic.

Per obtenir informació addicional de releases sobre els nous adaptadors, consulteu les AIXNotes del release que corresponguin al vostre nivell de l'AIX.

Important: No es permet barrejar adaptadors de diferents velocitats el mateix EtherChannel, fins i tot si un d'ells està funcionant com a adaptador de còpia de seguretat. Això *no* significa que aquestes configuracions no funcionin. El programa de control d'EtherChannel fa tot el possible per funcionar fins i tot en casos amb barreja de velocitats.

Informació relacionada:

Virtualització d'E/S arrel única

Resolució de problemes de l'EtherChannel

Si teniu problemes amb l'EtherChannel, hi ha uns quants casos a tenir en compte.

Podeu utilitzar la traça i les estadístiques com ajuda per emetre un diagnòstic d'un problema, que pot implicar problemes amb migració després d'un error i trames jumbo.

Rastreig de l'EtherChannel:

Utilitzeu **tcpdump** i **iptrace** per arreglar problemes a l'EtherChannel.

L'ID d'enganxament de la traça pels paquets de la transmissió és 2FA i per les altres incidències és 2FB. No podeu fer una traça de paquets a l'EtherChannel com un total, però podeu traçar els enganxaments de traça de cada adaptador.

Estadístiques de l'EtherChannel:

Utilitzeu l'ordre **entstat** per obtenir les estadístiques afegides de tots els adaptadors de l'EtherChannel.

Per exemple, `entstat ent3` mostrarà les estadístiques afegides de l'ent3. Si afegim el senyalador **-d** també es mostraran les estadístiques de cada adaptador de forma individual. Per exemple, si escrivim `entstat -d ent3` apareixeran les estadístiques afegides de l'EtherChannel i també les estadístiques de cada adaptador individual de l'EtherChannel.

Nota: A l'apartat `Estadístiques generals`, el nombre que apareix a `Recompte de restabliments d'adaptadors` és el nombre de migracions després d'un error. En la còpia de seguretat de l'EtherChannel, que torna a l'EtherChannel principal de l'adaptador de còpia de seguretat, no es comptarà com una migració després d'un error. Només es comptabilitzar una migració després d'un error del canal principal a la còpia de seguretat.

Al camp `Nombre d'adaptadors`, l'adaptador de còpia de seguretat es compta al nombre que es visualitza.

Migració després d'un error lenta:

Si la cadència de la migració després d'un error quan s'està utilitzant la modalitat de còpia de seguretat de la interfície de xarxa o la còpia de seguretat de l'EtherChannel és lenta, comproveu si el commutador està executant l'STP (Spanning Tree Protocol).

Quan el commutador detecta un canvi en el mapatge del port del commutador a l'adreça MAC, executa l'algorisme de diagrama per veure si hi ha bucles a la xarxa. La còpia de seguretat de la interfície de la xarxa i la còpia de seguretat de l'EtherChannel poden provocar un canvi al port del mapatge de l'adreça MAC.

Els ports del commutadors tenen un comptador de retards de reenviament que determina la freqüència en què cada port d'inicialització hauria d'enviar o reenviar paquets. Per aquest motiu, quan es torna a habilitar el canal principal, hi ha un retard fins que no es torna a establir la connexió, mentre que la migració després d'un error a l'adaptador de còpia de seguretat és més ràpida. Comproveu el comptador de retards de reenviament del vostre sistema i feu-lo tan petit com sigui possible perquè la tornada al canal principal sigui el més ràpida possible.

Perquè la funció de còpia de seguretat de l'EtherChannel funcioni correctament, el comptador de retards de reenviament no pot ser de més de 10 segons, o la tornada a l'EtherChannel principal podria no funcionar correctament. Es recomana establir el comptador de retards de reenviament al valor més baix que sigui permès.

Adaptadors que no tenen migració després d'un error:

Si els errors d'un adaptador no desencadenen en migracions després d'un error i esteu executant l'AIX 5.2 amb 5200-01 o una versió anterior, comproveu si la vostra targeta adaptadora necessita que se li habiliti el sondeig d'enllaços perquè detecti els errors d'enllaços.

Alguns adaptadors no poden detectar automàticament l'estat dels seus propis enllaços. Per detectar aquesta condició, aquests adaptadors han d'habilitar un mecanisme de sondeig d'enllaços que iniciï un temporitzador que periòdicament verifica l'estat de l'enllaç. El sondeig d'enllaços està inhabilitat per defecte. No obstant això, perquè l'EtherChannel funcioni correctament amb aquests adaptadors, el mecanisme de sondeig d'enllaços ha d'estar habilitat en cada adaptador abans que es creï l'EtherChannel. Si esteu executant l'AIX 5L Versió 5.2 amb el paquet de manteniment recomanat 5200-03 o alguna versió posterior, el sondeig d'enllaços s'inicia automàticament i no pot representar cap problema.

Els adaptadors que tenen un mecanisme de sondeig d'enllaços tenen un atribut ODM anomenat **poll_link**, que s'ha d'establir a `yes` per habilitar el sondeig d'enllaços. Abans de crear l'EtherChannel, utilitzeu l'ordre següent en cada adaptador que s'ha d'incloure al canal:

```
smitty chgenet
```

Canvieu el valor **Habilitar sondeig d'enllaços** a `yes` i feu clic a Intro.

Trames jumbo:

A banda d'habilitar l'atribut **use_jumbo_frame** a l'EtherChannel, també heu d'habilitar les trames a cada adaptador abans de crear l'EtherChannel.

Per fer-ho, executeu l'ordre següent:

```
smitty chgenet
```

Les trames jumbo estan habilitades automàticament a cada adaptador subjacent quan l'atribut **use_jumbo_frame** d'un EtherChannel s'ha establert l'opció a sí.

Buidatge remot:

No es dóna suport al buidatge remot a través de l'EtherChannel.

Protocol d'Internet a través d'InfiniBand (IPoIB)

Els paquets del protocol d'Internet (IP) es poden enviar a través de la interfície InfiniBand (IB). Aquest transport es du a terme encapsulant paquets IP de paquets IB mitjançant una interfície de xarxa.

Per tal d'utilitzar l'IP a través d'IB, heu d'instal•lar i configurar el programa de control gestor de connexió d'InfiniBand ICM) al menys en un dispositiu IB del sistema. Si voleu veure si ja hi ha un dispositiu IB instal•lat, executeu l'ordre **lsdev -C | grep iba**. El nom del catàleg de fitxers que conté la interfície IB és: `devices.common.IBM.ib`. El catàleg de fitxers `devices.chrp.IBM.lhca` és un exemple d'un catàleg de fitxers de l'adaptador al qual es dóna suport actualment.

Per tal de configurar un programa de control d'ICM, consulteu l'apartat "Configuració d'un programa de control del gestor de comunicacions InfiniBand" a la pàgina 396.

Per crear la interfície InfiniBand (IB IF), l'IB IF s'ha de poder acoblar a un grup de difusió múltiple ja existent amb un PKEY proporcionat per l'usuari (o s'utilitza un PKEY = 0xFFFF per defecte si l'usuari no en proporciona cap) i un Q_Key proporcionat per l'usuari (o un Q_Key = 0x1E per defecte si l'usuari no en proporciona cap). Un grup de difusió múltiple és un grup emissió simultània al qual s'ha d'acoblar la interfície per enviar difusions i paquets **ARP**. Si no existeix cap grup de difusió múltiple, o la interfície no el pot crear, es produirà un error quan es creï l'IB IF.

Podeu crear o canviar un IB IF utilitzant la interfície de línia d'ordres o la interfície d'usuari de la SMIT. Els paràmetres necessaris per crear un IB IF són els següents:

- *nom d'interfície*
- *nom d'adaptador*
- *número de port*
- *adreça IP de l'interfície*

Els paràmetres següents són per canviar l'IB IF:

- *adreça d'Internet*
- *màscara de xarxa*
- *grandària de MTU* (equival a l'MTU desitjada, menys de 4 octets per capçalera IB)
- *estat*
- *Mida de la cua d'enviament i recepció (el valor per defecte és 4000)*
- *Clau de cua de transmissió a grups*
- *Superpaquet activat i desactivat*

A continuació trobareu un exemple de de l'ordre utilitzada per crear un IB IF des de la línia d'ordres:

```
$ /usr/sbin/mkiba -i ib0 -p 1 -A iba0 -a 1.2.3.8 [-P -1 -S "up" -m "255.255.254.0" -M 2044]
```

en què:

Element	Descripció
`-M 2044`	Unitat de transmissió màxima.
`-m "255.255.254.0"`	Màscara de xarxa.
`-p 1`	Número de port (pren per defecte el valor *1* si no se n'indica cap).
`-A iba0`	Nom de dispositiu IB.
`-a 1.2.3.8`	Adreça IF IP.
`-i ib0`	Nom d'interfície.
`-P -1`	Clau de partició (pren per defecte el valor *PKEY* si no se'n proporciona cap. Després de crear una interfície, no es podrà canviar el valor PKEY. L'usuari haurà d'obtenir de l'administrador de xarxa un PKEY que no sigui el valor per defecte.)
`-S "up"`	Estat de la interfície.
`-q 8000`	Mida de les cues de recepció i transmissió (cadascuna).
`-Q 0x1E`	Clau de cua de transmissió a grups assignada al grup de transmissió a grups (el valor per defecte és Q_KEY = 0x1E si no es proporciona).
`-k "on"`	El superpaquet permetrà que l'MTU TCP/IP de la interfície sigui de 64K. Per funcionar s'ha d'habilitar a l'amfitrió remot.

A continuació trobareu un exemple de l'ordre utilitzada per crear un IB IF a partir de la interfície d'usuari de la SMIT.

```
$ smitty inet
```

Després de visualitzar el menú Selecció d'interfície de xarxa, seguiu aquest procediment:

1. Seleccioneu **Afegir una interfície de xarxa** o **Canviar / Mostrar característiques duna interfície de xarxa**. Apareixerà el menú Afegir una interfície de xarxa.
2. Al menú Afegir una interfície de xarxa, seleccioneu **Afegir una interfície de xarxa IB**. Apareixerà el menú Afegir una interfície de la xarxa IB.
3. A menú Afegir una interfície de la xarxa IB, feu els canvis que calgui i feu clic a Intro.

Creació, visualització, addició i supressió d'entrades ARP i modificació de temporitzadors ARP

Una entrada **Protocol de resolució d'adreces (ARP - Address Resolution Protocol)** permet que una interfície es comuniqui amb una altra interfície fins i tot si no estan al mateix grup de difusió múltiple.

Una entrada **ARP** es pot crear manualment utilitzant l'ordre **arp -t ib**.

Per visualitzar totes les entrades **ARP**, executeu l'ordre **$ arp -t ib -a**. Si voleu visualitzar un nombre específic d'entrades **ARP**, podeu especificar-ne el nombre. Per exemple, `$ arp -t ib -a 5` mostra 5 entrades **ARP**.

L'ordre següent afegeix una entrada **ARP**:

```
$ arp -t ib -s nom interfície IB dlid <16 bits DLID> dqp
16 bits hex Destination Queue Pair Number
ipaddr <Adreça IP de destinació>
```

en què:

Element	Descripció
DLID	és l'ID local de la destinació.
DGID	és l'ID global de la destinació.

Amb l'ordre següent s'elimina una entrada **ARP**:

```
$ arp -t ib -d Adreça IP
```

L'ordre següent modifica els valors de temporitzador d'entrada ARP per a les entrades ARP completes i incompletes. Aquests valors s'utilitzen per eliminar les entrades ARP després d'un període de temps:

```
arp –t ib –i <número en minuts complets per eliminar entrades ARP incompletes>
-c <número en minuts complets per eliminar entrades ARP completes>
```

El temps per defecte actual per a les entrades ARP incompletes que s'han d'eliminar és de 3 minuts. Per a les entrades ARP completes, el temps per defecte és de 24 hores. Si els valors s'han de canviar, l'execució de l'ordre canviarà només els valors de totes les interfícies actuals configurades (o en estat definit). Si es configuren noves interfícies, l'ordre s'ha de tornar a executar. Els valors també canvien a l'ODM.

Per canviar els valors dinàmicament a una interfície específica, executeu l'ordre **ifconfig**:

```
To change the incomplete ARP entry timer
ifconfig ib0 inc_timer 4
ifconfig ib0 com_timer 60
```

Canvi dels paràmetres d'una interfície InfiniBand

Per canviar els paràmetres d'una IB IF, utilitzeu la interfície d'usuari de la SMIT o les ordres de la línia d'ordres.

Per canviar els paràmetres d'una IB IF utilitzant la SMIT:

1. Executeu l'ordre **$ smitty inet**. Apareixerà el menú Selecció d'interfície de xarxa.
2. Al menú Selecció d'interfície de xarxa seleccioneu **Canviar / Mostrar les característiques d'una interfície de xarxa**. Apareixerà el menú Interfícies de xarxa disponibles.
3. Al menú Interfícies de xarxa disponibles, seleccioneu **Interfície InfiniBand**. Apareixerà el menú Canviar / Mostrar una interfície IB.
4. Canvieu els paràmetres que vulgueu.

Per canviar els paràmetres d'IB IF a la línia d'ordres, executeu l'ordre **$ ifconfig**. L'ordre següent canvia els paràmetres d'IB IF des de la línia d'ordres:

```
$ ifconfig ib0 [ib_port número de port mtu unitat de transmissió màxima p_key
clau de partició hexadecimal de 16 bits  ib_adapter nom adaptador InfiniBand netmask
decimals amb punt]
$ ifconfig ib0 inc_timer  3  com_timer 60
```

- *inc_timer* és el temps en minuts que ha de transcórrer per tal que una entrada ARP incompleta caduqui. El valor per defecte és de 2 minuts.
- *com_timer* és el temps en minuts que ha de transcórrer per tal que una entrada ARP completa caduqui. El valor per defecte és 24 hores.

Configuració d'un programa de control del gestor de comunicacions InfiniBand

Utilitzeu aquest procediment per configurar un gestor de comunicacions InfiniBand.

1. Executeu l'ordre **$ smitty icm**. Apareixerà el menú del gestor de comunicacions InfiniBand.
2. Al menú del gestor de comunicacions InfiniBand, seleccioneu **Afegir un gestor de comunicacions InfiniBand**.
3. Al menú Afegir gestor de comunicacions InfiniBand, seleccioneu **Afegir un gestor de comunicacions InfiniBand**. Apareixerà el menú Nom del gestor de comunicacions IB que s'ha d'afegir.
4. Al menú Nom del gestor de comunicacions IB que s'ha d'afegir, seleccioneu **icm InfiniBand de gestió**.
5. Utilitzeu els valors per defecte o canvieu els paràmetres necessaris i, a continuació, feu clic a Intro.

Iniciador de programari iSCSI i destinació de programari

L'iniciador de programari iSCSI permet que AIX accedeixi als dispositius d'emmagatzematge utilitzant TCP/IP als adaptadors de xarxa Ethernet. La destinació del programari iSCSI permet a AIX exportar emmagatzematge local al qual es pot accedir mitjançant altres iniciadors iSCSI utilitzant el protocol iSCSI que es defineix a RFC 3720.

La utilització de tecnologia iSCSI, a la que habitualment es fa referència com SAN en tecnologia IP, permet fer un desplegament d'emmagatzematge del treball en xarxa de l'àrea d'emmagatzematge en una xarxa IP. L'iSCSI és un mètode obert que es basa en patrons que tenen informació SCSI encapsulada per **TCP/IP** que permet que es transporti a través d'Ethernet i de xarxes Ethernet de gigabits. L'iSCSI permet que una xarxa Ethernet existent pugui transferir ordres i dades de SCSI amb total independència de la ubicació. Les solucions iSCSI utilitzen els components següents diferents però relacionats íntegrament:

- Iniciadors

  Es tracta dels programes de control de dispositiu que resideixen al client. Encapsulen ordres de SCSI i les encaminen a través de la xarxa IP al dispositiu de destinació.
- Programari de destinació

  El programari rep les ordres de SCSI encapsulades a través de la xarxa IP. El programari també pot proporcionar suport de configuració i suport de gestió d'emmagatzematge.
- Maquinari de destinació

  el maquinari pot ser una aplicació d'emmagatzematge que contingui emmagatzematge intercalat. El maquinari també pot ser una passarel•la o un producte pont que no contin emmagatzematge intern propi.

Configuració DE L'iniciador de programari iSCSI

L'iniciador de programari es configura utilitzant la SMIT tal com mostra aquest procediment.

1. Seleccioneu **Dispositius**.
2. Seleccioneu **iSCSI**.
3. Seleccioneu **Configurar dispositiu del protocol iSCSI**.
4. Seleccioneu **Canviar / Mostrar característiques d'un dispositiu del protocol iSCSI**
5. Verifiqueu que el valor **Nom de l'iniciador** sigui correcte. El valor **Nom de l'iniciador** l'utilitza la destinació d'iSCSI durant l'inici de sessió.

   Nota: Quan s'instal•la el programari s'assigna un nom d'iniciador per defecte. Aquest nom d'iniciador el pot canviar l'usuari per fer-lo coincidir amb els convenis de denominació de la xarxa local.
6. El camp **Nombre màxim de destinacions permeses** correspon al nombre màxim de de destinacions iSCSI que es poden configurar. Si en reduïu aquest nombre, també reduireu la quantitat de memòria de xarxa preassignada pel programa de control del protocol iSCSI durant la configuració.
7. Configureu el mètode descobriment iSCSI utilitzant el camp **Política de descobriments** per descobrir les destinacions d'iSCSI. El programari iniciador d'iSCSI admet els 4 mètodes de descobriment següents:

   fitxer La informació sobre destinacions està emmagatzemada en un fitxer de configuració.

   odm La informació sobre destinacions està emmagatzemada en els objectes gestor de dades d'objecte (ODM). Quan utilitzeu un disc iSCSI com a disc d'arrencada o com a part de l'arrencada **rootvg**, heu d'utilitzar el mètode de descobriment **odm**. Vegeu Afegir una destinació iSCSI descoberta estàticament a ODM .

   isns La informació sobre les destinacions està emmagatzemada en un servidor Internet Storage Name Service (iSNS) i es recupera automàticament durant la configuració de l'iniciador iSCSI.

   slp La informació sobre les destinacions està emmagatzemada en un agent de servidors d'Internet Storage Name Service (SLP) i es recupera automàticament durant la configuració de l'iniciador iSCSI.

Després de configurar l'iniciador de programari, feu el següent:

1. Si la política de descobriments és **fitxer**, editeu el fitxer `/etc/iscsi/targets` per incloure les destinacions iSCSI necessàries durant la configuració del dispositiu.

   Cada línia descomentada del fitxer representa una destinació iSCSI.Per obtenir més informació, consulteu l'apartat sobre el Fitxer de destinacions de la publicació *Files Reference*.

Si la política de descobriments és **odm**, utilitzeu l'ordre **mkiscsi** o els panells smit per crear les definicions de destinació a ODM. Per obtenir més informació, vegeu Afegir una destinació iSCSI descoberta estàticament a ODM.

Si la política de descobriments és **isns** o **slp**, assegureu-vos que el servidor iSNS o SLP estigui ben configurat i sigui accessible mitjançant l'iniciador iSCSI.

La configuració de dispositius iSCSI requereix que es pugui arribar a les destinacions iSCSI a través d'una interfície de xarxa degudament configurada. Tot i que l'iniciador del programari d'iSCSI pugui funcionar utilitzant una xarxa d'àrea local d'Ethernet 10/100, està dissenyada perquè s'utilitzi amb una xarxa Ethernet gigabit diferent d'un altre trànsit de xarxa.

2. Després de definir les destinacions, escriviu l'ordre següent:

   ```
   cfgmgr -l iscsi0
   ```

   Així es tornarà a configurar el controlador iniciador del programari.

   Aquesta ordre fa que el programa de control intenti comunicar-se amb les destinacions llistades al fitxer `/etc/iscsi/targets` i definir un nou hdisk per a cada LUN de les destinacions que trobi. Per obtenir més informació, consulteu l'apartat sobre la descripció de l'ordre **cfgmgr** de la publicació *Commands Reference, Volume 1*.

   Nota: Si no s'han definit els discs corresponents, reviseu la configuració de l'iniciador, la destinació i totes les passarel•les d'iSCSI per tal de garantir que siguin correctes i, a continuació, torneu a executar l'ordre **cfgmgr**.

Si voleu configurar altres paràmetres pels dispositius de l'iniciador de programari iSCSI, utilitzeu la SMIT tal com s'indica a continuació:

1. Seleccioneu **Dispositius**.
2. Seleccioneu **Disc fix**.

Un dispositiu de l'iniciador de programari típic s'assemblaria al següent:

```
hdisk2   Available             Other iSCSI Disk Drive
```

Si el disc d'iSCSI dóna suport a la cua d'etiquetes d'ordres i NACA=1 en l'octet de control, considereu la possibilitat de canviar el valor de profunditat de cua del disc per un valor més gran. Un valor més gran podria millorar el rendiment del dispositiu. El valor òptim de profunditat de la cua no ha de superar la grandària actual de la cua de la unitat. Si establiu la profunditat de la cua en un valor més gran que la grandària de la cua de la unitat, probablement es degradaria el rendiment. Per tal de determinar la grandària de la cua de la unitat, consulteu la documentació de la unitat.

Configuració de la destinació del programari iSCSI

El programa de control del programari iSCSI permet que l'AIX actuï com a dispositiu de destinació iSCSI o com a diversos dispositius de destinació iSCSI. El programa de control de destinació iSCSI exporta els discos locals, els volums lògics o els fitxers locals als iniciadors iSCSI que es connecten a l'AIX per mitjà del protocol iSCSI i TCP/IP.

Cada dispositiu de destinació té un nom qualificat d'iSCSI i un conjunt de números d'unitat lògica (LUN) que estan disponibles per als iniciadors que es connecten a la destinació iSCSI virtual. Per a cada dispositiu de destinació, podeu especificar quina interfície de xarxa i quins números de port TCP/IP pot utilitzar el programa de control de destinació per acceptar les connexions entrants.

Nota: El catàleg de fitxers de destinació iSCSI ha d'estar instal•lat. El nom del catàleg de fitxers és devices.tmiscsw.rte i forma part del paquet d'expansió de l'AIX.

Per configurar un programa de control de destinació iSCSI, realitzeu els passos següents:

1. Creeu una sola instància del programa de control de destinació d'iSCSI mitjançant el següent camí d'accés de l'SMIT. Aquesta instància actua com a contenidor d'altres objectes d'iSCSI.

Dispositius > **iSCSI** > **Dispositiu de destinació iSCSI** > **Dispositiu de protocol de destinació iSCSI** > **Afegir un dispositiu de protocol de destinació iSCSI**

2. Creeu un dispositiu de destinació iSCSI per a cada destinació iSCSI virtual assignada pel programa de control de destinació iSCSI. Utilitzeu el següent camí d'accés de l'SMIT per crear cadascun dels dispositius de destinació iSCSI:

   Dispositius > **iSCSI** > **Dispositius de destinació iSCSI** > **Destinacions iSCSI** > **Afegir una destinació iSCSI**

3. Definiu un o diversos LUN per a cada dispositiu de destinació mitjançant el següent camí d'accés de l'SMIT:

   Nota: Els LUN estan accessibles pels iniciadors que es connecten a una destinació virtual. A la destinació iSCSI, cada LUN es pot associar amb un volum lògic prèviament definit, amb un volum físic o amb un fitxer creat prèviament en un sistema de fitxers local. El sistema AIX que executa el programa de control de destinació iSCSI no pot utilitzar cap volum físic que estigui associat amb una unitat lògica de destinació iSCSI.

   Dispositius > **iSCSI** > **Dispositiu de destinació iSCSI** > **Números d'unitat lògica de destinació iSCSI**

   Amb aquest pas s'acostuma a finalitzar la configuració. Tanmateix, si utilitzeu el protocol CHAP (Challenge Handshake Authentication Protocol), o si feu servir ACL (Llistes de control d'accés) per indicar quins iniciadors poden accedir als LUN, potser cal realitzar un pas addicional per completar la configuració de la destinació.

   - Si utilitzeu l'autenticació CHAP dels iniciadors, editeu el fitxer `/etc/tmiscsi/autosecrets` i afegiu-hi els secrets utilitzats pels iniciadors per iniciar la sessió. El fitxer `/etc/tmiscsi/autosecrets` conté una entrada per destinació. Cada entrada té el format següent:

     nom_destinació nom_chap secret_chap

   - Si utilitzeu les ACL per indicar quins iniciadors poden accedir als LUN, editeu el fitxer `/etc/tmiscsi/access_lists` i afegiu-hi una entrada per destinació. Cada entrada té el format següent:

     nom_destinació|*nom_lun nom_iSCSI*, *nom_iSCSI,...*

Informació relacionada:

/etc/tmiscsi/autosecrets

/etc/tmiscsi/access_lists

/etc/tmiscsi/isns_servers

Consideracions sobre l'iniciador de programari iSCSI.

Tingueu en compte el següent a l'hora de tractar amb iniciadors de programari iSCSI.

- Descoberta de la destinació

  L'iniciador de programari iSCSI admet les 4 formes següents de descobriment de destinacions:

  fitxer Per configurar cada destinació s'utilitza un fitxer de text.

  odm Els objectes ODM s'utilitzen per configurar cada destinació. Quan utilitzeu un disc iSCSI com a disc d'arrencada o com a part de l'arrencada rootvg, heu d'utilitzar el mètode de descobriment **odm**.

  isns Cada destinació està registrada en un o diversos servidors d'Internet Storage Name Service (iSNS).

  slp Cada destinació està registrada en un o diversos agents de serveis o de directoris de Service Location Protocol (SLP).

- Autenticació iSCSI

  Només es pot utilitzar CHAP(MD5) per configurar la autenticació de l'iniciador. L'autenticació de la destinació no s'implementa.

- Nombre de LUN configurades

El nombre màxim de LUN configurades i provades que utilitzin l'iniciador de programari iSCSI és de 128 per destinació iSCSI. L'iniciador de programari utilitza una connexió TCP simple per cada destinació iSCSI (una connexió per sessió iSCSI). Aquesta connexió TCP es comparteix amb totes les LUN que estiguin configurades a una destinació. L'espai de rebre i d'enviar del sòcol TCP de l'iniciador de programari s'han establert al valor màxim del buffer del sòcol del sistema. El valor màxim s'estableix mitjançant l'opció de xarxa **sb_max**. El valor per defecte és 1 MB.

- Grups de volums

  Per tal d'evitar problemes de configuració i entrades d'enregistrament d'errors quan creeu grups de volums utilitzant els dispositius iSCSI, seguiu aquestes directrius:

  – Configureu grups de volums que es creïn mitjançant dispositius iSCSI per tal que tingui un estat d'inactivitat després de la reengegada. Un cop hagueu configurat els dispositius iSCSI, activeu manualment els grups de volums amb còpia de seguretat iSCSI. Aleshores, munteu els sistemes de fitxers associats.

    Els grups de volums s'activen durant una fase d'engegada diferent de la del programa de control de programari iSCSI. Per aquesta raó, no es poden activar grups de volums iSCSI durant el procés d'engegada.

  – No amplieu grups de volums per dispositius que no siguin iSCSI.

- Anomalies d'E/S

  Si es perd la connectivitat amb els dispositius de destinació iSCSI, es produiran anomalies d'E/S. Per tal d'evitar les anomalies d'E/S i la corrupció del sistema de fitxers, atureu del tot l'activitat d'E/S i desmunteu tots els sistemes de fitxer dels que s'hagi fent còpia de seguretat iSCSI abans de fer res que pugui provocar una gran pèrdua de connectivitat per activar les destinacions iSCSI.

  Si es produeix una pèrdua de connectivitat en les destinacions iSCSI mentre les aplicacions intenten dur a terme activitats d'E/S amb dispositius iSCSI, a la llarga es produiran errors d'E/S. Potser no serà possible desmuntar els sistemes de fitxers dels que s'ha fet còpia de seguretat d'iSCSI perquè el dispositiu iSCSI subjacent continua ocupat.

  Cal dur a terme un manteniment del sistema de fitxers si es produeixen anomalies d'E/S per una pèrdua de connectivitat si es volen activar les destinacions d'iSCSI. Per dur a terme un manteniment del sistema, executeu l'ordre **fsck**.

- No utilitzeu l'iniciador de programari iSCSI de l'AIX ni la destinació de programari iSCSI de l'AIX amb la interfície de bucle de retorn (`lo0`). El processament de les interrupcions de la interfície de bucle de retorn és diferent del processament de les interrupcions de les interfícies dels adaptadors de xarxa Ethernet físics o virtuals. El sistema operatiu AIX podria aturar-se si s'utilitza la interfície de bucle de retorn amb els controladors de programari iSCSI.

Informació relacionada:

Addició d'una destinació iSCSI descoberta estàticament a ODM

Consideracions de seguretat iSCSI:

El directori `/etc/iscsi`, el directori `/etc/tmiscsi` i els fitxers d'aquests directoris estan protegits contra els usuaris no privilegiats mitjançant un permís i una propietat de fitxer.

Els secrets del CHAP es desen al fitxer `/etc/iscsi/targets` i al fitxer `/etc/tmiscsi/autosecrets` en text clar.

Nota: No canvieu el permís ni la propietat originals d'aquests fitxers.

Consideracions de rendiment d l'iSCSI:

Estabiu les configuracions següents per tal d'obtenir el millor rendiment de l'iSCSI.

Per tal de garantir el millor rendiment:

- Habiliteu les funcions d'enviament llarg TCP, de control de fluxos d'enviament i recepció de TCP i de les trames jumbo de l'adaptador Ethernet de gigabits de l'AIX i de la interfície de destinació de l'iSCSI.
- Sintonitzeu les opcions de xarxa i els paràmetres de la interfície per obtenir el màxim rendiment d'E/S en el sistema de l'AIX tal com s'indica a continuació:
  - Habiliteu l'opció de xarxa de l'RFC 1323.
  - Configureu les opcions de xarxa **tcp_sendspace**, **tcp_recvspace**, **sb_max** i **mtu_size** i les opcions de la interfície de la xarxa amb els valors adequats.

    La grandària màxima de transferència de l'iniciador de programari iSCSI és de 256 KB. Si suposem que els màxims del sistema per **tcp_sendspace** i **tcp_recvspace** estan establerts a 262144 octets, una ordre **ifconfig** utilitzada per configurar una interfície Ethernet de gigabits podria tenir un aspecte similar al següent:

    ```
    ifconfig en2 10.1.2.216 mtu 9000 tcp_sendspace 262144 tcp_recvspace 262144
    ```
  - Estabiu l'opció de xarxa **sb_max** al valor 524288, com a mínim. Seria preferible el valor 1048576.
  - Estabiu **mtu_size** a 9000.
  - Per algunes destinacions iSCSI, cal que l'algorisme Nagle de TCP estigui inhabilitat per obtenir el millor rendiment. Utilitzeu l'ordre **no** per establir el paràmetre **tcp_nagle_limit** a `0`, per inhabilitar l'algorisme Nagle.

Nota: Per obtenir informació sobre com establir les opcions de xarxa, consulteu la descripció de l'ordre **no** a la publicació *Commands Reference, Volume 4*.

Per obtenir més informació i paràmetres addicionals per la sintonització, consulteu l'apartat Ajustament del rendiment TCP i UDP.

Consideracions sobre la destinació de programari iSCSI.

Quan definiu una destinació de programari iSCSI i exporteu números d'unitat lògica (LUN), tingueu en compte aquestes consideracions:

- El nom qualificat d'iSCSI (IQN) de cada destinació virtual està especificat a l'SMIT quan es defineix una destinació de programari. El panell de l'SMIT no restringeix el format del nom. Tanmateix, alguns iniciadors iSCSI necessiten que l'IQN s'especifiqui en el format definit pel protocol d'iSCSI. L'ús d'un format de nom incorrecte pot impedir que l'iniciador inicii la sessió a la destinació i que accedeixi als discos exportats per la destinació.

  Per visualitzar el nom actual d'un dispositiu de destinació iSCSI, realitzeu els passos següents:

  1. Executeu una ordre semblant a la següent. Per a aquest exemple, es pressuposa que el dispositiu de destinació iSCSI és `target0`.

     ```
     lsattr -E -l target0
     ```
  2. Comproveu l'atribut `iscsi_name`.
- Les dades de la consulta tornades per a un LUN exportat tenen els valors següents:
  - `Identificador de proveïdor: AIX`
  - `Identificador de producte: iSCSI_VDASD`
  - `Número de versió ANSI: 3`
- No utilitzeu l'iniciador de programari iSCSI de l'AIX ni la destinació de programari iSCSI de l'AIX amb la interfície de bucle de retorn (`lo0`). El processament de les interrupcions de la interfície de bucle de retorn és diferent del processament de les interrupcions de les interfícies dels adaptadors de xarxa Ethernet físics o virtuals. El sistema operatiu AIX podria aturar-se si s'utilitza la interfície de bucle de retorn amb els controladors de programari iSCSI.

Protocol de transmissió de control de corrent

El **protocol de control de transmissió de corrent (SCTP)** és un protocol orientat a connexions, semblant a TCP, però que proporciona una transferència de dades orientada als missatges semblant a **UDP**. El sistema operatiu AIX compleix amb el RFC 4960.

A la taula següent, es ressalten les diferències generals de comportament entre SCTP i els protocols de transport existents TCP i UDP.

Taula 82. Diferències entre TCP, UDP i SCTP

Atribut	TCP	UDP	SCTP
Fiabilitat	Fiable	No fiable	Fiable
Gestió de les connexions	Orientat a connexions	Sense connexió	Orientat a connexions
Transmissió	Orientat a octets	Orientat a missatge	Orientat a missatge
Control de flux	Sí	No	Sí
Control de congestió	Sí	No	Sí
Tolerància a errors	No	No	Sí
Lliurament de dades	Ordenades de manera estricta	Desordenades	Ordenades de forma parcial
Seguretat	Sí	Sí	Millorada

En general, **SCTP** pot proporcionar més flexibilitat per determinades aplicacions, com **Voice over IP (VoIP)**, que requereixen una transferència de dades fiable i orientada als missatges. En el caso d'aquesta categoria d'aplicacions, **SCTP** resulta més adient que **TCP** o **UDP**.

- **TCP** proporciona un lliurament de dades en ordre de transmissió estricte i fiable. En els cas de les aplicacions que necessiten fiabilitat però que poden tolerar un lliurament de dades desordenades o parcialment ordenades, **TCP** pot causar un retard innecessari degut al blocatge d'inici de línia. Amb el concepte de múltiples corrents dins d'una sola connexió, **SCTP** pot proporcionar un lliurament de dades estrictament ordenades dins d'un corrent a la vegada que les dades s'aïllen de forma lògica de diferents corrents.
- **SCTP** està orientat als missatges i **TCP** als octets. Donada la naturalesa d'orientació a octets de **TCP**, l'aplicació ha d'afegir la seva pròpia marca d'enregistrament per mantenir els límits del missatge.
- **SCTP** proporciona un grau determinat de tolerància a errors mitjançant la funció Multihoming. Es considera que un amfitrió té vàries targetes quan té més d'una interfície de xarxa adjunta, ja sigui a la mateixa o en diferents xarxes. Es pot establir una associació **SCTP** entre dos amfitrions amb vàries targetes. En aquest cas, totes les adreces IP d'ambdós punts finals s'intercanvien a l'inici de l'associació. Això permet a cada punt final utilitzar qualsevol d'aquestes adreces mentre duri la connexió en el cas que una de les interfícies estigui desconnectada per qualsevol motiu i sempre que el similar sigui accessible a través d'interfícies alternatives.
- **SCTP** proporciona funcions de seguretat addicionals que **TCP** i **UDP** no ofereixen. A **SCTP**, l'assignació de recursos durant la configuració de l'associació es retarda fins que es pugui verificar l'identitat del client mitjançant un mecanisme d'intercanvi de cookies. D'aquesta manera, es redueix la possibilitat d'atacs de negació de servei.

Inici i aturada de l'associació SCTP

Les directrius d'inici i aturada de l'associació **SCTP** es descriuen a continuació.

L'associació **SCTP** està composta per un reconeixement de quatre bandes que es produeix en l'ordre següent:

1. El client envia un senyal **INIT** al servidor per iniciar una associació.
2. Quan es rep la senyal **INIT**, el servidor envia una resposta **INIT-ACK** al client. Aquesta senyal **INIT-ACK** conté una galeta d'estat. Aquesta galeta d'estat ha de contenir un codi d'autenticació de missatge, junt amb una indicació de l'hora que correspongui a la creació de la galeta, la durada de la galeta d'estat i l'informació necessària per establir l'associació. El servidor calcula el codi d'autenticació de missatge segons una clau secreta que només ell coneix.
3. Quan rep aquest senyal **INIT-ACK**, el client envia una resposta **COOKIE-ECHO**, la qual només és un eco de la galeta d'estat.

4. Després de verificar l'autenticitat de la galeta d'estat mitjançant la clau secreta, el servidor assigna els recursos de l'associació, envia una resposta **COOKIE-ACK** que reconeix el senyal **COOKIE-ECHO** i mou l'associació a l'estat **ESTABLISHED**.

SCTP dóna suport també de prop a una associació activa quan ho sol•licita un usuari **SCTP**. Es produeix la següent seqüència d'incidents:

1. El client envia un senyal **SHUTDOWN** al servidor, el qual indica al servidor que el client està preparat per tancar la connexió.
2. El servidor respon enviant un reconeixement **SHUTDOWN-ACK**.
3. A continuació, el client retorna un senyal **SHUTDOWN-COMPLETE** al servidor.

SCTP també dóna suport a una tancada abrupta (senyal **ABORT**) d'una associació activa quan ho sol•licita el client **SCTP** o quan es deu a un error de pila **SCTP**. De tota manera,**SCTP** no suporta connexions mig actives. més informació sobre el protocols i els seus elements interns es pot trobar a RFC 4960.

A més de les diferències especificades anteriorment entre **SCTP** i els protocols de transport existents, **SCTP** proporciona les funcions següents:

- **Lliurament seqüencial dins de corrents**: un corrent del context **SCTP** fa referència a una seqüència de missatges d'usuari que es transfereixen entre punts finals. Una associació **SCTP** pot donar suport a múltiples corrents. En el moment de la configuració de l'associació, l'usuari pot especificar el número de corrents. El valor efectiu del número de corrent es fixa un cop s'ha negociat amb el similar. Dins de cada corrent, es manté l'ordre de les dades de manera estricta. De tota manera, als corrents, el lliurament de dades és independent. D'aquesta manera, la pèrdua de dades d'un corrent no evita que les dades es lliurin en un altre corrent. Això permet a una aplicació d'usuari utilitzar diferents corrents per dades independents de forma lògica. Les dades també es poden lliurar de manera desordenada mitjançant una opció especial. Això pot resultar útil per enviar dades urgents.
- **Fragmentació de dades d'usuari**: **SCTP** pot fragmentar missatges d'usuari per garantir que la grandària del paquet que es passa a la capa inferior no supera la MTU de camí d'accés. En el moment de la recepció, els fragments es reacoblen en un missatge sencer i es passen a l'usuari. Encara que la fragmentació també es pot realitzar a nivell de xarxa, la fragmentació de capa de transport proporciona diferents avantatges respecte a la fragmentació de capa d'IP. Alguns d'aquests avantatges inclouen el fet de no haver de tornar a enviar missatges sencers quan es perden fragments a la xarxa i reduir la càrrega dels encaminadors, la qual cosa pot provocar que, en cas contrari, s'hagi de realitzar la fragmentació d'IP.
- **Reconeixement i control de congestió**: el reconeixement de paquets és necessari per a què el lliurament de dades sigui fiable. Si **SCTP** no obté un reconeixement d'un paquet que envia dins d'un temps especificat, desencadenarà una retransmissió del paquet en qüestió. **SCTP** segueix els algorismes de control de congestió semblants als utilitzats per **TCP**. A més d'utilitzar reconeixements d'acumulació com **TCP**, **SCTP** utilitza el mecanismes SACK, el qual li permet reconèixer paquets de forma selectiva.
- **Paquets de blocs**: un bloc pot contenir dades d'usuari o informació de control de **SCTP**. És possible empaquetar múltiples blocs de forma conjunta a la mateixa capçalera **SCTP**. L'empaquetat de blocs requereix l'acoblament de blocs en paquets **SCTP** a l'extrem de l'enviament i el desacoblament posterior del paquet en blocs a l'extrem del receptor.
- **Validació de paquets**: cada paquet **SCTP** té un camp d'etiqueta de verificació que s'estableix durant l'inici de l'associació de cada punt final. Tots els paquets s'envien amb la mateixa etiqueta de verificació mentre estigui activa l'associació. Si, mentre estigui activa l'associació, es rep un paquet amb una etiqueta de verificació no previst, aquest paquet es rebutja. A més, l'emissor de cada paquet **SCTP** ha d'establir la suma de comprovació CRC-32 per tal que proporcioni una major protecció enfront a la corrupció de les dades a la xarxa. Es rebutja qualsevol paquet rebut amb una suma de comprovació CRC-32 no vàlida.
- **Gestió de camins d'accés**: en el moment de la configuració de l'associació, cada punt final ha de mostrar la llista d'adreces de transport de les quals disposa. De tota manera, només es defineix un camí d'accés principal per l'associació **SCTP** i s'utilitza per la transferència de dades normal. En el cas de

que no funcioni el camí d'accés principal, s'utilitzarà la resta d'adreces de transport. Mentre estigui activa l'associació, s'envien batecs a intervals regulars a través del camins d'accés per controlar l'estat del camí d'accés.

API de sòcol SCTP

Les funcions de les API de sòcol **SCTP** inclouen la coherència, l'accessibilitat i la compatibilitat.

Les API de sòcol SCTP s'han dissenyat per proporcionar les funcions següents:

- Mantenir la coherència amb API de sòcol existents
- Proporcionar una base per accedir a les noves funcions **SCTP**
- Proporcionar compatibilitat per tal que les aplicacions **TCP** i **UDP** més comunes es puguin migrar a **SCTP** amb pocs canvis.

Per facilitar la migració de les aplicacions **TCP** i **UDP** existents, s'ha formulat dos estils diferents d'API **SCTP**:

- API d'estil **UDP**: la semàntica és similar a la que s'ha definit pels protocols sense connexió com **UDP**.
- API d'estil **TCP**: la semàntica és similar a la que s'ha definit pels protocols orientats a connexió com **TCP**

Encara que **SCTP** permet definir i utilitzar API d'estil de sòcol **TCP** i **UDP**, a AIX 5.3, només es proporciona suport per sintaxis de sòcol d'estil **UDP** perquè l'API d'estil **UDP** proporciona més flexibilitat a l'hora d'accedir a les noves funcions de **SCTP**. Mitjançant l'API d'estil **UDP**, un servidor típic utilitza la seqüència següent de crides durant la durada de l'associació.

1. **sòcol**()
2. **vincular**()
3. **escoltar**()
4. **recvmsg**()
5. **sendmsg**()
6. **tancar**()

Un client típic utilitza la seqüència següent de crides API de sòcol:

1. **sòcol**()
2. **sendmsg**()
3. **recvmsg**()
4. **tancar**()

Les associacions creades mitjançant la seqüència de crides anterior s'anomenen associacions creades explícitament. Es pot crear una associació implícitament després de crear un sòcol, simplement cridant **sendmsg**(), **recvmsg**() o **sendto**() i **recvto**(). En el caso de l'associació implícita, les crides **bind**() i **listen**() no són necessàries. La sintaxis de totes aquestes crides de sistema és semblant a la que s'utilitza amb els sòcols **UDP**. En el cas de la subrutina de sòcol, el camp **Type** s'hauria d'establir en `SOCK_SEQPACKET` i el camp **Protocol** hauria de ser `IPPROTO_SCTP`. A més d'aquestes API de sòcol estàndard, **SCTP** proporciona dos API noves: **sctp_peeloff**() i **sctp_opt_info**(). Podeu trobar més informació sobre la utilització de l'API de sòcol de **SCTP** a l'esborrany de l'API de sòcol SCTP. **SCTP** s'ha implementat com a extensió kernel a AIX 5.3. Un usuari pot utilitzar l'ordre **sctpctrl** per carregar i descarregar l'extensió del kernel SCTP.

A més, aquesta ordre també es pot fer servir per veure i modificar altres estadístiques i opcions de l'extensió del kernel **SCTP** mitjançant diferents opcions com, per exemple, les d'obtenció i d'establiment. Per obtenir més informació sobre l'ordre **sctpctrl**, consulteu la descripció de l'ordre **sctpctrl** que apareix a *Commands Reference, Volume 5*

Subrutina sctp_bindx:

Afegeix o elimina una adreça vinculada al sòcol.

Biblioteca

`/usr/lib/libsctp.a`

Sintaxi

```
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/sctp.h>

int sctp_bindx(int sd, struct sockaddr * addrs, int addrcnt, int flags);
```

Descripció

La subrutina **sctp_bindx** afegeix o elimina un conjunt d'adreces d'enllaç passades a la matriu **addrs** o des del sòcol **sd**. El paràmetre **addrcnt** és el nombre d'adreces a la matriu, i el paràmetre **flags** especifica si s'han d'afegir o eliminar les adreces.

Si el sòcol **sd** és un sòcol IPv4, les adreces que es passen han de ser IPv4. Si el sòcol **sd** és un sòcol IPv6, les adreces que es passen poden ser IPv4 o IPv6.

El paràmetre **addrs** és un punter a una matriu d'una o diverses adreces de sòcol. Cada adreça està dins de la seva estructura apropiada, o sigui, **struct sockaddr_in** o **struct sockaddr_in6**. La familia del tipus d'adreça s'ha d'utilitzar per distingir la longitud de l'adreça. L'emissor especifica el nombre d'adreces de la matriu a més a més de **addrcnt**.

El paràmetre **flags** pot ser **SCTP_BINDX_ADD_ADDR** o bé **SCTP_BINDX_REM_ADDR**. Una aplicació pot utilitzar SCTP_BINDX_ADD_ADDR per associar adreces addicionals amb un punt final després de cridar l'ordre **bind**. El paràmetre **SCTP_BINDX_REM_ADDR** es dirigeix a SCTP per eliminar les adreces determinades des de l'associació. Un emissor no pot eliminar totes les adreces d'una associació. L'ordre fallarà i donarà com a resultat el codi d'error **EINVAL**.

Valors de retorn

Un cop s'hagin completat correctament, l'ordre **sctp_bindx()** retorna 0. En fallar, l'ordre **sctp_bindx()** retorna -1 i estableix el paràmetre **errno** en el codi d'error apropiat.

Codis d'error

Error	Descripció
EINVAL	El codi d'error **EINVAL** indica que el port o l'adreça no és vàlida o que l'ordre intenta eliminar totes les adreces d'una associació.
EOPNOTSUPP	El codi d'error **EOPNOTSUPP** indica que l'ordre intenta afegir o eliminar adreces d'una associació connectada.

Subrutines sctp_getladdrs i sctp_freeladdrs:

Retorna totes les adreces vinculades localment a un sòcol.

Biblioteca

`/usr/lib/libsctp.a`

Sintaxi

```
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/sctp.h>

int sctp_getladdrs(int sd, sctp_assoc_t assoc_id, struct sockaddr **addrs);
void sctp_freeladdrs(struct sockaddr *addrs);
```

Descripció

La subrutina **sctp_getladdrs** retorna totes les adreces vinculades localment a un sòcol. A la vegada, el paràmetre **addrs** apunta a una matriu empaquetada assignada dinàmicament de les estructures de **sockaddr** del tipus apropiat per a cada adreça local. Heu d'utilitzar el paràmetre **sctp_freeladdrs** per alliberar la memòria.

Nota: El paràmetre d'entrada o de de sortida **addrs** no ha de ser NULL.

Si el paràmetre **sd** és un sòcol IPv4, totes les adreces retornades són IPv4. Si el paràmetre **sd** és un sòcol IPv6, les adreces retornades poden ser tant adreces IPv4 com IPv6.

Per a sòcols d'un a diversos estils, el camp **id** especifica l'associació que es consultarà. Per a sòcols d'un a diversos estils, s'ignorarà el camp **id**. Si el camp **id** s'estableix com a 0, les adreces vinculades localment es retornen sense tenir en compte cap associació particular.

La subrutina **sctp_freeladdrs** allibera tots els recursos assignats per la subrutina **sctp_getladdrs**.

Valor de retorn

En finalitzar, la subrutina **sctp_getladdrs** retorna el nombre d'adreces vinculades localment al sòcol. Si el sòcol no està vinculat, es retorna 0 i el valor del camp ***addrs** no estarà definit. Si hi ha un error, la subrutina **sctp_getladdrs** retorna -1, i el valor del camp ***addrs** no estarà definit.

Subrutines sctp_getpaddrs i sctp_freepaddrs:

Retorna totes les adreces iguals d'una associació.

Biblioteca

/usr/lib/libsctp.a

Sintaxi

```
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/sctp.h>

int sctp_getpaddrs(int sd, sctp_assoc_t assoc_id, struct sockaddr **addrs);
void sctp_freepaddrs(struct sockaddr *addrs);
```

Descripció

La subrutina **sctp_getpaddrs** retorna totes les adreces iguals d'una associació. A la vegada, el paràmetre **addrs** apunta a una matriu empaquetada assignada dinàmicament de les estructures **sockaddr** del tipus apropiat per a cada adreça.Heu d'utilitzar la subrutina **sctp_freepaddrs** per alliberar la memòria.

Nota: El paràmetre d'entrada o de sortida **addrs** no ha de ser NULL.

Si el paràmetre **sd** és un sòcol IPv4, les adreces retornades són totes IPv4. Si el paràmetre **sd** és un sòcol IPv6, les adreces retornades poden ser tant adreces IPv4 com IPv6. Per a sòcols d'un a diversos estils, el camp **id** especifica l'associació que es consultarà. Per a sòcols d'un a diversos estils, s'ignorarà el camp **id**.

La subrutina **sctp_freepaddrs** allibera tots els recursos assignats per la subrutina **sctp_getpaddrs**.

Valor de retorn

En finalitzar, la subrutina **sctp_getpaddrs** retorna el nombre d'adreces iguals de l'associació. Si no hi ha cap associació en aquest sòcol, es retorna 0 i el valor del camp ***addrs** no estarà definit. Si hi ha un error, la subrutina **sctp_getpaddrs** retorna -1, i el valor del camp ***addrs** no estarà definit.

Descobriment de la MTU del camí d'accés

Per a dos amfitrions que s'estan comunicant a través d'un camí d'accés de múltiples xarxes, un paquet transmès es fragment si la seva grandària és major que la MTU més petita de qualsevol xarxa del camí d'accés. Donat que la fragmentació del paquet pot donar com a resultat una reducció en el rendiment de la xarxa, és aconsellable evitar la fragmentació transmetent paquets amb una grandària que no sigui major que la MTU més petita del camí d'accés de la xarxa. Aquesta grandària s'anomena MTU del camí d'accés.

El sistema operatiu dóna suport a un algorisme de descobriment de la MTU de camí d'accés tal com es descriu a RFC 1191. El descobriment de la MTU de camí d'accés es pot habilitar per aplicacions **TCP** i **UDP** modificant les opcions **tcp_pmtu_discover** i **udp_pmtu_discover** de l'ordre **no**. Quan s'habilita per **TCP**, el descobriment de la MTU de camí d'accés obligarà automàticament a que la grandària de tots els paquets transmesos per aplicacions **TCP** no siguin majors que la MTU de camí d'accés. Donat que les aplicacions **UDP** determinen la grandària dels paquets transmesos, les aplicacions **UDP** han d'ésser escrites específicament per utilitzar informació de MTU de camí d'accés utilitzant l'opció de sòcol **IP_FINDPMTU**, encara que l'opció **udp_pmtu_discover no** no estigui habilitada. Per defecte, el **tcp_pmtu_discover** i l'**udp_pmtu_discover** estan habilitades.

Quan s'intenta realitzar el descobriment d'una MTU de camí d'accés per a una destinació, es crea una entrada pmtu a la taula de la MTU de camí d'accés (PMTU). Aquesta taula es pot visualitzar mitjançant l'ordre de visualització **pmtu**. L'acumulació d'entrades pmtu es pot evitar permetent que les entrades no utilitzades caduquin i es puguin eliminar. La caducitat de l'entrada PMTU es control•la mitjançant l'opció pmtu_expire de l'ordre **no**. pmtu_expire s'estableix en 10 minuts per defecte.

Donat que les rutes poden canviar de forma dinàmica, el valor MTU de camí d'accés d'un camí d'accés també pot variar amb el temps. Les reduccions en el valor MTU de camí d'accés poden donar lloc a la fragmentació de paquet i, per tant, es comprova periòdicament si els valor MTU de camí d'accés descoberts presenten reduccions. Per defecte, les reduccions es comproven cada 10 minuts i aquest valor es pot canviar modificant el valor de l'opció **pmtu_default_age** de l'ordre **no**.

Les aplicacions **UDP** sempre han d'establir l'opció de sòcol **IP_DONTFRAG** per detectar les reduccions de la PMTU. Això habilitarà immediatament la detecció de reduccions a la MTU de camí d'accés enlloc de comprovar si existeixen reduccions cada pmtu_default_age minuts.

Els augments en el valor MTU del camí d'accés poden donar com a resultat un augment potencial en el rendiment de la xarxa. Per tant, periòdicament es comprova si existeixen augments als valors MTU de camí d'accés. Per defecte, els augments es comproven cada 30 minuts i aquest valor es pot canviar modificant el valor de l'opció **pmtu_rediscover_interval** de l'ordre **no**.

Si tots els encaminadors del camí d'accés de la xarxa no donen suport a RFC 1191, és possible que no es pugui determinar el valor MTU de camí d'accés exacte. En aquests casos, es pot utilitzar l'ordre **mmtu** per afegir o eliminar els valors MTU de camí d'accés que s'intenten realitzar.

Nota:

1. El descobriment MTU de camí d'accés no es pot utilitzar en rutes duplicades, incloses les que es configuren per l'encaminament de grup (consulteu “Restriccions d'ús dels camins” a la pàgina 360). Es pot utilitzar el descobriment de MTU del camí d'accés en rutes duplicades.
2. L'habilitació del descobriment MTU de camí d'accés estableix el valor de l'opció **arpqsize** de l'ordre **no** en el valor mínim de 5. Aquest valor no disminueix si el descobriment MTU de camí d'accés s'inhabilita posteriorment.

Qualitat de servei de TCP/IP

Qualitat de servei (QoS) és una família d'estàndards d'Internet en evolució que proporcionen maneres de proporcionar tractament de preferència a determinats tipus de tràfic IP.

Amb el suport adient per QoS i una ruta, això pot millorar els efectes del retards de cua de variables i la congestió que contribueixen a que el rendiment de la xarxa sigui pobre. Els sistemes operatius proporcionen suport d'amfitrió per QoS per classificar tràfic de sortida en distintes classes de servei i per anunciar i establir reserves de recursos tal com ho hagin sol•licitat les aplicacions de client.

Una institució pot utilitzar QoS per desplegar i aplicar polítiques de xarxa que controlin la utilització de l'amplada de banda de la xarxa. Amb QoS, un amfitrió pot realitzar el següent:

- Regular la quantitat de tràfic d'un tipus determinat inserit a una xarxa;
- Marcar paquets seleccionats segons alguna política per tal que els encaminadors següents puguin proporcionar el servei indicat;
- Donar suport a serveis com, per exemple, el servei de línia llogada virtual amb suport QoS adient i la ruta
- Participar en sol•licituds de reserva de recursos de receptors i anunciar sessions d'emissor disponibles per les sol•licituds de reserva de recursos.

El suport QoS proporciona les funcions següents:

- Serveis diferenciats tal com es defineixen a RFC 2474
- Polítiques de trànsit
- Marcatge de paquets dins i fora de paquet
- Formació de trànsit
- Mesurament
- Serveis integrats d'aplicacions de client i servidor tal com es defineixen a RFC 1633
- Assenyalament RSVP (RFC 2205)
- Servei garantit (RFC 2212)
- Servei de càrrega controlada (RFC 2211)
- Treball en xarxa basat en política
- Biblioteca compartida RAPI per aplicació

El subsistema QoS consta de quatre components:

Extensió del kernel QoS (/usr/lib/drivers/qos)
: L'extensió del kernel QoS es troba a `/usr/lib/drivers/qos` i es carrega i es descarrega mitjançant els mètodes de configuració **cfgqos** i **ucfgqos**. Aquesta extensió del kernel habilita el suport QoS.

Agent de política (/usr/sbin/policyd)
: L'agent de política és un daemon de nivell d'usuari que es troba a `/usr/sbin/policyd`. Proporciona suport per la gestió de polítiques i interfícies amb l'extensió de kernel QoS per instal•lar, modificar i suprimir regles de política. Les regles de política es poden definir en un fitxer de configuració local (`/etc/policyd.conf`), que s'obté d'un servidor de política de xarxa central mitjançant LDAP o ambdós both.

Agent RSVP (/usr/sbin/rsvpd)
L'agent RVSP és un daemon de nivell d'usuari que es troba a /usr/sbin/rsvpd. Implementa la semàntica de protocol d'assenyalament RSVP.

Biblioteca compartida RAPI (/usr/lib/librapi.a)
Les aplicacions poden utilitzar RSVP API (RAPI) per sol•licitar la millora de la qualitat de servei tal com ho defineix el model QoS d'Internet de serveis integrats. Aquesta biblioteca interactua amb l'agent RSVP local per propagar la sol•licitud QoS amb el camí d'accés del flux de dades mitjançant el protocol RSVP. Aquesta API és un estàndard obert.

Nota: Aquesta implementació de QoS es basa en un conjunt d'estàndards d'Internet en evolució i estàndards d'esborrany que s'estan desenvolupant actualment mitjançant IETF i els seus diferents grups de treball. Aquesta tecnologia serà més coherent i estarà millor definida a mesura que progressin aquests esforços d'estandarditzación dins de IETF. També és important ressaltar que QoS és una tecnologia d'Internet emergent que acaba de començar a desplegar-se a Internet. Existeixen molts beneficis de QoS a totes les etapes del desplegament. De tota manera, els serveis integrals vertaders només es poden realitzar quan existeix suport QoS a tota una ruta.

Models QoS

Els models QoS d'Internet són estàndards oberts definits per IETF.

Existeixen dos models QoS d'Internet que actualment s'estan estandarditzen dins d'IETF: *serveis integrats* i *serveis diferenciats*. Aquests dos models QoS d'Internet augmenten el model de servei òptim tradicional descrit a RFC 1812.

Serveis integrats:

Serveis integrats (IS) és un model de reserva de recursos dinàmic per Internet que es descriu a RFC 1633.

Els amfitrions utilitzen un protocol de senyals anomenat Resource ReSerVation Protocol (RSVP) per sol•licitar dinàmicament una qualitat de servei específica des de la xarxa. Els paràmetres QoS s'inclouen en aquests missatges RSVP i cada node de la xarxa del camí d'accés instal•la els paràmetres per obtenir la qualitat de servei sol•licitada. Aquests paràmetres QoS descriuen un dels dos serveis definits actualment, el servei garantit i el servei de càrrega controlada. Una característica important d'IS es que aquesta assignació de senyals es realitza per a cada flux de tràfic i les reserves s'instal•len a cada salt de la ruta. Encara que aquest model està ben preparat per satisfer dinàmicament les necessitats canviants de les aplicacions, existeixen alguns problemes d'escalat significants que impliquen que no es pot desplegar en una xarxa on encaminadors individuals manipulen molts fluxes simultanis.

Serveis diferenciats:

Els serveis diferenciats (DS) eliminen problemes d'escalabilitat per flux i per salt i els substitueix per un mecanisme simplificat de classificació de paquets.

Enlloc d'utilitzar una aproximació d'assenyalament dinàmic, DS utilitza bits a l'octet de tipus de servei d'IP per separar paquets en classes. El patró de bit particular de l'octet de tipus de servei d'IP s'anomena punt de codi DS i l'utilitzen els encaminadors per definir la qualitat del servei que es proporciona en un salt determinat, d'una manera molt semblant a com els encaminadors realitzen el reenviament d'IP a través de cerques de taula d'enrutament. El tractament que es dóna a un paquet amb un punt de codi DS determinat s'anomena PHB (comportament per salt) i s'administra de forma independent a cada node de la xarxa. Quan es concatenen els efectes d'aquests PHB independents i individuals, això dóna com a resultat un servei integral.

El grup de treball IETF s'encarrega d'estandarditzar els serveis diferenciats. Aquest grup ha definit tres PHB: el PHB de reenviament enviat (EF), el grup PHB de reenviament assegurat (AF) i el PHB per defecte (DE). El EF PHB es pot utilitzar per implementar una latència baixa, un jitter lent, una pèrdua lenta o un servei integral com, per exemple, la línia VLL. AF forma part de la família de PHB,

denominada grup PHB, que s'utilitza per classificar paquets en diferents nivells de prioritat d'eliminació. La prioritat d'eliminació assignada a un paquet determina l'importància relativa d'un paquet dins de la classe AF. Es pot utilitzar per implementar el servei anomenat *Olympic*, el qual consta de tres classes: bronze, plata i or. El DE PHB és el model de servei tradicional més complet segons s'ha estandardizat a RFC 1812.

Estàndards suportats i estàndards d'esborrany

Aquests RFC i esborranys d'Internet descriuen els estàndards en els quals es basa aquesta implementació QoS.

Element	Descripció
RFC 2474	Definició del camp Serveis diferenciats (camp DS) a les capçaleres IPv4 i IPv6
RFC 2475	Una arquitectura per serveis diferenciats
RFC 1633	Descripció general de serveis integrats a l'arquitectura d'Internet
RFC 2205	Protocol de reserva de recursos (RSVP)
RFC 2210	La utilització de RSVP amb els serveis integrats IETF
RFC 2211	Especificació del servei d'elements de xarxa de càrrega controlada
RFC 2212	Especificació de la qualitat de servei garantida
RFC 2215	Paràmetres de caracterització general per elements de xarxa de serveis integrats

Element	Descripció
draft-ietf-diffserv-framework-01.txt, Octubre 1998	Una estructura per serveis diferenciats
draft-ietf-diffserv-rsvp-01.txt, Novembre 1998	Una estructura per utilitzar RSVP amb xarxes de servei diferenciat
draft-ietf-diffserv-phb-ef-01.txt	PHB de reenviament accelerat
draft-ietf-diffserv-af-04.txt	Grup PHB de reenviament assegurat
draft-rajan-policy-qosschema-00.txt, Octubre 1998	Esquema de serveis diferenciats i serveis integrats en xarxes
draft-ietf-rap-framework-01.txt, Novembre 1998	Estructura per control d'admissió basat en política[25]
draft-ietf-rap-rsvp-ext-01.txt, Novembre 1998	Extensions RSVP pel control de política

Nota: QoS és una tecnologia d'Internet emergent. Existeixen molts beneficis de QoS a totes les etapes del desplegament. De tota manera, els serveis integrals vertaders només es poden realitzar quan existeix suport QoS a tota una ruta.

Instal•lació de QoS

QoS s'inclou al mateix paquet que `bos.net.tcp.server`. Per utilitzar QoS, cal instal•lar el catàleg de fitxers.

Per utilitzar la biblioteca compartida `RAPI`, també cal instal•lar `bos.adt.include`.

Aturada i inici del subsistema QoS

QoS es pot iniciar o aturar a través de la SMIT amb el camí d'accés ràpid `smit qos` o les ordres **mkqos** i **rmqos**.

1. Per inhabilitar el subsistema QoS en aquest moment i al proper reinici de sistema:
   ```
   /usr/sbin/rmqos -B
   ```
2. Per habilitar el subsistema QoS només ara:
   ```
   /usr/sbin/mkqos -N
   ```

Consulteu la descripció d'ordres de **mkqos** i **rmqos** pels senyaladors de les ordres de reinici i de supressió.

Els daemons **policyd** i **rsvpd** es configuren a través dels fitxers de configuració `/etc/policyd.conf` i `/etc/rsvpd.conf`, respectivament. Aquests fitxers de configuració *s'han* d'editar per personalitzar el subsistema QoS amb l'entorn local. QoS no funciona correctament amb les configuracions d'exemple proporcionades.

Configuració de l'agent RSVP

L'agent RSVP és necessari si l'amfitrió ha de donar suport al protocol RSVP.

El fitxer de configuració `/etc/rsvpd.conf` s'utilitza per configurar l'agent RSVP. La sintaxis del fitxer de configuració es descriu al fitxer de configuració d'exemple de `/etc/rsvpd.conf`.

L'exemple següent mostra una configuració RSVP possible en la qual l'amfitrió té 4 interfícies (virtuals i físiques) proporcionades per 4 adreces IP, `1.2.3.1`, `1.2.3.2`, `1.2.3.3` i `1.2.3.4`.

```
interface 1.2.3.1
interface 1.2.3.2 disabled
interface 1.2.3.3 disabled
interface 1.2.3.4
{
  trafficControl
}

rsvp 1.2.3.1
{
  maxFlows 64
}

rsvp 1.2.3.4
{
  maxFlows 100
}
```

S'ha habilitat l'interfície `1.2.3.1` per RSVP. De tota manera, el control de tràfic no s'ha especificat i els missatges RSVP RESV no fan que es produeixin reserves de recursos dins del subsistema TCP. Aquesta interfície pot donar suport a un màxim de 64 sessions RSVP simultànies.

S'han inhabilitat les interficies `1.2.3.2` i `1.2.3.3`. L'agent RSVP no pot utilitzar aquesta interfície per transmetre ni rebre missatges RSVP.

L'interfície `1.2.3.4` s'ha habilitat per RSVP. A més, pot instal•lar reserves de recursos al subsistema **TCP** com a resposta al un missatge RSVP RESV. Aquesta interfície pot donar suport a un màxim de 100 RSVP.

Qualsevol altra interfície present a l'amfitrió però no mencionada explícitament a `/etc/rsvpd.conf` s'inhabilita.

Configuració d'agent de política

L'agent de política és un component necessari del subsistema QoS.

El fitxer de configuració `/etc/policyd.conf` s'utilitza per configurar l'agent de política. La sintaxis d'aquest fitxer de configuració es descriu al fitxer de configuració d'exemple de `/etc/policyd.conf`.

L'agent de política es pot configurar editant `/etc/policyd.conf`. A més, es proporcionen les ordres següents per ajudar a configurar polítiques:

- **qosadd**
- **qosmod**
- **qoslist**
- **qosremove**

A l'exemple següent, es crea i s'utilitza una categoria de servei premium a la regla de política tcptraffic. Aquesta categoria de servei té una velocitat màxima de 110000 Kbps, una profunditat de receptacle de token de 10000 bits i un valor TOS d'IP de sortida de 11100000 en binari. La regla de política tcptraffic ofereix aquest servei premium a tot el tràfic amb l'adreça IP d'origen proporcionada per `1.2.3.6`, l'adreça de destinació `1.2.3.3` i el port de destinació en un interval de 0 a 1024.

```
ServiceCategories  premium
{
   PolicyScope     DataTraffic
   MaxRate         110000
   MaxTokenBucket  10000
   OutgoingTOS     11100000
}

ServicePolicyRules   tcptraffic
{
   PolicyScope   DataTraffic
   ProtocolNumber 6  # tcp
   SourceAddressRange      1.2.3.6-1.2.3.6
   DestinationAddressRange 1.2.3.3-1.2.3.3
   DestinationPortRange    0-1024
   ServiceReference        premium
}
```

Les sentències següents configuren una categoria de servei per defecte i l'utilitzen per limitar el tràfic UDP provinent de les interfícies `1.2.3.1` a través de `1.2.3.4` fins a les adreces IP `1.2.3.6` a través de `1.2.3.10`, port 8000.

```
ServiceCategories  default
{
   MaxRate         110000
   MaxTokenBucket  10000
   OutgoingTOS     00000000
}

ServicePolicyRules   udptraffic
{
   ProtocolNumber 17  # udp
   SourceAddressRange      1.2.3.1-1.2.3.4
   DestinationAddressRange 1.2.3.6-1.2.3.10
   DestinationPortRange    8000-8000
   ServiceReference        default
}
```

L'exemple de configuració següent es pot utilitzar per descarregar regles del servidor LDAP mitjançant el nom de subarbre distingit, per buscar les polítiques a l'amfitrió del servidor LDAP.

```
ReadFromDirectory
{
  LDAP_Server      1.2.3.27
  Base             ou=NetworkPolicies,o=myhost.mydomain.com,c=us
}
```

Resolució de problemes QoS

L'ordre **qosstat** es pot utilitzar per mostrar informació d'estat sobre les polítiques instal•lades i actives al subsistema QoS. Aquesta informació pot resultar útil a l'hora de determinar on existeix un problema i si s'està solucionant la configuració de QoS.

qosstat es pot utilitzar per generar l'informe següent.

```
Action:
  Token bucket rate (B/sec): 10240
  Token bucket depth (B): 1024
  Peak rate (B/sec): 10240
  Min policied unit (B): 20
  Max packet size (B): 1452
  Type: IS-CL
  Flags: 0x00001001 (POLICE,SHAPE)

  Statistics:
    Compliant packets: 1423 (440538 bytes)
```

```
  Conditions:
    Source address        Dest address          Protocol
    192.168.127.39:8000   192.168.256.29:35049  tcp       (1 connection)

Action:
  Token bucket rate (B/sec): 10240
  Token bucket depth (B): 1024
  Peak rate (B/sec): 10240
  Outgoing TOS (compliant): 0xc0
  Outgoing TOS (non-compliant): 0x00
  Flags: 0x00001011 (POLICE,MARK)
  Type: DS

  Statistics:
    Compliant packets: 335172 (20721355 bytes)
    Non-compliant packets: 5629 (187719 bytes)

  Conditions:
    Source address        Dest address          Protocol
    192.168.127.39:80     *:*                   tcp       (1 connection)
    192.168.127.40:80     *:*                   tcp       (5 connections)
```

Especificació de política QoS

Les classe d'objecte i els atributs utilitzats per l'agent de política per especificar polítiques per la qualitat de servei (QoS) en tràfic de sortida es descriuen aquí.

Després de la definició de les classes d'objecte i dels atributs, es proporcionen les directrius per habilitar el marcatge, la creació de polítiques i l'assignació de forma.

Aquestes convencions s'utilitzen a les explicacions següents.

```
p  : choose one in the allowed parameter set
B  : integer value of a byte (i.e., 0 =< B =< 255)
b  : bit string starting with left most bit (e.g., 101 is
     equivalent 10100000 in a byte field)
i  : integer value
s  : a character string
a  : IP address format B.B.B.B
(R) : Required parameter
(O) : Optional parameter
```

Sentència ReadFromDirectory:

Aquesta sentència especifica paràmetres per establir una sessió LDAP.

La sentència `ReadFromDirectory` s'utilitza al fitxer `/etc/policyd.conf` per establir la sessió LDAP.

```
ReadFromDirectory
{
  LDAP_Server    a   # IP address of directory server running LDAP
  LDAP_Port     i    # Port number LDAP server is listening to
  Base     s         # Distinguished Name for LDAP usage
  LDAP_SelectedTag s # Tag to match SelectorTag in object classes
}
```

where

```
LDAP_Server (R): IP address of LDAP server
LDAP_Port   (0): Unique port number, default port is 389
Base        (R): Example is o=ibm, c=us where o is your organization and c is country
LDAP_SelectedTag (R): Unique string matching SelectorTag attribute in the object class
```

Sentència ServiceCategories:

Aquesta sentència especifica el tipus de servei que un flux de paquets IP (per exemple, des d'una connexió **TCP** o dades **UDP**) ha de rebre de forma integral a mesura que travessen la xarxa.

Les categories ServiceCategories es poden repetir tenint cadascuna un nom diferent amb el qual es puguin fer referència posteriorment. Un objecte ServiceCategories requereix ServicePolicyRules per completar la definició de política.

```
ServiceCategories   s
{
   SelectorTag    s     # Required tag for LDAP Search
   MaxRate        i     # Target rate for traffic in this service class
   MaxTokenBucket i     # The bucket depth
   OutgoingTOS    b     # TOS value of outbound traffic for this service class
   FlowServiceType   p  # Type of traffic

}
```

where

```
s           (R)     : is the name of this service category
SelectorTag (R)     : Required only for LDAP to Search object classes
MaxRate     (O)     : in Kbps (K bits per second), default is 0
MaxTokenBucket(O)   : in Kb, default is system defined maximum
OutgoingTOS (O)     : default is 0
FlowServiceType  (O): ControlledLoad | Guaranteed, default is ControlledLoad
```

Sentència ServicePolicyRules:

Aquesta sentència especifica les característiques de paquets IP que s'utilitzen per coincidir amb la categoria de servei corresponent.

En altres paraules, defineix un conjunt de datagrames IP que han de rebre un servei determinat. ServicePolicyRules s'associen amb ServiceCategories a través de l'atribut ServiceReference. Si dues regles fan referència a la mateixa ServiceCategory, cada regla s'associarà amb l'instància exclusiva de ServiceCategory.

```
ServicePolicyRules   s
{
   SelectorTag       s   # Required tag for LDAP Search
   ProtocolNumber    i   # Transport protocol id for the policy rule
   SourceAddressRange      a1-a2
   DestinationAddressRange a1-a2
   SourcePortRange         i1-i2
   DestinationPortRange    i1-i2
   PolicyRulePriority  i       # Highest value is enforced first
   ServiceReference        s  # Service category name which for this policy rule
}
```

where

```
s           (R): is the name of this policy rule
SelectorTag (R): required only for LDAP to Search object class
ProtocolNumber     (R): default is 0 which causes no match, must explicity specify
SourceAddressRange (O): from a1 to a2 where a2 >= a1, default is 0, any source address
SourcePortRange    (O): from i1 to i2 where i2 >= i1, default is 0, any source port
DestinationAddressRange (O): same as SourceAddressRange
DestinationPortRange    (O): same as SourcePortRange
PolicyRulePriority (O): Important to specify when ovelapping policies exist
ServiceReference   (R): service category this rule uses
```

Directrius per entorns de serveis diferenciats

A continuació, es mostren les directrius per especificar polítiques per marcar, donar formar i/o crear polítiques d'un entorn de serveis diferenciats.

1. **Només marcar**

```
OutgoingTOS     : Desired Type Of Service
FlowServiceType : ControlledLoad
MaxRate         : Take default of 0
```

2. **Només donar forma**

```
OutgoingTOS     : Take default of 0
FlowServiceType : Guaranteed
MaxRate         : Target rate desired for traffic as a positive integer
```

3. **Marcar i crear política (vegeu nota)**

```
OutgoingTOS     : Desired Type of Service
FlowServiceType : ControlledLoad
MaxRate         : Target rate desired for traffic as a positive integer
```

4. **Marcar i donar forma**

```
OutgoingTOS     : Desired Type of Service
FlowServiceType : Guaranteed
MaxRate         : Target rate desired for traffic as a positive integer
```

Nota: El tipus de servei establert pels paquets fora del perfil s'estableix en zero en el cas de la creació de política.

Exemple de fitxer de configuració de política

A continuació, es mostra un exemple complet de fitxer de configuració `/etc/policyd.conf`.

```
#loglevel  511    # Verbose logging

######################################################################
#
# Mark rsh traffic on TCP source ports 513 and 514.
ServiceCategories       tcp_513_514_svc
{
        MaxRate                 0               # Mark only
        OutgoingTOS             00011100        # binary
        FlowServiceType         ControlledLoad
}

ServicePolicyRules      tcp_513_514_flt
{
        ProtocolNumber          6  # TCP
        SourceAddressRange      0.0.0.0-0.0.0.0 # Any IP src addr
        DestinationAddressRange 0.0.0.0-0.0.0.0 # Any IP dst addr
        SourcePortRange         513-514
        DestinationPortRange    0-0             # Any dst port
        ServiceReference        tcp_513_514_svc
}
#
######################################################################
#
# Shape connected UDP traffic on source port 9000.
ServiceCategories       udp_9000_svc
{
        MaxRate                 8192     # kilobits
        MaxTokenBucket          64       # kilobits
        FlowServiceType         Guaranteed
}

ServicePolicyRules      udp_9000_flt
{
        ProtocolNumber          17  # UDP
        SourceAddressRange      0.0.0.0-0.0.0.0 # Any IP src addr
        DestinationAddressRange 0.0.0.0-0.0.0.0 # Any IP dst addr
        SourcePortRange         9000-9000
        DestinationPortRange    0-0             # Any dst port
        ServiceReference        udp_9000_svc
```

```
}
#
#####################################################################
#
# Mark and police finger traffic on TCP source port 79.
ServiceCategories       tcp_79_svc
{
        MaxRate                 8         # kilobits
        MaxTokenBucket          32        # kilobits
        OutgoingTOS             00011100  # binary
        FlowServiceType         ControlledLoad
}

ServicePolicyRules      tcp_79_flt
{
        ProtocolNumber          6  # TCP
        SourceAddressRange      0.0.0.0-0.0.0.0 # Any IP src addr
        DestinationAddressRange 0.0.0.0-0.0.0.0 # Any IP dst addr
        SourcePortRange         79-79
        DestinationPortRange    0-0             # Any dst port
        ServiceReference        tcp_79_svc
}
#
#####################################################################
#
# Mark and shape ftp-data traffic on TCP source port 20.
ServiceCategories       tcp_20_svc
{
        MaxRate                 81920        # kilobits
        MaxTokenBucket          128          # kilobits
        OutgoingTOS             00011101     # binary
        FlowServiceType         Guaranteed
}

ServicePolicyRules      tcp_20_flt
{
        ProtocolNumber          6  # TCP
        SourceAddressRange      0.0.0.0-0.0.0.0 # Any IP src addr
        DestinationAddressRange 0.0.0.0-0.0.0.0 # Any IP dst addr
        SourcePortRange         20-20
        DestinationPortRange    0-0             # Any dst port
        ServiceReference        tcp_20_svc
}
#
#####################################################################
#
# LDAP server entry.
#ReadFromDirectory
#{
#   LDAP_Server             9.3.33.138  # IP address of LDAP server
#   Base                    o=ibm,c=us  # Base distinguished name
#   LDAP_SelectedTag        myhost      # Typically client hostname
#}
#
#####################################################################
```

Càrregues de política de servidor d'IBM SecureWay Directory

Si s'utilitza el daemon de política amb el servidor LDAP de directoris IBM SecureWay, utilitzeu aquest esquema com a guia per actualitzar `/etc/ldapschema/V3.modifiedschema` abans d'iniciar el servidor LDAP.

Consulteu “Planificació i configuració per la resolució de noms LDAP (esquema d'IBM SecureWay Directory schema)” a la pàgina 204 per obtenir informació detallada.

```
objectClasses {
( ServiceCategories-OID NAME 'ServiceCategories' SUP top MUST
( objectClass $ SelectorTag $ serviceName ) MAY
( description $ FlowServiceType $ MaxRate $ MaxTokenBucket $ OutgoingTos ) )
( ServicePolicyRules-OID NAME 'ServicePolicyRules' SUP top MUST
( objectClass $ PolicyName $ SelectorTag ) MAY
( description $ DestinationAddressRange $ DestinationPortRange $
ProtocolNumber $ ServiceReference $ SourceAddressRange $ SourcePortRange ) )
}
attributeTypes {
( DestinationAddressRange-OID NAME 'DestinationAddressRange' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
( DestinationPortRange-OID NAME 'DestinationPortRange' SYNTAX
 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
( FlowServiceType-OID NAME 'FlowServiceType'
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
( MaxRate-OID NAME 'MaxRate' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
( MaxTokenBucket-OID NAME 'MaxTokenBucket' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
( OutgoingTos-OID NAME 'OutgoingTos' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
( PolicyName-OID NAME 'PolicyName' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
( ProtocolNumber-OID NAME 'ProtocolNumber' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
( SelectorTag-OID NAME 'SelectorTag' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
( ServiceReference-OID NAME 'ServiceReference' SYNTAX
 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
( SourceAddressRange-OID NAME 'SourceAddressRange' SYNTAX
 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
( SourcePortRange-OID NAME 'SourcePortRange' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
}

IBMattributeTypes {
( DestinationAddressRange-OID DBNAME ( 'DestinationAddressRange' 'DestinationAddressRange' ) )
( DestinationPortRange-OID DBNAME ( 'DestinationPortRange' 'DestinationPortRange' ) )
( FlowServiceType-OID DBNAME ( 'FlowServiceType' 'FlowServiceType' ) )
( MaxRate-OID DBNAME ( 'MaxRate' 'MaxRate' ) )
( MaxTokenBucket-OID DBNAME ( 'MaxTokenBucket' 'MaxTokenBucket' ) )
( OutgoingTos-OID DBNAME ( 'OutgoingTos' 'OutgoingTos' ) )
( PolicyName-OID DBNAME ( 'PolicyName' 'PolicyName' ) )
( ProtocolNumber-OID DBNAME ( 'ProtocolNumber' 'ProtocolNumber' ) )
( SelectorTag-OID DBNAME ( 'SelectorTag' 'SelectorTag' ) )
( ServiceReference-OID DBNAME ( 'ServiceReference' 'ServiceReference' ) )
( SourceAddressRange-OID DBNAME ( 'SourceAddressRange' 'SourceAddressRange' ) )
( SourcePortRange-OID DBNAME ( 'SourcePortRange' 'SourcePortRange' ) )
}

ldapSyntaxes {
}

matchingRules {
}
```

Configuració del sistema QoS

Les polítiques que se superposen s'instal•len al gestor de QoS Manager en un ordre no determinista. En el cas que se superposin polítiques, caldrà especificar l'atribut `PolicyRulePriority` de `ServicePolicyRules` per determinar l'ordre de l'aplicació de polítiques. L'atribut `PolicyRulePriority` pren un enter com a paràmetre i, en el cas de polítiques superposades, s'aplica la regla amb el valor d'enter més elevat.

Per QoS només es dóna suport a sòcols **UDP** connectats.

Els agents RSVP i de política són independents els uns respecte dels altres. D'aquesta manera, s'ha d'anar amb compte per no especificar una política que entri en conflicte amb una reserva RSVP existent o que estigui coberta per aquesta. En la presència d'aquests conflictes, el sistema accepta la primera política o reservar a l'hora que assenyala una infracció de les altres.

Per un funcionament correcte, l'atribut `MaxTokenBucket` s'ha d'establir com a mínim a la MTU màxima de totes les interfícies configurades al sistema.

L'agent de política gestiona les modificacions de política eliminant automàticament les polítiques existents i instal•lant les noves. Això pot donar lloc a una finestra de temps breu i temporal durant la qual el tràfic corresponent rep servei per defecte (normalment el servei òptim).

Compliment dels estàndards IETF pels models IntServ i DiffServ

Aquest release és compatible amb els estàndards IETF que s'estan desenvolupant pels serveis diferenciats (DiffServ) i integrats (IntServ) a Internet.

Els RFC següents descriuen diferents components del model IntServ:

- La utilització de RSVP amb els serveis integrats IETF (RFC 2210)
- Especificació del servei d'elements de xarxa de càrrega controlada (RFC 2211)
- Especificació de la qualitat garantida del servei (RFC 2212)

Els RFC següents descriuen diferents components del model DiffServ:

- Definició del camp de serveis diferenciats (camp DS) de les capçaleres IPv4 i IPv6 (RFC 2474)
- Una arquitectura per serveis diferenciats (RFC 2475)

El RFC següent descriu la utilització actual de l'octet TOS d'IP:

- Tipus de servei del paquet ofimàtic de protocol d'Internet (RFC 1349)

El RFC següent descriu les pràctiques futures que controlen l'ús de l'octet TOS d'IP:

- Definició del camp de serveis diferenciats (camp DS) de les capçaleres IPv4 i IPv6 (RFC 2474)
- Reenviament garantit del grup PHB (RFC 2597)
- Reenviament accelerat de PHB (RFC 2598)

Suport IPv6

QoS només dóna suport a IPv4.IPv6 no rep suport.

Control de daemon de política

Podeu control el daemon de política utilitzant el controlador de recursos del sistema (SRC).

Per exemple, l'ordre:

```
startsrc -s policyd -a "-i 60"
```

inicia l'agent de política amb l'interval de renovació de 60 segons.

L'ordre

```
stopsrc -s policyd
```

atura el daemon de política.

Nota: En aturar el daemon de política no s'eliminen les polítiques instal•lades al kernel. En tornar a iniciar el daemon de política, les polítiques antigues (instal•lades anteriorment al kernel) s'eliminen i les polítiques definides al fitxer `/etc/policyd.conf` es reinstal•len.

L'ordre de SRC **refresh** no rep suport actualment.

Ordres i mètodes QoS

Les ordres i els mètodes de qualitat de servei **TCP/IP** es llisten a continuació.

Per conèixer actualitzacions importants per aquesta documentació, consulteu el fitxer README de `/usr/samples/tcpip/qos`.

Es dóna suport a les ordres QoS següents:

- **qosadd**
- **qoslist**
- **qosmod**
- **qosremove**
- **qosstat**
- **mkqos**
- **rmqos**

Es dóna suport als mètodes QoS següents:

- **cfgqos**
- **ucfgqos**

Resolució de problemes del TCP/IP

L'ordre **netstat** és una bona eina per diagnosticar els problemes més freqüents en un entorn de xarxa del **Transmission Control Protocol/Internet Protocol (TCP/IP)**.

L'ordre **netstat** us permet determinar quina àrea de la xarxa té un problema. Un cop hagueu aïllat el problema una àrea, podeu utilitzar eines més sofisticades per continuar. Per exemple, podeu utilitzar **netstat -i** i **netstat -v** per determinar si teniu un problema amb una interfície de maquinari en particular i, a continuació, executar diagnòstics per seguir aïllant el problema. O bé, si l'ordre **netstat -s** mostra que hi ha errors de protocol, aleshores podríeu utilitzar les ordres **trpt** o **iptrace**.

Problemes de comunicació

Els problemes de comunicació habituals del **TCP/IP** inclouen la incapacitat de comunicar-se amb un amfitrió de la xarxa i també problemes d'encaminament. A continuació, us presentem algunes solucions.

Si no aconseguiu comunicar-vos amb un amfitrió a la xarxa:

- Intenteu posar-vos en contacte amb l'amfitrió mitjançant l'ordre **ping**. Executeu l'ordre **ping** a l'amfitrió local per verificar que la interfície local de la xarxa es troba activada i en execució.
- Intenteu resoldre el nom de l'amfitrió mitjançant l'ordre **amfitrió**. Si no es resol el nom, teniu un problema de resolució de noms. Vegeu l'apartat “Problemes de la traducció de noms” per obtenir més informació.

Si el nom es resol i esteu intentant contactar un amfitrió en una altra xarxa, pot ser que tingueu un problma d'encaminament. Vegeu l'apartat “Problemes d'encaminament del TCP/IP” a la pàgina 421 per obtenir més informació.

- Si la xarxa és token-ring, comproveu que l'amfitrió de destinació no es trobi en un altre anell. Si és així, pot ser que el camp **allcast** no s'hagi establert correctament. Utilitzeu el camí d'accés ràpid de la System Management Interface Tool (SMIT) `smit chinet`. A continuació, al diàleg token ring, seleccioneu **no** al camp Confine Broadcast to Local Ring.
- Si hi ha una quantitat important de paquets del **Protocol de resolució d'adreces (ARP)** a la xarxa, comproveu que la màscara de subxarxa s'hagi establert correctament. Aquesta condició es coneix amb el nom de tempesta de difusió i pot afectar el rendiment del sistema.

Problemes de la traducció de noms

Les rutines de solucionador als amfitrions que executen el **TCP/IP** intenten resoldre noms, mitjançant aquests orígens en l'ordre en què apareixen.

1. Servidor de noms de domini (**named**)

2. Network Information Service (NIS)
3. Fitxer /etc/hosts local

Resolució de problemes de l'amfitrió del client:

Si no aconseguiu resoldre un nom d'amfitrió i esteu emprant una resolució de noms plana (mitjançant el fitxer /etc/hosts), comproveu que el nom d'amfitrió i l'adreça IP (Internet Protocol) correcta són al fitxer /etc/hosts.

Si no aconseguiu resoldre un nom d'amfitrió i esteu emprant un servidor de noms, seguiu els passos següents:

1. Comproveu que teniu un fitxer resolv.conf que especifica el nom de domini i l'adreça d'Internet d'un servidor de noms.
2. Comproveu que el servidor de noms local està en funcionament mitjançant l'execució de l'ordre **ping** amb l'adreça IP del servidor de noms (que es troba al fitxer local resolv.conf).
3. Si el servidor de noms local està en funcionament, comproveu que el daemon **named** del servidor de noms local està actiu mitjançant l'execució de l'ordre **lssrc -s named** al servidor de noms.
4. Si esteu executant el **syslogd**, comproveu els missatges enregistrats. La sortida per aquests missatges es defineix al fitxer /etc/syslog.conf.

Si amb aquests passos no aconseguiu identificar el problema, comproveu l'amfitrió del servidor de noms.

Resolució de problemes de l'amfitrió del servidor de noms:

Utilitzeu aquest procediment per resoldre els problemes del servidor de noms d'amfitrió.

Si no aconseguiu resoldre un nom d'amfitrió:

1. Verifiqueu que el daemon **named** es troba actiu executant l'ordre següent:
   ```
   lssrc -s named
   ```
2. Verifiqueu que l'adreça de l'amfitrió de destinació existeix i és correcta a la base de dades del servidor de noms. Envieu un senyal **SIGINT** al daemon **named** per buidar la base de dades i la memòria cau al fitxer /var/tmp/named_dump.db. Verifiqueu que l'adreça que intenteu resoldre hi surt i és correcta.

   Afegiu o corregiu la informació de resolució de nom a adreça al fitxer de dades dels amfitrions del **named** per al servidor de noms mestre del domini. A continuació, executeu l'ordre **SRC** següent per tornar a llegir els fitxers de dades:
   ```
   refresh -s named
   ```
3. Verifiqueu que les sol•licituds de resolució de noms s'estan processant. Per fer-ho, introduïu el daemon **named** des de la línia d'ordres i especifiqueu un nivell de depuració. Els nivells de depuració vàlids són de l'1 al 9. Com més alt sigui el nivell, més informació enregistra el mecanisme de depuració.
   ```
   startsrc -s named -a "-d Nivell_depuració"
   ```
4. Comproveu si hi ha problemes de configuració als fitxers de dades del **named**. Per obtenir més informació, consulteu l'apartat “Resolució de servidors de noms” a la pàgina 184. A més, consulteu les seccions "Format de fitxer de dades de DOMINI,", "Format de fitxer de dades invers de DOMINI," "Format de fitxer de memòria cau de DOMINI," i "Format de fitxer de dades local de DOMINI" al *Files Reference*.

   Nota: Un error comú és l'ús incorrecte del **.** (punt) i l'@ (a encerclada) als fitxers de dades DOMAIN.

Si els usuaris externs no poden accedir als vostres dominis, assegurar-vos que tots els vostres servidors de noms no mestres (esclaus, d'orientació) tenen la mateixa informació de duració (TTL) als fitxers de dades DOMAIN.

Si els solucionadors externs consulten constantment els vostres servidors, assegureu-vos que els vostres servidors distribueixen els fitxers de dades DOMAIN amb valors TTL raonables. Si el valor TTL és zero o un altre valor petit, les dades que transferiu esgotaran el temps d'espera molt ràpid. Establiu el valor mínim dels enregistraments d'inici d'autorització (SOA) en una setmana o més per solucionar aquest problema.

Problemes d'encaminament del TCP/IP

Si no podeu accedir a un amfitrió de destinació, tingueu en consideració les solucions a les situacions següents.

- Si rebeu un missatge d'error del tipus `Xarxa inaccessible`, assegureu-vos que s'ha definit un camí cap a la passarel•la i que és correcte. Comproveu-ho mitjançant l'ordre **netstat -r** per llistar les taules d'encaminament del kernel.
- Si rebeu un missatge d'error del tipus `No hi ha camí a l'amfitrió`, verifiqueu que la interfície de xarxa local es troba activa executant l'ordre **ifconfig** nom_interfície. La sortida indica si la interfície es troba activa o no. Utilitzeu l'ordre **ping** per provar i accedir a un altre amfitrió de la xarxa.
- Si rebeu un missatge d'error del tipus `Temps d'espera de la connexió esgotat`:
  - Verifiqueu que la passarel•la local es troba activa mitjançant l'ordre **ping** amb el nom o l'adreça d'Internet de la passarel•la.
  - Assegureu-vos que s'ha definit un camí cap a la passarel•la i que és correcte. Comproveu-ho mitjançant l'ordre **netstat -r** per llistar les taules d'encaminament del kernel.
  - Assegureu-vos que l'amfitrió amb el qual voleu comunicar-vos té una entrada de taula d'encaminament en la vostra màquina.
- Si utilitzeu un encaminament estàtic, assegureu-vos que s'ha definit un camí a l'amfitrió de destinació i l'amfitrió de passarel•la. Comproveu-ho mitjançant l'ordre **netstat -r** per llistar les taules d'encaminament del kernel.

  Nota: Assegureu-vos que l'amfitrió amb el qual voleu comunicar-vos té una entrada de taula d'encaminament en la vostra màquina.
- Si utilitzeu un encaminament dinàmic, verifiqueu que la passarel•la està llistada i és correcta a les taules d'encaminament del kernel executant l'ordre **netstat -r**.
- Si l'amfitrió de passarel•la utilitza el **Routing Information Protocol** (RIP) amb el daemon **routed**, assegureu-vos que s'ha configurat un encaminament estàtic cap a l'amfitrió de destinació al fitxer `/etc/gateways`.

  Nota: Només cal que ho feu si el daemon d'encaminament no pot identificar el camí a un amfitrió distant a través de les consultes a altres passarel•les.
- Si l'amfitrió de passarel•la utilitza el **RIP** amb el daemon **gated**, assegureu-vos que s'ha configurat un encaminament estàtic cap a l'amfitrió de destinació al fitxer `gated.conf`.
- Si utilitzeu un encaminament dinàmic amb el daemon **routed**:
  - Si el **routed** no pot identificar el camí a través de les consultes (per exemple, si l'amfitrió de destinació no executa el **RIP**), comproveu el fitxer `/etc/gateways` per verificar que s'hagi definit un camí a l'amfitrió de destinació.
  - Assegureu-vos que les passarel•les responsables de reenviar paquets a l'amfitrió estan actives i executen el **RIP**. Si no, haureu de definir un encaminament estàtic.
  - Executeu el daemon **routed** mitjançant l'opció de depuració per enregistrar aquesta informació com a paquets erronis rebuts. Invoqueu el daemon des de la línia d'ordres mitjançant l'ordre següent:

    ```
    startsrc -s routed -a "-d"
    ```
  - Executeu el daemon **routed** mitjançant el senyalador **-t**, cosa que fa que tots els paquets enviats o rebuts s'escriguin a la sortida estàndard. Quan el **routed** s'executa en aquesta modalitat, roman sota el control del terminal que el va iniciar. Per tant, una interrupció des del terminal de control elimina el daemon.
- Si utilitzeu un encaminament dinàmic amb el daemon **gated**:

- Verifiqueu que el fitxer `/etc/gated.conf` està ben configurat i que esteu executant els protocols correctes.
- Assegureu-vos que la passarel•la de la xarxa d'origen utilitza el mateix protocol que la passarel•la de la xarxa de destinació.
- Assegureu-vos que la màquina amb la qual intenteu comunicar-vos té un camí de tornada a la vostra màquina d'amfitrió.
- Verifiqueu que els noms de passarel•la del fitxer `gated.conf` corresponen als noms de passarel•la llistats al fitxer `/etc/networks`.

- Si utilitzeu els protocols **RIP** o **HELLO**, i els camins a la destinació no es poden identificar a través de les consultes d'encaminament, comproveu el fitxer `gated.conf` per verificar que s'ha definit un camí a l'amfitrió de destinació. Estabiu encaminaments estàtics en les condicions següents:
  - L'amfitrió de destinació no executa el mateix protocol que l'amfitrió d'origen, per la qual cosa no poden intercanviar informació d'encaminament.
  - Cal accedir a l'amfitrió mitjançant una passarel•la distant (una passarel•la que es troba en un sistema autònom diferent del de l'amfitrió d'origen). El **RIP** només es pot utilitzar entre amfitrions del mateix sistema autònom.

Si tota la resta falla, potser voldreu activar el traçat per al vostre daemon d'encaminament (sigui el **routed** o el **gated**). Utilitzeu l'ordre SRC **traceson** des de la línia d'ordres, o envieu un senyal al daemon per especificar diferents nivells de traçat. Vegeu el daemon **gated** o el daemon **routed** per obtenir informació específica sobre enviar senyals a aquests daemons.

Resolució de problemes amb suport de l'SRC

Utilitzeu aquests suggeriments per resoldre els problemes més freqüents amb el Controlador de recursos del sistema

- Si no tenen efecte els canvis fets al fitxer `/etc/inetd.conf`:

  Actualitzeu el daemon **inetd** executant l'ordre **refresh -s inetd** o l'ordre **kill -1** *InetdPID*.
- Si **startsrc -s** [*nom_subsistema*] torna el missatge d'error següent:

  ```
  0513-00  El Controlador de recursos del sistema no està actiu.
  ```

  No s'ha activat el subsistema del Controlador de recursos del sistema. Executeu l'ordre **srcmstr &** per iniciar l'SRC, i torneu a executar l'ordre **startsrc**.

  És possible que també vulgueu intentar iniciar el daemon des de la línia d'ordres sense suport de l'SRC.
- Si **refresh -s** [*nom_subsistema*] o **lssrc -ls** [*nom_subsistema*] torna el missatge d'error següent:

  ```
  [nom_subsistema] no dóna suport a aquesta opció.
  ```

  El subsistema no dóna suport a l'opció SRC executada. Comproveu la documentació del subsistema per verificar les opcions a les quals dóna suport el subsistema.
- Si apareix el missatge següent:

  ```
  No s'ha trobat l'SRC; es continua sense suport de l'SRC.
  ```

  S'ha invocat un daemon directament des de la línia d'ordres en comptes d'utilitzar l'ordre **startsrc**. Això no representa un problema. Tanmateix, les ordres SRC, com ara **stopsrc** i **refresh,** no manipularan un subsistema invocat directament.

Si el daemon **inetd** es troba actiu i s'executa correctament i sembla que el servei adequat és correcte però seguiu sense poder connectar-vos, intenteu executar els processos del daemon **inetd** a través d'un depurador.

1. Atureu el daemon **inetd** temporalment:

   ```
   stopsrc -s inetd
   ```

   L'ordre **stopsrc** atura subsistemes com el daemon **inetd**.

2. Editeu el fitxer `syslog.conf` per afegir-hi una línia de depuració al final. Per exemple:
   ```
   vi /etc/syslog.conf
   ```
   a. Afegiu la línia `*.debug /tmp/mfitxer` al final del fitxer i sortiu.
   b. Cal que el fitxer que especifiqueu existeixi (`/tmp/mfitxer` en aquest exemple). Podeu utilitzar l'ordre **touch** per fer que el vostre fitxer existeixi.
3. Renoveu el fitxer:
   - Si utilitzeu l'SRC, escriviu:
     ```
     refresh -s syslogd
     ```
   - Si no utilitzeu l'SRC, elimineu el daemon **syslogd**:
     ```
     kill -1 `ps -e | grep /etc/syslogd | cut -c1-7`
     ```
4. Inicieu la còpia de seguretat del daemon **inetd** amb la depuració habilitada:
   ```
   startsrc -s inetd -a "-d"
   ```

   El senyalador **-d** habilita la depuració.
5. Intenteu establir una connexió per enregistrar errors al fitxer de depuració `/tmp/mfitxer`. Per exemple:
   ```
   tn bastet
   Intentant...
   connectat a bastet
   inici de sessió:>
   Connexió tancada
   ```
6. Comproveu si hi ha res que es mostri com un problema al fitxer de depuració. Per exemple:
   ```
   tail -f /tmp/mfitxer
   ```

Resolució de problemes telnet o rlogin

Aquestes explicacions poden ser útils en la resolució de problemes amb l'ordre **telnet** o **rlogin**.

Si teniu problemes amb la distorsió de la pantalla en aplicacions de pantalla completa:

1. Comproveu la variable d'entorn **TERM** executant una de les ordres següents:
   ```
   env
   ```
   ```
   echo $TERM
   ```
2. Verifiqueu que la variable **TERM** estigui establerta en un valor que coincideixi amb el tipus de pantalla de terminal que feu servir.

Les subordres **telnet** que ajuden en els problemes de depuració inclouen:

Element	Descripció
display	Visualitza els valors establerts i de commutació.
toggle	Commuta la visualització de totes les dades de xarxa en valor hexadecimal.
toggle options	Commuta la visualització de les opcions internes del procés **telnet**.

Si el daemon **inetd** ha pogut executar el servei **telnet** però encara no podeu connectar-vos mitjançant l'ordre **telnet**, segurament hi ha algun problema amb la interfície **telnet**.

1. Verifiqueu que **telnet** utilitza el tipus de terminal correcte.
   a. Comproveu la variable **$TERM** a la vostra màquina:
      ```
      echo $TERM
      ```
   b. Inicieu sessió en la màquina a la qual intenteu adjuntar-vos i comproveu la variable **$TERM**:
      ```
      echo $TERM
      ```
2. Utilitzeu les funcions de depuració de la interfície **telnet** introduint l'ordre **telnet** sense senyaladors.
   ```
   telnet
   tn>
   ```
   a. Escriviu `open` *`amfitrió`* on *amfitrió* és el nom de la màquina.

b. Premeu Ctrl-T per obtenir l'indicador `tn%gt;`.
c. A l'indicador `tn>`, escriviu `debug` per a la modalitat de depuració.

3. Intenteu connectar-vos a una altra màquina mitjançant la interfície **telnet**:

```
telnet bastet
Intentant...
Connectat a bastet
El caràcter d'escapament és '^T'.
```

Observeu la pantalla a mesura que s'hi van desplaçant les diferents ordres. Per exemple:

```
SENT do ECHO
SENT do SUPPRESS GO AHEAD
SENT will TERMINAL TYPE (reply)
SENT do SUPPORT SAK
SENT will SUPPORT SAK (reply)
RCVD do TERMINAL TYPE (don't reply)
RCVD will ECHO (don't reply)
RCVD will SUPPRESS GO AHEAD (don't reply)
RCVD wont SUPPORT SAK (reply)
SENT dont SUPPORT SAK (reply)
RCVD do SUPPORT SAK (don't reply)
SENT suboption TELOPT_NAWS Width 80, Height 25
RCVD suboption TELOPT_TTYPE SEND
RCVD suboption TELOPT_TTYPE aixterm
...
```

4. Comproveu la definició d'`aixterm` a `/etc/termcap` o `/usr/lib/terminfo`. Per exemple:

```
ls -a /usr/lib/terminfo
```

5. Si falta la definició d'`aixterm`, afegiu-la muntant el fitxer `ibm.ti`. Per exemple:

```
tic ibm.ti
```

L'ordre **tic** és un compilador d'informació de terminal.

Poden sorgir problemes amb les tecles de funció i de cursor quan utilitzeu les ordres **rlogin** i **telnet** amb programes que utilitzen curses ampliat. Les tecles de funció i de cursor generen seqüències d'escapament, que es divideixen si s'ha assignat massa poc temps per a tota la seqüència de tecles. Curses esperar durant un període específic de temps per decidir si un Esc indica només la tecla d'escapament o l'inici d'una seqüència d'escapament multioctet generada per altres tecles, com ara les tecles del cursor, la tecla d'acció i les tecles de funció.

Si no hi ha cap dada que segueixi l'Esc, o les dades no són vàlides, en el període de temps assignat, curses decideix que Esc és la tecla d'escapament i la seqüència de tecles es divideix. El retard que resulta de l'ordre **rlogin** o **telnet** depèn de la xarxa. De vegades les tecles de funció i de cursor funcionen i d'altres vegades no, en funció de la velocitat de la xarxa a la qual esteu connectats. Aquest problema es resol de forma efectiva si s'estableix la variable d'entorn **ESCDELAY** en un valor gran (de 1000 a 1500).

Problemes de configuració del TCP/IP

Les interfícies de xarxa es configuren automàticament durant la primera engegada del sistema després de la instal•lació de la targeta adaptadora. De totes maneres, encara heu d'establir alguns valors inicials per al **TCP/IP**, inclosos el nom d'amfitrió, l'adreça d'Internet i la màscara de subxarxa.

Per fer-ho, podeu utilitzar la interfície de la SMIT de les maneres següents:

- Utilitzeu el camí d'accés ràpid `smit mktcpip` per establir els valors inicials del nom d'amfitrió, l'adreça d'Internet i la màscara de subxarxa.
- Utilitzeu el camí d'accés ràpid `smit mktcpip` per especificar un servidor de noms que proporcioni el servei de resolució de noms. (Tingueu en compte que l'`smit mktcpip` només configura una interfície de xarxa.)
- Utilitzeu el camí d'accés ràpid `smit chinet` per establir altres atributs de xarxa.

També pot ser que vulgueu configurar els encaminaments estàtics que l'amfitrió necessiti per enviar informació de transmissió, com ara un encaminament a la passarel•la local. Utilitzeu el camí d'accés ràpid de la SMIT `smit mkroute`, per configurar-los permanentment a la base de dades de configuració.

Si us trobeu amb altres problemes de configuració, consulteu l'apartat “Configuració d'una xarxa TCP/IP” a la pàgina 106 per obtenir més informació.

Problemes més freqüents del TCP/IP amb interfícies de xarxa

Les interfícies de xarxa es configuren automàticament durant la primera engegada del sistema després de la instal•lació de la targeta adaptadora. No obstant això, hi ha determinats valors que s'han d'establir en ordre perquè s'iniciï el **TCP/IP**. Entre aquests valors s'inclouen el nom d'amfitrió i l'adreça d'Internet, i es poden establir mitjançant el camí d'accés ràpid de la SMIT, `smit mktcpip`.

Si trieu el mètode de la SMIT, utilitzeu el camí d'accés ràpid `smit mktcpip` per establir aquests valors de forma permanent a la base de dades de configuració. Utilitzeu els camins d'accés ràpid `smit chinet` i `smit hostname` per canviar-los en un sistema en execució. El camí d'accés ràpid `smit mktcpip` configura mínimament el **TCP/IP**. Per afegir adaptadors, utilitzeu el menú de configuració addicional, al qual es pot arribar amb el camí d'accés ràpid `smit tcpip`.

Si ja heu comprovat aquests valors per verificar-ne la precisió i encara continueu tenint problemes a l'hora d'enviar i rebre informació, comproveu el següent:

- Verifiqueu que el vostre adaptador de xarxa té una interfície de xarxa executant l'ordre **netstat -i**. La sortida hauria de llistar una interfície, com ara **tr0**, a la columna `Nom`. Si no ho fa, creeu una interfície de xarxa entrant al camí d'accés ràpid de la SMIT `smit mkinet`.
- Verifiqueu que l'adreça IP de la interfície és correcta executant l'ordre **netstat -i**. La sortida hauria de llistar l'adreça IP a la columna Xarxa. Si és incorrecta, estabiu l'adreça IP entrant al camí d'accés ràpid de la SMIT `smit chinet`.
- Utilitzeu l'ordre **arp** per assegurar-vos que teniu l'adreça IP completa de la màquina de destinació. Per exemple:

  ```
  arp -a
  ```

  L'ordre **arp** cerca l'adreça de l'adaptador físic. Aquesta ordre pot mostrar una adreça incompleta. Per exemple:

  ```
  ? (192.100.61.210) a (incomplet)
  ```

  Això podria ser a causa d'una màquina no endollada, una adreça perduda sense màquina en aquesta adreça en particular, o un problema de maquinari (com ara una màquina que es connecta i rep paquets però que no pot enviar-los).
- Cerqueu errors a la targeta adaptadora. Per exemple:

  ```
  netstat -v
  ```

  L'ordre **netstat -v** mostra estadístiques per als programes de control de dispositius adaptadors d'Ethernet, Token Ring, X.25 i 802.3. L'ordre també mostra dades d'inici de sessió d'error i de xarxa per a tots els programes de control de dispositius actius en una interfície incloent-hi: `Sense errors mbuf`, `Sense errors d'extensió mbuf` i `Paquets transmesos i errors d'adaptador detectats`.
- Comproveu el enregistrament d'errors executant l'ordre **errpt** per assegurar-vos que no hi ha problemes d'adaptador.
- Verifiqueu que la targeta adaptadora és correcta executant els diagnòstics. Utilitzeu l'aplicació de dispositius del camí d'accés ràpid `smit diag` o bé l'ordre **diag**.

Problemes del TCP/IP amb una interfície de xarxa SLIP:

En general, el mètode més efectiu per depurar problemes amb la interfície **Protocol d'interfície de línia sèrie (SLIP)** és tornar a traçar la configuració, verificant cada pas.

No obstant això, també podeu:

- Verificar que el procés **slattach** s'està executant i que utilitza el port tty correcte executant l'ordre **ps -ef**. Si no, executeu l'ordre **slattach**. (Consulteu els apartats “Configuració d'SLIP a través d'un mòdem” a la pàgina 619 o “Configuració d'SLIP a través d'un cable de mòdem nul” a la pàgina 621 per veure la sintaxi exacta que hauríeu de fer servir.)
- Verifiqueu que les adreces punt a punt estan especificades correctament introduint el camí d'accés ràpid `smit chinet`.

  Seleccioneu la interfície **SLIP**. Assegureu-vos que els camps **ADREÇA D'INTERNET** i **ADREÇA DE DESTINACIÓ** són correctes.

Si el mòdem no funciona correctament:

- Assegureu-vos que el mòdem s'hagi instal•lat de forma correcta. Consulteu el manual d'instal•lació del mòdem.
- Verifiqueu que els controls de flux que faci el mòdem estan desactivats.

Si el tty no funciona de forma correcta, verifiqueu que la velocitat en bauds del tty i les característiques del mòdem estiguin ben establertes en la base de dades de configuració introduint el camí d'accés ràpid `smit tty`.

Problemes del TCP/IP amb una interfície de xarxa Ethernet:

Consulteu aquesta llista de verificació si persisteixen els problemes del **TCP/IP** amb una interfície de xarxa Ethernet.

Si s'ha inicialitzat la interfície de xarxa, s'han especificat correctament les adreces i heu verificat que la targeta adaptadora està bé:

- Verifiqueu que esteu utilitzant un connector T endollat directament al transceptor d'intrabord/forabord.
- Assegureu-vos que esteu utilitzant un cable Ethernet. (El cable Ethernet és de 50 OHM.)
- Assegureu-vos que esteu utilitzant terminadors Ethernet. (Els terminadors Ethernet són de 50 OHM.)
- Els adaptadors Ethernet es poden utilitzar tant amb el transceptor que hi ha a la targeta com amb un transceptor extern. A l'adaptador hi ha un pont per especificar quin esteu fent servir. Verifiqueu que el vostre pont estigui ben establert (consulteu el manual de l'adaptador per obtenir instruccions).
- Verifiqueu que esteu utilitzant el tipus de connector Ethernet correcte (lleuger és BNC; pesant és DIX). Si canvieu aquest tipus de connector, utilitzeu el camí d'accés ràpid de la SMIT **smit chgenet** per establir el camp Aplica el canvi només a la base de dades. (Establiu en Sí a la SMIT.) Reinicieu la màquina per aplicar el canvi de configuració. (Consulteu l'apartat “Configuració i gestió d'adaptadors” a la pàgina 161.)

Problemes del TCP/IP amb una interfície de xarxa Token-Ring:

Utilitzeu aquestes directrius per resoldre problemes de comunicació amb la vostra interfície de xarxa.

Si no podeu comunicar amb alguna de les màquines de la vostra xarxa malgrat que s'ha inicialitzat la interfície de xarxa, s'han especificat correctament les adreces i heu verificat que la targeta adaptadora està bé:

- Comproveu si els amfitrions amb els quals no podeu comunicar es troben en un anell diferent. Si és així, utilitzeu el camí d'accés ràpid de la SMIT `smit chinet` per comprovar el camp Limitar la difusió al Token-Ring local. *No* establiu en No a la SMIT.
- Comproveu si l'adaptador Token-Ring està configurat per executar-se a una velocitat d'anell correcta. Si està configurat de forma incorrecta, utilitzeu la SMIT per canviar l'atribut de velocitat d'anell de l'adaptador (consulteu l'apartat “Configuració i gestió d'adaptadors” a la pàgina 161). Quan es reinicïi el **TCP/IP**, l'adaptador Token-Ring tindrà la mateixa velocitat d'anell que la resta de la xarxa.

Problemes del TCP/IP amb un pont Token-Ring/Ethernet:

Si no podeu comunicar entre un Token-Ring i una xarxa Ethernet mitjançant un pont, i heu verificat que el pont funciona correctament, és possible que l'adaptador Ethernet estigui eliminant paquets.

Una màquina elimina paquets si el paquet d'entrada (incloses les capçaleres) és més gran que el valor de la unitat de transmissió màxima (MTU) de l'adaptador de xarxa. Per exemple, un paquet de 1500 octets enviat per un adaptador Token-Ring per un pont recopila una capçalera de control d'enllaços lògics (LLC) de 8 octets, cosa que fa que la grandària total del paquet sigui 1508. Si la MTU de l'adaptador Ethernet receptor està establerta en 1500, el paquet s'eliminarà.

Comproveu els valors MTU d'ambdós adaptadors de xarxa. Per permetre la capçalera LLL de vuit octets, que l'adaptador Token-Ring adjunta als paquets de sortida, establiu el valor MTU per a l'adaptador Token-Ring com a mínim vuit octets per sota del valor MTU per a l'adaptador Ethernet. Per exemple, establiu la MTU per a un adaptador Token-Ring en 1492 per comunicar amb un adaptador Ethernet amb una MTU de 1500.

Problemes del TCP/IP amb un pont Token-Ring/Token-Ring:

Quan treballeu amb un pont, canvieu el valor per defecte de 1500 per a la unitat de transmissió màxima (MTU) per un valor que sigui vuit menys que el camp d'informació màxima (trama d'informació màxima) anunciat pel pont al camp de control d'encaminament.

Per cercar el valor del camp de control d'encaminament, utilitzeu el daemon**iptrace** per mirar als paquets d'entrada. Els bits 1, 2 i 3 de l'octet 1 són els bits de la trama més gran, que especifiquen el camp d'informació màxima que es pot transmetre entre dues estacions en comunicació en un camí específic. A continuació, vegeu el format del camp de control d'encaminament:

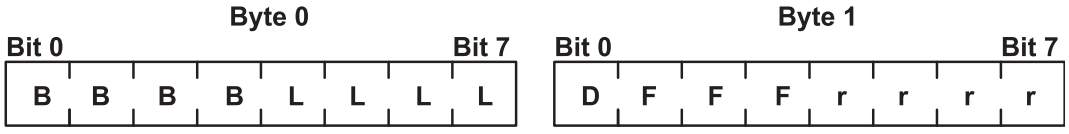


Figura 25. Camp de control d'encaminament

Aquesta il•lustració mostra l'octet 0 i l'octet 1 d'un camp de control d'encaminament. Els vuit bits de l'octet 1 són B, B, B, B, L, L, L, L. Els vuit bits de l'octet 1 són D, F, F, F, r, r, r, r.

Els valors dels bits de la trama més gran són els següents:

Element	Descripció
000	Especifica un màxim de 516 octets al camp d'informació.
001	Especifica un màxim de 1500 octets al camp d'informació.
010	Especifica un màxim de 2052 octets al camp d'informació.
011	Especifica un màxim de 4472 octets al camp d'informació.
100	Especifica un màxim de 8144 octets al camp d'informació.
101	Reservat.
110	Reservat.
111	Usat a les trames de difusió de tots els camins.

Per exemple, si el valor de trama d'informació màxima és 2052 al camp de control d'encaminament, la grandària de la MTU s'hauria d'establir en 2044. Això només és per a interfícies de xarxa Token-Ring.

Nota: Quan s'utilitza **iptrace**, el fitxer de sortida *no* ha d'estar en un Sistema de fitxers de xarxa (NFS).

Problemes del TCP/IP en la comunicació amb un amfitrió remot

Si no podeu comunicar-vos amb un amfitrió remot, proveu aquests suggeriments.

- Executeu l'ordre **ping** a l'amfitrió local per verificar que la interfície local de la xarxa es troba activada i en execució.
- Utilitzeu l'ordre **ping** per als amfitrions i passarel•les que progressivament es troben a més salts de l'amfitrió local per determinar el punt en què falla la comunicació.

Si teniu problemes amb la pèrdua de paquets o experimenteu retards en el lliurament de paquets, intenteu el següent:

- Utilitzeu l'ordre **trpt** per traçar els paquets al nivell del sòcol.
- Utilitzeu l'ordre **iptrace** per traçar totes les capes de protocol.

Si no podeu comunicar entre un Token-Ring i una xarxa Ethernet mitjançant un pont, i heu verificat que el pont és correcte:

- Comproveu els valors MTU d'ambdós adaptadors. Els valors MTU han de ser compatibles per permetre la comunicació. Una màquina elimina paquets si el paquet entrant (incloses les capçaleres) és més gran que els valors MTU de l'adaptador. Per exemple, un paquet de 1500 octets enviat per un pont recopila una capçalera LLC de 8 octets, cosa que fa que la grandària total del paquet sigui 1508. Si la MTU de la màquina receptora està establerta en 1500, un paquet de 1508 octets s'eliminarà.

Problemes del TCP/IP amb resposta snmpd a les consultes

Si **snmpd** no respon a les consultes i no s'ha rebut cap missatge d'enregistrament, és possible que el paquet sigui massa gran per al manejador de paquets del protocol **User Datagram Protocol (UDP)** del kernel.

Si aquest és el cas, augmenteu les variable del kernel **udp_sendspace** i **udp_recvspace** executant l'ordre següent:

```
no -o udp_sendspace=64000
no -o udp_recvspace=64000
```

La grandària màxima per a un paquet **UDP** és 64 K. Si la vostra consulta és superior a 64 K, es rebutjarà. Dividiu el paquet en paquets més petits per evitar aquest problema.

Problemes del TCP/IP amb el Protocol de Configuració d'Amfitrió Dinàmic

En cas que no es pugui obtenir les dades de configuració, intenteu les solucions següents.

Si no aconseguiu obtenir una adreça IP o altres paràmetres de configuració:

- Comproveu que heu especificat una interfície per configurar. Això es pot fer mitjançant el camí d'accés ràpid SMIT `smit dhcp`.
- Comproveu que s'ha configurat un servidor de la xarxa local o un agent de retransmissió per treure les vostres sol•licituds de la xarxa local.
- Comproveu que s'està executant el programa **dhcpcd**. Si no, utilitzeu l'ordre **startsrc -s dhcpcd**.

Ordres TCP/IP

El **TCP/IP** és part de l'estructura subjacent del sistema. Us permet comunicar-vos amb un altre terminal o sistema simplement executant una ordre o programa.

El **TCP/IP** és part de l'estructura subjacent del sistema. Us permet comunicar-vos amb un altre terminal o sistema simplement executant una ordre o programa. El sistema s'encarrega de la resta.

Element	Descripció
chnamsv	Canvia la configuració de servei de noms basada en el **Transmission Control Protocol/Internet Protocol (TCP/IP)** en un amfitrió.
chprtsv	Canvia una configuració de servei d'impressió en un client o en un servidor.
hostent	Manipula directament les entrades de mapatge d'adreces a la base de dades de configuració del sistema.
ifconfig	Configura o visualitza els paràmetres d'interfície de xarxa per a una xarxa mitjançant l'ús del **TCP/IP**.
mknamsv	Configura el servei de noms basat en el **TCP/IP** en un amfitrió per a un client.
mkprtsv	Configura el servei d'impressió basat en el **TCP/IP** en un amfitrió.
mktcpip	Estableix els valors obligatoris per iniciar el **TCP/IP** en un amfitrió.
no	Configura les opcions de xarxa.
rmnamsv	Desconfigura el servei de noms basat en el **TCP/IP** en un amfitrió.
rmprtsv	Desconfigura un servei d'impressió en un client o en un servidor.
slattach	Connecta línies en sèrie com a interfícies de xarxa.
arp	Visualitza o transforma l'adreça d'Internet en taules de conversió d'adreces de maquinari que utilitza el **Protocol de resolució d'adreces (ARP)**.
gettable	Obté taules d'amfitrió amb format del Centre d'informació de xarxa (NIC) d'un amfitrió.
hostid	Estableix o visualitza l'identificador de l'amfitrió local corrent.
nom_amfitrió	Estableix o visualitza el nom de l'amfitrió local corrent.
htable	Converteix els fitxers de l'amfitrió al format que empren les rutines de biblioteca de la xarxa.
ipreport	Genera un informe de traça de paquets a partir del fitxer de traça de paquets especificat.
iptrace	Proporciona la traça de paquets a nivell d'interfície per als protocols d'Internet.
lsnamsv	Mostra la informació de servei de noms emmagatzemada a la base de dades.
lsprtsv	Mostra la informació de servei d'impressió emmagatzemada a la base de dades.
mkhosts	Genera el fitxer de taula de l'amfitrió.
namerslv	Manipula directament entrades del servidor de noms de domini per a rutines de solucionador local a la base de dades de configuració del sistema.
netstat	Mostra l'estat de la xarxa.
route	Manipula manualment les taules d'encaminament.
ruser	Manipula directament les entrades de tres bases de dades de sistemes separats que controlen l'accés d'amfitrions externs als programes.
ruptime	Visualitza l'estat de cada amfitrió en una xarxa.
securetcpip	Habilita la funció de seguretat de la xarxa.
setclock	Estableix l'hora i la data d'un amfitrió en una xarxa.
timedc	Retorna informació sobre el daemon **timed**.
trpt	Du a terme la traça de protocol als sòcols del **Protocol de control de transmissió(TCP)**.

Ordres SRC

Les ordres SRC poden afectar un daemon, un grup de daemons, o un daemon i els daemons que aquest controla (subsistema amb subservidors).

A més, alguns daemons **TCP/IP** no responen a totes les ordres SRC. A continuació es mostra una llista de les ordres SRC que es poden utilitzar per controlar els daemons **TCP/IP** i les seves excepcions.

Element	Descripció
startsrc	Inicia tots els subsistemes **TCP/IP** i els subservidors **inetd**. L'ordre **startsrc** funciona per a tots els subsistemes **TCP/IP** i subservidors **inetd**.
stopsrc	Atura tots els subsistemes **TCP/IP** i els subservidors **inetd**. Aquesta ordre també s'anomena l'ordre **stop normal**. L'ordre **stop normal** permet als subsistemes processar tot el treball pendent i finalitzar correctament. Per als subservidors **inetd**, totes les connexions pendents poden iniciar-se i totes les connexions existents poden completar-se. L'ordre **stop normal** funciona per a tots els subsistemes **TCP/IP** i subservidors **inetd**.
stopsrc -f	Atura tots els subsistemes **TCP/IP** i els subservidors **inetd**. Aquesta ordre també s'anomena **stop force**. L'ordre **stop force** finalitza immediatament tots els subsistemes. Per als subservidors**inetd**, totes les connexions pendents i les connexions existents finalitzen de forma immediata.
refresh	Renova els subsistemes i subservidors següents: els subsistemes **inetd**, **syslogd**, **named**, **dhcpsd** i **gated**.
lssrc	Proporciona l'estat curt dels subsistemes, que és l'estat del subsistema especificat (actiu o inoperatiu). També proporciona l'estat curt dels subservidors **inetd**. L'estat curt dels subservidors **inetd** inclou: el nom del subservidor, l'estat, la descripció del subservidor, el nom de l'ordre i els arguments amb què es va invocar.

Element	Descripció
lssrc -l	Proporciona l'estat curt més informació addicional (estat llarg) dels subsistemes següents: **gated** Estat de depuració o traça, protocols d'encaminament activats, taules d'encaminament, senyals acceptats i llur funció. **inetd** Estat de depuració, llista de subservidors actius i el seu estat curt; senyals acceptats i llur funció. **named** Estat de depuració, informació del fitxer `named.conf`. **dhcpsd** Estat de depuració, totes les adreces IP controlades i llur estat actual. **routed** Estat de depuració i traça, estat d'especificació d'informació d'encaminament, taules d'encaminament. **syslogd** Informació de configuració de **syslogd**. L'ordre **lssrc -l** també proporciona l'estat llarg dels subservidors **inetd**. L'estat llarg inclou la informació de l'estat curt i informació de la connexió activa. Alguns subservidors proporcionaran informació addicional. La informació addicional per cada subservidor inclou: **ftpd** Estat de depuració i inici de sessió **telnetd** Tipus d'emulació de terminal **rlogind** Estat de depuració **fingerd** Estat de depuració i inici de sessió Els subservidors **rwhod** i **timed** no proporcionen l'estat llarg.
traceson	Engega la depuració de nivell de sòcol. Utilitzeu l'ordre **trpt** per formatar la sortida. Els subsistemes **timed** i **iptraced** no donen suport a l'ordre **traceson**.
tracesoff	Apaga la depuració de nivell de sòcol. Utilitzeu l'ordre **trpt** per formatar la sortida. Els subsistemes **timed** i **iptraced** no donen suport a l'ordre **tracesoff**.

Per obtenir exemples de com utilitzar aquestes ordres, vegeu els temes sobre les ordres individuals. Per obtenir més informació sobre el Controlador de recursos del sistema, consulteu System Resource Controller a *Operating system and device management*.

Ordres de transferència de fitxers

A continuació, teniu una llista amb descripcions breus de les ordres de transferència de fitxers.

Element	Descripció
ftp *nom_amfitrió*	Transfereix fitxers entre un amfitrió local i un de remot.
rcp*fitxer amfitrió:fitxer*	Transfereix fitxers entre un amfitrió local i un de remot o entre dos amfitrions remots.
tftp	Transfereix fitxers entre amfitrions.

Ordres d'inici de sessió remota

A continuació, teniu una llista amb descripcions breus de les ordres d'inici de sessió remota **TCP/IP**.

Element	Descripció
rexec *ordre amfitrió*	Executa ordres una a una en un amfitrió remot.
rlogin *amfitrió_remot*	Connecta un amfitrió local amb un amfitrió remot.
rsh i **remsh** *ordre amfitrió_remot*	Executa una ordre especificada en un amfitrió remot o inicia la sessió en un amfitrió remot.
telnet, **tn** i **tn3270** *nom_amfitrió*	Connecta l'amfitrió local amb un amfitrió remot, mitjançant la interfície **TELNET**.

Ordres d'estat

A continuació, teniu una llista amb descripcions breus de les ordres d'estat **TCP/IP**.

Element	Descripció
finger o **f** *usuari@amfitrió*	Mostra informació de l'usuari.
host *nom_amfitrió*	Resol un nom d'amfitrió en una adreça d'Internet o una adreça d'Internet en un nom d'amfitrió.
ping *nom_amfitrió*	Envia una sol•licitud d'eco a un amfitrió de xarxa.
rwho	Mostra quins usuaris inicien la sessió en amfitrions de la xarxa local.
whois *nom*	Identifica un usuari mitjançant un ID d'usuari o un àlies.

Ordre de comunicació remota

L'ordre de comunicació remota **TCP/IP**, **talk** *usuari@amfitrió*, us permet conversar amb un altre usuari.

Element	Descripció
talk *usuari@amfitrió*	Conversa amb un altre usuari

Ordres d'impressió

A continuació, teniu una llista amb descripcions breus de les ordres d'impressió **TCP/IP**.

Element	Descripció
enq *fitxer*	Col•loca en cua un fitxer.
refresh	Demana una renovació d'un subsistema o grup de subsistemes.
smit	Duu a terme la gestió del sistema.

Daemons TCP/IP

Un *subsistema* és un daemon, o servidor, controlat pel SRC. Un *subservidor* és un daemon controlat per un subsistema. (Les ordres i els noms de daemon es denoten normalment per una **d** al final del nom.)

Les categories de subsistema i de subservidor s'exclouen mútuament. És a dir, no es fa una llista de daemons com a subsistema i subservidor alhora. L'únic subsistema **TCP/IP** que controla altres daemons és el daemon **inetd**. Tots els subservidors **TCP/IP** són també subservidors **inetd**.

A continuació, us presentem els daemons **TCP/IP** que controla l'SRC:

Subsistemes

Element	Descripció
gated	Proporciona funcions d'encaminament de passarel•la i dóna suport al **Protocol d'informació d'encaminament (RIP)**, al **Protocol d'informació d'encaminament Next Generation (RIPng)**, a l'**Exterior Gateway Protocol (EGP)**, al **Border Gateway Protocol (BGP)** i al **BGP4+**, al **Defense Communications Network Local-Network Protocol (HELLO)**, a l'**Open Shortest Path First (OSPF)**, a l'Intermediate System to Intermediate System (IS-IS) i a l'**Internet Control Message Protocol (ICMP** i **ICMPv6)/Router Discovery routing**. A més a més, el daemon **gated** dóna suport al **Simple Network Management Protocol (SNMP)**. El daemon **gated** és un dels dos daemons d'encaminament disponibles per a l'encaminament a adreces de xarxa i és el preferit. El daemon **gated** es prefereix al **routed** perquè el **gated** dóna suport a un nombre major de protocols de passarel•la.
inetd	Invoca i planifica altres daemons quan es reben les sol•licituds dels serveis de daemon. Aquest daemon també en pot iniciar d'altres. El daemon **inetd** també es coneix com a súper daemon.
iptrace	Proporciona la funció de traça de paquets a nivell d'interfície per als protocols d'Internet.
named	Proporciona la funció de denominació per al protocol **Servidor de noms de domini** (DOMAIN).
routed	Gestiona les taules d'encaminament de xarxa i dóna suport al **Protocol d'informació d'encaminament (RIP)**. El daemon **gated** es prefereix al **routed** perquè el **gated** dóna suport a un nombre major de protocols de passarel•la.
rwhod	Envia difusions a tots els altres amfitrions cada tres minuts i emmagatzema la informació sobre els usuaris connectats i l'estat de la xarxa. Utilitzeu el daemon **rwhod** amb molta cura, perquè pot emprar grans quantitats de recursos de la màquina.
timed	Proporciona la funció de servidor horari.

Nota: Tant el daemon **routed** com el **gated** apareixen llistats com a subsistemes TCP/IP. No executeu l'ordre **startsrc -g tcpip**, que inicia aquests dos daemons d'encaminament, amb tots els altres subsistemes **TCP/IP**. L'execució simultània d'ambdós daemons en una sola màquina pot tenir conseqüències imprevisibles.

Els daemons TCP/IP controlats pel subsistema **inetd** són els següents:

Subservidors inetd

Element	Descripció
comsat	Notifica als usuaris que ha entrat correu.
fingerd	Proporciona un informe d'estat sobre tots els usuaris connectats i sobre l'estat de la xarxa a l'amfitrió remot especificat. Aquest daemon utilitza el protocol **Finger**.
ftpd	Proporciona la funció de transferència de fitxers per a un procés de client mitjançant el **File Transfer Protocol (FTP)**.
rexecd	Proporciona la funció de servidor de l'amfitrió extern per a l'ordre **rexec**.
rlogind	Proporciona la funció de mitjà d'inici de sessió remota per a l'ordre **rlogin**.
rshd	Proporciona la funció de servidor per a l'execució d'ordres remotes per a les ordres **rcp** i **rsh**.
talkd	Proporciona la funció de conversa per a l'ordre **talk**.
syslogd	Llegeix i enregistra els missatges del sistema. Aquest daemon es troba al grup de subsistemes **Remote Access Service** (RAS).
telnetd	Proporciona la funció de servidor per al protocol **TELNET**.
tftpd	Proporciona la funció de servidor per al **Trivial File Transfer Protocol (TFTP)**.
uucpd	Gestiona les comunicacions entre els Basic Network Utilities (BNU) i el **TCP/IP**.

Mètodes de dispositiu

Els mètodes de dispositiu són programes associats amb un dispositiu que realitzen les operacions bàsiques de configuració del dispositiu.

Consulteu l'apartat List of TCP/IP Programming References de la publicació *Communications Programming Concepts* per obtenir informació sobre els mètodes **TCP/IP**.

Sol•licitud de comentaris

El sistema AIX dóna suport a les següents Sol•licituds de comentaris (RFC) **TCP/IP**.

Per veure una llista de les RFC (Sol•licitud de comentaris) suportades per aquest sistema operatiu, consulteu l'apartat List of TCP/IP Programming References de la publicació *Communications Programming Concepts*.

- RFC 1359 *Connecting to the Internet: What connecting institutions should anticipate*
- RFC 1325 *FYI on questions and answers: Answers to commonly asked 'new Internet user' questions*
- RFC 1244 *Site Security Handbook*
- RFC 1178 *Choosing a Name for Your Computer*
- RFC 1173 *Responsibilities of host and network managers: A summary of the `oral tradition' of the Internet*

Basic Networking Utilities (BNU)

Els BNU són un grup de programes, directoris i fitxers que estableixen comunicacions entre sistemes informàtics de xarxes locals i remotes. Poden utilitzar-se per la comunicació amb qualsevol sistema UNIX en el que s'executa una versió del Programa de còpia UNIX a UNIX (UUCP). Els BNU són un dels programes dels serveis ampliats que es poden instal•lar amb el sistema operatiu base.

Els BNU contenen un grup d'ordres relacionades amb l'UUCP, un programa de comunicació d'UNIX a UNIX desenvolupat per AT&T i modificat com a part de BSD (Berkeley Software Distribution). Els BNU proporcionen ordres, processos i una base de dades de suport per a connexions a sistemes locals i remots.

Les xarxes de comunicació com ara Token-Ring i Ethernet s'utilitzen per connectar sistemes de xarxes locals. Una xarxa local es pot connectar a un sistema remot mitjançant cable o mitjançant mòdem telefònic. Es poden intercanviar aleshores ordres i fitxers entre la xarxa local i el sistema remot.

Abans que els usuaris del vostre sistema puguin executar programes BNU, els BNU han d'estar instal•lats i configurats.

Els BNU es controlen mitjançant un conjunt de fitxers de configuració que determinen si els sistemes remots poden iniciar una sessió en el sistema local i què poden fer després d'iniciar la sessió. Aquests fitxers de configuració s'han de configurar d'acord amb els requisits i recursos del vostre sistema.

Per mantenir els BNU, heu de llegir i eliminar periòdicament els fitxers de registre i heu de comprovar les cues dels BNU per assegurar-vos que els treballs es transfereixen correctament al sistemes remots. També heu d'actualitzar periòdicament els fitxers de configuració per tal que reflecteixin els canvis realitzats en el vostre sistema o en els sistemes remots.

Com funcionen els BNU

Els BNU utilitzen un conjunt de programari i de connexions de maquinari per la comunicació entre sistemes.

Una estructura de directoris i fitxers efectua el seguiment de les activitats dels BNU. Aquesta estructura inclou un conjunt de directoris públics, un grup de directoris i fitxers administratius, fitxers de configuració i fitxers de bloqueig. La majoria dels directoris per als BNU es creen durant el procés d'instal•lació. Alguns dels directoris i fitxers administratius es creen utilitzant diversos programes dels BNU.

Amb l'excepció de les ordres d'inici de sessió remota, els BNU funcionen com un sistema de procés per lots. Quan un usuari sol•licita un treball enviat a un sistema remot, els BNU emmagatzemen la informació necessària per dur a terme el treball. Això es coneix com a *col•locar en cua* el treball. A intervals planificats, o quan un usuari dóna instruccions per fer-ho, els BNU es posen en contacte amb diversos sistemes remots, transfereixen el treball posat en cua i accepten els treballs. Aquestes transferències es controlen mitjançant els fitxers configuració del vostre sistema i els del sistema remot.

Suport d'idioma nacional per a les ordres dels BNU

Totes les ordres dels BNU, excepte l'ordre **uucpadm**, estan disponibles per al Suport d'idioma nacional.

Els noms d'usuari no cal que estiguin en caràcters ASCII. No obstant això, tots els noms de sistema han d'estar en caràcters ASCII. Si un usuari intenta planificar una transferència o l'execució d'una ordre remota que impliqui noms de sistema que no siguin ASCII, els BNU tornen un missatge d'error.

Estructura de directoris i fitxers dels BNU

Els BNU utilitzen una estructura de directoris i fitxers per realitzar el seguiment de les activitats.

Aquesta estructura inclou els directoris públics, els fitxers de configuració, els directoris administratius i el fitxers de bloqueig.

La majoria dels directoris dels BNU es creen durant el procés d'instal•lació. Alguns dels directoris i fitxers administratius es creen utilitzant diversos programes dels BNU a mesura que s'executen.

Directoris públics dels BNU

Quan s'especifica, el directori públic dels BNU (`/var/spool/uucppublic`) emmagatzema els fitxers que s'han transferit al sistema local des d'altres sistemes.

Els fitxers s'esperen al directori públic fins que els usuaris els reclamen. El directori públic es crea quan s'instal•len els BNU. Dins del directori públic, els BNU creen un subdirectori per a cada sistema remot que envia fitxers al sistema local.

Fitxers de configuració dels BNU

Els fitxers de configuració dels BNU, també coneguts com la base de dades de suport dels BNU, resideixen al directori `/etc/uucp`. Els fitxers s'han de configurar específicament per al vostre sistema.

Els fitxers de configuració pertanyen a l'ID d'inici de sessió `uucp` i només es poden editar amb autorització root. Els fitxers de configuració contenen informació sobre:

- Sistemes remots accessibles
- Dispositius per contactar amb els sistemes remots
- Hores per contactar amb els sistemes remots
- El que els sistemes remots poden fer al vostre sistema.

Alguns fitxers de configuració també especifiquen límits sobre les activitats dels BNU per tal d'impedir la sobrecàrrega del sistema.

Els fitxers de configuració dels BNU inclouen:

Element	Descripció
`Devices`	Conté informació sobre els dispositius disponibles, que inclouen tant els mòdems com les connexions directes.
`Dialcodes`	Conté abreviatures de codis de marcatge, que permeten escurçar el números de telèfon del fitxer `Systems`.
`Dialers`	Especifica la sintaxi d'ordres de crida per a un determinat tipus de mòdem ("marcador").
`Maxuuscheds`	Limita els treballs planificats simultanis.
`Maxuuxqts`	Limita les execucions d'ordres remotes simultànies.
`Permissions`	Conté codis de permís d'accés. Aquest fitxer és el fitxer principal per determinar la seguretat dels BNU.
`Poll`	Especifica el moment en què el programa dels BNU ha de sondejar els sistemes remots per iniciar tasques.
`Sysfiles`	Llista els fitxers que serveixen com a fitxers `Systems`, `Devices` i `Dialers` per a la configuració dels BNU. Si no s'utilitza aquest fitxer, els fitxers per defecte són `/etc/uucp/Systems`, `/etc/uucp/Devices` i `/etc/uucp/Dialers`.
`Systems`	Llista els sistemes remots accessibles i la informació necessària per contactar-hi, que inclou el dispositiu que cal utilitzar i les combinacions de nom d'usuari i paraula clau necessàries per iniciar una sessió. A més, especifica les hores a les que es pot contactar amb els sistemes.

Els fitxers de configuració es fan referència entre sí quan s'utilitzen els BNU. Per exemple:

- El fitxer `Devices` conté un camp *Testimoni* que fa referència a les entrades del camp `Dialers`.
- El fitxer `Systems` conté una entrada per a una *Classe* de dispositiu. Un dispositiu de cada *Classe* a la que es fa referència al fitxer `Systems` ha d'estar definit al fitxer `Devices`.
- El fitxer `Poll` conté entrades per als sistemes que el vostre sistema crida. Cadascun d'aquests sistemes ha d'estar definit al fitxer `Systems`.

Les entrades dels fitxers de configuració dels BNU depenen dels tipus de connexions entre el vostre sistema i cada sistema remot. Per exemple, s'han de realitzar entrades especials si s'utilitzen connexions directes o TCP/IP (Transmission Control Protocol/Internet Protocol) per contactar amb altres sistemes. Si s'utilitzen mòdems per contactar amb altres sistemes, els mòdems han d'estar definits al fitxer `Dialers`.

Els fitxers `Systems`, `Devices` i `Permissions` han d'estar configurats al vostre sistema abans de què pugueu contactar amb sistemes remots utilitzant els BNU. Altres fitxers de configuració permeten utilitzar possibilitats dels BNU, com ara el sondeig automàtic. Molts dels fitxers de configuració s'han de modificar periòdicament per què reflecteixin els canvis realitzats al vostre sistema o als sistemes contactats. El fitxer `Sysfiles` es pot utilitzar per especificar fitxers que no siguin els fitxers `Systems`, `Devices` i `Dialers` per defecte per què realitzin la mateixa funció.

Directoris i fitxers administratius dels BNU

El directoris i fitxers administratius dels BNU es troben en subdirectoris del directori `/var/spool/uucp`.

Aquests directoris i fitxers contenen dos tipus d'informació:

- Dades que esperen ser transferides a altres sistemes
- Informació d'enregistraments i errors sobre les activitats dels BNU.

Dins del directori `/var/spool/uucp`, els BNU creen els següents directoris:

Element	Descripció
`.Admin`	Conté quatre fitxers administratius: • `audit` • `Foreign` • `errors` • `xferstats` Aquests fitxers contenen informació d'enregistraments i errors sobre les activitats dels BNU.
`.Corrupt`	Conté còpies dels fitxers que el programa dels BNU no pot processar.
`.Log` i `.Old`	Conté fitxers de registre de les transaccions dels BNU.
`.Status`	Emmagatzema la darrera vegada que el daemon **uucico** va intentar posar-se en contacte amb els sistemes remots.
`.Workspace`	Conté fitxers temporals que els programes de transport de fitxers utilitzen internament.
`.Xqtdir`	Conté fitxers d'execució amb llistes d'ordres que els sistemes remots poden executar.
Nom_sistema	Conté els fitxers que utilitzen els programes de transport de fitxers. Són els fitxers següents: • Ordre (**C.***) • Dades (**D.***) • Executar (**X.***) • Temporal (**TM.***) Els BNU creen un directori *Nom_sistema* per a cada sistema remot contactat.

Els directoris els noms dels quals comencen amb un punt estan *ocults*. No es poden trobar amb una ordre **ls** o **li** a no ser que s'utilitzi el senyalador **-a**. Quan el daemon **uucico** s'inicia, cerca fitxers de treball al directori `/var/spool/uucp` i transfereix els fitxers des de qualsevol directori que no estigui ocult. El daemon **uucico** només veu els directoris *Nom_sistema*, però no els altres directoris administratius.

Els fitxers dels directoris ocults pertanyen a l'ID d'inici de sessió UUCP. Només es pot accedir a aquests fitxers amb autorització root o amb un ID d'inici de sessió amb un ID d'usuari de 5.

Per obtenir més informació sobre com mantenir els directoris administratius dels BNU, consulteu l'apartat "Manteniment dels BNU" a la pàgina 449.

Fitxers de bloqueig dels BNU

Els fitxers de bloqueig dels BNU s'emmagatzemen al directori `/var/locks`. Quan els BNU utilitzen un dispositiu per establir una connexió amb un ordinador remot, col•loquen un fitxer de bloqueig per a aquest dispositiu al directori `/var/locks`.

Quan un programa dels BNU o qualsevol altre programa necessita el dispositiu, aquest programa comprova si al directori `/var/locks` hi ha un fitxer de bloqueig. Si existeix un fitxer de bloqueig, el programa espera fins que el dispositiu estigui disponible o bé utilitza un altre dispositiu per a la comunicació.

A més, el daemon **uucico** col•loca fitxers de bloqueig per als sistemes remots al directori `/var/locks`. Abans de contactar amb un sistema remot, el daemon **uucico** comprova si al directori `/var/locks` hi ha un fitxer de bloqueig per a aquest sistema. Aquests fitxers impedeixen que altres instàncies del daemon **uucico** estableixin connexions duplicades amb el mateix sistema remot.

Nota: A més dels BNU, altres programes com ara ATE (Emulació de Terminal Asíncron) i TCP/IP, utilitzen el directori `/var/locks`.

Configuració dels BNU

Aquest procediment explica com configurar els BNU (Basic Network Utilities) per a diversos tipus de connexions, com ara les connexions directes, per mòdem i TCP/IP (Transmission Control Protocol/Internet Protocol

Prerequisits

- Els BNU han d'estar instal•lats al sistema.
- Cal tenir autorització d'usuari root per editar els fitxers de configuració dels BNU.
- Si utilitzeu connexions directes per a les comunicacions dels BNU, cal configurar les connexions the apropiades entre el vostre sistema i els sistemes remots.
- Si utilitzeu mòdems per a les comunicacions dels BNU, heu d'instal•lar i configurar cada mòdem.
- S i una o més connexions utilitzen TCP/IP, cal que el TCP/IP s'executi entre el vostre sistema i els sistemes remots corresponents.
- Recopileu la informació que necessiteu per configurar els BNU (vegeu la llista següent). Aquesta informació inclou una llista de sistemes remots i llistes de dispositius i mòdems que s'utilitzaran per connectar als sistemes.

Recopilació d'informació del sistema necessària

Abans de configurar els BNU, recopileu la informació següent:

- Per a cada *sistema remot* que el vostre sistema cridarà, recolliu la següent informació:
  - El nom del sistema
  - El nom d'inici de sessió que el vostre sistema utilitza en el sistema remot
  - La contrasenya per l'inici de sessió.
  - Indicadors de nom d'usuari i contrasenya en el sistema remot.
  - El tipus de connexió que utilitzeu per arribar al sistema remot (directe, mòdem o TCP/IP)

  Si la connexió és directa, recopileu la informació següent:
  - La velocitat de bits de la connexió
  - El port del sistema local al qual està adjuntada la connexió.

  Si la connexió és a través d'un mòdem (connexió telefònica), recopileu la informació següent.
  - El número de telèfon del sistema remot.
  - La velocitat del mòdem que és compatible amb la velocitat del sistema remot.

  Nota: Si alguns dels sistemes remots crida al vostre sistema, assegureu-vos que l'administrador del BNU en cada un dels sistemes remots, té tota la informació anterior sobre el vostre sistema.
- Per a cada *mòdem local* que utilitzeu per connexions del BNU, recopileu la informació següent:
  - La seqüència chat del mòdem (consulteu la documentació del mòdem).

    Nota: Per alguns mòdems, la seqüència xat està disponible al fitxer `/etc/uucp/Dialers` file.
  - El port local del mòdem.

Crear una llista de dispositius del sistema

Utilitzeu la informació que heu recopilat per fer una llista de cada dispositiu del sistema que necessiteu connectar al sistema remot. A continuació hi ha un llistat d'exemple pel sistema local `morgan`:

```
direct:
hera 9600 tty5
zeus& 2400 tty2
ariadne 2400 tty1
hayes modem (tty3):  apollo, athena
TCP/IP:  merlin, arthur, percy
```

A l'exemple anterior, per connectar-se al sistema `hera`, s'utilitza una connexió `directa` a una velocitat de connexió de `9600` des del port `tty5`. Per connectar-se al sistema `apollo`, s'utilitza el mòdem `hayes`, el qual està connectat al port `tty3`. El TCP/IP s'utilitza per connectar-se amb el sistemes `merlin`, `arthur` i `percy`.

Configurar els recursos de comunicació remota

Per tal que els BNU funcionin correctament al vostre indret, heu de configurar els recursos de comunicacions remotes de la següent manera:

- Llistar els dispositius que s'utilitzen per establir un enllaç de comunicacions directe, per telèfon o per mòdem.
- Llistar els mòdems que s'utilitzen per contactar amb els sistemes remots a través de la xarxa telefònica.
- Llistar els sistemes remots accessibles.
- Llistar les abreviatures que representen els prefixes dels números de telèfon que utilitzats per contactar els sistemes remots especificats (opcional).
- Establir els permisos d'accés que especifiquen les maneres en què els sistemes locals i remots poden comunicar-se.
- Planificar la supervisió dels sistemes remots en xarxa (opcional).

Per crear aquestes llistes, permisos i planificacions, completeu els passos següents:

- Canviar els fitxers de configuració dels BNU.
- Editar el fitxer `/var/spool/cron/crontabs/uucp` per eliminar els caràcters de comentari de l'inici de les línies que planifiquen les rutines de manteniment automàtiques.

Nota: Heu de configurar el fitxers `Systems`, `Devices` i `Permissions` per assegurar-vos que els BNU s'executen correctament al vostre indret. No obstant això, no és necessari modificar els fitxers de configuració dels BNU en un ordre determinat.

Després de completar els procediments anteriors, podreu configurar els BNU en el vostre sistema.

Configurar els BNU al vostre sistema

Per configurar els BNU, seguiu els passos següents:

1. Assegure-vos que els BCNU estan instal•lats al vostre sistema mitjançant l'ordre següent:
   ```
   lslpp -h bos.net.uucp
   ```

   Si els BNU estan instal•lats, veureu `bos.net.uucp` a la sortida. Si no ho veieu, instal•leu-los de la cinta d'instal•lació.
2. Definiu els ID d'inici de sessió i contrasenyes apropiats pels sistemes remots que criden al vostre sistema i proporcioneu a la persona responsable d'administrar els BNU o el programa de còpia UNIX a UNIX (UUCP) dels sistemes remots el nom d'inici de sessió i la contrasenya. Aquest pas es completa amb l'edició dels arxius `/etc/passwd`, `/etc/group`, `/etc/security/login.cfg` i `/etc/security/passwd`.

Atenció: El fet de permetre als sistemes remots iniciar sessió al sistema local amb l'ID d'inici de sessió UUCP compromet seriosament la seguretat del vostre sistema. Els sistemes remots que han iniciat sessió amb l'ID UUCP poden visualitzar i possiblement canviar els arxius `Systems` i `Permissions` locals. Aquestes accions del sistema remot depenen dels permisos que especificats a l'entrada LOGNAME del fitxer `Permissions`. Es recomana que creeu altres ID d'inici de sessió dels BNU per a sistemes remots i que reserveu l'ID d'inici de sessió UUCP per a la persona que administra els BNU al sistema local. Per més seguretat, cada sistema remot que contacta amb el sistema local ha de tenir un ID d'inici de sessió exclusiu amb un número d'ID d'usuari exclusiu. Aquests ID d'inici de sessió han de tenir uns ID de grup (GIDs) de 5. Per defecte, el sistema operatiu inclou l'ID d'inici de sessió NUUCP per transferir fitxers.

a. Si necessiteu mantenir el control total sobre l'accés per cada màquina individual, heu de crear ID d'inici de sessió diferents, a més de combinar les entrades MACHINE i LOGNAME del fitxer `Permissions`. Teniu l'opció de mantenir inicis de sessió diferents o de tenir un sol inici de sessió per a totes les connexions dels BNU. A continuació es mostren algunes entrades `/etc/passwd` d'exemple:

```
Umicrtk:!:105:5:micrtk uucp:/usr/spool/uucppublic:/usr/sbin/uucp/uucico
Ufloydl:!:106:5:floydl uucp:/usr/spool/uucppublic:/usr/sbin/uucp/uucico
Uicus:!:107:5:icus uucp:/usr/spool/uucppublic:/usr/sbin/uucp/uucico
Urisctkr:!:108:5::/usr/spool/uucppublic:/usr/sbin/uucp/uucico
```

b. Si voleu tenir un conjunt de permisos i no voleu mantenir un control diferent per a les connexions UUCP, podeu tenir un únic inici de sessió per a tots els sistemes. A continuació es mostra un exemple d'aquest cas:

```
nuucp:!:6:5::/usr/spool/uucppublic:/usr/sbin/uucp/uucico
```

Nota:

- El UID, que és el tercer camp separat per dos punts, ha de ser exclusiu per tal d'evitar un risc de seguretat.
- El GID, que és el quart camp separat per dos punts, ha de ser 5 per assegurar que pertany al mateix grup que el UUCP.
- El directori d'inici, que és el sisè camp separat per dos punts, pot canviar-se per qualsevol directori vàlid.
- L'intèrpret d'ordres, que és el setè camp separat per dos punts, ha de ser sempre `/usr/sbin/uucp/uucico`.

c. Assegureu-vos que el fitxer `/etc/group` conté els nous usuaris. Un exemple d'aquesta entrada és:

```
uucp:!:5:uucp,uucpadm,nuucp,Umicrtk,Uicus,Urisctakr
```

d. Afegiu els usuaris al grup UUCP que utilitzaran mòdems per connectar-se a altres programes a més de l'ordre **cu**.

e. Després d'editar aquests fitxers com a usuari root, configureu una contrasenya pels nous usuaris amb l'ordre **passwd** *UserName*.

Nota: Si canvieu una contrasenya des de l'inici de sessió de l'usuari root, l'entrada de senyaladors a l'stanza de l'usuari al fitxer `/etc/security/passwd` contindrà la línia següent:

```
flags = ADMCHG
```

Heu de canviar la línia següent, com es mostra en l'exemple següent:

```
flags =
```

En cas contrari, quan el procés remot **uucico** inicii sessió en el vostre sistema, el sistema li sol•licitarà una nova contrasenya. Aquesta acció no és possible i, per tant, l'inici de sessió falla.

f. Per evitar interrupcions en el transcurs de l'inici de sessió causat pel procés **uucico**, el qual pot iniciar-se per l'indicador per defecte amb tots els seus Control-J, comenteu l'stanza per defecte (amb asteriscos) i definiu una stanza per al vostre tty, tal com es mostr a continuació:

```
/dev/tty0:
            herald = "\nrisc001 login:"
```

g. Utilitzen un editor de text ASCII o l'ordre **uucpadm** per editar el fitxer `Poll`. Afegiu una entrada per a cada sistema que el vostre sistema sondejarà.

   Nota: Els sistemes que estan llistats al fitxer `Poll` han d'estar llistats també al fitxer `/etc/uucp/Systems`.

h. Utilitzen un editor de text ASCII per editar el fitxer `/var/spool/cron/crontabs/uucp`. Elimineu els caràcters de comentari (#) de les línies que executen les ordres **uudemon.hour** i **uudemon.poll**. Podeu canviar el nombre de vegades que s'executen aquestes ordres. No obstant això, assegureu-vos de programar l'ordre **uudemon.poll** aproximadament 5 minuts abans de programar l'ordre **uudemon.hour**.

i. Assegureu-vos que els canvis entren en vigor executant l'ordre següent:

```
crontab -l uucp
```

j. Configureu els fitxers de dades dels BNU: `Systems`, `Permissions`, fu`Devices`, `Dialers` i `Sysfiles`. Podeu utilitzar l'ordre `/usr/sbin/uucp/uucpadm` per configurar inicialment els fitxers i, a continuació, editar-los segons les vostres necessitats. Utilitzeu el fitxer `Sysfiles` per especificar altres fitxers que no són `/etc/uucp/Systems`, `/etc/uucp/Devices` i `/etc/uucp/Dialers` per a la configuració dels BNU. Per obtenir més informació, consulteu l'apartat `Sysfiles`.

3. Si decidiu utilitzar abreviatures de codi de marcatge per als números de telèfon al fitxer `Systems`, configureu l'entrada `Dialcodes` per a cada abreviatura. Per a obtenir més informació més detallada, vegeu l'apartat Format del fitxer Dialcodes per als BNU.

   Si utilitzeu TCP/IP per a les connexions dels BNU, utilitzeu l'ordre **netstat** per veure si el dimoni **uucpd** funciona mitjançant l'ordre:

```
netstat -a
```

   El dimoni **uucpd** s'inicia mitjançant el dimoni **inetd**. Si el dimoni **uucpd** no s'executa, reconfigureu el dimoni **inetd** per iniciar el dimoni **uucpd**. Per obtenir més informació, consulteu l'apartat “Configuració del daemon inetd” a la pàgina 354).

4. Abans de començar aquest procediment, utilitzeu la llista de dispositius que heu recopilat per canviar el fitxer `Devices` en el vostre sistema. Realitzeu una entrada per a cada mòdem i cada connexió directa. Si utilitzeu TCP/IP, descomenteu l'entrada TCP/IP al fitxer `Devices`. Podeu configurar el fitxer `/etc/uucp/Sysfiles` per especificar altres fitxers que cal utilitzar per a la configuració de dispositius. Per obtenir informació més detallada del fitxer Devices, consulteu l'apartat Format del fitxer Devices per als BNU.

   A més, si utilitzeu TCP/IP, verifiqueu que el fitxer `/etc/services` inclou la línia següent:

```
uucp        540/tcp          uucpd
```

   Si no hi és, afegiu-la.

5. Abans de començar aquest procediment, utilitzeu la informació sobre cada sistema remot que heu recopilat per canviar el fitxer `Systems` en el vostre sistema. Utilitzeu els exemples comentats del fitxer `Systems` com a guia a l'hora d'especificar la configuració. Si utilitzeu TCP/IP, assegureu-vos que la taula del sistema principal del fitxer `/etc/hosts` inclou el nom del sistema remot al qual voleu connectar-vos. Podeu configurar el fitxer `/etc/uucp/Sysfiles` per especificar altres fitxers que cal utilitzar per a la configuració de sistemes.

6. Abans de començar aquest procediment, utilitzeu la informació sobre dispositius i mòdems que heu recopilat per assegurar-vos que el fitxer `Dialers` conté una entrada per a cada mòdem del vostre sistema. Si utilitzeu TCP/IP i connexions directes, assegureu-vos que l'entrada del TCP/IP i les entrades directes estan presents al fitxer. Podeu configurar el fitxer `/etc/uucp/Sysfiles` per especificar altres fitxers que cal utilitzar per a la configuració de marcadors.

7. Decidiu quant accés al vostre sistema voleu proporcionar a cada sistema remot que crideu i a cada sistema remot que us cridi a vosaltres. Configureu les entrades apropiades per a cada sistema i per cada nom d'inici de sessió del fitxer `Permissions`.

8. Utilitzeu l'ordre **uucheck** per verificar que els directores, programes i fitxers de suport estan configurats correctament:
   ```
   /usr/sbin/uucp/uucheck -v
   ```

   L'ordre **uucheck** verifica que els directoris, programes i fitxers de suport estan configurats correctament i que les entrades del fitxer `Permissions` són coherents. Si l'ordre **uucheck** informa sobre alguns errors, arregleu els errors.
9. Opcional: Configureu la supervisió automàtica de les operacions dels BNU i el sondeig automàtic de sistemes remots. Per obtenir més informació, consulteu els apartats "Configuració de la supervisió automàtica dels BNU" i "Configuració dels BNU per sondejar sistemes remots").

Configuració de la supervisió automàtica dels BNU

Els BNU utilitzen el daemon **cron** per iniciar els daemons dels BNU i supervisar l'activitat dels BNU.

Prerequisits

- Realitzeu els passos de l'apartat "Configuració dels BNU" a la pàgina 436.
- Cal tenir autorització d'usuari root per editar el fitxer `/var/spool/cron/crontabs/uucp`.

El daemon **cron** llegeix el fitxer `/var/spool/cron/crontabs/uucp` per obtenir instruccions sobre quan ha d'iniciar els procediments dels BNU.

Per configurar la supervisió automàtic adels BNU, completeu els passos següents:

1. Inicieu una sessió com a usuari amb autorització d'usuari root.
2. Utilitzeu un editor de text ASCII per editar el fitxer `/var/spool/cron/crontabs/uucp`.
3. Descomenteu les línies sobre els procediments de manteniment dels BNU, `uudemon.admin` i `uudemon.cleanup`. Podeu canviar les hores a les quals s'executen aquests procediments si el vostre sistema necessita realitzar el manteniment a intervals més o menys freqüents. No obstant això, s'aconsella executar l'ordre `uudemon.admin` com a mínim un cop al dia i l'ordre `uudemon.cleanup` almenys un cop a la setmana.
4. Podeu utilitzar el fitxer `crontabs/uucp` per planificar altres ordres de manteniment dels BNU, com ara les ordres **uulog**, **uuclean** o **uucleanup**. A més, podeu utilitzar el fitxer `crontabs/uucp` per donar instruccions al daemon **cron** per què iniciï els daemons **uucico**, **uuxqt** o **uusched** a unes hores concretes.

Configuració dels BNU per sondejar sistemes remots

Per tal d'habilitar els BNU per què sondegin els treballs dels sistemes remots, llisteu els sistemes del fitxer `/etc/uucp/Poll`.

Prerequisits

- Realitzeu els passos de l'apartat "Configuració dels BNU" a la pàgina 436.
- Cal tenir autorització root per editar el fitxer `/var/spool/cron/crontabs/uucp` i el fitxer `/etc/uucp/Poll`.

A més de llistar els sistemes del fitxer `/etc/uucp/Poll`, executeu periòdicament les ordres **uudemon.hour** i **uudemon.poll**.

Per configurar els BNU per sondejar sistemes remots, realitzeu els passos següents:

1. Decidiu quins sistemes remots voleu sondejar automàticament. Decidiu amb quina freqüència els voleu sondejar. Especifiqueu les hores per a cada sistema amb el fitxer `Poll`, tan poc sovint com un cop al dia o tan sovint com vulgueu.
2. Inicieu una sessió com a usuari amb autorització root.
3. Utilitzant un editor de textos ASCII o l'ordre **uucpadm**, editeu el fitxer `Poll`. Afegiu una entrada per a cada sistema que el vostre sistema sondejarà.

Nota: Els sistemes que estan llistats al fitxer `Poll` han d'estar llistats també al fitxer `/etc/uucp/Systems`.

4. Utilitzant un editor de textos ASCII, editeu el fitxer `/var/spool/cron/crontabs/uucp`. Elimineu els caràcters de comentari (#) de les línies que executen les ordres **uudemon.hour** i **uudemon.poll**. Podeu canviar les hores en què s'executen aquestes ordres. No obstant això, assegureu-vos de planificar l'ordre **uudemon.poll** aproximadament 5 minuts abans de planificar l'ordre **uudemon.hour**.

Ara els BNU sondejaran automàticament els sistemes llistats al fitxer `Poll` a les hores que heu especificat.

Fitxer /etc/uucp/Systems

Els sistemes remots es llisten als fitxers `/etc/uucp/Systems`.

El fitxer `/etc/uucp/Systems` és el fitxer `Systems` per defecte. L'administrador del sistema pot especificar fitxers addicionals del fitxer **/etc/uucp/Sysfiles**.

Cada entrada el fitxer `Systems` conté els elements següents:

- El nom del sistema remot
- Les vegades que els usuaris poden connectar-se al sistema remot
- El tipus d'enllaç (línia directa o per mòdem)
- La velocitat de transmissió a través de l'enllaç
- La informació que és necessària per iniciar sessió en el sistema remot

Cada entrada d'un fitxer `Systems` representa un sistema remot. Per establir comunicacions, el sistema remot s'ha de llistar al fitxer `Systems` local. Un fitxer `Systems` ha d'estar present a cada sistema que utilitza el recurs dels BNU. Normalment, només l'usuari root pot llegir els fitxers `Systems`. No obstant això, qualsevol usuari pot llistar els noms de els sistemes BNU remots mitjançant l'ordre **uuname**.

Edició del fitxer Devices per a una connexió directa

Per editar el fitxer `Devices` per a una connexió directa, heu de tenir autorització root per editar el fitxer `/etc/uucp/Devices` o el que s'especifiqui en el fitxer `/etc/uucp/Sysfiles` com a fitxer `Devices`.

Per configurar una connexió directa que especifiqui un port i un sistema remot, realitzeu una entrada com la següent:

1. Escriviu el nom del sistema remot al qual voleu connectar el sistema local a través de la línia directa al camp **Type** a la segona línia de l'entrada.
2. Escriviu el nom del dispositiu apropiat per la connexió directa que s'utilitzarà en el vostre indret al camp **Line** a les dues línies de l'entrada.
3. Escriviu un guió (-) com a agafador d'espai al camp **Line2** a les dues línies de l'entrada.
4. Escriviu una taxa de transmissió apropiada per la connexió directa que s'utilitzarà en el vostre indret al camp **Speed** a les dues línies de l'entrada.
5. Escriviu `direct` (tot en minúscules) al camp **Parelles marcador-testimoni** que es troba a les dues línies de l'entrada.

   Per exemple:

   ```
   type device - speed direct
   ```

Continueu afegint entrades al fitxer `Devices` fins que llisteu cada dispositiu del sistema local que es connectarà directament al sistema remot.

Per configurar una connexió directa entre ds sistemes que utilitizin una connexió en sèrie asíncrona permanent, realitzeu una entrada d'una línia com la següent:

1. Escriviu el nom del sistema remot al camp **Tipus**.
2. Escriviu el nom del dispositiu tty al camp **Línia**.

3. Escriviu un guió (-) com a agafador d'espai al camp **Línia2**.
4. Escriviu una taxa de transmissió apropiada per la connexió directa que s'utilitzarà en el vostre indret al camp **Classe**.
5. Escriviu `direct` (tot en minúscules) al camp **Parelles marcador-testimoni**. Per exemple:
   ```
   type device - speed direct
   ```

Continueu afegint entrades al fitxer `Devices` fins que llisteu cada dispositiu directe del sistema local que es connectarà al sistema remot.

Edició del fitxer Devices per a una connexió del marcador automàtic

Seguiu aquests passos quan editeu el fitxer `/etc/uucp/Devices`.

Heu de tenir autorització root per editar el fitxer `/etc/uucp/Devices` o el que s'especifiqui en el fitxer `/etc/uucp/Sysfiles` com a fitxer `Devices`.

A les entrades de connexió telefònica, el camp **Tipus** s'especifica com una unitat de crides automàtiques (ACU). Escriviu ACU com a entrada del camp **Tipus** en totes les connexions remotes establertes a través d'una línia telefònica. A l'hora de configurar entrades del fitxer `Devices` per a les connexions del marcador automàtic, realitzeu una entrada d'una línia per a cada mòdem:

1. En el camp **Tipus**, escriviu `ACU`.
2. En el camp **Línia**, escriviu el nom del dispositiu que està connectat al mòdem.
3. En el camp **Línia2**, escriviu un guió (-) com a agafador d'espai, excepte que el marcador automàtic és un marcador 801 automàtic. Si el marcador automàtic és un marcador 801 estàndard, escriviu `801`.
4. En el camp **Velocitat**, escriviu la velocitat en bauds apropiada pel mòdem i la línia o per la classe del vostre modem (per exemple, D2400). El valor de la velocitat en bauds pot ser 300, 1200, 2400 o superior, fet que depèn del mòdem.

   Nota: Si el mòdem es pot utilitzar en més d'una velocitat, feu una entrada independent al fitxer `Devices` per a cada velocitat. Si el mòdem es pot utilitzar en qualsevol velocitat, escriviu la paraula `Any` al camp **Velocitat**.
5. Escriviu el nom del mòdem com a entrada del camp **Marcador** al camp **Parella marcador-testimoni**. Si teniu la intenció d'incloure números de telèfon complets al fitxer `/etc/uucp/Systems` o a un altre fitxer `Systems`, que s'especifica al fitxer `/etc/uucp/Sysfiles`, deixeu el camp **Testimoni** en blanc. Un espai en blanc indica al programa dels BNU que utilitzi el testimoni `\D` per defecte. Si teniu la intenció d'utilitzar les abreviatures de codis de marcatge especificades al fitxer `/etc/uucp/Dialcodes`, especifiqueu el testimoni `\T`.

   Per exemple:
   ```
   type line - speed dialer - token pair
   ```

Continueu afegint entrades al fitxer `Devices` fins que hagueu llistat totes les connexions entre el sistema local i un sistema remot que utilitzen una línia telefònica i un mòdem.

Edició del fitxer Devices per a TCP/IP

Seguiu aquests passos per editar el fitxer `/etc/uucp/Devices`.

Heu de tenir autorització root per editar el fitxer `/etc/uucp/Devices` o el que s'especifiqui en el fitxer `/etc/uucp/Sysfiles` com a fitxer `Devices`.

Si el vostre indret utilitza TCP/IP per connectar sistemes, incloeu l'entrada TCP/IP corresponent al fitxer `Devices`. Si voleu configurar el fitxer per tal d'utilitzar-lo amb el sistema TCP/IP, escriviu la línia següent al fitxer `Devices`:

```
TCP - - - TCP
```

Exemples: configuració dels BNU per a una connexió TCP/IP

Aquest grup d'exemples configura els BNU per a una connexió TCP/IP

Els següents fitxers estan configurats per a una connexió entre els sistemes zeus i hera, on zeus es considera que és el sistema local i hera el sistema remot.

Fitxers dels BNU per a les entrades de la connexió TCP/IP als fitxers del sistema local:

Aquests fitxers dels BNU són entrades en el sistema local zeus.

- **Fitxer Systems:** El fitxer Systems al sistema zeus conté l'entrada següent de manera que zeus pot contactar amb el sistema hera:

  ```
  hera Any TCP,t - - in:--in: uzeus word: birthday
  ```

  Aquest exemple especifica que el sistema zeus pot cridar el sistema hera en qualsevol moment mitjançant el protocol **t** per a comunicacions amb el sistema hera. El sistema zeus inicia una sessió en el sistema hera com a uzeus amb la paraula clau birthday.

  Nota: El protocol **t** admet **TCP**. Per tant, utilitzeu sempre el protocol **t** per a les comunicacions dels BNU a través de connexions TCP/IP. No obstant això, el protocol **t** no es pot utilitzar quan el camp **Tipus** és ACU (unitat de crides automàtiques) o quan s'utilitza una connexió via mòdem.

  Els BNU utilitzen els camps **Tipus** i **Classe** del fitxer Systems per cercar el dispositiu apropiat per a la connexió. Comprova si el fitxer Devices si hi ha una entrada del tipus TCP.

- **Fitxer Devices:** El fitxer Devices que utilitza el dimoni **uucico** al sistema zeus conté l'entrada següent per a les connexions TCP/IP:

  ```
  TCP  -  -  -  TCP
  ```

  Com que el tipus de dispositiu és TCP, no hi ha cap entrada *Classe*, *Línia* o *Línia2*. El *Marcador* també s'especifica com TCP. Els BNU examinen els fitxers Dialers per si hi ha una entrada TCP.

- **Fitxer Dialers:** El fitxer Dialers que utilitza el dimoni **uucico** al sistema zeus conté una entrada TCP/IP, tal com s'indica a continuació:

  ```
  TCP
  ```

  Aquesta entrada especifica que no cal cap configuració de marcador.

  Nota: La configuració de marcador no fa falta mai a través d'una connexió TCP/IP.

- **Fitxer Permissions:** El fitxer Permissions del sistema zeus conté l'entrada següent que atorga al sistema hera accés al sistema zeus:

  ```
  LOGNAME=uhera SENDFILES=yes REQUEST=yes \
  MACHINE=zeus:hera VALIDATE=uhera \
  READ=/var/spool/uucppublic:/home/hera \
  WRITE=/var/spool/uucppublic:/home/hera COMMANDS=ALL
  ```

  L'entrada combinada de LOGNAME i MACHINE proporciona els permisos següents al sistema hera quan el sistema zeus i hera estan connectats:

  – El sistema hera pot sol•licitar i enviar fitxers independentment de qui hagi iniciat la crida.
  – El sistema hera pot llegir i escriure en el directori públic i en el directori /home/hera del sistema zeus.
  – El sistema hera pot executar totes les ordres del sistema zeus.
  – El sistema hera ha d'iniciar sessió en el sistema zeus com a l'usuari uhera, i el sistema and system hera no pot utilitzar cap altre ID d'inici de sessió per a les transaccions dels BNU.

  Nota: Com que els permisos són els mateixos independentment de quin sistema inicia la crida, les entrades LOGNAME i MACHINE anteriors es combinen. Si els permisos no són iguals per als sistemes hera i zeus, les entrades LOGNAME i MACHINE són tal com s'indica a continuació:

  ```
  LOGNAME=uhera VALIDATE=hera SENDFILES=yes REQUEST=yes \
  READ=/var/spool/uucppublic:/home/hera \
  WRITE=/var/spool/uucppublic:/home/hera
  ```

```
MACHINE=zeus:hera REQUEST=yes COMMANDS=ALL\
READ=/var/spool/uucppublic:/home/hera \
WRITE=/var/spool/uucppublic:/home/hera
```

Fitxers dels BNU per a les entrades de la connexió TCP/IP als fitxers del sistema remot:

Aquests fitxers es troben al sistema remot hera.

- **Fitxer Systems:** El fitxer Systems al sistema hera conté l'entrada següent per permetre que hera pugui contactar amb el sistema zeus:

  ```
  zeus Any TCP,t - - ogin:--ogin: uhera ord: lightning
  ```

  Aquest exemple especifica que el sistema hera pot cridar el sistema zeus en qualsevol moment mitjançant el protocol **t** per a les comunicacions amb el sistema zeus. El sistema hera inicia una sessió en el sistema zeus com a usuari uhera amb la paraula clau lightning. A continuació, els BNU comproven si als fitxers Devices hi ha una entrada del tipus TCP.

  Nota: El protocol **t** dóna suport al protocol **TCP**. Per tant, utilitzeu sempre el protocol **t** per a les comunicacions dels BNU a través de connexions TCP/IP. No obstant això, el protocol **t** no pot utilitzar-se quan el camp *Tipus* és ACU o quan s'utilitza una connexió via mòdem.

- **Fitxer Devices:** El fitxer Devices que utilitza el dimoni **uucico** al sistema hera conté l'entrada següent per a les connexions TCP/IP:

  ```
  TCP  -  -  -  TCP
  ```

  Com que el tipus de dispositiu és TCP, no hi ha cap entrada *Tipus*, *Línia* o *Línia2*. El *Marcador* també s'especifica com TCP. Els BNU examinen els fitxers Dialers per si hi ha una entrada TCP.

- **Fitxer Dialers:** El fitxer Dialers que utilitza el dimoni **uucico** al sistema hera conté una entrada TCP/IP, tal com s'indica a continuació:

  ```
  TCP
  ```

  Aquesta entrada especifica que no cal cap configuració de marcador.

  Nota: La configuració de marcador no fa falta mai a través d'una connexió TCP/IP.

- **Fitxer Permissions**: El fitxer Permissions del sistema hera conté l'entrada següent que atorga al sistema zeus accés al sistema hera:

  ```
  LOGNAME=uzeus SENDFILES=yes REQUEST=yes \
  MACHINE=hera:zeus VALIDATE=zeus COMMANDS=rmail:who:uucp
  ```

  L'entrada combinada de LOGNAME i MACHINE proporciona els permisos següents al sistema zeus quan el sistema zeus i hera estan connectats:

  – El sistema zeus pot sol•licitar i enviar fitxers independentment de qui hagi iniciat la crida.
  – El sistema zeus només pot llegir i escriure en el directori públic (el valor per defecte).
  – El sistema zeus només pot executar les ordres **rmail**, **who** i **uucp**.
  – El sistema zeus ha d'iniciar una sessió en el sistema hera com a usuari uzeus i el sistema zeus no pot utilitzar cap altre ID d'inici de sessió per a les transaccions dels BNU.

    Nota: Si els permisos no són iguals per als sistemes hera i zeus, les entrades LOGNAME i MACHINE són tal com s'indica a continuació:

    ```
    LOGNAME=uzeus VALIDATE=zeus SENDFILES=yes REQUEST=yes
    MACHINE=hera:zeus COMMANDS=rmail:who:uucp REQUEST=yes
    ```

Exemples: configuració dels BNU per a una connexió telefònica

Els fitxers d'exemple s'han configurat per connectar els sistemes venus i merlin a través d'una línia telefònica mitjançant mòdems.

El sistema venus és el sistema local i el sistema merlin n'és el remot.

A ambdós sistemes, el dispositiu tty1 està connectat a un mòdem Hayes a 1200 bauds. El ID d'inici de sessió utilitzat perquè el sistema venus iniciï sessió al sistema merlin és uvenus i la contrasenya associada és mirror. L'ID d'inici de sessió perquè merlin iniciï sessió al sistema venus és umerlin i la contrasenya associada és oaktree. El número de telèfon del mòdem connectat a venus és 9=3251436 i el número de telèfon del mòdem de merlin modem és 9=4458784. Els dos ordinadors inclouen números de telèfon parcials en els seus fitxers Systems i codis de marcatge en els seus fitxers Dialcodes.

Els següents fitxers d'exemple estan configurats per connectar els sistemes venus i merlin::

- **Fitxer Systems:** El fitxer Systems del sistema venus conté l'entrada següent per al sistema merlin, que inclou un número de telèfon i un prefix de marcatge:

  ```
  merlin Any ACU 1200 local8784 "" in:--in: uvenus word: mirror
  ```

  El sistema venus pot cridar el sistema merlin en qualsevol moment mitjançant un dispositiu ACU a 1200 bauds i iniciant una sessió com a uvenus amb la contrasenya mirror. El número de telèfon s'amplia en funció del codi local del fitxer Dialcodes i el dispositiu que s'utilitzarà es determina en funció de les entrades *Tipus* i *Classe*. Els BNU comproven als fitxers Devices si hi ha un dispositiu del tipus ACU i de la classe 1200.
- **Fitxer Dialcodes:** El fitxer Dialcodes del sistema venus conté el següent prefix de codi de marcatge que s'utilitzarà amb el número del fitxer Systems:

  ```
  local 9=445
  ```

  A partir d'aquest codi, el número de telèfon per al sistema merlin del fitxer Systems s'amplia a 9=4458784.
- **Fitxer Devices:** El fitxer Devices al sistema venus conté l'entrada següent per a la connexió amb el sistema merlin:

  ```
  ACU tty1  -  1200  hayes \T
  ```

  El port que s'utilitzarà és tty1 i l'entrada *Marcador* del camp *Parelles marcador-testimoni* és hayes. L'entrada *Testimoni*, \T, indica que el número de telèfon s'ha d'ampliar utilitzant un codi del fitxer Dialcodes. Els BNU comproven si als fitxers Dialers hi ha un tipus de marcador hayes.
- **Fitxer Dialers:** El fitxer Dialers que utilitza el dimoni **uucico** al sistema venus conté l'entrada següent per al mòdem hayes:

  ```
  hayes =,-, "" \dAT\r\c OK \pATDT\T\r\c CONNECT
  ```

  Nota: Els caràcters d'enviament-recepció es defineixen en el format del fitxer Dialers.
- **Fitxer Permissions:** El fitxer Permissions al sistema venus conté les entrades següents, les quals especifiquen les maneres en què el sistema merlin pot dur a terme les transaccions **uucico** i **uuxqt** amb el sistema venus:

  ```
  LOGNAME=umerlin REQUEST=yes SENDFILES=yes \
  READ=/var/spool/uucppublic:/home/merlin \
  WRITE=/var/spool/uucppublic:/home/merlin
  MACHINE=venus:merlin VALIDATE=umerlin REQUEST=yes SENDFILES=yes    \
  COMMANDS=ALL \
  READ=/var/spool/uucppublic:/home/merlin \
  WRITE=/var/spool/uucppublic:/home/merlin
  ```

  El sistema merlin inicia una sessió en el sistema venus com a umerlin, que és un inici de sessió exclusiu per al sistema merlin. El sistema merlin pot sol•licitar i enviar fitxers independentment de qui hagi iniciat la crida. A més, el sistema merlin pot llegir i escriure en el directori /var/spool/uucppublic i en el directori /home/merlin del sistema venus. El sistema merlin pot executar totes les ordres del conjunt d'ordres per defecte del sistema venus.

Fitxers dels BNU amb entrades de connexió telefònica al sistema local:

Aquests fitxers contenen entrades de connexió telefònica al sistema local venus.

- **Fitxer Systems:** El fitxer Systems al sistema venus conté l'entrada següent per al sistema merlin, que inclou un número de telèfon i un prefix de marcatge:

  ```
  merlin Any ACU 1200 local8784 "" in:--in: uvenus word: mirror
  ```

El sistema venus pot cridar el sistema merlin en qualsevol moment, utilitzant un dispositiu ACU a 1200 bauds i iniciant una sessió com a usuari uvenus amb la paraula clau mirror. El número de telèfon s'amplia en funció del codi local del fitxer Dialcodes i el dispositiu que s'utilitzarà es determina en funció de les entrades *Tipus* i *Classe*. Els BNU comproven als fitxers Devices si hi ha un dispositiu de tipus ACU i de classe 1200.

- **Fitxer Dialcodes:** El fitxer Dialcodes del sistema venus conté el següent prefix de codi de marcatge que s'utilitzarà amb el número del fitxer Systems:

  ```
  local 9=445
  ```

  A partir d'aquest codi, el número de telèfon per al sistema merlin del fitxer Systems s'amplia a 9=4458784.

- **Fitxer Devices:** El fitxer Devices al sistema venus conté l'entrada següent per connectar-se amb el sistema merlin:

  ```
  ACU  tty1  -  1200  hayes \T
  ```

  El port que s'utilitzarà és tty1 i l'entrada *Marcador* del camp **Parelles marcador-testimoni** és hayes. L'entrada *Testimoni*, \T, indica que el número de telèfon s'ha d'ampliar utilitzant un codi del fitxer Dialcodes. Els BNU comproven si als fitxers Dialers hi ha una entrada per a un tipus de marcador hayes.

- **Fitxer Dialers:** El fitxer Dialers que utilitza el dimoni **uucico** al sistema venus conté l'entrada següent per al mòdem hayes:

  ```
  hayes  =,-,  ""  \dAT\r\c OK \pATDT\T\r\c CONNECT
  ```

  Nota: Els caràcters d'enviament-recepció es defineixen en el format del fitxer Dialers.

- **Fitxer Permissions:** El fitxer Permissions al sistema venus conté les entrades següents, que especifiquen les maneres en què merlin pot dur a terme les transaccions **uucico** i **uuxqt** amb el sistema venus:

  ```
  LOGNAME=umerlin REQUEST=yes SENDFILES=yes \
  READ=/var/spool/uucppublic:/home/merlin \
  WRITE=/var/spool/uucppublic:/home/merlin
  MACHINE=venus:merlin VALIDATE=umerlin REQUEST=yes SENDFILES=yes    \
  COMMANDS=ALL \
  READ=/var/spool/uucppublic:/home/merlin \
  WRITE=/var/spool/uucppublic:/home/merlin
  ```

  El sistema merlin inicia una sessió en el sistema venus com a umerlin, que és un inici de sessió exclusiu per al sistema merlin. El sistema merlin pot sol•licitar i enviar fitxers independentment de qui hagi iniciat la crida. A més, el sistema merlin pot llegir i escriure en el directori /var/spool/uucppublic i en el directori /home/merlin del sistema venus. El sistema merlin pot executar totes les ordres del conjunt d'ordres per defecte del sistema venus.

Fitxers dels BNU amb entrades de connexió telefònica al sistema remot:

Aquests fitxers contenen entrades de connexió telefònica en el sistema remot merlin.

- **Fitxer Systems:** El fitxer Systems al sistema merlin conté l'entrada següent per al sistema venus, que inclou un número de telèfon i un prefix de marcatge:

  ```
  venus Any ACU 1200 intown4362 "" in:--in: umerlin word: oaktree
  ```

  El sistema merlin pot cridar al sistema venus en qualsevol moment mitjançant un dispositiu ACU a 1200 bauds i iniciant sessió com a usuari umerlin amb la contrasenya oaktree. El número de telèfon s'amplia en funció del codi intown del fitxer Dialcodes i el dispositiu que s'utilitzarà es determina en funció de les entrades *Tipus* i *Classe*. Els BNU comproven als fitxers Devices si hi ha un dispositiu del tipus ACU i de la classe 1200.

- **Fitxer Dialcodes:** El fitxer Dialcodes del sistema merlin conté el següent prefix de codi de marcatge que s'utilitzarà amb el número del fitxer Systems:

  ```
  intown 9=325
  ```

  Per tant, el número de telèfon ampliat per accedir al sistema venus és 9=3254362.

- **Fitxer Devices:** El fitxer Devices al sistema merlin conté l'entrada següent per a la connexió amb el sistema venus:

  ```
  ACU  tty1  -  1200  hayes \T
  ```

  L'ACU està connectat al port tty1 i el marcador és hayes. El número de telèfon s'amplia amb la informació del fitxer Dialcodes. Els BNU comproven si als fitxers Dialers hi ha una entrada per un mòdem hayes.
- **Fitxer Dialers:** El fitxer Dialers que utilitza el dimoni **uucico** al sistema merlin conté l'entrada següent per al seu mòdem:

  ```
  hayes  =,-,  ""  \dAT\r\c OK \pATDT\T\r\c CONNECT
  ```
- **Fitxer Permissions:** El fitxer Permissions al sistema merlin conté les següents entrades, que atorguen al sistema venus accés al sistema merlin:

  ```
  LOGNAME=uvenus SENDFILES=call REQUEST=no \
  WRITE=/var/spool/uucppublic:/home/venus \
  READ=/var/spool/uucppublic:/home/venus
  MACHINE=merlin:venus VALIDATE=uvenus  \
  READ=/ WRITE=/ COMMANDS=ALL REQUEST=yes \
  NOREAD=/etc/uucp:/usr/etc/secure \
  NOWRITE=/etc/uucp:/usr/etc/secure
  ```

Exemples: configuració dels BNU per a una connexió directa

Els següents fitxers d'exemple estan configurats per a una connexió directa entre els sistemes zeus i hera, on zeus es considera que és el sistema local i hera el sistema remot.

El dispositiu directe al sistema zeus és tty5. Al sistema hera, el dispositiu directe és tty1. La velocitat de la connexió és 1200 bps. L'ID d'inici de sessió per al sistema zeus del sistema hera és uzeus i la paraula clau associada és thunder. L'ID d'inici de sessió per al sistema hera del sistema zeus és uhera i la paraula clau associada és portent.

Fitxers dels BNU amb comunicació directa als fitxers del sistema local:

Aquests fitxers contenen entrades de connexió telefònica del sistema local zeus.

- **Fitxer Systems:** El fitxer Systems file al sistema zeus conté l'entrada següent per al sistema remot hera:

  ```
  hera Any hera 1200 - "" \r\d\r\d\r in:--in: uzeus word:  thunder
  ```

  Aquesta entrada especifica que el sistema hera pot iniciar sessió en el sistema zeus en qualsevol moment mitjançant una connexió directa, la qual s'especifica en el fitxer Devices. Per trobar l'entrada als fitxers Devices, els BNU utilitzen el tercer i quart camps de l'entrada Systems. Per tant, els BNU busquen una entrada als fitxers Devices amb un *Tipus* de hera i una *Classe* de 1200. El sistema zeus inicia una sessió en el sistema hera com a usuari uzeus amb la paraula clau thunder.
- **Fitxer Devices:** El fitxer Devices al sistema zeus conté l'entrada següent per connectar-se al sistema remot hera:

  ```
  hera    tty5  -  1200  direct
  ```

  Aquesta entrada especifica que el sistema zeus utilitza el dispositiu tty5 a 1200 bps per comunicar-se amb el sistema hera. Tingueu en compte que el *Marcador* en els dos camps **Parelles marcador-testimoni** és direct. Quan us connecteu al sistema hera, els BNU comproven al fitxer Dialers si hi ha una entrada direct.
- **Fitxer Dialers:** El fitxe Dialers al sistema zeus conté l'entrada següent per a una connexió directa:

  ```
  direct
  ```

  Aquesta entrada especifica que no cal cap conformitat de connexió a la connexió directa.
- **Fitxer Permissions:** El fitxer Permissions al sistema local zeus conté l'entrada següent, que especifica les maneres en què el sistema remot hera pot dur a terme les transaccions **uucico** i **uuxqt** amb el sistema zeus:

  ```
  LOGNAME=uhera MACHINE=hera VALIDATE=uhera REQUEST=yes \
  SENDFILES=yes MACHINE=zeus READ=/ WRITE=/ COMMANDS=ALL
  ```

Aquesta entrada especifica que el sistema hera inicia una sessió com a uhera. Com que s'inclou l'opció VALIDATE=uhera, el sistema hera no pot iniciar una sessió en el sistema zeus amb un altre ID d'inici de sessió, i un altre sistema remot tampoc pot utilitzar l'ID uhera. El sistema hera pot llegir i escriure en qualsevol directori del sistema zeus i pot enviar i sol•licitar fitxers independentment de qui hagi iniciat la crida. El sistema hera també pot iniciar ordres al sistema zeus.

Nota: Com que els permisos que s'atorguen són els mateixos independentment del sistema que hagi iniciat la connexió, s'han combinat les entrades LOGNAME i MACHINE. Si els permisos no són iguals per als sistemes hera i zeus, les entrades LOGNAME i MACHINE son tal com s'indica a continuació:

```
LOGNAME=uhera REQUEST=yes SENDFILES=yes READ=/ WRITE=/
MACHINE=zeus:hera VALIDATE=uhera READ=/ WRITE=/ REQUEST=yes \
COMMANDS=ALL
```

Atenció: Proporcionar els permisos de l'exemple anterior és equivalent a donar a qualsevol usuari del sistema remot un ID d'inici de sessió del sistema local. Aquests permisos liberals poden posar en perill la seguretat i normalment només s'haurien de donar a sistemes remots de molta confiança del mateix indret.

Els fitxers dels BNU amb connexió directa en els arxius del sistema remot:

Aquests fitxers contenen entrades de connexió telefònica en el sistema remot hera.

- **Fitxer Systems:** El fitxer Systems al sistema hera conté l'entrada següent per al sistema zeus:

  ```
  zeus Any zeus 1200 - "" \r\d\r\d\r in:--in: uhera word: portent
  ```

  Aquesta entrada especifica que el sistema hera pot iniciar sessió en el sistema zeus en qualsevol moment mitjançant una connexió directa, la quan s'especifica al fitxer Devices. Per trobar l'entrada als fitxers Devices, els BNU utilitzen el tercer i quart camps de l'entrada Systems. Per tant, els BNU busquen una entrada en el fitxer Devices amb el camp **Tipus** amb valor zeus i un camp **Classe** amb valor 1200. El sistema hera inicia una sessió en el sistema zeus com a usuari uhera amb la paraula clau portent.
- **Fitxer Devices:** El fitxer Devices al sistema hera conté l'entrada següent per comunicacions amb el sistema zeus:

  ```
  zeus    tty1  -  1200  direct
  ```

  Aquesta entrada especifica que el sistema hera utilitza el dispositiu tty1 a 1200 bps per comunicar-se amb el sistema zeus. Com que el *Marcador* s'especifica com a direct, els BNU comproven als fitxers Dialers si hi ha una entrada direct.
- **Fitxer Dialers:** El fitxer Dialers al sistema hera conté l'entrada següent per a connexions directes:

  ```
  direct
  ```

  Aquesta entrada especifica que no cal cap configuració de marcador a la connexió directa.
- **Fitxer Permissions:** El fitxer Permissions al sistema hera conté les entrades següents que especifiquen les maneres en què zeus pot dur a terme les transaccions **uucico** i **uuxqt** amb sistemes hera:

  ```
  LOGNAME=uzeus REQUEST=yes SENDFILES=yes READ=/ WRITE=/
  MACHINE=hera:zeus VALIDATE=uzeus REQUEST=yes COMMANDS=ALL READ=/\
  WRITE=/
  ```

  Aquestes entrades especifiquen que el sistema zeus inicia una sessió en el sistema hera com a uzeus. Com que s'inclou el paràmetre VALIDATE=uzeus, el sistema zeus no pot iniciar sessió al sistema hera amb un altre ID d'inici de sessió i un altre sistema remot tampoc pot utilitzar l'ID uzeus. El sistema zeus pot llegir i escriure en qualsevol directori del sistema hera i pot enviar i sol•licitar fitxers independentment de qui hagi iniciat la crida. El sistema zeus també pot iniciar ordres al sistema hera.

  Atenció: L'equivalent a proporcionar tots els permisos en l'exemple anterior seria donar accés a qualsevol usuari del sistema remot un ID d'inici de sessió al sistema local. Aquests permisos liberals poden posar en perill la seguretat i només s'haurien de donar a sistemes remots del mateix indret.

Manteniment dels BNU

Cal realitzar el manteniment dels BNU per què funcionin correctament en el vostre sistema.

Per realitzar el manteniment dels BNU:

- Llegiu i elimineu periòdicament els fitxers de registre.
- Utilitzeu les ordres **uuq** i **uustat** per comprovar les cues dels BNU i assegurar-vos que els treballs es transfereixen correctament als sistemes remots.
- Planifiqueu les ordres automàtiques que sondegen els treballs en els sistemes remots, tornen els fitxers no enviats als usuaris i us envien periòdicament missatges sobre l'estat dels BNU.
- Actualitzeu periòdicament els fitxers de configuració per tal que reflecteixin els canvis realitzats en el vostre sistema.

A més, de tant en tant poseu-vos en contacte amb els administradors del sistemes remots per tal que us posin al dia dels canvis realitzats en els seus sistemes que poguessin afectar la vostra configuració. Per exemple, si el supervisor del sistema `venus` canvia la paraula clau del vostre sistema, heu de posar la paraula clau nova al fitxer `/etc/uucp/Systems` (o al fitxer Systems corresponent especificat per `/etc/uucp/Sysfiles`) abans que el vostre sistema pugui iniciar una sessió en el sistema `venus`.

Fitxers d'enregistrament dels BNU

Els BNU creen fitxers de registre i fitxers d'errors per fer un seguiment de les seves pròpies activitats.

Aquests fitxers s'han de comprovar i eliminar periòdicament per tal d'evitar que omplin l'espai d'emmagatzematge del sistema. Els BNU proporcionen diverses ordres que es poden utilitzar per netejar els fitxers de registre:

- `uulog`
- `uuclean`
- `uucleanup`
- `uudemon.cleanu.`

Executeu aquestes ordres o bé utilitzeu les entrades del fitxer `/var/spool/cron/crontabs/uucp` per executar les ordres mitjançant el daemon **cron**.

Fitxers d'enregistrament dels directoris .Log i .Old:

Els BNU creen fitxers de registre individuals al directori `/var/spool/uucp/.Log`.

Els BNU creen aquests fitxers de registre per a cada sistema remot accessible, utilitzant les ordres **uucp**, **uucico**, **uux** i **uuxqt**. Els BNU col•loquen la informació sobre l'estat de cada transacció al fitxer de registre corresponent cada vegada que algú del sistema utilitza els BNU. Quan s'executa més d'un procés dels BNU, el sistema no pot accedir al fitxer de registre. En comptes d'això, col•loca la informació d'estat en un fitxer diferent amb un prefix `.LOG`.

L'ordre **uulog** mostra un resum de les sol•licituds **uucp** o **uux**, per usuari o per sistema. L'ordre **uulog** mostra els fitxers. No obstant això, també podeu fer que els BNU combinin automàticament els fitxers de registre en un fitxer de registre primari. Aquesta acció s'anomena *compactar* els fitxers de registre i pot realitzar-se amb l'ordre **uudemon.cleanu**, que normalment executa el daemon **cron**.

El daemon **cron** executa l'ordre **uudemon.cleanu**. L'ordre **uudemon.cleanu** combina els fitxers de registre **uucico** i **uuxqt** del sistema local i els emmagatzema al directori `/var/spool/uucp/.Old`. Al mateix temps, l'ordre elimina els fitxers de registre antics emmagatzemats prèviament al directori `.Old`. Per defecte, l'ordre **uudemon.cleanu** desa els fitxers de registre que tenen dos dies d'antiguitat.

Si l'espai d'emmagatzematge és un problema, considereu la possibilitat de reduir el nombre de dies que es mantenen els fitxers. Per fer un seguiment de les transaccions dels BNU durant un període de temps

més llarg, podeu augmentar el nombre de dies que es mantenen els fitxers. Per canviar el temps per defecte per desar els fitxers de registre, modifiqueu el procediment d'intèrpret d'ordres de l'ordre **uudemon.cleanu**. Aquesta seqüència s'emmagatzema al directori `/usr/sbin/uucp` i pot modificar-se amb l'autorització root.

Fitxers d'enregistrament /.Admin dels BNU:

Els BNU també recopilen informació i l'emmagatzemen al directori `/var/spool/uucp/.Admin`. Aquest directori conté els fitxers `errors`, `xferstats`, `Foreign` i `audit`.

Aquests fitxers s'han de comprovar i eliminar de tant en tant per tal d'estalviar espai d'emmagatzematge. Els BNU creen cada fitxer quan es necessita.

Quan un altre sistema es posa en contacte amb el vostre sistema amb el mode de depuració del daemon **uucico** activat, invoca el daemon **uucico** del vostre sistema amb la depuració activada. Els missatges de depuració que genera el daemon al sistema local s'emmagatzemen al fitxer `audit`. Aquest fitxer es pot arribar a fer molt gran. Tot sovint comproveu el fitxer `audit` i elimineu-o.

El fitxer `errors` enregistra els errors que troba el daemon **uucico**. La comprovació d'aquest fitxer pot ajudar a corregir problemes, com ara permisos incorrectes als fitxers de treball dels BNU.

El fitxer `xferstats` conté informació sobre l'estat de cada transferència de fitxers. Comproveu i elimineu tot sovint aquest fitxer.

El fitxer `Foreign` és important per la seguretat del sistema. Sempre que un sistema desconegut intenta iniciar una sessió en el sistema local, els BNU criden el procediment d'intèrpret d'ordres `remote.unknown`. Aquest procediment d'intèrpret d'ordres enregistra l'intent al fitxer `Foreign`. El fitxer `Foreign` conté els noms dels sistemes que han intentat cridar el sistema local i han estat rebutjats. Si un sistema ha estat intentant crides de manera freqüent, utilitzeu aquesta informació a l'hora de considerar si heu de permetre l'accés d'aquest sistema.

Fitxers d'enregistrament de tot el sistema que utilitzen els BNU:

Com que molts processos dels BNU necessiten autorització root per dur a terme les seves tasques, els BNU creen sovint entrades al fitxer `/var/spool/sulog log`.

De la mateixa manera, la utilització del daemon **cron** per planificar les tasques dels BNU crea diverses entrades al fitxer `/var/spool/cron/log`. Quan utilitzeu els BNU, comproveu i netegeu aquests fitxers.

Ordres de manteniment dels BNU

Els BNU (Basic Networking Utilities) contenen diverses ordres per supervisar les activitats dels BNU i netejar els directoris i fitxers dels BNU.

Ordres de neteja dels BNU:

Els BNU contenen tres ordres que netegen directoris i eliminen els fitxers que no s'han enviat.

Element	Descripció
uuclean	Suprimeix dels directoris administratius dels BNU tots els fitxers que són posteriors a un nombre especificat d'hores. Utilitzeu l'ordre **uuclean** per especificar un directori que s'ha de netejar o un tipus de fitxer que s'ha de suprimir. També podeu donar instruccions a l'ordre per què notifiqui als propietaris dels fitxers suprimits. L'ordre **uuclean** és l'equivalent en els sistemes Berkeley de l'ordre **uucleanup**.
uucleanup	Realitza funcions semblants a l'ordre **uuclean**. No obstant això, l'ordre **uucleanup** comprova l'edat dels fitxers basant-se en els *dies* més que no pas en les hores. Utilitzeu l'ordre **uucleanup** per enviar un missatge d'avís als usuaris els fitxers dels quals no s'han transferit, notificant-los que els fitxers encara estan a la cua. L'ordre **uucleanup** també elimina els fitxers relacionats amb un sistema remot especificat.
uudemon.cleanu	Un procediment d'intèrpret d'ordres que executa les ordres **uulog** i **uucleanup** per comprimir els fitxers de registre dels BNU i eliminar els fitxers de registre i treball que tenen més de tres dies. L'ordre **uudemon.cleanu** s'executa mitjançant el daemon **cron**.

Ordres de comprovació d'estat dels BNU:

Els BNU també proporcionen ordres per comprovar l'estat de les transferències i dels fitxers de registre.

Element	Descripció
uuq	Mostra el treballs que actualment es troben a la cua de treballs dels BNU. Utilitzeu l'ordre **uuq** per visualitzar l'estat d'un treball especificat o de tots els treballs. Amb l'autorització root, podeu utilitzar l'ordre **uuq** per suprimir un treball de la cua.
uustat	Proporciona informació semblant a la que proporciona l'ordre **uuq**, però en un format diferent. Utilitzeu l'ordre **uustat** per comprovar l'estat dels treballs i suprimir els treballs de la vostra propietat. Amb l'autorització root, també podeu suprimir els treballs que pertanyen a altres usuaris.
uulog	Mostra un resum de les sol•licituds **uucp** o **uux**, per usuari o per sistema. L'ordre **uulog** mostra els noms de fitxers. Consulteu l'apartat "Fitxers d'enregistrament dels BNU" a la pàgina 449.
uupoll	Força un sondeig d'un sistema remot. Aquesta ordre és útil quan el treball per a aquest sistema espera a la cua i ha de ser transferit, abans que el sistema es planifiqui per ser cridat automàticament.
uusnap	Mostra un resum molt breu de l'estat dels BNU. Per a cada sistema remot, aquesta ordre mostra el nombre de fitxers que esperen ser transferits. No obstant això, no mostra el temps que han estat esperant. L'ordre **uusnap** és l'equivalent en els sistemes Berkeley de l'ordre **uustat**.

Procediments d'intèrpret d'ordres dels BNU:

Els BNU se subministren amb dos procediments d'intèrpret d'ordres que s'utilitzen per al manteniment:

Element	Descripció
uudemon.cleanu	Es descriu a l'apartat "Ordres de neteja dels BNU" a la pàgina 450.
uudemon.admin	Executa l'ordre **uustat**. L'ordre **uustat** informa sobre l'estat dels treballs dels BNU. Envia els resultats a l'ID d'inici de sessió uucp com a correu. Podeu modificar el procediment d'intèrpret d'ordres **uudemon.admin** per enviar el correu a un altre lloc, o bé utilitzar un programa de correu per reencaminar tot el correu per a l'ID d'inici de sessió uucp a l'usuari responsable de l'administració dels BNU.

Aquests procediments d'intèrpret d'ordres estan emmagatzemats al directori `/usr/sbin/uucp`. Copieu els procediments i modifiqueu la còpia, si voleu canviar el que fan. Executeu els procediments des de la línia d'ordres o planifiqueu la seva execució per part del daemon **cron**.

Per executar automàticament les ordres **uudemon.cleanu** i **uudemon.admin**, elimineu els caràcters de comentari (#) que estan al principi de les línies pertinents del fitxer `/var/spool/cron/crontabs/uucp`.

Nom de camí d'accés dels BNU

Els noms de camí d'accés utilitzats amb les ordres dels BNU (Basic Networking Utilities) es poden especificar de diferents maneres.

Els noms de camí d'accés estan formats pel directori arrel o per un camí d'accés escurçat de la destinació, que és el nom d'un sistema o sistemes remots. Cada variació de camí d'accés segueix directrius específiques.

Nom de camí d'accés sencer

Un nom de camí d'accés sencer comença a l'arrel i traça tots els directoris fins al directori i fitxer de destinació.

Per exemple, `/etc/uucp/Devices` es refereix al fitxer `Devices` del directori `uucp` del directori arrel `etc`.

Escriviu-hi sempre al davant una barra inclinada (/) per indicar que es tracta d'un directori arrel. Separeu sempre els elements d'un camí d'accés amb una barra inclinada (/).

Nom de camí d'accés relatiu

El nom de camí d'accés relatiu llista només els directoris que són relatius al directori actual.

Per exemple, si el directori actual és `/usr/bin` i el directori de destinació es `/usr/bin/reports`, escriviu el nom de camí d'accés relatiu `reports` (sense la barra inclinada inicial).

Els noms de camí d'accés relatiu es poden utilitzar amb les ordres **cu**, **uucp** i **uux** i amb el nom del fitxer d'origen a l'ordre **uuto**.

> **Nota:** Pot ser que els noms de camí d'accés relatiu no funcionin amb totes les ordres dels BNU. Si teniu problemes amb un nom de camí d'accés relatiu, torneu a escriure l'ordre amb el nom de camí d'accés sencer.

Nom de camí d'accés ~ [opció]

El nom de camí d'accés `~ [opció]` representa el directori d'inici de l'usuari especificat.

La titlla (~) es pot utilitzar com a drecera per a alguns directoris.

Per exemple, `~marina` es refereix al directori d'inici de l'usuari `marina`. L'entrada `~uucp` o `~` (la titlla només) es refereix al directori públic dels BNU del sistema remot. El nom de camí d'accés sencer del directori públic dels BNU és `/var/spool/uucppublic`.

> **Nota:** Aquesta utilització de la titlla no s'ha de confondre amb l'altra utilització de la titlla als BNU. La titlla també s'utilitza per introduir ordres perquè s'executin en un sistema local quan s'inicïi la sessió en un sistema remot quan s'utilitzi l'ordre **cu**.

nom_sistema! nom de camí d'accés

El *nom_sistema*`!` identifica el camí d'accés d'un fitxer d'un altre sistema.

Per exemple, `distant!/account/march` fa referència al fitxer `march` del directori `account` del sistema remot `distant`.

nom_sistema!nom_sistema! nom de camí d'accés

El *nom_sistema*`!`*nom_sistema*`!` identifica un camí d'accés a través de diversos sistemes.

Per exemple, si només es pot arribar al sistema anomenat `distant` a través d'un altre sistema anomenat `proper`, el nom del camí d'accés és `proper!distant!/compte/novembre`.

Separeu els noms del sistema amb un signe d'exclamació (!). En cas de noms de camí d'accés de diversos sistemes, la norma de separar els elements amb una barra inclinada (/) no s'aplica als noms del sistema. De tota manera, la norma si es manté per al sistema final, on s'estipulen els directoris i els fitxers.

Nota: Si utilitzeu un intèrpret d'ordres bourne, separeu els noms del sistema amb un signe d'exclamació (!). Si feu servir els BNU en un intèrpret d'ordres C o korn, escriviu al davant del signe d'exclamació una barra inversa (\). La barra inversa és un caràcter d'escapament necessari per interpretar literalment el següent caràcter més que no pas com a caràcter especial.

Daemons dels BNU

El programari dels BNU inclou quatre daemons que estan emmagatzemats al directori `/usr/sbin/uucp`.

Element	Descripció
uucico	Facilita les transferències de fitxers (consulteu l'apartat "Daemon uucico")
uusched	Facilita la planificació de les sol•licituds de treball dels fitxers posats en cua al directori de cues local (consulteu l'apartat "Daemon uusched" a la pàgina 454)
uuxqt	Facilita les execucions d'ordres remotes (consulteu l'apartat "Daemon uuxqt" a la pàgina 454)
uucpd	Facilita les comunicacions quan s'utilitza TCP/IP (consulteu l'apartat "Daemon uucpd" a la pàgina 454)

Els daemons **uucico**, **uusched** i **uuxqt** s'inicien mitjançant el daemon **cron** d'acord amb una planificació establerta per l'administrador dels BNU. Amb l'autorització root, també podeu iniciar manualment aquests daemons. El daemon **uucpd** s'ha d'iniciar mitjançant el daemon **inetd** TCP/IP.

Daemon uucico

El daemon **uucico** transporta els fitxers necessaris per enviar dades d'un sistema a un altre.

Les ordres **uucp** i **uux** inicien el daemon **uucico** per transferir fitxers d'ordres, de dades i d'execució al sistema designat. El daemon **uucico** també s'inicia periòdicament mitjançant el planificador dels BNU, el daemon **uusched**. Quan s'inicia mitjançant el daemon **uusched**, el daemon **uucico** intenta contactar amb altres sistemes i executar les instruccions dels fitxers d'ordres.

Per executar les instruccions dels fitxers d'ordres, el daemon **uucico** primer comprova el fitxer `/etc/uucp/Systems` (o un o més fitxers especificats per `/etc/uucp/Sysfiles`) per al sistema que s'ha de cridar. A continuació, el daemon comprova si a l'entrada del fitxer `Systems` hi ha una hora vàlida per cridar. Si l'hora és vàlida, el daemon **uucico** comprova els camps *Tipus* i *Classe* i accedeix al fitxer `/etc/uucp/Devices` (o a un o més fitxers especificats per `/etc/uucp/Sysfiles`) per veure si hi ha un dispositiu que coincideixi.

Després de trobar un dispositiu, el daemon **uucico** comprova si al directori `/var/locks` existeix un fitxer de bloqueig per al dispositiu. Si n'existeix un, el daemon comprova un altre dispositiu del tipus i velocitat sol•licitats.

Quan no hi ha cap dispositiu disponible, el daemon torna als fitxers `Systems` per veure si existeix una altra entrada per al sistema remot. Si n'existeix una, el daemon repeteix el procés de cerca d'un dispositiu. Si no es troba una altra entrada, el daemon realitza una entrada al fitxer `/var/spool/uucp/.Status/`*Nom_sistema* per a aquest sistema remot i continua amb la següent sol•licitud. El fitxer d'ordres es queda a la cua. El daemon **uucico** torna a intentar la transferència més endavant. El darrer intent s'anomena *reintent*.

Quan el daemon **uucico** accedeix al sistema remot, utilitza les instruccions dels fitxers `Systems` per iniciar una sessió. Això fa que una instància del daemon **uucico** també s'invoqui al sistema remot.

Els dos daemons **uucico**, un en cada sistema, treballen conjuntament per realitzar la transferència. El daemon **uucico** del sistema que crida controla l'enllaç, especificant les sol•licituds que s'han de realitzar. El daemon **uucico** del sistema remot comprova els permisos locals per determinar si permeten realitzar la sol•licitud. En cas afirmatiu, s'inicia la transferència de fitxers.

Un cop el daemon **uucico** del sistema de crida ha finalitzat la transferència de totes les sol•licituds que té per al sistema remot, envia una sol•licitud de penjar. Quan el daemon **uucico** remot té transaccions per enviar al sistema de crida, denega la sol•licitud de penjar, i els dos daemons inverteixen els seus rols.

Nota: Tant el fitxer `/etc/uucp/Permissions` del sistema local com el fitxer `/etc/uucp/Permissions` del sistema remot poden prohibir que els daemon inverteixin els seus rols. En aquest cas, el sistema remot ha d'esperar a transferir els fitxers fins que cridi el sistema local.

Quan no queda res per transferir en ambdues direccions, els dos daemons **uucico** pengen. En aquest punt, es crida el daemon **uuxqt** ("Daemon uuxqt") per què executi les sol•licituds d'ordres remotes.

Durant tot el procés de transferència, els daemons **uucico** dels dos sistemes enregistren missatges als fitxers de registre i errors dels BNU.

Daemon uusched

El daemon **uusched** planifica la transferència dels fitxers que estan posats a la cua del directori de cues del sistema local.

El directori de cues és `/var/spool/uucppublic`. Quan s'invoca, el daemon **uusched** escaneja el directori de cues per trobar fitxers d'ordres i, a continuació, selecciona els fitxers de manera aleatòria i inicia el daemon **uucico**. El daemon **uucico** transfereix els fitxers.

Daemon uuxqt

Quan un usuari emet l'ordre **uux** per executar una ordre especificada en un sistema designat, el daemon **uuxqt** executa l'ordre.

Després de crear els fitxers necessaris, l'ordre **uux** inicia el daemon **uucico**, que transfereix aquests fitxers al directori públic de cua del sistema especificat.

El daemon **uuxqt** cerca periòdicament al directori de cues les sol•licituds d'execució d'ordres de cada sistema connectat. Quan localitza una sol•licitud, el daemon **uuxqt** comprova els fitxers i permisos necessaris. A continuació, si té permís, el daemon executa l'ordre especificada.

Daemon uucpd

El daemon **uucpd** ha de poder executar-se en el sistema remot per tal que els BNU puguin establir comunicacions amb un ordinador remot amb **TCP/IP (Transmission Control Protocol/Internet Protocol)**.

El daemon **uucpd** és un subservidor del daemon **inetd** TCP/IP i s'inicia mitjançant el daemon **inetd**.

Per defecte, el daemon **uucpd** està comentat al fitxer `inetd.conf`. Per utilitzar-lo, heu d'eliminar el caràcter de comentari i reiniciar **inetd**. No obstant això, si el caràcter de comentari s'ha canviat al vostre sistema, és possible que hagueu de tornar a configurar el daemon **inetd** per iniciar el daemon **uucpd**.

Seguretat dels BNU

Posat que altres sistemes contacten amb el vostre sistema per iniciar una sessió, transferir fitxers i especificar ordres, els BNU proporcionen un mitjà per establir la seguretat.

La seguretat dels BNU us permeten restringir el que els usuaris de sistemes remots poden fer al sistema local (els usuaris dels sistemes remots també us poden restringir el que vosaltres feu en els seus sistemes). Els BNU executen diversos daemons per dur a terme les seves activitats i utilitzen directoris administratius per emmagatzemar els fitxers que necessiten. Els BNU també mantenen un enregistrament de les seves pròpies activitats.

La seguretat dels BNU funcionen en diversos nivells. Quan configureu els BNU, podeu determinar:

- Qui del vostre sistema té accés als fitxers dels BNU.
- Els sistemes remots amb els que el vostre sistema pot contactar
- Com inicien una sessió els usuaris de sistemes remots en el vostre sistema.
- Què poden fer els usuaris dels sistemes remots al vostre sistema un cop han iniciat una sessió.

ID d'inici de sessió uucp

Quan els BNU estan instal•lats, tots els fitxers de configuració, daemons i moltes de les ordres i procediments d'intèrpret d'ordres són propietat de l'ID d'inici de sessió uucp.

L'ID d'inici de sessió uucp té un ID d'usuari (UID) de 5 i un ID de grup (GID) de 5. El dimoni **cron** llegeix el fitxer `/var/spool/cron/crontabs/uucp` per planificar tasques automàtiques per BNU.

Normalment, l'inici de sessió com a usuari uucp no està permès. Per canviar els fitxers que pertanyen a l'ID d'inici de sessió uucp, inicieu una sessió amb autorització root.

Atenció: El fet de permetre als sistemes remots iniciar una sessió en el sistema local amb l'ID d'inici de sessió uucp compromet seriosament la seguretat del sistema local. Els sistemes remots que han iniciat una sessió amb l'ID uucp poden visualitzar i possiblement modificar els fitxers `Systems` i `Permissions` locals depenent dels altres permisos especificats a l'entrada LOGNAME. Es recomana vivament que creeu altres ID d'inici de sessió dels BNU per a sistemes remots i que reserveu l'ID d'inici de sessió uucp per a la persona responsable d'administrar els BNU al sistema local. Per més seguretat, cada sistema remot que contacta amb el sistema local ha de tenir un ID d'inici de sessió exclusiu amb un número d'ID d'usuari exclusiu.

El sistema operatiu proporciona un ID d'inici de sessió nuucp per defecte amb la finalitat de transferir fitxers.

ID d'inici de sessió dels BNU

L'intèrpret d'ordres d'engegada per als ID d'inici de sessió dels BNU és el daemon **uucico** (`/usr/sbin/uucp/uucico`).

Quan els sistemes remots criden el vostre sistema, inicien automàticament el daemon **uucico** del vostre sistema. Els ID d'inici de sessió per als BNU tenen un ID de grup uucp de 5.

Els ID d'inici de sessió que utilitzen els sistemes remots necessiten paraules clau. Per tal d'evitar que la seguretat us sol•liciti un nou ID d'inici de sessió dels BNU per a una nova paraula clau quan el sistema remot inicia una sessió, heu d'establir la paraula clau tan bon punt creeu el compte. Per fer-ho, utilitzeu l'ordre **passwd** seguida de l'ordre **pwdadm**. Per exemple, per establir una paraula clau per al ID d'inici de sessió `nuucp`, inicieu una sessió com a usuari root i especifiqueu les ordres següents:

```
passwd nuucp

pwadm -f NOCHECK
nuucp
```

El sistema us sol•licita una paraula clau per a l'ID d'inici de sessió `nuucp`. Dur a terme aquests passos permet que el sistema remot iniciï una sessió sense que se li sol•liciti immediatament una nova paraula clau (que l'ID d'inici de sessió `nuucp` orientat a lots no pot proporcionar).

Després de crear l'ID d'inici de sessió per a un sistema remot, notifiqueu a l'administrador dels BNU d'aquest sistema l'ID d'inici de sessió i la paraula clau per accedir al vostre sistema.

Un usuari amb autorització root pot configurar un ID d'inici de sessió administratiu dels BNU. Això és útil si voleu delegar responsabilitats de l'administrador dels BNU a un usuari sense autorització root. L'ID d'inici de sessió administratiu dels BNU ha de tenir seguretat de paraula clau, un ID d'usuari de 5 i estar en un ID de grup uucp 5. L'intèrpret d'ordres d'inici de sessió per a l'inici de sessió administratiu ha de ser el programa `/usr/bin/sh` (en comptes del daemon **uucico**). Donat l'inici de sessió administratiu

dels BNU, un ID d'usuari de 5 fa que tingui els mateixos privilegis que l'inici de sessió **uucp**. Per tant, per seguretat, no s'hauria de permetre que els sistemes remots iniciessin una sessió com a administrador dels BNU.

Seguretat i els fitxers Systems i remote.unknown

A la majoria de sistemes dels BNU, només els sistemes remots llistats al fitxer `/etc/uucp/Systems` o un dels seus substituts (especificats al fitxer `Sysfiles`) poden iniciar una sessió en el sistema local.

La seqüència `/usr/sbin/uucp/remote.unknown` s'executa sempre que un sistema desconegut intenta cridar el sistema local. Aquesta seqüència no permet que el sistema desconegut iniciï una sessió i realitza una entrada al fitxer `/var/spool/uucp/.Admin/Foreign` enregistrant l'hora d'intent d'inici de sessió.

Amb autorització root, o com a administrador dels BNU, podeu modificar el procediment d'intèrpret d'ordres `remote.unknown` per enregistrar més informació sobre el sistema remot o emmagatzemar la informació en un altre fitxer. Per exemple, podeu modificar el procediment d'intèrpret d'ordres per enviar correu a l'administrador dels BNU sempre que un sistema desconegut intenta iniciar una sessió.

Si traieu els permisos d'execució sobre el procediment d'intèrpret d'ordres `remote.unknown`, permeteu que les màquines desconegudes puguin iniciar una sessió. En aquest cas, heu d'afegir una entrada MACHINE=OTHER al fitxer `/etc/uucp/Permissions` per establir permisos a les màquines desconegudes.

El vostre sistema només pot contactar amb els sistemes remots llistats al fitxer `Systems`. D'aquesta manera, els usuaris del vostre sistema no poden contactar amb sistemes desconeguts.

Seguretat i el fitxer Permissions

Tingueu en compte els següents aspectes sobre la seguretat a l'hora d'utilitzar el fitxer `Permissions`.

El fitxer `/etc/uucp/Permissions` determina el següent:

- Noms d'usuari d'inici de sessió remota per iniciar una sessió en el sistema local
- Ordres i privilegis aprovats per a sistemes remots que inicien una sessió en el sistema local.

El fitxer `/etc/uucp/Permissions` conté dos tipus d'entrades:

Element	Descripció
LOGNAME	Defineix noms d'inici de sessió i els privilegis associats amb ells. Les entrades LOGNAME entren en vigor quan un sistema remot crida el sistema local i intenta iniciar-hi una sessió.
MACHINE	Defineix els noms de màquina i els privilegis associats amb ells. Les entrades MACHINE entren en vigor quan el sistema remot intenta executar ordres en el sistema local.

Les opcions del fitxer `Permissions` permeten establir diversos nivells de seguretat per a cada sistema remot. Per exemple, si molts sistemes remots comparteixen un ID d'inici de sessió del sistema local, utilitzeu l'opció VALIDATE per exigir que cada sistema remot utilitzi un ID d'inici de sessió exclusiu. Les opcions SENDFILES, REQUEST i CALLBACK especifiquen quin sistema té el control, fent que el sistema local mantingui el control de les transaccions si és necessari.

Les opcions READ, WRITE, NOREAD i NOWRITE defineixen l'accés a directoris específics del sistema local. Aquestes opcions també controlen en quin lloc del vostre sistema poden posar dades els usuaris remots. L'opció COMMANDS limita el nombre d'ordres que els usuaris dels sistemes remots poden executar al sistema local. L'opció COMMANDS=ALL permet privilegis totals sobre els sistemes estretament associats amb el vostre sistema.

Atenció: L'opció COMMANDS=ALL pot comprometre seriosament la seguretat del vostre sistema.

Comunicació entre el sistema local i el sistema remot

Per tal d'establir comunicació entre un sistema remot i un sistema local, el sistema remot ha de tenir un enllaç mitjançant cable o mòdem amb el sistema local, un sistema operatiu basat en UNIX instal•lat i els BNU o una altra versió del Programa de còpia UNIX a UNIX (UUCP) en execució.

> **Nota:** Podeu utilitzar els BNU per comunicar-vos amb un sistema no UNIX, però és probable que aquesta connexió requereixi maquinari o programari addicional.

Els BNU disposen de dues ordres que us permeten comunicar-vos amb sistemes remots. L'ordre **cu** connecta sistemes a través de cable o de línies telefòniques. L'ordre **ct** connecta sistemes a través només de línies telefòniques gràcies a un mòdem.

Utilitzeu l'ordre **cu** per establir comunicació entre xarxes quan sapigueu el número de telèfon o el nom del sistema de destinació. Per utilitzar l'ordre **ct**, *cal* que tingueu el número de telèfon del sistema de destinació.

> **Nota:** Una tercera ordre, **tip**, funciona de manera molt semblant a l'ordre **cu**. L'ordre **tip**, però, és un component de la versió BSD (Berkeley Software Distribution) del programa UUCP. La seva instal•lació amb els BNU requereix una configuració especial.

Comunicació amb altres sistemes mitjançant cable o mòdem

Utilitzeu l'ordre **cu** des del sistema local per dur a terme les següents tasques de comunicació:

- Establir una connexió amb un sistema remot especificat
- Iniciar la sessió en un sistema remot
- Dur a terme tasques al sistema remot
- Commutar enrere o endavant, treballant simultàniament a tots dos sistemes

Si el sistema remot està funcionant al mateix sistema operatiu, podeu executar ordres regulars des del sistema local. Per exemple, podeu executar ordres per canviar directoris, llistar el contingut del directori, veure fitxers o enviar fitxers a la cua d'impressió del sistema remot. Per executar ordres per utilitzar-les al sistema local o per iniciar intercanvis remots d'ordres i fitxers, utilitzeu les ordres locals especials **cu** introduïdes amb una titlla (~).

Comunicació amb un altre sistema mitjançant mòdem

Executeu l'ordre **ct** per comunicar-vos via mòdem amb un altre sistema.

Introduïu l'ordre **ct**, seguida d'un número de telèfon, per cridar el mòdem remot. Quan s'estableixi la connexió, l'indicador d'inici de sessió remota apareix a la pantalla.

L'ordre **ct** pot ser útil en algunes circumstàncies. Per obtenir detalls sobre la manera com utilitzar l'ordre **ct** dels BNU, consulteu:

- “Marcar un número fins que s'efectua una connexió”
- “Marcar diversos números fins que s'efectua una connexió” a la pàgina 458

Marcar un número fins que s'efectua una connexió

Aquest procediment descriu la utilització de l'ordre **ct** per continuar marcant un número de mòdem remots fins que s'efectua una connexió o fins que ha passat un interval de temps especificat.

El sistema que s'ha de cridar cal que estigui executant els BNU (Basic Networking Utilities) o alguna versió del Programa de còpia UNIX a UNIX (UUCP).

Escriviu a la línia d'ordres del sistema local:

```
ct -w3 5550990
```

Això marca els números de telèfon `555-0990` del mòdem remot. El senyalador i el número **-w3** dóna instruccions a l'ordre **ct** perquè marqui el número del mòdem remot a intervals d'un minut fins que s'efectua la connexió o fins que han passat tres minuts.

> **Nota:** Escriviu el número de telèfon del mòdem remot a la línia de l'ordre **ct**, abans o després del senyalador.

Marcar diversos números fins que s'efectua una connexió

Aquest procediment descriu la utilització de l'ordre **ct** per continuar marcant diversos números de mòdems remots fins que s'efectua una connexió o fins que ha passat un interval de temps especificat.

El sistema que s'ha de cridar cal que estigui executant els BNU (Basic Networking Utilities) o alguna versió del Programa de còpia UNIX a UNIX (UUCP).

Escriviu a la línia d'ordres del sistema local:

```
ct -w6 5550990 5550991 5550992 5550993
```

Això marca els números de telèfon `555-0990`, `555-0991`, `555-0992` i `555-0993`. El senyalador i el número **-w6** dóna instruccions a l'ordre **ct** perquè marqui els números dels mòdems remots a intervals d'un minut fins que s'efectua la connexió o fins que han passat sis minuts.

> **Nota:** Escriviu els números de telèfon dels mòdems remots a la línia de l'ordre **ct** abans o després del senyalador.

Intercanvis de fitxers en els sistemes locals i remots

La transferència de fitxers entre sistemes és l'aplicació més comuna dels BNU (Basic Networking Utilities). Els BNU utilitzen quatre ordres, **uucp**, **uusend**, **uuto** i **uupick**, per intercanviar fitxers entre sistemes locals i remots.

L'ordre **uucp** és la utilitat principal de transferència de dades dels BNU. L'ordre **uusend** és l'ordre de transferència BSD (Berkeley Software Distribution) incorporada als BNU. Les ordres **uuto** i **uupick** són ordres especialitzades en l'enviament i recepció que treballen amb l'ordre **uucp**.

Les ordres dels BNU, **uuencode** i **uudecode**, ajuden a la transferència de fitxers. Aquestes ordres codifiquen i descodifiquen fitxers binaris transmesos a través del recurs de correu dels BNU.

Enviament i recepció de fitxers

Les ordres utilitzades per enviar i rebre fitxer a través d'una connexió dels BNU inclouen l'ordre **uucp** i l'ordre **uusend**.

Utilitzeu l'ordre i les opcions **uucp** per intercanviar fitxers dins el sistema local, entre el sistema local i un de remot, i entre sistemes remots. Les opcions del programa **uucp** poden, per exemple, crear directoris per retenir fitxers a la màquina receptora o enviar missatges durant transferències de fitxers satisfactòries o no satisfactòries.

Utilitzeu l'ordre **uusend** per enviar fitxers a un sistema remot que no estigui enllaçat directament amb el sistema emissor però que sigui accessible a través d'una sèrie de connexions dels BNU. Encara que està equipada amb menys opcions que l'ordre **uucp**, **uusend** s'inclou entre les utilitats dels BNU per satisfer les preferències dels usuaris de l'UUCP (Programa de còpia UNIX a UNIX) de BSD.

Enviar fitxers a un usuari específic

Per tal d'enviar fitxers a un usuari específic, els sistemes emissor i receptor han d'estar executant els BNU (Basic Networking Utilities) o alguna versió del Programa de còpia UNIX a UNIX (UUCP).

Utilitzeu l'ordre **uuto** per enviar fitxers d'un sistema a un altre. És part de l'ordre **uucp** i simplifica el procés d'intercanvi de fitxers per a emissors i receptors. L'ordre **uuto** envia fitxers a un usuari específic i

els diposita directament al directori personal de l'usuari dins el directori públic dels BNU d'aquell sistema. Notifica al destinatari que ha arribat un fitxer. El destinatari utilitza l'ordre **uupick** per manejar el nou fitxer.

Enviament d'un fitxer amb l'ordre uuto:

Quan utilitzeu l'ordre **uuto** per enviar un fitxer, incloeu el fitxer per enviar, la destinació del sistema remot i l'usuari de la destinació.

Per exemple:

```
uuto /home/bin/fitxer1 distant!pep
```

Això envia el `fitxer1` des del directori local `/home/bin` a l'usuari `joe` del sistema remot `distant`.

L'ordre **uuto** s'executa dins l'ordre **uucp**. El fitxer es transfereix al sistema remot, a `/var/spool/uucppublic`. El fitxer es diposita al directori `/var/spool/uucppublic/receive/`*usuari*`/System` del sistema remot. Si el directori de destinació no existeix, es crea durant l'intercanvi de fitxers.

L'ordre **rmail** dels BNU notifica al receptor que ha arribat un fitxer.

> **Nota:** Per enviar un fitxer a un usuari d'un sistema *local*, especifiqueu l'ordre **uuto**, i inclogueu el fitxer a enviar, la destinació del sistema local i l'usuari de la destinació local. Per exemple:
>
> ```
> uuto /home/bin/fitxer2 proper!sebas
> ```
>
> Això envia el `fitxer2` del directori `/home/bin` local a l'usuari `sebas` del sistema local `proper`.

Recepció de fitxers

Per tal de poder rebre i gestionar fitxers, els sistemes emissor i receptor han d'estar executant els BNU (Basic Networking Utilities) o alguna versió del Programa de còpia UNIX a UNIX (UUCP).

Utilitzeu l'ordre **uupick** per rebre i manipular fitxers enviats amb l'ordre **uuto**. Disposa d'opcions de gestió de fitxers que permeten que el destinatari, trobi els fitxers enviats, desplaci fitxers a un directori especificat, executi ordres o suprimeixi fitxers.

Rebre un fitxer amb l'ordre uupick:

Utilitzeu l'ordre **uupick** per rebre un fitxer.

Per exemple:

```
uupick
```

L'ordre **uupick** cerca al directori públic els fitxers que inclouen l'ID d'usuari remot en els noms de camí d'accés. L'ordre **uupick** mostra aleshores a la pantalla remota un missatge semblant a:

```
del sistema base: fitxer fitxer1?
```

Les subordres ? (signe d'interrogació) de la segona línia de la pantalla de notificació sol•licita al receptor que utilitzi les opcions **uupick** per manejar fitxers al directori públic dels BNU.

Per obtenir una llista de totes les opcions disponibles, escriviu un asterisc (*) a la línia que apareix sota de l'indicador d'interrogant (?) . Les opcions de visualitzar, desar i sortir són:

Element	Descripció
p	Mostra el contingut del fitxer.
m *[Directori]*	Desa el fitxer al directori especificat per la variable *[Directori]*. Si no es determina cap destinació amb l'opció **m**, el fitxer es desplaça al directori de treball actual.
q	Surt (abandona) del procés de maneig de fitxers **uupick**.

Codificació i descodificació de fitxers per a transferència

Utilitzeu les ordres **uuencode** i **uudecode** a fi de preparar els fitxers per transmetre'ls via mòdem.

Aquestes ordres treballen conjuntament. L'ordre **uuencode** transforma fitxers binaris en fitxers ASCII. El recurs de correu pot enviar aquests fitxers a un sistema remot.

Amb l'ordre **uudecode** l'usuari receptor torna a convertir els fitxers codificats en ASCII en fitxers de format binari.

Informes sobre l'estat dels intercanvis d'ordres i fitxers

Per veure els informes sobre l'estat dels intercanvis de fitxers, utilitzeu les ordres **uusnap**, **uuq** i **uustat**.

Visualització dels estats dels sistemes connectats per BNU

L'ordre **uusnap** mostra una taula d'informació sobre tots els sistemes connectats mitjançant els BNU.

La taula mostra una línia de cada sistema, que reporta els noms i els números de fitxers d'ordres, de fitxers de dades i les execucions d'ordres remotes que es mantenen a les cues dels sistemes. El darrer element de cada línia és un missatge d'estat. Aquest missatge indica una connexió satisfactòria dels BNU o una explicació dels motius pels quals no s'ha establert un enllaç.

Consulteu l'ordre **uusnap**.

Visualització de la cua de treballs dels BNU

L'ordre **uuq** llista les entrades de la cua de treball dels BNU.

El format de la llista és semblant al format que mostra l'ordre **ls**. La visualització de cada entrada inclou el número del treball, seguit d'un resum en la mateixa línia, incloent-hi el nom del sistema, el nombre de treballs del sistema i el nombre total d'octets a enviar. Els usuaris amb autorització root poden utilitzar una ordre **uuq** per identificar treballs específics col•locats en cua mitjançant el seu número de treball.

Consulteu l'ordre **uuq** a *Commands Reference, Volume 5*.

Estat de les operacions BNU

L'ordre **uustat** proporciona l'estat d'un intercanvi d'ordres o fitxers concret al sistema dels BNU.

Si s'especifica sense opcions de senyalador, l'ordre **uustat** mostra una sola línia per a cada treball sol•licitat per l'usuari actual, incloent-hi:

- Número d'ID del treball
- Data i hora
- Estat (enviar o rebre)
- Nom del sistema
- ID d'usuari de la persona que ha executat l'ordre
- Grandària i nom del fitxer de treball

Equipada amb nombrosos senyaladors, l'ordre **uustat** pot proporcionar informes sobre tots els treballs en cua de tots els usuaris o sobre els treballs sol•licitats per altres sistemes de la xarxa.

L'ordre **uustat** ofereix als usuaris un control limitat dels treballs en cua que cal executar en un sistema remot. Podeu examinar l'estat de les connexions dels BNU amb altres sistemes i efectuar un seguiment dels intercanvis de fitxers i d'ordres. Podeu, per exemple, anul•lar les sol•licituds de còpia iniciades per l'ordre **uucp**.

Consulteu l'ordre **uustat**.

Intercanvis d'ordres entre els sistemes locals i remots

Els BNU (Basic Networking Utilities) permeten que els usuaris intercanviïn ordres entre sistemes locals i remots.

L'ordre **uux** executa ordres en un sistema remot. L'ordre **uupoll** controla la sincronització de l'execució d'ordres.

Sol•licituds d'execució d'ordres en un sistema remot

Utilitzeu l'ordre **uux** per sol•licitar l'execució d'una ordre en un sistema remot.

L'ordre **uux** no executa les ordres al sistema remot. Per comptes d'això, prepara els fitxers de dades i de control necessaris a `/var/spool/uucp`. S'invoca el daemon **uucico** perquè dugui a terme la transferència. Quan la transferència s'ha dut a terme, l'**uucico** del sistema remot crea un fitxer d'execució al seu directori de cues.

Quan els dos daemons **uucico** es posen d'acord per penjar, el daemon **uuxt** explora el directori de cues per trobar les sol•licituds d'execució pendents, verifica els permisos i comprova si es necessita informació addicional. Llavors fa un procés fork a una ordre perquè faci el que s'havia sol•licitat.

> **Nota:** Podeu utilitzar l'ordre **uux** en qualsevol sistema configurat per executar una ordre especificada. De tota manera, per motius de seguretat, la política d'alguns indrets pot restringir l'ús de determinades ordres. És probable que alguns indrets, per exemple, només permetin l'execució de l'ordre **mail**.

Després de rebre els fitxers al sistema remot, el daemon **uuxqt** executa l'ordre especificada en aquest sistema. El daemon **uuxqt** explora periòdicament el directori públic de cua del sistema per trobar fitxers rebuts en transmissions **uux**. El daemon **uuxqt** comprova que les dades a les quals s'ha d'accedir estan presents al sistema remot. També verifica si el sistema emissor té permís per accedir a les dades. El daemon **uuxqt** executa aleshores l'ordre o notifica al sistema emissor que l'ordre no s'ha executat.

Supervisió d'una connexió remota dels BNU

Utilitzeu el següent procediment per supervisar una connexió remota dels BNU.

- El programa dels BNU ha d'estar instal•lat al sistema.
- S'ha de configurar un enllaç (per cable, mòdem o TCP/IP) entre el vostre sistema i el sistema remot.
- Els fitxers de configuració dels BNU, que inclouen el fitxer `Systems`, el fitxer `Permissions`, el fitxer `Devices` i el fitxer `Dialers` (i el fitxer `Sysfiles`, si s'escau), s'han de configurar per a les comunicacions entre el vostre sistema i el sistema remot.

  Nota: Cal tenir autorització d'usuari root per modificar els fitxers de configuració dels BNU.

L'ordre **Uutry** us pot ajudat a supervisar el procés del daemon **uucico** si els usuaris del vostre indret informen de problemes de transferència de fitxers.

1. Executeu l'ordre **uustat** per determinar l'estat de tots els treballs de transferència que hi ha a la cua actual, tal com s'indica a continuació:

   ```
   uustat -q
   ```

   El sistema mostra un informe d'estat semblant al següent:

```
venus 3C (2) 05/09-11:02 CAN'T ACCESS DEVICE
hera 1C 05/09-11:12 SUCCESSFUL
merlin 2C 5/09-10:54 NO DEVICES AVAILABLE
```

Aquest informe indica que tres fitxers d'ordres (`C.*`) previstos per al sistema remot `venus` han estat a la cua durant dos dies. Pot haver diverses causes per a aquest retard. Per exemple, potser el sistema `venus` ha estat aturat per realitzar el manteniment o bé el mòdem s'ha desconnectat.

2. Abans d'iniciar activitats de resolució de problemes més completes, executeu l'ordre **Uutry** tal com s'indica a continuació per determinar si el sistema local pot contactar ara amb el sistema `venus`:

   ```
   /usr/sbin/uucp/Uutry -r venus
   ```

   Aquesta ordre inicia el daemon **uucico** amb una quantitat moderada de depuració i la instrucció d'alterar temporalment l'hora de reintent per defecte. L'ordre **Uutry** dirigeix la sortida de depuració a un fitxer temporal, `/tmp/venus`.

3. Si el sistema local aconsegueix establir una connexió amb el sistema `venus`, la sortida de depuració conté una gran quantitat d'informació. No obstant això, la línia final d'aquesta seqüència, indicada a continuació, és la més important:

   ```
   Conversation Complete: Status SUCCEEDED
   ```

   Si la connexió és satisfactòria, cal suposar que els problemes de transferència de fitxers temporals ja s'han resolt. Torneu a executar l'ordre **uustat** per assegurar-vos que els fitxers del directori de cues s'han transferit satisfactòriament al sistema remot. En cas contrari, utilitzeu els passos descrits a l'apartat “Supervisió d'una transferència de fitxers dels BNU” a la pàgina 463 per comprovar si hi ha problemes de transferència de fitxers entre el vostre sistema i el sistema remot.

4. Si el sistema local no pot contactar amb el sistema remot, la sortida de depuració que genera l'ordre **Uutry** conté el següent tipus d'informació (el format exacte de la sortida pot variar):

   ```
   mchFind called (venus)
   conn (venus)
   getto ret -1
   Call Failed: CAN'T ACCESS DEVICE
   exit code 101
   Conversation Complete: Status FAILED
   ```

   En primer lloc, comproveu les connexions físiques entre el sistema local i el sistema remot. Assegureu-vos que l'ordinador remot estigui encés i que tots els cables estiguin degudament connectats, que els ports estiguin habilitats o inhabilitats (segons calgui) en ambdós sistemes, i que els mòdems (si s'escau) funcionin.

   Si les connexions físiques són correctes i segures, verifiqueu tots els fitxers de configuració pertinents tant del sistema local com del sistema remot, que inclouen els següents:

   - Assegureu-vos que les entrades dels fitxers `Devices`, `Systems` i `Permissions` (i del fitxer `Sysfiles`, si s'escau) del directori **/etc/uucp** són correctes en ambdós sistemes.
   - Si utilitzeu un mòdem, assegureu-vos que el fitxer `/etc/uucp/Dialers` (o un fitxer alternatiu especificat a **/etc/uucp/Sysfiles**) conté l'entrada correcta. Si utilitzeu abreviatures de codis de marcatge, assegureu-vos que les abreviatures estan definides al fitxer `/etc/uucp/Dialcodes`.
   - Si utilitzeu una connexió TCP/IP, assegureu-vos que el daemon **uucpd** pot executar-se en el sistema remot i que els fitxers de configuració contenen les entrades TCP correctes.

5. Després de comprovar les connexions físiques i els fitxers de configuració, torneu a executar l'ordre **Uutry**. Si la sortida de depuració encara indica que la connexió no és satisfactòria, possiblement haureu de posar-vos en contacte amb un membre del vostre equip de suport de sistemes. Deseu la sortida de depuració que ha generat l'ordre **Uutry**. Aquesta acció podria ser d'utilitat a l'hora de diagnosticar el problema.

Transferència d'un fitxer a un sistema remot per imprimir-lo

Utilitzeu l'ordre **uux** per transferir un fitxer a un sistema remot per imprimir-lo.

Per transferir un fitxer a un sistema remot per imprimir-lo, s'han de complir els següents prerequisits:

- Cal establir una connexió dels BNU (Basic Networking Utilities) amb el sistema remot
- Cal que tingueu permís per executar operacions al sistema remot

Escriviu a la línia d'ordres del sistema local:

```
uux remote!/usr/bin/lpr local!nom_fitxer
```

Això imprimeix el fitxer local *nom_fitxer* al sistema remot.

Supervisió d'una transferència de fitxers dels BNU:

Utilitzeu aquest procediment per supervisar una transferència de fitxers a un sistema remot.

- El programa dels BNU ha d'estar instal•lat al sistema i configurat per a ell.
- Estabiu una connexió amb un sistema remot utilitzant els passos especificats a l'apartat "Supervisió d'una connexió remota dels BNU" a la pàgina 461.

La supervisió d'una transferència de fitxers és útil quan les transferències de fitxers al sistema remot en qüestió no es realitzen satisfactòriament per causes desconegudes. La informació de depuració que genera el daemon **uucico** (cridat per l'ordre **Uutry**) us pot ajudar a esbrinar què és el que no funciona correctament.

L'ordre **Uutry** us permet supervisar les transferències de fitxers de la manera següent:

1. Prepareu un fitxer per a la transferència utilitzant l'ordre **uucp** amb el senyalador **-r**. Per fer-ho, escriviu el següent.

   ```
   uucp -r test1 venus!~/test2
   ```

   El senyalador **-r** indica al programa UUCP que ha de crear i posar en cua tots els fitxers de transferència necessaris però *no* ha d'iniciar el daemon **uucico**.
2. Executeu l'ordre **Uutry** amb el senyalador **-r** per iniciar el daemon **uucico** amb la depuració activada. Per fer-ho, escriviu el següent:

   ```
   /usr/sbin/uucp/Uutry -r venus
   ```

   Aquesta ordre dóna instruccions al daemon **uucico** per què es posi en contacte amb el sistema `venus` alterant temporalment l'hora de reintent per defecte. El daemon es posa en contacte amb el sistema `venus`, inicia una sessió i transfereix el fitxer, mentre que l'ordre **Uutry** genera la sortida de depuració que permet supervisar el procés de l'**uucico**. Premeu la seqüència de tecles d'interrupció per aturar la sortida de depuració i torneu a l'indicador d'ordres.

   L'ordre **Uutry** també emmagatzema la sortida de depuració al fitxer `/tmp/Nom_sistema`. Si sortiu de la sortida de depuració abans que finalitzi la connexió, podeu examinar el fitxer de sortida per veure el resultat de la connexió.

Transmissions de treballs en cua:

Utilitzeu l'ordre **uupoll** per iniciar la transmissió de treballs emmagatzemats al directori públic de cua del sistema local.

L'ordre **uupoll** crea un treball nul al directori públic del sistema remot i inicia el daemon **uucico**. Això força el daemon **uucico** a posar-se en contacte immediatament amb el sistema remot i transferir els treballs posats en cua.

Identificació de sistemes compatibles

Utilitzeu l'ordre **uuname** per visualitzar una llista de tots els sistemes als quals pot accedir el sistema local.

Per exemple, si escriviu:

```
uuname
```

a la línia d'ordres, el sistema visualitza una llista com la següent:

```
artur
hera
merlin
zeus
```

Aquesta informació s'utilitza per determinar el nom d'un sistema accessible abans de copiar-hi un fitxer. L'ordre **uuname** també s'utilitza per establir la identitat del sistema local. L'ordre **uuname** adquireix la seva informació llegint el fitxer `/etc/uucp/systems`.

Comunicació amb sistemes UNIX connectats utilitzats l'ordre tip

Utilitzeu l'ordre **tip** per contactar amb qualsevol sistema connectat que executa el sistema operatiu UNIX.

L'ordre **tip** s'instal•la amb els BNU (Basic Networking Utilities) i pot utilitzar les mateixes connexions asíncrones que utilitzen els BNU.

L'ordre **tip** utilitza variables i senyals d'escapament, així com senyaladors, per controlar les seves operacions. Els senyaladors poden especificar-se a la línia d'ordres. Els senyals d'escapament poden utilitzar-se a través d'una connexió amb un sistema remot per iniciar i aturar transferències de fitxers, canviar la direcció d'una transferència de fitxers i sortir a un subintèrpret d'ordres.

Variables de l'ordre tip:

Les variables de l'ordre **tip** defineixen valors, com ara el caràcter de final de línia, el senyal d'interrupció i el mode de les transferències de fitxers.

Els valors de les variables poden inicialitzar-se en temps d'execució utilitzant un fitxer `.tiprc`. Els valors de les variables també poden modificar-se durant l'execució utilitzant el senyal d'escapament `~s`. Algunes variables, com ara el caràcter de final de línia, poden establir-se per a un sistema individual a l'entrada del sistema del fitxer `remote`.

L'ordre **tip** llegeix tres fitxers, el fitxer `phones`, el fitxer `remote` i el fitxer `.tiprc` per determinar els valors inicials de les seves variables. El fitxer `.tiprc` ha d'estar sempre al directori d'inici de l'usuari. Els noms i les ubicacions dels fitxers `remote` i `phones` poden variar. Els noms del fitxer `remote` i del fitxer `phones` es poden determinar mitjançant variables d'entorn.

Element	Descripció
PHONES	Especifica el fitxer de telèfon de l'usuari. El fitxer pot tenir qualsevol nom de fitxer vàlid i ha de configurar-se en el format del fitxer `/usr/lib/phones-file`. El fitxer per defecte és `etc/phones`. Si un fitxer s'especifica amb la variable `PHONES`, s'utilitza en comptes (no a més a més) del fitxer `/etc/phones`.
REMOTE	Especifica el nom del fitxer de definició del sistema remot de l'usuari. El fitxer pot tenir qualsevol nom de fitxer vàlid i ha de configurar-se en el format del fitxer `/usr/lib/remote-file`. El fitxer per defecte és `/etc/remote`. Si un fitxer s'especifica amb la variable **REMOTE**, s'utilitza en comptes (no a més a més) del fitxer `/etc/remote`.

Per utilitzar una variable d'entorn, estabiu-la abans d'iniciar l'ordre **tip**. Com a alternativa, els noms dels fitxers `phones` i `remote` es poden determinar utilitzant la variable `phones` i la variable `remote`, respectivament, de l'ordre **tip**, que es troben al fitxer `.tiprc`.

Nota: L'ordre **tip** només llegeix el *darrer* fitxer `remote` o `phones` especificat. Per tant, si especifiqueu un fitxer `remote` o `phones` amb una variable, el fitxer nou s'utilitza en comptes (no a més a més) de qualsevol fitxer anterior que hagueu especificat.

L'ordre **tip** utilitza valors de variables en el següent ordre:

1. L'ordre comprova els valors de les variables d'entorn **PHONES** i **REMOTE** dels fitxers que s'han d'utilitzar com a fitxers `phones` i `remote`.
2. L'ordre llegeix el fitxer `.tiprc` i estableix totes les variables de forma corresponent. Si la variable `phones` o `remote` s'estableix en el fitxer `.tiprc`, aquest valor altera temporalment el valor de la variable d'entorn.
3. Quan s'inicia una connexió amb un sistema remot, l'ordre llegeix l'entrada del fitxer `remote` per a aquest sistema. Els valors de l'entrada del fitxer `remote` alteren temporalment els valors especificats al fitxer `.tiprc`.
4. Si s'utilitza el senyalador `- BaudRate` amb l'ordre **tip**, la velocitat especificada altera temporalment tots els valors anteriors de velocitat en bauds.
5. Un valor establert amb el senyal d'escapament `~s` altera temporalment tots els valors anteriors d'una variable.

   Nota: Qualsevol usuari **tip** pot crear un fitxer `.tiprc` i utilitzar aquest fitxer per especificar valors inicials per a les variables **tip**. El fitxer `.tiprc` ha de col•locar-se al directori `$HOME` de l'usuari.

Fitxers de configuració de l'ordre tip:

Per tal que l'ordre **tip** pugui connectar amb un sistema remot, s'han d'establir els fitxers `/etc/remote` i `/etc/phones`.

Element	Descripció
`/etc/remote`	Defineix els atributs dels sistemes remots, com ara el port i el tipus de dispositiu que cal utilitzar per comunicar-se amb el sistema, així com els senyals que s'han d'utilitzar per indicar els començaments i els acabaments de les transmissions.
`/etc/phones`	Mostra una llista dels números de telèfon utilitzats per contactar amb els sistemes remots a través d'una línia de mòdem.

Els fitxers `remote` i `phones` d'exemple se subministren amb el paquet bos.net.uucp. El fitxer `remote` d'exemple s'anomena `/usr/lib/remote-file`. El fitxer `phones` d'exemple s'anomena `/usr/lib/phones-file`. Copieu `/usr/lib/remote-file` a `/etc/remote` i modifiqueu `/etc/remote`. Per establir un d'aquests fitxers, copieu un fitxer d'exemple amb el nom correcte i modifiqueu-lo segons les necessitats del vostre indret.

Un usuari **tip** també pot crear fitxers `remote` i `phones` personalitzats. Un fitxer `remote` individual ha d'estar en el format del fitxer `/usr/lib/remote-file` i s'ha d'especificar amb la variable `remote` o amb la variable d'entorn `REMOTE`. Un fitxer `phones` individual ha d'estar en el format del fitxer `/usr/lib/phones-file` i s'ha d'especificar amb la variable `phones` o amb la variable d'entorn `PHONES`. Si un fitxer `phones` o `remote` individual s'especifica amb una de les variables, el fitxer es llegeix en comptes (no a més a més) del fitxer `/etc/phones` o `/etc/remote`.

Els usuaris de **tip** poden utilitzar combinacions de fitxers `phones` i `remote` individuals. Per exemple, un usuari podria utilitzar el fitxer `remote` per defecte, `/etc/remote`, però utilitzar un fitxer `phones` individual especificat amb la variable `phones`.

Anul•lació de treballs remots

Utilitzeu l'ordre **uustat** per anul•lar un procés dels BNU executat en un sistema remot.

Per cancel•lar un treball remot, s'han de complir els següents requisits:

- Cal establir una connexió dels BNU (Basic Networking Utilities) amb el sistema remot de destinació
- Cal haver executat un treball remot des del sistema local

1. Determineu el número d'ID de treball del procés llistat a la cua remota. Escriviu a la línia d'ordres del sistema local:

   ```
   uustat -a
   ```

   L'opció **-a** mostra tots els treballs de la cua en espera del sistema remot i les sol•licituds de treball de qualsevol altre usuari dels BNU que hi hagi al sistema.

   Els BNU responen amb un missatge semblant a:

   ```
   heraC3113   11/06-17:47  S hera    tu      289 D.venus471afd8
   merlinC3119 11/06-17:49  S merlin  marina  338 D.venus471bc0a
   ```

2. A continuació escriviu:

   ```
   uustat -k heraC3113
   ```

   L'opció **-k** cancel•la sol•licitud de treball `heraC3113`.

Resolució de problemes dels BNU

Els missatges d'error dels BNU poden enllaçar-se a una fase específica del flux de la conversió. Utilitzeu el "Diagrama de flux de la conversió dels BNU" i les següents descripcions d'errors com a ajuda per diagnosticar els problemes dels BNU.

És possible que alguns del missatges següents no s'enviïn des dels BNU, però s'inclouen per si s'utilitza una altra versió de l'UUCP.

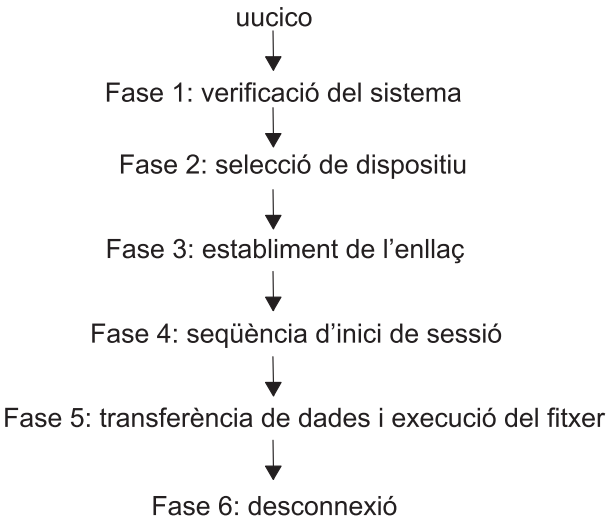


Figura 26. Diagrama de flux de la conversió dels BNU

Aquesta il•lustració mostra el flux i les diferents fases de la conversió dels BNU. Des d'uucico al principi de tot, les dades passen a la Fase 1-Verificació del sistema, després a la Fase 2-Selecció de dispositiu i Fase 3-Establiment de l'enllaç, a continuació a la Fase 4-Seqüència d'inici de sessió, després a la Fase 5-Transferència de dades i execució del fitxer i, finalment, a la Fase 6-Desconnexió.

Missatges d'estat de la FASE 1 dels BNU

Hi ha cinc missatges d'estat de la FASE 1 dels BNU. La taula següent els descriu.

Element	Descripció
Assert Error	La unitat del sistema local té problemes. Comproveu a l'informe d'errors les causes possibles executant l'ordre `errpt -a | pg`.
System not in Systems	Si especifiqueu un nom de sistema remot que no es troba als fitxers `Systems`, es crearà aquest missatge d'estat i els BNU finalitzaran. Utilitzeu l'ordre **uuname** per tornar a comprovar el nom del sistema.
Wrong time to call	El fitxer `Systems` té restriccions sobre les hores a les que es permeten les crides de sortida. Els BNU seguiran intentant-ho fins que l'hora sigui la correcta. Comproveu el fitxer `Systems`.
Callback required	La xarxa té restriccions d'ús, ja sigui per motius de seguretat o econòmics, i l'accés s'ha denegat en aquest moment.
Cannot call No Call	Aquests errors signifiquen que els BNU han intentat cridar el sistema remot i no han tingut èxit. No ho tornaran a intentar immediatament. També es poden generar a causa d'un antic fitxer d'estat del sistema que està retingut i que impedeix al daemon **uucico** torna-ho a intentar.

Missatges d'estat de la FASE 2 dels BNU

Hi ha quatre missatges d'estat de la FASE 2 dels BNU. La taula següent els descriu.

Element	Descripció
Dialer Script Failed	La seqüència del fitxer `Dialers` no s'ha dut a terme satisfactòriament.
No Device Available Can't Access Device	El mòdem o la línia telefònica de sortida del sistema estan ocupats. Comproveu si ha un error a l'entrada de dispositiu del fitxer `Systems`. A més, comproveu els fitxers `Devices` i `Dialers` per tal d'assegurar-vos que els dispositius lògics tenen dispositius físics associats. El fitxer `/etc/uucp/Sysfiles` podria estar especificant un fitxer `Systems`, `Devices` o `Dialers` alternatiu que no està configurat correctament. Algun altre programa està utilitzant el dispositiu? Comproveu si al directori `/var/locks` hi ha un bloqueig al port. Si existeix un fitxer de bloqueig (per exemple, `LCK..TTY0`), comproveu si el procés identificat pel número del fitxer de bloqueig encara està actiu. Si no ho està, podeu eliminar-lo (per exemple, `rm /var/locks/LCK..TTY0`). A més, comproveu els permisos del port.
Dial Failed Failed (call to system)	Aquests errors apareixen quan el sistema marca un altre sistema satisfactòriament però l'altre sistema no respon. També podria indicar un problema en els fitxers `Devices`. Especifiqueu l'ordre `uucico -r1 -x6 -s` *`Nom_sistema`*. Podria ser que els BNU esperen alguna sèrie que no estan rebent. Realitzeu la connexió manualment per tal d'esbrinar què cal incorporar a l'entrada dels fitxers `Systems` per satisfer la sol•licitud. Tingueu en compte la "temporització"; potser calen alguns retards a la sèrie de marcatge del mòdem. Això també podria significar que el port està ocupat, que heu marcat un número incorrecte o que els BNU han perdut la propietat del port.
OK Auto Dial	Aquests missatges només són informatius i no indiquen cap error.

Missatges d'estat de la FASE 3 dels BNU

Hi ha cinc missatges d'estat de la FASE 3 dels BNU. La taula següent els descriu.

Element	Descripció
Handshake Failed (LCK)	El dispositiu està sent utilitzat per una altra persona; el procés no ha pogut crear el fitxer `LCK`. A vegades, l'administrador ha d'eliminar manualment els fitxers `LCK`. Després d'uns quants reintents, poseu-vos en contacte amb l'administrador del sistema. Comproveu si un altre procés té el control del port (per exemple, una altra instància del daemon **uucico**).
Login Failed	L'inici de sessió no ha sigut satisfactori com a conseqüència d'una mala connexió o possiblement d'una màquina lenta.
Timeout	El sistema remot no ha respost dins del període de temps establert. Això també podria indicar un problema amb la seqüència chat.
Succeeded (Call to System)	La crida s'ha dut a terme.
BNU (continued)	Aquests missatges només són informatius i no indiquen cap error.

Missatges d'estat de la FASE 4 dels BNU

Hi ha sis missatges d'estat de la FASE 4 dels BNU. La taula següent els descriu.

Element	Descripció
`Startup Failed Remote reject after login`	Després de l'inici de sessió, el daemon **uucico** s'inicia al sistema remot. Si hi ha un problema per iniciar una conversa entre els dos sistemes, es creen aquests missatges. També és possible que hagueu iniciat una sessió en un compte incorrecte dels BNU o que la conformitat de connexió inicial hagi fallat.
`Wrong machine name`	Una màquina s'ha cridat incorrectament o s'ha canviat el nom de la màquina.
`Bad login/machine combination`	L'inici de sessió en el sistema remot no s'ha realitzat satisfactòriament. El problema podria ser un número de telèfon incorrecte, un inici de sessió o una paraula clau incorrectes, o un error en la seqüència chat.
`Remote has a LCK file for me`	Els dos sistemes intentaven cridar-se al mateix temps. La sol•licitud local fallarà temporalment.
`OK Talking`	Aquests missatges només són informatius i no indiquen cap error.
`LOGIN: PASSWORD:`	Si l'indicador d'inici de sessió o paraula clau està tot en majúscules, el mòdem podria estar en mode d'eco (E1 als mòdems compatibles amb Hayes). Com a conseqüència d'això, el mòdem fa un eco de tornada, o envia, un RING al vostre sistema quan es rep una crida d'entrada. L'ordre **getty** rep la sèrie i canvia de manera corresponent els indicadors `login:` o `password:` a tot majúscules. Canvieu el mode d'eco del mòdem a desconnectat (utilitzeu `ATE0` per als mòdems compatibles amb Hayes). **Nota:** Tingueu en compte que un cop s'ha fet aquest canvi, heu d'utilitzar `ATE1` a la seqüència chap dels vostres fitxers `Dialers`, o bé no rebreu de l'`OK` esperat procedent del mòdem. Si el port remot està establert per a `delay` o `getty -r` i la seqüència chat espera entrada de tecles, aleshores els ports establerts per a `delay` esperen un o més retorns de carro abans de continuar amb l'inici de sessió. Proveu de començar la seqüència chat en el sistema de realitza el marcatge tal com s'indica a continuació: `"" \r\d\r\d\r\d\r in:--in: ...` Un cop interpretada, aquesta seqüència de chap es llegeix de la següent manera: expect nothing, send return, delay, return, delay, return, delay, return.

Missatges d'estat de la FASE 5 dels BNU

Hi ha cinc missatges d'estat de la FASE 5 dels BNU. La taula següent els descriu.

Element	Descripció
`Alarm`	El daemon **uucico** té problemes amb la connexió. La connexió és errònia o bé "xon/xoff" està establert en sí al mòdem.
`Remote access to path/file denied copy (failed)`	Aquests missatges indiquen un problema amb els permisos; comproveu els permisos del camí d'accés i del fitxer.
`Bad read`	El sistema remot s'ha quedat sense espai, probablement a l'àrea de la cua, o bé el daemon **uucico** no ha pogut llegir ni escriure en el dispositiu.
`Conversation failed`	S'ha perdut la detecció de portadora del mòdem. Possiblement el mòdem s'ha apagat, el cable està fluix o desconnectat o bé el sistema remot ha patit una caiguda o està aturat. La desconnexió del telèfon també pot provocar aquest error.
`Requested Copy (succeeded)`	Aquests missatges només són informatius i no indiquen cap error.

Missatges d'estat de la FASE 6 dels BNU

Hi ha dos missatges d'estat de la FASE 6 dels BNU. La taula següent els descriu.

Element	Descripció
`OK (Conversation Complete)`	El sistema remot pot denegar la sol•licitud de penjar i invertir els rols (la qual cosa indica que el sistema remot té treballs que el sistema local ha de realitzar). Un cop els dos daemons **uucico** acorden que no hi ha cap més treball per fer, pengen.
`Conversation succeeded`	Aquest missatge només és informatiu i no indica cap error.

Depuració de les fallades d'inici de sessió dels BNU utilitzant el daemon uucico

Utilitzeu el daemon **uucico** per depurar les fallades d'inici de sessió dels BNU.

- Els BNU han d'estar instal•lats al sistema.
- S'ha de configurar un enllaç (per cable, mòdem o TCP/IP) entre el vostre sistema i el sistema remot.

- Els fitxers de configuració dels BNU, que inclouen el fitxer Sysfiles (si s'escau), el fitxer Systems, el fitxer Permissions, el fitxer Devices i el fitxer Dialers, s'han de configurar per a les comunicacions entre el vostre sistema i el sistema remot.

  Nota: Cal tenir autorització d'usuari root per modificar els fitxers de configuració dels BNU.
- Cal tenir autorització d'usuari root per invocar el daemon **uucico** en mode de depuració.

1. Per generar informació de depuració sobre una connexió que no funciona entre el sistema local i el sistema remot, inicieu el daemon **uucico** amb el senyalador **-x**, tal com s'indica a continuació:

   ```
   /usr/sbin/uucp/uucico -r 1 -s venus -x 9
   ```

   on -r 1 especifica el mode mestre o d'emissor; -s venus, el nom del sistema remot al que esteu intentant connectar-vos; i -x 9, el nivell de depuració que genera la informació de depuració més detallada.
2. Si l'entrada seqüència d'enviament-recepció d'un fitxer Systems en el format /etc/uucp/Systems és:

   ```
   venus Any venus 1200 - "" \n in:--in: uucp1 word:
    mirror
   ```

   el daemon **uucico** connecta el sistema local amb el sistema remot venus. La sortida de depuració és semblant a la següent:

   ```
   expect: ""
   got it
   sendthem (^J^M)
   expect (in:)^
   M^Jlogin:got it
   sendthem (uucp1^M)
   expect (word:)^
   M^JPassword:got it
   sendthem (mirror^M)
   imsg >^M^J^PShere^@Login Successful: System=venus
   ```

   on:

Element	Descripció
expect: ""	Especifica que el sistema local no esperarà informació del sistema remot.
got it	Confirma que s'ha rebut el missatge.
sendthem (^J^M)	Especifica que el sistema local enviarà al sistema remot un retorn de carro i una nova línia.
expect (in:)	Especifica que el sistema local espera rebre l'indicador d'inici de sessió del sistema remot, que finalitza en la sèrie de caràcters in:.
^M^Jlogin:got it	Confirma que el sistema local ha rebut l'indicador d'inici de sessió remota.
sendthem (uucp1^M)	Especifica que el sistema local enviarà l'ID d'inici de sessió uucp1 al sistema remot.
expect (word:)	Especifica que el sistema local espera rebre l'indicador de paraula clau del sistema remot, que finalitza en la sèrie de caràcters word:.
^M^JPassword:got it	Confirma que el sistema local ha rebut l'indicador de paraula clau remota.
sendthem (mirror^M)	Especifica que el sistema local enviarà la paraula clau per a l'ID d'inici de sessió uucp1 al sistema remot.
imsg >^M^J^PShere^@Login Successful: System=venus	Confirma que el sistema local ha iniciat satisfactòriament una sessió en el sistema remot venus.

Nota:

1. La sortida de depuració d'enviament-recepció que genera l'ordre **uucico** pot procedir de la informació del fitxer /etc/uucp/Dialers o de la informació del fitxer /etc/uucp/Systems. La informació sobre la

comunicació amb el mòdem prové del fitxer `Dialers`, mentre que la informació sobre la comunicació amb el sistema remot prové del fitxer `Systems`. (Observeu que `/etc/uucp/Systems` i `/etc/uucp/Dialers` són els fitxers de configuració per defecte dels BNU. Es poden especificar altres fitxers a `/etc/uucp/Sysfiles` per fer la mateixa funció).

2. Per configurar una connexió amb un sistema remot, heu d'estar familiaritzats amb la seqüència d'inici de sessió d'aquest sistema en qüestió.

SNMP per la gestió de xarxes

El recurs de gestió de xarxes proporciona un sistema complet de xarxes de sistema a través de la utilització del protocol **Simple Network Management Protocol (SNMP)** que permet als amfitrions de xarxa intercanviar informació de gestió.

SNMP és un protocol de treball d'Internet dissenyat per utilitzar-se amb internets basades en **TCP/IP**.

Quan el sistema operatiu AIX està instal•lat, la versió no encriptada de **SNMPv3** s'instal•la per defecte i s'inicia durant el temps d'inici del sistema. Si disposa de les seves pròpies comunitats i les entrades SMUX configurades al fitxer `/etc/snmpd.conf`, haureu de migrar les comunitats de forma manual al fitxer `/etc/snmpdv3.conf`. Per obtenir informació sobre la migració de comunitats, consulteu “Migració d'SNMPv1 a SNMPv3” a la pàgina 479.

És aconsellable consulta l'informació que apareix a Descripció general de SNMP per a programadorsOverview que apareix a *Communications Programming Concepts*.

La gestió de xarxes **SNMP** es basa en un modelo de client/servidor familiar que s'utilitza àmpliament a les aplicacions de xarxa basades en **TCP/IP**. Cada amfitrió que s'ha de gestionar executa un procés anomenat *agent*. L'agent és un procés de servidor que actualitza la base de dades MIB per a l'amfitrió. Els amfitrions que estan implicats en la presa de decisions de gestió de la xarxa poden executar un procés anomenat gestor. Un *manager* és una aplicació de client que genera sol•licituds per informació MIB i respostes de processos. A més, un gestor pot enviar sol•licituds a servidors d'agent per modificar informació MIB.

SNMP de AIX proporciona suport pels RFC següents:

Element	Descripció
RFC 1155	Estructura i identificació d'informació de gestió per Internets basades en **TCP/IP**
RFC 1157	Un **Simple Network Management Protocol (SNMP)**
RFC 1213	Base d'informació de gestió per la gestió de xarxa d'Internets basades en **TCP/IP**: MIB-II
RFC 1227	Protocol de multiplexor simple de **Simple Network Management Protocol (SNMP)** (SMUX) i base d'informació de gestió (MIB)
RFC 1229	Extensions de la base d'informació de gestió d'interfície genèrica (MIB)
RFC 1231	Base d'informació de gestió de token ring IEEE 802.5 (MIB)
RFC 1398	Definicions d'objectes gestionats per tipus d'interfície semblants a Ethernet
RFC 1512	Base d'informació de gestió FDDI
RFC 1514	MIB de recursos d'amfitrió
RFC 1592	Interfície de programa versió 2 distribuïda per **Protocol simple de xarxa**
RFC 1905	Operacions de protocol per la versió 2 del protocol de gestió de xarxa simple (SNMPv2)
RFC 1907	Base d'informació de gestió per la versió 2 del protocol de gestió de xarxa simple (SNMPv2)
RFC 2572	Processament i tramesa de missatges pel protocol **Simple Network Management Protocol (SNMP)**
RFC 2573	Aplicacions **SNMP**
RFC 2574	Model de seguretat basat en usuari (USM) per la versió 3 del protocol **Simple Network Management Protocol (SNMPv3)**
RFC 2575	Model de control d'accés de vista (VACM) pel protocol **Simple Network Management Protocol (SNMP)**

SNMPv3

En versions anteriors d'AIX, l'**SNMPv1** va ser l'única versió disponible del **SNMP**. **SNMPv3**, que es proporciona amb l'AIX, ofereix una estructura potent i flexible per la seguretat de missatges i el control d'accés.

L'informació d'aquesta secció només és vàlida per **SNMPv3**.

La seguretat de missatges implica proporcionar l'informació següent:

- Comprovació de l'integritat de dades per garantir que les dades no s'han alterat durant el seu trànsit.
- Verificació de l'origen de les dades per garantir que la sol•licitud o la resposta s'han originat a partir de l'origen del qual s'afirma que procedeixen.
- Comprovació de l'oportunitat dels missatges i, opcionalment, la confidencialitat de les dades per protegir-los contra espies.

L'arquitectura **SNMPv3** introdueix el model USM per la seguretat dels missatges i el model VACM pel control d'accés. L'arquitectura dóna suport a l'ús concorrent de diferents models de seguretat, control d'accés i processament de missatges. Per exemple, la seguretat basada en la comunitat pot utilitzar-se simultàniament amb USM, si es desitja.

USM utilitza el concepte d'un usuari per al qual es configuren paràmetres de seguretat (nivells de seguretat, autenticació i privacitat, així com claus) a l'agent i al gestor. Els missatges enviats mitjançant USM es protegeixen millor que els que s'envien amb seguretat basada en la comunitat. En aquest cas, les paraules clau s'envien de forma clara i es mostren en traces. Amb USM, per als missatges intercanviats entre el gestor i l'agent, s'ha realitzat la comprovació d'integritat de dades i l'autenticació d'origen de dades. Els retards i les reproduccions dels missatges (més enllà del que normalment succeeix degut a protocols de transport sense connexió) s'eviten mitjançant l'ús d'indicadors de temps i ID de sol•licituds. La confidencialitat de dades o l'encriptació també estan disponibles, sempre que estiguin permeses, com a un producte que s'instal•la per separat. La versió encriptada de **SNMP** es troba al Paquet d'ampliació de AIX

La utilització de VACM implica definir recopilacions de dades (anomenades vistes), grups d'usuaris de dades i sentències d'accés que defineixen les vistes que un grup particular d'usuaris pot utilitzar per llegir, escriure o rebre en un error trap.

SNMPv3 també introdueix la capacitat de configurar dinàmicament l'agent **SNMP** mitjançant ordres SET **SNMP** contra objectes MIB que representin la configuració de l'agent. Aquest suport de configuració dinàmica habilita l'addició, la supressió i la modificació d'entrades de configuració de forma local o remota.

Les polítiques d'accés i els paràmetres de seguretat de **SNMPv3** s'especifiquen al fitxer `/etc/snmpdv3.conf` de l'agent **SNMP** i al fitxer `/etc/clsnmp.conf` del gestor **SNMP**. Per veure un cas sobre com configurar aquests fitxers, consulteu “Creació d'usuaris a l'SNMPv3” a la pàgina 483. També podeu consultar els formats de fitxer `/etc/snmpdv3.conf` i `/etc/clsnmp.conf` que apareixen a *Files Reference*.

Arquitectura SNMPv3

Existeixen quatre parts principals de l'arquitectura **SNMPv3**.

L'interacció entre aquests sistemes per proporcionar les dades necessàries sol•licitades es descriu en la figura següent:

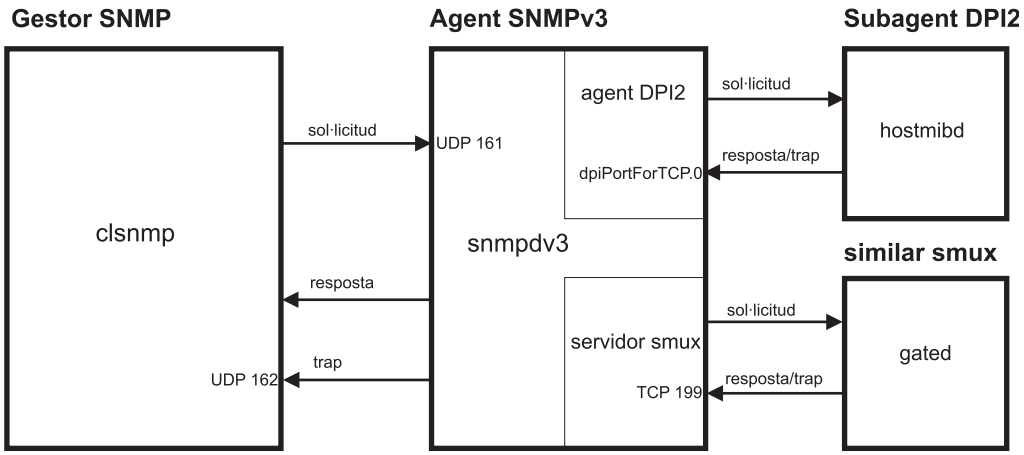


Figura 27. Les parts principals de l'arquitectura SNMPv3

Aquesta il•lustració mostra un exemple de l'arquitectura **SNMPv3**. Es mostren el subagent DPI2, el similar smux, el gestor **SNMP** i l'agent **SNMP**. A més, també es mostra com es comuniquen entre sí.

Agent SNMP:

L'agent **SNMP** rep sol•licituds del gestor **SNMP** i també envia resposta a aquest.

A més, l'agent **SNMP** es comunica amb tots els subagents DPI2 i similars SMUX del sistema. L'agent **SNMP** gestiona algunes variables MIB i tots els subagents DPI2 i els similars SMUX enregistren les seves variables MIB amb l'agent **SNMP**.

Quan **clsnmp** (el gestor **SNMP**) emet una sol•licitud, aquesta s'envia a UDP 161 dins de l'agent **SNMP**. Si la sol•licitud és **SNMPv1** o **SNMPv2c**, l'agent **SNMP** verificarà el nom de la comunitat i processarà la sol•licitud. Si la sol•licitud és **SNMPv3**, l'agent **SNMP** intentarà autenticar a l'usuari que sol•licita les dades i garantir que l'usuari té permisos d'accés per complir la sol•licitud mitjançant les claus d'autenticació. Si s'està executant la versió d'encriptació, s'utilitzaran claus privades. Si l'agent **SNMP** no pot autenticar l'usuari o si l'usuari no té els permisos d'accés adients per complir la sol•licitud, l'agent **SNMP** no realitzarà la sol•licitud. Per obtenir informació sobre la creació d'usuaris a **SNMPv3**, consulteu “Creació d'usuaris a l'SNMPv3” a la pàgina 483.

Si l'usuari s'autentica i té els permisos d'accés adients, l'agent **SNMP** durà a terme la sol•licitud. L'agent **SNMP** buscarà les variables MIB que s'estan sol•licitant. Si l'agent **SNMP** mateix gestiona les variables MIB sol•licitades, processarà la sol•licitud i retornarà una resposta al gestor **SNMP**. Si un subagent DPI2 o un similar SMUX gestiona les variables MIB sol•licitades, l'agent **SNMP** reenviarà la sol•licitud al subagent DPI2 o al similar SMUX en el qual es gestionen les variables MIB, permetrà que es processi la sol•licitud i, a continuació, enviarà una resposta al gestor **SNMP**.

Subagents DPI2:

Un subagent DPI2 com, per exemple **hostmibd**, es comunica amb l'agent DPI2, el qual a **SNMPv3**, forma part de l'agent SNMP.

El subagent DPI2 envia missatges i errors trap a l'agent DPI2 a través de dpiPortForTCP.0. Com que es tracta d'un port poc conegut, el subagent DPI2 primer ha d'emetre una sol•licitud pel número de port de dpiPortForTCP.0. Aquesta sol•licitud s'emet a UDP 161 a l'agent **SNMP**. Després d'això, l'agent **SNMP** respon al subagent DPI2 amb el número de port de dpiPortForTCP.0. Un cop s'ha rebut el número de port, el subagent DPI2 estableix una connexió amb l'agent DPI2 mitjançant el número de port proporcionat. A continuació, el subagent DPI2 enregistra els seus subarbres MIB amb l'agent DPI2.

Nota: Per habilitar l'agent **SNMP** per a què escolti a un port que no sigui UDP 161, haureu d'establir l'entorn **SNMP_PORT**. Existeixen dues maneres d'establir aquesta variable:

- **Mètode 1**: Aturar el subagent DPI2 i escriure les ordres següents:
  - `SNMP_PORT=<número_port> /usr/sbin/aixmibd -d 128`
  - `SNMP_PORT=<número_port> /usr/sbin/hostmibd -d 128`
  - `SNMP_PORT=<número_port> /usr/sbin/snmpmibd -d 128`

  on *número_port* és el número del port que desitgeu utilitzar.

  Un cop s'han acabat d'executar les ordres, inicieu el subagent DPI2.
- **Mètode 2**: incloure la variable **SNMP_PORT** al fitxer `/etc/environment` i assignar-li el nou valor de port. Permeteu que els daemons **aixmibd**, **hostmibd**, **snmpmibd** i **snmpd** s'executin des de `/etc/rc.tcpip` en el seu format original. En aquest mètode, no cal executar les ordres **aixmibd**, **hostmibd** i **snmpmibd** des de la línia d'ordres.

Un cop s'ha establert la connexió i s'han enregistrat els subarbres MIB, el subagent DPI2 ja està llest per respondre a les sol•licituds rebudes de l'agent. Quan es rep una sol•licitud, el subagent DPI2 processa la sol•licitud i respon amb l'informació necessària.

El subagent DPI2 també pot enviar errors trap si és necessari. Quan s'envia un error trap, l'agent **SNMP** comprovarà el seu fitxer `/etc/snmpdv3.conf` per determinar l'adreça o adreces IP a les quals s'ha de reenviar l'error trap i els les enviarà.

Similars SMUX:

Quan s'inicia un peer de multiplexatge SNMP (SMUX) com, per exemple, **gated**, s'establirà la connexió amb **TCP** 199 i s'inicialitzarà l'associació SMUX.

Després de l'inicialització, el similar SMUX enregistrarà els subarbre MIB que gestionarà.

Després de l'enregistrament, el similar SMUX està llest per acceptar qualsevol sol•licitud entrant del servidor SMUX i retorna les respostes. Quan un similar SMUX rep una sol•licitud, processarà la sol•licitud i retornarà una resposta al servidor SMU.

El similar SMUX també pot enviar un error trap al servidor SMUX. Quan s'envia un error trap, l'agent **SNMP** comprovarà el seu fitxer `/etc/snmpdv3.conf` per determinar l'adreça o adreces IP a les quals s'ha de reenviar l'error trap i els les enviarà.

Gestor SNMP:

El gestor **SNMP** executa **clsnmp**, el qual és compatible amb **SNMPv1**, **SNMPv2c** i **SNMPv3**.

Utilitzeu l'ordre **clsnmp** per emetre una sol•licitud com, per exemple, `get`, `get-next`, `get-bulk` o `set`. La sol•licitud s'envia a UDP 161 a l'agent **SNMP**. A continuació, la sol•licitud espera una resposta de l'agent **SNMP**.

Nota: Per permetre al gestor **SNMP** utilitzar un port que no sigui UDP 161, haureu de declara el número de port que voleu utilitzar i l'adreça IP al camp **targetAgent** del fitxer `/etc/clsnmp.conf`. Per obtenir informació sobre el fitxer `/etc/clsnmp.conf`, consulteu el Fitxer clsnmp.conf que apareix a *Files Reference*.

També pot escoltar errors trap **SNMP** a UDP 162. El gestor **SNMP** rebrà errors trap si la seva adreça IP s'ha especificat d'aquesta manera al fitxer `/etc/snmpdv3.conf` de l'agent **SNMP**.

Variables MIB:

A les ubicacions següents es pot trobar informació sobre variables MIB.

Per obtenir informació sobre variables MIB, consulteu Management Information Base, Terminologia relacionada amb les variables MIB, Treballa amb variables MIB i Bases de dades MIB que apareixen a *Communications Programming Concepts*.

Si desitgeu configurar el vostre subagent DPI2 o similar smux propi, consulteu els directoris `/usr/samples/snmpd/smux` i `/usr/samples/snmpd/dpi2`.

Claus d'autenticació SNMPv3

L'autenticació normalment és necessària per a què es processin les sol•licituds **SNMPv3** (tret que el nivell de seguretat sol•licitat sigui `noAuth`).

Quan s'autentica una sol•licitud, l'agent **SNMP** verifica que la clau d'autenticació enviada en una sol•licitud **SNMPv3** es pugui utilitzar per crear una conversió de missatge que coincideixi amb la conversió de missatge creada a partir de la clau d'autenticació definida per l'usuari.

Quan s'emet una sol•licitud des del gestor **SNMP**, l'ordre **clsnmp** utilitza la clau d'autenticació que utilitza en una entrada del fitxer `/etc/clsnmp.conf` del gestor **SNMP**. S'ha de correlacionar amb la clau d'autenticació especificada a l'entrada `USM_USER` per l'usuari en qüestió al fitxer `/etc/snmpdv3.conf` de l'agent **SNMP**. Les claus d'autenticació es generen mitjançant l'ordre **pwtokey**.

La clau d'autenticació es genera a partir de dos fragments d'informació:

- La paraula clau especificada
- L'identificació de l'agent **SNMP** on s'utilitzarà la clau. Si l'agent és IBM i el seu engineID s'ha generat mitjançant la fórmula engineID específica de proveïdor, l'agent es podrà identificar mitjançant una adreça IP o un nom d'amfitrió. En cas contrari, l'engineID haurà de proporcionar-se com a identificació d'agent.

La clau que incorpora l'identificació de l'agent on s'utilitzarà s'anomena clau localitzada. Es pot utilitzar només en aquest agent. La clau que no incorpora l'engineID de l'agent on s'utilitzarà s'anomena clau no localitzada.

Les claus emmagatzemades al fitxer de configuració de l'ordre **clsnmp**, `/etc/clsnmp.conf`, normalment són claus no localitzades. Les claus emmagatzemades al fitxer de configuració de l'agent **SNMP**, `/etc/snmpdv3.conf`, poden ser localitzades o no localitzades, encara que és més segur utilitzar claus localitzades.

Com a alternativa a emmagatzemar claus d'autenticació al fitxer de configuració del client, l'ordre **clsnmp** permet a emmagatzemar les paraules clau d'usuari. Si l'ordre **clsnmp** es configura amb una paraula clau, el codi genera una clau d'autenticació (clau privada si se sol•licita i s'instal•la una versió encriptada) per a l'usuari. Aquestes claus han de produir els mateixos valors d'autenticació que les claus configurades per `USM_USER` al fitxer `/etc/snmpdv3.conf` de l'agent o s'han de configurar dinàmicament amb les ordres SET **SNMP**. De tota manera, l'ús de paraules clau al fitxer de configuració del client es considera menys segur que l'us de claus al fitxer de configuració.

Claus de privacitat SNMPv3

L'encriptació està disponible com a producte separat al paquet d'ampliació AIX on ho permeten les lleis d'exportació. Les claus utilitzades per l'encriptació es generen mitjançant els mateixos algorismes que els que s'utilitzen per l'autenticació.

De tota manera, la longitud de les claus pot variar. Per exemple, una clau d'autenticació HMAC-SHA és de 20 octets, però una clau d'encriptació localitzada amb HMAC-SHA té només 16 octets de longitud.

La versió encriptada s'activa automàticament després de l'instal•lació. Per tornar a la versió no encriptada, utilitzeu l'ordre **snmpv3_ssw**.

Claus de generació SNMPv3

AIX utilitza l'ordre **pwtokey** per generar autenticació i, quan s'escau, claus de privacitat.

L'ordre **pwtokey** permet convertir paraules clau en claus d'autenticació i de privadesa localitzades i no localitzades. El procediment **pwtokey** pren una paraula clau i un identificador com a agent i genera claus d'autenticació i de privadesa. Com que el procediment utilitzat per l'ordre **pwtokey** és el mateix algorisme que el que utilitza l'ordre **clsnmp**, la persona que configura l'agent **SNMP** pot generar claus d'autenticació (i privadesa) adients per col•locar-les al fitxer `/etc/clsnmp.conf` del gestor **SNMP** per a un usuari, un cop s'hagi proporcionat una paraula clau particular i l'adreça IP on s'executarà la destinació.

Un cop que hagueu generat les claus d'autenticació (i les claus de privacitat si executeu la versió encriptada), haureu d'especificar les claus al fitxer `/etc/snmpdv3.conf` de l'agent **SNMP** i al fitxer `/etc/clsnmp.conf` del gestor **SNMP**.

A **SNMPv3**, existeixen nou configuracions d'usuari possibles. A continuació, es mostra cadascuna de les configuracions possibles amb un exemple. Aquestes claus particulars s'han generat mitjançant `defaultpassword` per la paraula clau i `9.3.149.49` com a adreça IP. S'ha utilitzat l'ordre següent:

```
pwtokey -u all -p all defaultpassword 9.3.149.49
```

S'han generat les claus d'autenticació i privacitat següents:

```
Display of 16 byte HMAC-MD5 authKey:
  18a2c7b78f3df552367383eef9db2e9f

Display of 16 byte HMAC-MD5 localized authKey:
  a59fa9783c04bcbe00359fb1e181a4b4

Display of 16 byte HMAC-MD5 privKey:
  18a2c7b78f3df552367383eef9db2e9f

Display of 16 byte HMAC-MD5 localized privKey:
  a59fa9783c04bcbe00359fb1e181a4b4

Display of 20 byte HMAC-SHA authKey:
  754ebf6ab740556be9f0930b2a2256ca40e76ef9

Display of 20 byte HMAC-SHA localized authKey:
  cd988a098b4b627a0e8adc24b8f8cd02550463e3

Display of 20 byte HMAC-SHA privKey:
  754ebf6ab740556be9f0930b2a2256ca40e76ef9

Display of 16 byte HMAC-SHA localized privKey:
  cd988a098b4b627a0e8adc24b8f8cd02
```

Aquestes entrades apareixerien al fitxer `/etc/snmpdv3.conf`. Són possibles les nou configuracions següents:

- Claus d'autenticació i privacitat localitzades mitjançant el protocol HMAC-MD5:

  ```
  USM_USER user1 - HMAC-MD5 a59fa9783c04bcbe00359fb1e181a4b4 DES a59fa9783c04bcbe00359fb1e181a4b4 L - -
  ```

- Claus d'autenticació i privacitat no localitzades mitjançant el protocol HMAC-MD5:

  ```
  USM_USER user2 - HMAC-MD5 18a2c7b78f3df552367383eef9db2e9f DES 18a2c7b78f3df552367383eef9db2e9f N  - -
  ```

- Clau d'autenticació localitzada mitjançant el protocol HMAC-MD5:

  ```
  USM_USER user3 - HMAC-MD5 a59fa9783c04bcbe00359fb1e181a4b4 - - L -
  ```

- Clau d'autenticació no localitzada mitjançant el protocol HMAC-MD5:

  ```
  USM_USER user4 - HMAC-MD5 18a2c7b78f3df552367383eef9db2e9f - - N -
  ```

- Claus d'autenticació i privacitat localitzades mitjançant el protocol HMAC-SHA:

  ```
  USM_USER user5 - HMAC-SHA cd988a098b4b627a0e8adc24b8f8cd02550463e3 DES
  cd988a098b4b627a0e8adc24b8f8cd02 L -
  ```

- Claus d'autenticació i privacitat no localitzades mitjançant el protocol HMAC-SHA:
  ```
  USM_USER user6 - HMAC-SHA 754ebf6ab740556be9f0930b2a2256ca40e76ef9 DES
  754ebf6ab740556be9f0930b2a2256ca40e76ef9 N -
  ```
- Clau d'autenticació localitzada mitjançant el protocol HMAC-SHA:
  ```
  USM_USER user7 - HMAC-SHA cd988a098b4b627a0e8adc24b8f8cd02550463e3 - - L -
  ```
- Clau d'autenticació no localitzada mitjançant el protocol HMAC-SHA:
  ```
  USM_USER user8 - HMAC-SHA 754ebf6ab740556be9f0930b2a2256ca40e76ef9 - - N -
  ```
- No s'utilitza cap clau d'autenticació ni de privacitat (**SNMPv1**)
  ```
  USM_USER user9 - none - none - - -
  ```

La configuració d'usuaris a **SNMPv3** requereix la configuració del fitxers `/etc/snmpdv3.conf` i `/etc/clsnmp.conf`. Per veure un cas en el qual es generen claus d'usuari i s'editen fitxers de configuració necessaris, consulteu "Creació d'usuaris a l'SNMPv3" a la pàgina 483. A més, vegeu l'ordre **pwtokey** que apareix a *Commands Reference, Volume 4* i l'odre **clsnmp** que apareix a *Commands Reference, Volume 1*, així com els formats de fitxer del fitxer `/etc/clsnmp.conf` i el fitxer `/etc/snmpdv3.conf` que apareixen a *Files Reference*. També podeu consultar el fitxer de configuració `snmpdv3.conf` d'exemple i el fitxer de configuració `clsnmp.conf` que es troba al directori `/usr/samples/snmpdv3`.

Actualització de claus mitjançant SNMPv3

SNMPv3 permet actualitzar claus d'usuari basades en paraules clau noves de forma dinàmica.

Això es realitza utilitzant l'ordre **pwchange** per generar claus d'usuari noves en una paraula clau actualitzada, mitjançant l'ordre **clsnmp** per actualitzar de forma dinàmica la clau d'usuari al fitxer `/etc/snmpdv3.conf` i editant el fitxer `/etc/clsnmp.conf` amb les claus noves. Durant el procés, no es comunica la nova paraula clau entre les màquines.

Per obtenir instruccions detallades sobre l'actualització de claus d'usuari, consulteu "Actualització dinàmica de les claus d'autenticació i privadesa a l'SNMPv3". A més, vegeu l'ordre **pwchange** que apareix a *Commands Reference, Volume 4* i l'ordre **clsnmp** que apareix a *Commands Reference, Volume 1*, així com els formats de fitxer del fitxer `/etc/clsnmp.conf` i el fitxer `/etc/snmpdv3.conf` que apareixen a *Files Reference*.

Actualització dinàmica de les claus d'autenticació i privadesa a l'SNMPv3

En aquest escenari es mostra com s'actualitzen dinàmicament les claus d'autenticació per a un usuari a l'**SNMPv3**.

En aquest escenari, l'usuari `u4` actualitzarà les claus d'autenticació per a l'usuari `u8`. Tant l'usuari `u4` com l'usuari `u8` ja tenen creades claus d'autenticació basades en la contrasenya `contrasenya_per_defecte` i l'adreça IP `9.3.149.49`, i tot funciona perfectament.

Durant aquest escenari, es crearan noves claus per a l'usuari `u8` i el fitxer `/etc/snmpdv3.conf` s'actualitzarà dinàmicament. A continuació, caldrà editar manualment la clau d'autenticació de l'usuari `u8` al fitxer `/etc/clsnmp.conf` del gestor per deixar constància de les noves claus.

Abans d'iniciar aquest procediment, feu una còpia de seguretat del fitxer `/etc/snmpdv3.conf` a l'agent **SNMP** i una còpia de seguretat del fitxer `/etc/clsnmp.conf` al gestor **SNMP**.

A continuació es mostra el fitxer `/etc/snmpdv3.conf` que s'actualitzarà dinàmicament:

```
USM_USER u4 - HMAC-MD5 18a2c7b78f3df552367383eef9db2e9f - - N -
USM_USER u8 - HMAC-SHA 754ebf6ab740556be9f0930b2a2256ca40e76ef9 - - N -

VACM_GROUP group1 SNMPv1 public -
VACM_GROUP group2 USM u4 -
VACM_GROUP group2 USM u8 -

VACM_VIEW defaultView        internet                  - included -
```

```
VACM_ACCESS  group1 - - noAuthNoPriv SNMPv1  defaultView - defaultView -
VACM_ACCESS  group2 - - noAuthNoPriv USM defaultView defaultView defaultView -
VACM_ACCESS  group2 - - AuthNoPriv USM defaultView defaultView defaultView -
VACM_ACCESS  group2 - - AuthPriv USM defaultView defaultView defaultView -

NOTIFY notify1 traptag trap -

TARGET_ADDRESS Target1 UDP 127.0.0.1       traptag trapparms1 - - -
TARGET_ADDRESS Target2 UDP 9.3.149.49       traptag trapparms2 - - -
TARGET_ADDRESS Target3 UDP 9.3.149.49       traptag trapparms3 - - -
TARGET_ADDRESS Target4 UDP 9.3.149.49       traptag trapparms4 - - -

TARGET_PARAMETERS trapparms1 SNMPv1  SNMPv1  public  noAuthNoPriv -
TARGET_PARAMETERS trapparms3 SNMPv2c  SNMPv2c  publicv2c  noAuthNoPriv -
TARGET_PARAMETERS trapparms4 SNMPv3  USM     u4 AuthNoPriv -
```

Below is the `/etc/clsnmp.conf` file that will be updated for user `u8`:

```
testu4 9.3.149.49 snmpv3 u4 - - AuthNoPriv HMAC-MD5 18a2c7b78f3df552367383eef9db2e9f - -
testu8 9.3.149.49 snmpv3 u8 - - AuthNoPriv HMAC-SHA 754ebf6ab740556be9f0930b2a2256ca40e76ef9 - -
```

Informació que cal tenir en compte

- La informació d'aquest cas s'ha provat amb versions específiques de l'AIX. Els resultats obtinguts poden variar força segons la versió i el nivell de l'AIX.

Actualització de la contrasenya i de les claus d'autenticació

Els noms de les comunitats al fitxer `/etc/snmpd.conf` es converteixen en part de les entrades de `VACM_GROUP` al fitxer `/etc/snmpdv3.conf`. Cada comunitat s'ha de col•locar en un grup. A continuació es proporcionen als grups els permisos de visualització i d'accés que necessitin.

1. Al gestor d'**SNMP**, executeu l'ordre **pwchange**. En aquest escenari hem executat l'ordre següent:

   ```
   pwchange -u auth -p HMAC-SHA contrasenya_per_defecte contrasenya_nova 9.3.149.49
   ```

   Aquesta ordre generarà una clau d'autenticació nova.

   - `-u auth` especifica que només es crearà una clau d'autenticació. Si també actualitzeu les claus de privadesa, utilitzeu `-u all`.
   - `-p HMAC-SHA` especifica el protocol que s'utilitzarà per crear la clau d'autenticació. Si també actualitzeu les claus de privadesa, utilitzeu `-p all`.
   - *`contrasenya_per_defecte`* és la contrasenya utilitzada per crear l'última clau d'autenticació (per exemple, si `bluepen` es va utilitzar per crear l'última clau d'autenticació, `bluepen` també s'utilitzarà aquí.
   - *`contrasenya_nova`* és la nova contrasenya que s'utilitzarà per generar la clau d'autenticació. Conserveu aquesta contrasenya per a futures ocasions.
   - `9.3.149.49` és l'adreça IP on s'està executant l'agent **SNMP**.

   Aquesta ordre ha generat la sortida següent:

   ```
   Dump of 40 byte HMAC-SHA authKey keyChange value:
     8173701d7c00913af002a3379d4b150a
     f9566f56a4dbde21dd778bb166a86249
     4aa3a477e3b96e7d
   ```

   Aquesta clau d'autenticació s'utilitzarà al següent pas.

   Nota: Deseu les contrasenyes que utilitzeu en un indret segur. les haureu de tornar a utilitzar quan feu canvis en el futur.

2. Al gestor d'**SNMP**, l'usuari `u4` utilitzarà l'ordre següent per canviar la clau d'autenticació per a l'usuari `u8`:

```
clsnmp -h testu4 set usmUserAuthKeyChange.12.0.0.0.2.0.0.0.0.9.3.149.49.2.117.56
 \'8173701d7c00913af002a3379d4b150af9566f56a4dbde21dd778bb166a862494aa3a477e3b96e7d\'h
```

- testu4 s'utilitza perquè està assignat a l'usuari u4 al fitxer /etc/clsnmp.conf.
- L'identificador de la instància d'*usmUserAuthKeyChange* inclou, en valors decimals, l'identificador del motor de l'agent SNMP on té lloc l'actualització i el nom d'usuari la clau d'autenticació del qual s'està actualitzant. L'identificador del motor es pot trobar al fitxer /etc/snmpd.boots (el fitxer /etc/snmpd.boots conté dues cadenes de números. L'identificador del motor és la primera. Passeu per alt la segona cadena de números).

  L'identificador del motor s'haurà de convertir de valors hexadecimals a valors decimals per poder-lo utilitzar aquí. Cada dos números de l'identificador del motor hexadecimal es converteixen en un valor decimal. Per exemple, l'identificador del motor 000000020000000009039531 es llegirà com a 00 00 00 02 00 00 00 00 09 03 95 31. Cadascun d'aquests números s'ha de convertir en valors decimals, resultant en 0.0.0.2.0.0.0.0.9.3.149.49 (per veure una taula de conversió, consulteu taula de conversió ASCII, decimal, hexadecimal, octal i binària.). El primer número de la cadena és el número d'octets de la cadena decimal. En aquest cas és 12 i el resultat obtingut és 12.0.0.0.2.0.0.0.0.9.3.149.49.

  El número següent és el número d'octets del nom d'usuari, seguit pels valors decimals del propi nom d'usuari. En aquest cas, el nom d'usuari és u8. Quan es converteix a valors decimals, u8 es converteix en 117.56. Atès que el nom d'usuari té 2 octets de longitud, el valor que representa els noms d'usuari es converteix en 2.117.56. Afegiu això al final de l'identificador de motor decimal (per veure una taula de conversió, consulteu taula de conversió ASCII, decimal, hexadecimal, octal i binària.).

  En aquest cas, el resultat és 12.0.0.0.2.0.0.0.0.9.3.149.49.2.117.56.
- El següent valor de l'ordre és la nova clau d'autenticació generada mitjançant l'ordre **pwchange** en el pas anterior.

  Nota: Si aquest usuari també té configurades claus de privadesa, aquest procediment s'ha de repetir per actualitzar les claus de privadesa. Quan actualitzeu les claus de privadesa, utilitzeu el valor usmUserPrivKeyChange en lloc del valor usmUserAuthKeyChange.

  L'ús d'usmUserOwnAuthKeyChange en comptes d'usmUserAuthKeyChange permetrà que un usuari pugui canviar la clau d'autenticació pròpia. Per exemple, l'usuari u4 pot canviar la seva pròpia clau d'autenticació mitjançant usmUserOwnAuthKeyChange.

La sortida de l'ordre és la següent:

```
1.3.6.1.6.3.15.1.2.2.1.6.12.0.0.0.2.0.0.0.0.9.3.149.49.2.117.56 = '8173701d7c00913af002a3379
d4b150af9566f56a4dbde21dd778bb166a862494aa3a477e3b96e7d'h
```

Un cop executada aquesta ordre, el fitxer /etc/snmpdv3.conf s'actualitzarà automàticament al cap de cinc minuts a l'agent **SNMP**. Per actualitzar el fitxer, també podeu aturar i iniciar el dimoni **SNMP**. L'entrada següent de l'usuari u8 s'actualitzarà dinàmicament al fitxer /etc/snmpdv3.conf:

```
USM_USER u8 000000020000000009039531 HMAC-SHA 4be657b3ae92beee322ee5eaeef665b338caf2d9
None - L nonVolatile
```

3. Al gestor d'**SNMP**, executeu l'ordre **pwtokey** per generar la clau d'autenticació nova basada en la contrasenya nova que es col•loca al fitxer /etc/clsnmp.conf. En aquest escenari hem executat l'ordre següent:

   ```
   pwtokey -u auth -p HMAC-SHA  contrasenya_nova 9.3.149.49
   ```

   - -u auth especifica que només es crearà una clau d'autenticació. Si també actualitzeu les claus de privadesa, utilitzeu -u all.
   - -p HMAC-SHA especifica el protocol que s'utilitzarà per crear la clau d'autenticació. Si també actualitzeu les claus de privadesa, utilitzeu -p all.
   - La contrasenya utilitzada (en aquest cas *contrasenya_nova*) ha de ser la mateixa que la contrasenya emprada per generar les noves claus d'autenticació amb l'ordre **pwchange**.
   - L'adreça IP utilitzada (en aquest cas 9.3.149.49) ha de ser l'adreça IP on s'està executant l'agent

   El resultat proporciona les claus d'autenticació localitzades i no localitzades.

```
Display of 20 byte HMAC-SHA authKey:
  79ce23370c820332a7f2c7840c3439d12826c10d

Display of 20 byte HMAC-SHA localized authKey:
  b07086b278163a4b873aace53a1a9ca250913f91
```

4. Obriu el fitxer `/etc/clsnmp.conf` amb l'editor de textos que vulgueu i col•loqueu la clau d'autenticació no localitzada a la línia de l'usuari les claus del qual s'estan actualitzant. En aquest escenari, l'entrada és la següent:

   ```
   testu8 9.3.149.49 snmpv3 u8 - - AuthNoPriv HMAC-SHA 79ce23370c820332a7f2c7840c3439d12826c10d - -
   ```

   Deseu i tanqueu el fitxer.

5. Executeu l'ordre següent per provar la configuració actualitzada:

   ```
   clsnmp -v -h testu8 walk mib
   ```

   en què *mib* és la variable MIB per a la qual l'usuari `u8` té accés de lectura. En aquest cas, l'usuari `u8` té accés a `internet`.

Sol•licituds SNMPv3

L'ordre **clsnmp** s'utilitza per enviar sol•licituds **SNMP** a agents **SNMP** a amfitrions locals o remots.

Les sol•licituds poden ser **SNMPv1**, **SNMPv2c** o **SNMPv3**. Per processar sol•licituds, s'ha de configurar el fitxer `/etc/clsnmp.conf`.

L'ordre **clsnmp** pot emetre sol•licituds get, getnext, getbulk, set, walk i findname. Cadascuna d'aquestes sol•licituds es descriu breument a continuació:

get permet a l'usuari recopilar dades d'una variable MIB.

getnext
proporciona la variable MIB següent al subarbre MIB.

getbulk
proporciona totes les variables MIB de múltiples subarbres MIB.

set permet a l'usuari establir una variable MIB.

walk proporciona totes les variables MIB d'un subarbre.

findname
correlaciona l'OID amb el nom de variable.

trap permet a **clsnmp** escoltar els errors trap al port 162.

Per obtenir informació detallada sobre com s'emeten sol•licituds **clsnmp**, consulteu l'ordre **clsnmp** a *Commands Reference, Volume 1*.

Migració d'SNMPv1 a SNMPv3

Aquest escenari mostra una típica migració d'**SNMPv1** a **SNMPv3**.

En el sistema operatiu AIX, l'agent d'**SNMP** per defecte que s'executa en iniciar el sistema és la versió no xifrada de la versió d'**SNMPv3**. **SNMPv3** utilitza el fitxer `/etc/snmpdv3.conf` com a fitxer de configuració. Qualsevol paràmetre que hagueu configurat al fitxer `/etc/snmpd.conf`, que l'**SNMPv1** utilitza en versions anteriors de l'AIX s'haurà de migrar manualment al fitxer `/etc/snmpdv3.conf`.

En aquest escenari, les comunitats i els traps configurats al fitxer `/etc/snmpd.conf` es migraran al fitxer `/etc/snmpdv3.conf`. En acabar l'escenari, l'**SNMPv3** proporcionarà una funcionalitat idèntica a la proporcionada per l'**SNMPv1**. Si no heu configurat cap de les vostres comunitats o traps propis de l'**SNMPv1**, no cal que completeu aquest procediment.

Aquest fitxer no conté cap informació sobre les característiques disponibles a l'**SNMPv3**. Per obtenir informació sobre la creació d'usuaris mitjançant les característiques de l'**SNMPv3** no disponibles a l'**SNMPv1**, consulteu “Creació d'usuaris a l'SNMPv3” a la pàgina 483.

El fitxer següent és un exemple de fitxer `/etc/snmpd.conf` que es migrarà. Hi ha configurades les comunitats següents: `daniel`, `vasu` i `david`. Aquestes comunitats s'han de migrar manualment.

```
logging         file=/usr/tmp/snmpd.log         enabled
logging         size=0                          level=0

community       daniel       0.0.0.0     0.0.0.0         readWrite  1.17.35
community       vasu         9.3.149.49  255.255.255.255 readOnly   10.3.5
community       david        9.53.150.67 255.255.255.255 readWrite  1.17.35

view 1.17.35    udp  icmp  snmp 1.3.6.1.2.1.25
view 10.3.5     system interfaces tcp icmp

trap            daniel          9.3.149.49      1.17.35   fe
trap            vasu            9.3.149.49      10.3.5   fe
trap            david           9.53.150.67     1.17.35   fe

smux            1.3.6.1.4.1.2.3.1.2.3.1.1         sampled_password  # sampled
```

Per completar els passos d'aquest escenari, consulteu el fitxer `/etc/snmpd.conf`. Quan comenceu aquest procediment, tingueu a punt una còpia d'aquest fitxer.

Informació que cal tenir en compte

- La informació d'aquest cas s'ha provat amb versions específiques de l'AIX. Els resultats obtinguts poden variar força segons la versió i el nivell de l'AIX.

Pas 1. Migració de la informació de la comunitat

Els noms de les comunitats al fitxer `/etc/snmpd.conf` es converteixen en part de les entrades de `VACM_GROUP` al fitxer `/etc/snmpdv3.conf`. Cada comunitat s'ha de col•locar en un grup. A continuació es proporcionen als grups els permisos de visualització i d'accés que necessitin.

1. Amb autoritat root, obriu el fitxer `/etc/snmpdv3.conf` amb l'editor de textos que vulgueu. localitzeu les entrades `VACM_GROUP` al fitxer.
2. Creeu una entrada `VACM_GROUP` per a cada comunitat que vulgueu migrar. Si diverses comunitats compartiran els mateixos permisos de visualització i d'accés, només haureu de crear un grup per a totes elles. Els noms de les comunitats del fitxer `/etc/snmpd.conf` es converteixen en els valors *securityName* de les entrades `VACM_GROUP`. En aquest escenari, les entrades següents s'han afegit per a `vasu`, `daniel` i `david`:

   ```
   #-------------------------------------------------------------------
   # VACM_GROUP entries
   #    Defines a security group (made up of users or communities)
   #    for the View-based Access Control Model (VACM).
   # Format is:
   #  groupName securityModel securityName storageType
   VACM_GROUP group2 SNMPv1  vasu -
   VACM_GROUP group3 SNMPv1  daniel -
   VACM_GROUP group3 SNMPv1  david -
   #-------------------------------------------------------------------
   ```

   - *groupName* pot ser qualsevol valor que trieu, excepte `group1`.
   - *securityModel* es manté com `SNMPv1` perquè estem migrant les comunitats SNMPv1.
   - En aquest escenari, `daniel` i `david` comparteixen els mateixos permisos de visualització i d'accés al fitxer `/etc/snmpd.conf`. Per tant, tots dos són membres de `group3` al fitxer `/etc/snmpdv3.conf`. La comunitat `vasu` està ubicada en un grup diferent perquè els seus permisos de visualització i d'accés són diferents als de `david` i `daniel`.

   Les comunitats es col•loquen ara en grups.

Pas 2. Migració de la informació de visualització

La informació de visualització al fitxer /etc/snmpd.conf es convertirà en entrades COMMUNITY, VACM_VIEW, i VACM_ACCESS al fitxer /etc/snmpdv3.conf. Aquestes entrades determinaran els permisos de visualització i d'accés de cada grup.

1. Creeu entrades COMMUNITY per a daniel, vasu, i david, mantenint les mateixes adreces IP per a netAddr i netMask que s'han especificat al fitxer /etc/snmpd.conf.

```
#--------------------------------------------------------------------
# COMMUNITY
#    Defines a community for community-based security.
# Format is:
#  communityName securityName securityLevel netAddr netMask storageType
COMMUNITY public    public     noAuthNoPriv 0.0.0.0     0.0.0.0         -
COMMUNITY daniel    daniel     noAuthNoPriv 0.0.0.0     0.0.0.0         -
COMMUNITY vasu      vasu       noAuthNoPriv 9.3.149.49  255.255.255.255 -
COMMUNITY david     david      noAuthNoPriv 9.53.150.67 255.255.255.255 -
#--------------------------------------------------------------------
```

2. Creeu una entrada VACM_VIEW per a cada variable o objecte MIB al qual tingui accés cada grup. Segons el fitxer /etc/snmpd.conf, daniel i david tenen accés a udp, icmp, snmp, i 1.3.6.1.2.1.25 (subarbre d'amfitrions tal com està definit a l'RFC 1514), i vasu té accés a system, interfaces, tcp, i icmp. Aquestes entrades de visualització es migren al fitxer /etc/snmpdv3.conf de la següent manera:

```
#--------------------------------------------------------------------
# VACM_VIEW entries
#    Defines a particular set of MIB data, called a view, for the
#    View-based Access Control Model.
# Format is:
#  viewName viewSubtree viewMask viewType storageType

VACM_VIEW group2View        system                    - included -
VACM_VIEW group2View        interfaces                - included -
VACM_VIEW group2View        tcp                       - included -
VACM_VIEW group2View        icmp                      - included -

VACM_VIEW group3View        udp                       - included -
VACM_VIEW group3View        icmp                      - included -
VACM_VIEW group3View        snmp                      - included -
VACM_VIEW group3View        1.3.6.1.2.1.25            - included -
#--------------------------------------------------------------------
```

3. Defineix els permisos d'accés a les variables MIB definides a les entrades VACM_VIEW afegint entrades VACM_ACCESS. Al fitxer /etc/snmpd.conf, daniel i david tenen permís readWrite a les variables MIB, mentre que vasu té readOnly.

   Per definir aquests permisos, afegiu entrades VACM_ACCESS. En aquest escenari, hem assignat a group2 (vasu) group2View per a readView, però li hem assignat - per a writeView perquè vasu tenia readOnly al fitxer /etc/snmpd.conf. Hem assignat a group3 (daniel i david) group3View tant per a readView com per a writeView perquè aquests grups tenien accés readWrite a /etc/snmpd.conf. Vegeu l'exemple següent.

```
#-----------------------------------------------------------------------------------------------------------
# VACM_ACCESS entries
#    Identifies the access permitted to different security groups
#    for the View-based Access Control Model.
# Format is:
# groupName contextPrefix contextMatch securityLevel securityModel readView writeView notifyView storageType
VACM_ACCESS  group1 - - noAuthNoPriv SNMPv1  defaultView - defaultView -
VACM_ACCESS  group2 - - noAuthNoPriv SNMPv1  group2View - group2View -
VACM_ACCESS  group3 - - noAuthNoPriv SNMPv1  group3View group3View group3View -
#-----------------------------------------------------------------------------------------------------------
```

Pas 3. Migració de la informació trap

Les entrades trap al fitxer /etc/snmpd.conf es convertiran en entrades NOTIFY, TARGET_ADDRESS, i TARGET_PARAMETERS al fitxer /etc/snmpdv3.conf. Tanmateix, només serà necessari migrar TARGET_ADDRESS i TARGET_PARAMETERS.

1. Les adreces IP enumerades a les entrades trap al fitxer /etc/snmpd.conf es converteixen en part de les entrades TARGET_ADDRESS del fitxer /etc/snmpdv3.conf. Aquesta línia especifica l'amfitrió al qual s'enviarà el trap. Podeu definit les entrades targetParams. En aquest escenari, utilitzem trapparms1, trapparms2, trapparms3, i trapparms4, que es definiran a les entrades TARGET_PARAMETERS.

```
#--------------------------------------------------------------------------------
# TARGET_ADDRESS
#    Defines a management application's address and parameters
#    to be used in sending  notifications.
# Format is:
#  targetAddrName tDomain tAddress tagList targetParams timeout retryCount storageType
TARGET_ADDRESS Target1 UDP 127.0.0.1    traptag trapparms1 - - -
TARGET_ADDRESS Target2 UDP 9.3.149.49   traptag trapparms2 - - -
TARGET_ADDRESS Target3 UDP 9.3.149.49   traptag trapparms3 - - -
TARGET_ADDRESS Target4 UDP 9.53.150.67  traptag trapparms4 - - -
#--------------------------------------------------------------------------------
```

2. Els noms de comunitat especificats a les entrades trap del fitxer /etc/snmpd.conf es converteixen en part de les entrades TARGET_PARAMETERS del fitxer /etc/snmpdv3.conf. Els noms de comunitat s'han d'assignar a una entrada TARGET_ADDRESS específica per mitjà dels valors targetParams. Per exemple, la comunitat daniel està assignada amb trapparms2 que, sota l'entrada TARGET_ADDRESS, s'assigna a l'adreça IP 9.3.149.49. La comunitat daniel i l'adreça IP 9.3.149.49 eren originalment una entrada trap del fitxer /etc/snmpd.conf. Vegeu l'exemple següent:

```
#--------------------------------------------------------------------------
# TARGET_PARAMETERS
#    Defines the message processing and security parameters
#    to be used in sending notifications to a particular management target.
# Format is:
#  paramsName mpModel securityModel securityName securityLevel storageType
TARGET_PARAMETERS trapparms1 SNMPv1  SNMPv1  public  noAuthNoPriv -
TARGET_PARAMETERS trapparms2 SNMPv1  SNMPv1  daniel  noAuthNoPriv -
TARGET_PARAMETERS trapparms3 SNMPv1  SNMPv1  vasu    noAuthNoPriv -
TARGET_PARAMETERS trapparms4 SNMPv1  SNMPv1  david   noAuthNoPriv -
#--------------------------------------------------------------------------
```

3. La informació trapmask del fitxer /etc/snmpd.conf no es migra al fitxer /etc/snmpdv3.conf.

Pas 4. Migració de la informació smux

Si teniu informació smux que heu de migrar, podeu copiar aquestes línies directament al fitxer nou. En aquest escenari, l'entrada smux sampled estava configurada al fitxer /etc/snmpd.conf. Aquesta línia s'ha de copiar al fitxer /etc/snmpdv3.conf.

```
#-------------------------------------------------------------------------------------------
#       smux <client OIdentifier> <password> <address> <netmask>
smux            1.3.6.1.4.1.2.3.1.2.3.1.1         sampled_password  # sampled
#-------------------------------------------------------------------------------------------
```

Pas 5. Aturada i inici del dimoni snmpd

Quan la la migració del fitxer /etc/snmpd.conf al fitxer /etc/snmpdv3.conf s'hagi completat, atureu i inicieu el dimoni **snmpd**. Haureu d'aturar i iniciar el dimoni **snmpd** cada vegada que feu canvis al fitxer /etc/snmpdv3.conf.

1. Escriviu l'ordre següent per aturar el dimoni:

```
stopsrc -s snmpd
```

2. Escriviu l'ordre següent per reiniciar el dimoni:

```
startsrc -s snmpd
```

Nota: La simple actualització de l'agent de l'**SNMPv3** no funcionarà com ho feia a l'**SNMPv1**. Si feu algun canvi al fitxer `/etc/snmpdv3.conf`, heu d'aturar i iniciar el dimoni tal com s'ha explicat més amunt. La funció de configuració dinàmica admesa a l'**SNMPv3** no us permetrà fer l'actualització.

Creació d'usuaris a l'SNMPv3

Aquest escenari mostra com es crea un usuari a l'SNMPv3 manualment per mitjà de l'edició dels fitxers `/etc/snmpdv3.conf` i `/etc/clsnmp.conf`.

En aquest escenari es crearà l'usuari `u1`. A l'usuari `u1` se li atorgaran claus d'autorització, però cap clau de privadesa (que només estan disponibles si el catàleg de fitxers `snmp.crypto` està instal•lat). El protocol HMAC-MD5 s'utilitzarà per crear les claus d'autorització de l'usuari u1. Quan l'usuari u1 ja està configurat, es posarà en un grup i, després, es definiran els permisos d'accés i de visualització d'aquest grup. Finalment, es crearan les entrades trap per a u1.

Cadascun dels valors utilitzats als fitxers `/etc/snmpdv3.conf` i `/etc/clsnmp.conf` no pot superar els 32 octets.

Informació que cal tenir en compte

- La informació d'aquest cas s'ha provat amb versions específiques de l'AIX. Els resultats obtinguts poden variar força segons la versió i el nivell de l'AIX.

Pas 1. Creació de l'usuari

1. Decidiu quins protocols de seguretat voleu utilitzar, HMAC-MD5 o HMAC-SHA. En aquest escenari, s'utilitzarà HMAC-MD5.
2. Genereu les claus d'autenticació mitjançant l'ordre `pwtokey`. La vostra sortida tindrà un aspecte diferent en funció del protocol d'autenticació que utilitzeu i si feu servir claus de privadesa. Aquestes claus s'utilitzaran als fitxers `/etc/snmpdv3.conf` i `/etc/clsnmp.conf`. A continuació es mostra l'ordre utilitzada per a l'usuari `u1`:

   ```
   pwtokey -p HMAC-MD5 -u auth qualsevol_contrasenya 9.3.230.119
   ```

   L'adreça IP especificada és l'adreça IP on s'està executant l'agent. La contrasenya pot ser qualsevol contrasenya, però assegureu-vos de desar-la en un lloc segur per a futures ocasions. La sortida se semblarà a la següent:

   ```
   Display of 16 byte HMAC-MD5 authKey:
     63960c12520dc8829d27f7fbaf5a0470

   Display of 16 byte HMAC-MD5 localized authKey:
     b3b6c6306d67e9c6f8e7e664a47ef9a0
   ```
3. Amb autoritat root, obriu el fitxer `/etc/snmpdv3.conf` amb l'editor de textos que vulgueu.
4. Per crear un usuari, afegiu una entrada `USM_USER` amb el format especificat al fitxer. El valor *authKey* serà la clau d'autenticació localitzada generada amb l'ordre **pwtokey**. A continuació es mostra l'entrada de l'usuari `u1`:

   ```
   #-------------------------------------------------------------------------
   # USM_USER entries
   #    Defines a user for the User-based Security Model (USM).
   # Format is:
   #  userName engineID authProto authKey privProto privKey keyType storageType
   #
   USM_USER u1 - HMAC-MD5 b3b6c6306d67e9c6f8e7e664a47ef9a0 - - L -
   #-------------------------------------------------------------------------
   ```

   - *userName* és el nom de l'usuari. En aquest cas, és `u1`.
   - *authProto* ha de ser el protocol que heu utilitzat per crear les claus. En aquest cas, és `HMAC-MD5`.
   - *authKey* és la clau d'autenticació localitzada creada per mitjà de l'ordre **pwtokey**.
   - *privProto* i *privkey* no s'han especificat perquè en aquest escenari no es fan servir claus de privadesa.

- *keyType* és L perquè s'utilitza una clau d'autenticació localitzada.

5. Deseu i tanqueu el fitxer /etc/snmpdv3.conf.
6. Obriu el fitxer /etc/clsnmp.conf al gestor d'SNMP amb l'editor de textos que vulgueu.
7. Afegiu l'usuari nou segons el format especificat al fitxer. A continuació es mostra l'entrada de u1:

```
#--------------------------------------------------------------------------------------------------
#
# Format of entries:
# winSnmpName targetAgent admin secName password context secLevel authProto authKey privProto privKey
#
user1  9.3.230.119  SNMPv3  u1  -  -  AuthNoPriv  HMAC-MD5  63960c12520dc8829d27f7fbaf5a0470  -  -
#--------------------------------------------------------------------------------------------------
```

   - *winSnmpName* pot ser qualsevol valor. Aquest valor s'utilitzarà quan es facin sol•licituds d'SNMP per mitjà de l'ordre **clsnmp**.
   - *targetAgent* és l'adreça IP on s'executa l'agent i que també s'ha utilitzat per crear les claus d'autenticació.
   - *admin* s'estableix en SNMPv3 perquè s'enviaran sol•licituds SNMPv3.
   - *secName* és el nom de l'usuari que esteu creant. En aquest cas, és u1.
   - *seclevel* s'estableix en AuthNoPriv perquè s'està configurant per utilitzar l'autenticació però no la privadesa (en conseqüència, no hi ha valors per a *privProto* i *privKey*).
   - *authproto* s'estableix en el protocol d'autenticació que s'ha utilitzat per crear les claus d'autenticació.
   - *authKey* és la clau no localitzada generada per l'ordre **pwtokey**.

8. Deseu i tanqueu el fitxer /etc/clsnmp.conf.

Pas 2. Configuració del grup

L'usuari s'ha de col•locar ara en un grup. Si ja teniu un grup que està configurat amb tots els permisos de visualització i d'accés que voleu atorgar a aquest usuari, podeu col•locar aquest usuari en aquest grup. Si voleu atorgar a aquest usuari permisos de visualització i d'accés que cap altre grup té, o si no teniu cap grup configurat, creeu un grup i afegiu-hi aquest usuari.

Per afegir l'usuari a un grup nou, creeu una entrada VACM_GROUP nova al fitxer /etc/snmpdv3.conf. A continuació es mostra l'entrada de l'usuari u1:

```
#-------------------------------------------------------------
# VACM_GROUP entries
#    Defines a security group (made up of users or communities)
#    for the View-based Access Control Model (VACM).
# Format is:
#  groupName securityModel securityName storageType
VACM_GROUP group1 USM u1 -
#-------------------------------------------------------------
```

- *groupName* pot ser qualsevol nom. Es converteix en el nom del grup. En aquest cas, és group1.
- *securityModel* s'estableix en USM, que es beneficia dels avantatges de les característiques de seguretat d'SNMPv3.
- *securityName* és el nom de l'usuari. En aquest cas, és u1.

Pas 3. Configuració dels permisos de visualització i d'accés

Els permisos de visualització i d'accés s'han d'establir per al grup nou que s'acaba de crear. Aquests permisos s'estableixen afegint les entrades VACM_VIEW i VACM_ACCESS al fitxer /etc/snmpdv3.conf.

1. Decidiu quins permisos de visualització i d'accés voleu atorgar a aquest grup nou.
2. Afegiu entrades VACM_VIEW al fitxer /etc/snmpdv3.conf per definir a quins objectes MIB pot accedir al grup. En aquest escenari, group1 tindrà accés als subarbres MIB interfaces, tcp, icmp, i system. Tanmateix, restringirem l'accés de group1 a la variable MIB sysObjectID dins del subarbre MIB del sistema.

```
#-----------------------------------------------------------------
# VACM_VIEW entries
#    Defines a particular set of MIB data, called a view, for the
#    View-based Access Control Model.
# Format is:
#  viewName viewSubtree viewMask viewType storageType
VACM_VIEW group1View  interfaces    - included -
VACM_VIEW group1View  tcp        - included -
VACM_VIEW group1View  icmp        - included -
VACM_VIEW group1View  system     - included -
VACM_VIEW group1View  sysObjectID    - excluded -
#-----------------------------------------------------------------
```

- *viewName* és el nom de la visualització. En aquest escenari, és group1View.
- *viewSubtree* és el subarbre MIB al qual voleu donar accés.
- *viewType* determina si els subarbres MIB definits s'inclouen a la visualització. En aquest cas, tots els subarbres estan inclosos, però la variable MIB sysObjectID, que forma part del subarbre system, s'exclou.

3. Afegiu l'entrada VACM_ACCESS al fitxer /etc/snmpdv3.conf per definir els permisos que el grup té als objectes MIB especificats més amunt. Per a group1, s'atorga accés de només de lectura.

```
#-----------------------------------------------------------------------------------------------------------
# VACM_ACCESS entries
#    Identifies the access permitted to different security groups
#    for the View-based Access Control Model.
# Format is:
# groupName contextPrefix contextMatch securityLevel securityModel readView writeView notifyView storageType
VACM_ACCESS  group1 - - AuthNoPriv USM group1View - group1View -
#-----------------------------------------------------------------------------------------------------------
```

- *groupName* és el nom del grup. En aquest cas, és group1.
- *securityLevel* és el nivell de seguretat que s'està utilitzant. En aquest escenari, s'utilitzen claus d'autenticació, però no claus de privadesa. Per tant, el valor s'estableix en AuthNoPriv.
- *securityModel* és el model de seguretat que esteu fent servir (SNMPv1, SNMPv2c o USM). En aquest escenari, està establert en USM per permetre l'ús de les característiques de seguretat d'SNMPv3.
- *readView* determina a quins VACM_VIEW té accés de lectura el grup. En aquest escenari, s'especifica group1View, que atorga a group1 accés de lectura a les entrades group1View VACM_VIEW.
- *writeView* determina a quins VACM_VIEW té accés d'escriptura el grup. En aquest escenari, no s'assigna cap accés d'escriptura a group1.
- *notifyView* especifica el nom de la visualització que s'aplicarà quan es realitzi un trap sota el control de l'entrada a la taula d'accés.

Nota: En alguns casos, poden ser necessàries diverses entrades VACM_ACCESS per a un grup. Si els usuaris del grup tenen una configuració d'autenticació i de privadesa diferent (noAuthNoPriv, AuthNoPriv o AuthPriv), es necessitaran diverses entrades VACM_ACCESS amb el paràmetre securityLevel establert en conseqüència.

Pas 4. Configuració d'entrades trap per a l'usuari

Les entrades trap a l'SNMPv3 es creen afegint entrades NOTIFY, TARGET_ADDRESS i TARGET_PARAMETERS al fitxer /etc/snmpdv3.conf. L'entrada TARGET_ADDRESS especificarà on voleu que s'enviïn els traps, i l'entrada TARGET_PARAMETERS maparà la informació TARGET_ADDRESS amb group1.

L'entrada NOTIFY s'ha configurat per defecte. A continuació es mostra l'entrada NOTIFY per defecte:

```
NOTIFY notify1 traptag trap -
```

En aquest escenari, utilitzem el valor que està especificat a l'entrada per defecte, traptag.

1. Afegiu l'entrada TARGET_ADDRESS per especificar on voleu que s'enviïn els traps.

```
#--------------------------------------------------------------------------------
# TARGET_ADDRESS
#    Defines a management application's address and parameters
#    to be used in sending  notifications.
# Format is:
#  targetAddrName tDomain tAddress tagList targetParams timeout retryCount storageType
#--------------------------------------------------------------------------------
TARGET_ADDRESS Target1 UDP 9.3.207.107     traptag trapparms1 - - -
```

- *targetAddrName* pot ser qualsevol nom. En aquest escenari, hem utilitzat `Target1`.
- *tAddress* és l'adreça IP on s'han d'enviar els traps per al grup.
- *tagList* és el nom configurat a l'entrada `NOTIFY`. En aquest escenari, és `traptag`.
- *targetParams* pot ser qualsevol valor. Hem utilitzat `trapparms1`, que s'utilitzarà a l'entrada `TARGET_PARAMETERS`.

2. Afegiu una entrada `TARGET_PARAMETERS`.

```
#--------------------------------------------------------------------------
# TARGET_PARAMETERS
#    Defines the message processing and security parameters
#    to be used in sending notifications to a particular management target.
# Format is:
#  paramsName mpModel securityModel securityName securityLevel storageType
#--------------------------------------------------------------------------
TARGET_PARAMETERS trapparms1 SNMPv3  USM     u1        AuthNoPriv -
```

- *paramsName* és igual que el valor `targetParams` a l'entrada `TARGET_ADDRESS`, que, en aquest cas, és `trapparms1`.
- *mpModel* és la versió de l'SNMP que s'està utilitzant.
- *securityModel* és el model de seguretat que esteu utilitzant (SNMPv1, SNMPv3 o USM). En aquest escenari, està establert en `USM` per permetre l'ús de les característiques de seguretat d'SNMPv3.
- *securityName* és el nom de l'usuari especificat a l'entrada `USM_USER`, que, en aquest cas, és `u1`.
- *securityLevel* s'estableix en `AuthNoPriv` perquè estem utilitzant claus d'autenticació però no claus de privadesa.

Pas 5. Aturada i inici del dimoni snmpd

Després de fer els canvis al fitxer `/etc/snmpdv3.conf`, atureu i després inicieu el dimoni **snmpd**.

1. Escriviu l'ordre següent per aturar el dimoni **snmpd**:
   ```
   stopsrc -s snmpd
   ```
2. Escriviu l'ordre següent per iniciar el dimoni **snmpd**:
   ```
   startsrc -s snmpd
   ```

La configuració nova tindrà efecte ara mateix.

Nota: La simple actualització de l'agent SNMPv3 amb l'ordre `refresh -s snmpd` no funcionarà com a l'SNMPv1. Si feu algun canvi al fitxer `/etc/snmpdv3.conf`, heu d'aturar i iniciar el dimoni tal com s'ha explicat més amunt. La funció de configuració dinàmica admesa a l'SNMPv3 no permet l'actualització.

Pas 6. Comprovació de la configuració

Per comprovar si la configuració és correcta, podeu executar l'ordre següent al gestor de l'SNMP.

```
clsnmp -h user1 walk mib
```

en què *mib* és un subarbre de MIB al qual l'usuari té accés. En aquest escenari, podria ser `interfaces`, `tcp`, `icmp` o `system`. Si la configuració és correcta, veureu la informació del subarbre especificat.

Si no obteniu la sortida correcta, reviseu els passos d'aquest document i comproveu que heu introduït correctament tota la informació.

Resolució de problemes SNMPv3

Aquests problemes poden sorgir quan s'utilitza **SNMPv3**.

- Durant la migració, haureu de migrar les entrades de comunitat i SMUX definides al fitxer `/etc/snmpd.conf` al fitxer `/etc/snmpdv3.conf`. Per obtenir informació sobre la migració d'aquesta migració, consulteu "Migració d'SNMPv1 a SNMPv3" a la pàgina 479.
- Les sol•licituds no generen cap resposta.

  La causa més probable d'aquest problema pot ser un error de configuració del fitxer `/etc/snmpdv3.conf`, del fitxer `/etc/clsnmp.conf`, o ambdós. Reviseu amb cura aquests fitxers per assegurar-vos que tota l'informació s'ha especificat correctament. Per obtenir informació sobre l'edició d'aquests fitxers a l'hora de crear usuaris nous, consulteu "Creació d'usuaris a l'SNMPv3" a la pàgina 483.
- S'ha configurat un usuari nou mitjançant les claus d'autenticació i de privacitat, però s'ha retornar un missatge d'error en utilitzar aquest usuari.

  La causa més probable d'això és que no està executant la versió encriptada **SNMPv3**. Seguiu els passos per determinar la versió que esteu executant:

  1. Executeu `ps -e|grep snmpd`.
     - Si no rebeu cap sortida, probablement haureu d'iniciar el daemon **snmpd**. Executeu `startsrc -s snmpd`.
     - Si la sortida incloïa `snmpdv1`, estareu executant **SNMPv1**. Podreu realitzar sol•licituds **SNMPv1** en executar aquesta versió.
     - Si la sortida incloïa `snmpdv3ne`, estareu executant la versió **SNMPv3** no encriptada. Després d'instal•lar l'AIX, aquesta versió s'executarà per defecte. Aquesta versió no permet utilitzar claus de privacitat.
     - Si la sortida incloïa `snmpdv3e`, estareu executant la versió **SNMPv3** encriptada, la qual és un producte que s'instal•la per separat. La versió **SNMPv3** encriptada es troba disponible al paquet d'ampliació AIX on es permet. La versió **SNMPv3** encriptada permet utilitzar claus de privadesa.
  2. Determineu si la versió que utilitzeu és la versió que desitgeu. Si no l'és, utilitzeu l'ordre **snmpv3_ssw** per canviar la versió de la manera següent:
     - `snmpv3_ssw -1` canviarà a **SNMPv1**
     - `snmpv3_ssw -n` canviarà a **SNMPv3** no encriptada
     - `snmpv3_ssw -e` canviarà a **SNMPv3** encriptada si està instal•lada.
- Després de realitzar els canvis al fitxer `/etc/snmpdv3.conf` i haver renovat el daemon, els canvis propis no s'aplicaran.

  Després de realitzar les modificacions al fitxer `/etc/snmpdv3.conf`, caldrà aturar i iniciar el daemon **SNMP**. La renovació del daemon no funcionarà. Utilitzeu el procediment següent:

  1. Atureu el daemon **SNMP** executant `stopsrc -s snmpd`.
  2. Inicieu el daemon **SNMP** executant `startsrc -s snmpd`.
- S'inicia el subagent DPI2, però no es pot utilitzar per realitzar consultes a variables MIB.

  La causa més probable és que la comunitat `public` no està configurada al fitxer `/etc/snmpdv3.conf`. Per defecte, un subagent DPI2 entregat amb AIX utilitza el nom de comunitat `public` per connectar-se amb l'agent **SNMP**. La comunitat `public` es configura al fitxer `/etc/snmpdv3.conf` per defecte. Si heu eliminat la comunitat `public` del fitxer `/etc/snmpd.conf`, afegiu les línies següents al fitxer:

  ```
  VACM_GROUP group1 SNMPv1 public -
  VACM_VIEW defaultView 1.3.6.1.4.1.2.2.1.1.1.0 - included -
  VACM_ACCESS  group1 - - noAuthNoPriv SNMPv1  defaultView - defaultView -
  COMMUNITY public    public     noAuthNoPriv 0.0.0.0     0.0.0.0         -
  ```

  `1.3.6.1.4.1.2.2.1.1.1.0` is the OID for dpiPortForTCP.0.
- Ja no es poden realitzar consultes a les variables MIB gestionades pel similar SMUX les quals es podien consultar abans de la migració.

Assegureu-vos que l'entrada SMUX està present al fitxer `/etc/snmpdv3.conf` i al fitxer `/etc/snmpd.peers`. Si configureu similars SMUX nous, assegureu-vos que també s'especifiquen en ambdós fitxers.

- S'ha implementat un conjunt personal de variables MIB però les variables no es poden incloure ni excloure de la visió d'altres usuaris.

  A l'entrada VACM_VIEW del fitxer `/etc/snmpdv3.conf`, haureu d'especificar l'OID de la variable MIB, enlloc del nom de la variable MIB.

- No s'estan reben errors trap de recepció.

  Assegureu-vos que heu configurat les entrades d'error trap correctament al fitxer `/etc/snmpdv3.conf`. A més, si l'error trap és un error trap **SNMPv3**, també s'haurà de configurar el fitxer `/etc/clsnmp.conf`. Per obtenir informació sobre com configurar errors trap, consulteu "Creació d'usuaris a l'SNMPv3" a la pàgina 483.

  A més, assegureu-vos que la màquina especificada per rebre errors trap (al fitxer `/etc/snmpdv3.conf`) els està intentant detectar. Podeu iniciar aquest procés executant `clsnmp trap` a la línia d'ordres de la màquina receptora.

- Per què el servidor DPI2 no s'executa a l'entorn **SNMPv3**?

  A l'arquitectura **SNMPv3**, l'agent **SNMPv3** executa el servidor DPI2. Vegeu l'apartat "Arquitectura SNMPv3" a la pàgina 471 per obtenir més informació.

SNMPv1

Aquesta informació és específica de **SNMPv1**. Quan s'utilitza **SNMPv1**, l'agent **snmpd** utilitza un esquema d'autenticació simple per determinar les estacions de gestor de **Simple Network Management Protocol (SNMP)** que poden accedir a les seves variables MIB.

Aquest esquema d'autenticació implica l'especificació de polítiques d'accés **SNMP** per **SNMPv1**. Una política d'accés **SNMP** és una relació administrativa que implica una associació entre una comunitat **SNMP**, un mode d'accés i una vista MIB.

Una *comunitat SNMP* és un grup d'un o més amfitrions i un nom de comunitat. Un nom de comunitat és una sèrie d'octets que un gestor **SNMP** ha d'intercalar en un paquet de sol•licitud **SNMP** per realitzar autenticacions.

La *modalitat d'accés* especifica l'accés dels amfitrions dins de les comunitats pel que fa a la recuperació i la modificació de variables MIB des d'un agent **SNMP** específic. La modalitat d'accés ha d'ésser una de les següents: *cap*, *només lectura*, *lectura-escriptura* o *només escriptura*.

Una *vista MIB* defineix un o més subarbres MIB al qual pot accedir una comunitat **SNMP** específica. La vista MIB pot ser tot l'arbre MIB o un subconjunt limitat de tot l'arbre MIB.

Quan un agent **SNMP** rep una sol•licitud, l'agent verifica el nom de la comunitat amb l'adreça IP de l'amfitrió de la sol•licitud per determinar si l'amfitrió de la sol•licitud és membre d'una comunitat **SNMP** identificada per un nom de comunitat. Si l'amfitrió de la sol•licitud és membre de la comunitat **SNMP**, a continuació, l'agent **SNMP** determinarà si aquest amfitrió té l'accés específic per a les variables MIB especificades tal com es defineix a la política d'accés associada amb aquesta comunitat. Si es compleixen tots els criteris, l'agent **SNMP** intentarà acceptar la sol•licitud. En cas contrari, l'agent **SNMP** genera un error trap *authenticationFailure* o retorna el missatge d'error adient a l'amfitrió de la sol•licitud.

Les polítiques d'accés **SNMPv1** de l'agent **snmpd** poden ser configurades per l'usuari i s'especifiquen al fitxer `/etc/snmpd.conf`. Per configurar les polítiques d'accés del **SNMP** per a l'agent **snmpd** consulteu el fitxer `/etc/snmpd.conf` a *Files Reference*.

Configuració de daemons SNMP

El daemon de **Simple Network Management Protocol (SNMP)** és un procés de servidor de fons que es pot executar en qualsevol amfitrió d'estació de treball de **Transmission Control Protocol/Internet Protocol (TCP/IP)**.

El daemon, actuant com a agent **SNMP**, rep, autentica i processa sol•licituds **SNMP** des d'aplicacions de gestor. Consulteu Protocol simple de gestió de xarxes, Funcionament d'un gestor i Funcionament d'un agent a *Communications Programming Concepts* per obtenir més informació detallada sobre les funcions d'agent i de gestor.

Nota: Els termes daemon **SNMP**, agent **SNMP** i agent s'utilitzen indistintament.

El daemon **snmpd** requereix que l'interfície **TCP/IP** de bucle de retorn estigui activa per realitzar tasques mínimes de configuració. Escriviu l'ordre següent abans d'iniciar **TCP/IP**:

```
ifconfig lo0 loopback up
```

El daemon **SNMP** intentarà vincular sòcols amb determinats ports de **User Datagram Protocol (UDP)** i **Transmission Control Protocol (TCP)**, els quals s'han de definir al fitxer `/etc/services` de la manera següent:

```
snmp            161/udp
snmp-trap       162/udp
smux            199/tcp
```

Al servei `snmp` s'ha d'assignar el port `161`, tal com s'especifica a RFC 1157. El fitxer `/etc/services` assigna els ports 161, 162 i 199 a aquests dispositius. Si el fitxer `/etc/services` està oferint serveis a una altra màquina, aquests ports assignats han d'estar disponibles al fitxer `/etc/services` del servidor al servidor abans de que es pugui executar el daemon **SNMP**.

El daemon **SNMP** llegeix el fitxer de configuració a la versió **SNMP** que s'estigui executant durant l'inici i quan s'emet una ordre **refresh** (si s'invoca el daemon **snmpd** des del control del controlador de recursos del sistema) o el senyal **kill -1**.

Fitxer /etc/snmpd.conf:

El fitxer de configuració `/etc/snmpd.conf` especifica noms de comunitat i privilegis i vistes d'accés associades, amfitrions per notificacions d'errors trap, atributs d'inici de sessió, configuracions de paràmetre específiques de **snmpd** i configuracions de multiplexors individuals pel daemon **SNMP** de **SNMPv1**.

Consulteu el fitxer /etc/snmpd.conf a *Files Reference* per obtenir més informació.

Processament de daemon SNMP

El daemon **Simple Network Management Protocol (SNMP)** processa sol•licituds **SNMP** a partir d'aplicacions de gestor.

Llegiu Simple Network Management Protocol (SNMP), Funcionament d'un gestor i Funcionament d'un agent de *Communications Programming Concepts* per obtenir més informació detallada sobre les funcions d'agent i de gestor.

Processament i autenticació de missatges SNMP:

Totes les sol•licituds, tots els errors traps i totes les respostes es transmeten en la forma de missatges amb el codi ASN.1.

Un missatge, tal com ho defineix RFC 1157, té l'estructura següent:

PDU de comunitat de versió

on *Versió* és la versió SNMP (actualment la versió 1), *Comunitat* és el nom de la comunitat i *PDU* és l'unitat de dades de protocol que conté la sol•licitud **SNMP**, la resposta o les dades d'error trap. Les PDU també es codifiquen segons les regles ASN.1.

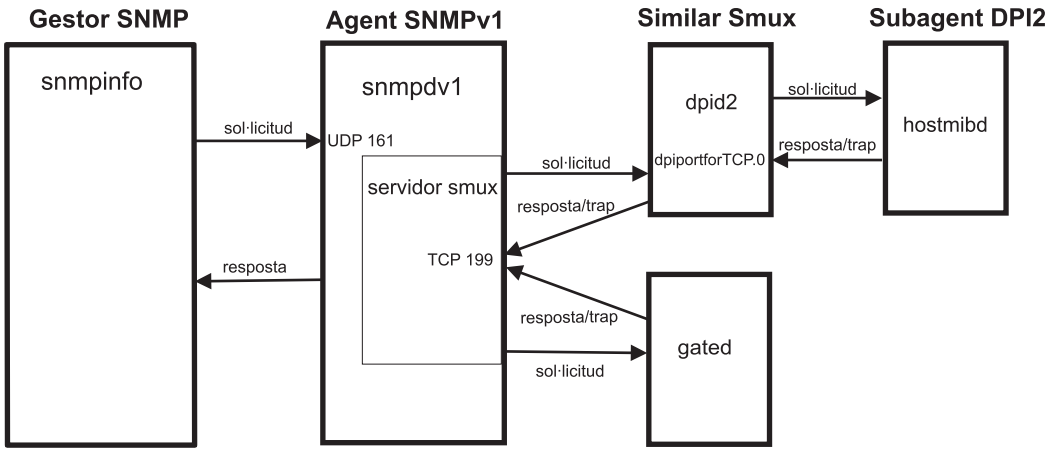


Figura 28. Les parts principals de l'arquitectura SNMPv1

Aquesta il•lustració mostra un exemple de l'arquitectura **SNMPv1**. Es mostren el subagent DPI2, el similar smux, el gestor **SNMP** i l'agent **SNMP**. A més, també es mostra com es comuniquen entre sí.

El daemon **SNMP** rep i transmet tots els missatges de protocol **SNMP** a través del protocol UDP de **Transmission Control Protocol/Internet Protocol (TCP/IP)**. Les sol•licituds s'accepten al conegut port 161. Els errors trap es transmeten als amfitrions llistats a les entrades d'error trap del fitxer `/etc/snmpd.conf` que estan escoltant al conegut port 162.

Quan es rep una sol•licitud, es comproven l'adreça IP i el nom de comunitat amb una llista que conté adreces IP, noms de comunitat, permisos i vistes tal com s'especifiquen a les entrades de comunitat i de vista del fitxer `/etc/snmpd.conf`. L'agent **snmpd** llegeix aquest fitxer a l'inici i quan s'emet una ordre **refresh** o un senyal **kill -1**. Si no es troba cap entrada coincident, s'ignora la sol•licitud. Si es troba una entrada coincident, es permet l'accés segons els permisos especificats a les entrades de comunitat i de vista per l'associació d'adreça, comunitat i nom de vista al fitxer `/etc/snmpd.conf`. El missatge i la PDU han de codificar-se segons les regles ASN.1.

Aquest esquema d'autenticació no està dissenyat per proporcionar una seguretat completa. Si el daemon **SNMP** només s'utilitza per sol•licituds get i get-net, és possible que no apareguin problemes de seguretat. Si es permeten sol•licituds d'establiment, es pot restringir el privilegi d'establiment.

Consulteu el fitxer `/etc/snmpd.conf` a *Files Reference* per obtenir més informació. Consulteu Base d'informació de gestió (MIB) a *Communications Programming Concepts* per obtenir més informació.

Processament de sol•licituds SNMP:

Existeixen tres tipus de PDU de sol•licitud que es pot rebre el daemon **SNMP**.

Els tipus de sol•licitud es defineixen a RFC 1157 i totes les PDU tenen el format següent:

Taula 83. Format de PDU de sol•licitud

ID de sol•licitud	Estat d'error	Índex d'error	vinculacions de variable
GET	0	0	*VarBindList*
GET-NEXT	0	0	*VarBindList*
SET	0	0	*VarBindList*

El camp d'ID de sol•licitud identifica la naturalesa de la sol•licitud. El camp d'estat d'error i el camp d'índex d'error no s'utilitzen i s'han d'establir en 0 (zero). El camp de vinculacions de variable conté la longitud d'una variable d'ID d'instància de format numèric els valors dels quals se sol•liciten. Si el valor del camp ID de sol•licitud és SET, el camp de vinculacions de variable serà una llista de parelles d'ID i valors d'instància.

Llegiu Utilització de la base de dades MIB a *Communications Programming Concepts*per obtenir informació detallada sobre els tres tipus de sol•licitud.

Processament de respostes SNMP:

Les PDU de resposta tenen un format molt semblant a les PDU de sol•licitud.

Taula 84. Format de PDU de resposta

ID de sol•licitud	Estat d'error	Índex d'error	vinculacions de variable
GET-RESPONSE	*ErrorStatus*	*ErrorIndex*	*VarBindList*

Si la sol•licitud s'ha processat correctament, el valor dels camps estat d'error i índex d'error serà o (zero) i el camp de vinculacions de variable contindrà una llista completa de parelles de ID i valors d'instància.

Si qualsevol ID d'instància del camp de vinculacions de variable de la PDU de la sol•licitud no s'ha processat correctament, l'agent SNMP aturarà el processament, escriurà l'índex de l'ID d'instància erroni al camp d'índex d'errors, enregistrarà un codi d'error al camp d'estat d'error i copiarà la llista de resultats parcialment completada al camp de vinculacions de variable.

RFC 1157 defineix els valors següents pel camp d'estat d'error:

Taula 85. Valors del camp estat d'error

Valor	Valor	Explicació
noError	0	El processament s'ha completat correctament (l'índex d'error és 0).
tooBig	1	La grandària de la PDU de resposta excedeix un límit definit per l'implementació (l'índex d'error és 0).
noSuchName	2	No existeix cap ID d'instància a la vista MIB relevant dels tipus de sol•licitud GET i SET o no hi ha cap successor a l'arbre MIB de la vista MIB rellevant de sol•licituds GET-NEXT (índex d'error diferent de zero).
badValue	3	Només per sol•licituds SET, un valor especificat és sintàcticament incompatible amb l'atribut de tipus de l'ID d'instància corresponent (índex d'error diferent de zero).
readOnly	4	No definit.

Taula 85. Valors del camp estat d'error (continuació)

Valor	Valor	Explicació
genErr	5	S'ha produït un error definit per implementació (índex d'error diferent de cero). Per exemple, un intent d'assignar un valor que supera els límits d'implementació.

Processament d'errors trap SNMP:

El format de les PDU d'errors trap es defineixen a RFC 1157 i és el que es mostra a la taula següent.

Taula 86. Format de PDU d'errors trap

empresa	adreça d'agent	trap genèric	trap específic	indicació de l'hora	vinculacions de variable
ID d'objecte	*Enter*	*Enter*	*Enter*	*Cicles de temps*	*Llista de vinculació de variable*

Els camps s'utilitzen de la manera següent:

Element	Descripció
empresa	Identificador d'objecte assignat al proveïdor que implementa l'agent. Aquest és el valor de la variable **sysObjectID** i és exclusiu de cada implementador de l'agent **SNMP**. El valor assignat a aquesta implementació l'agent és **1.3.6.1.4.1.2.3.1.2.1.1.3**, or **risc6000snmpd.3**.
adreça d'agent	Adreça IP de l'objecte que genera l'error trap.
trap genèric	Enter, tal com s'indica a continuació: **0** *coldStart* **1** *warmStart* **2** *linkDown* **3** *linkUp* **4** *authenticationFailure* **5** *egpNeighborLoss* **6** *enterpriseSpecific*
error trap específic	No s'utilitza i es reserva per desenvolupament futur.
indicació de l'hora	Temps transcorregut, en centèssimes de segon, des de l'última reinicialització de l'agent fins a l'incidència que ha generat l'error trap.
vinculacions de variable	Informació addicional que depèn del tipus *error trap genèric*.

Els valors d'error trap genèrics següents indiquen que s'han detectat determinades incidències de sistema:

Element	Descripció
coldStart	L'agent s'està reinicialitzant. És possible que els valors de les dades de configuració o de les variables MIB hagin canviat. Reinicieu les èpoques de mesura.
warmStart	L'agent s'està reinicialitzant però els valors de dades de configuració i de variable MIB no han canviat. En aquesta implementació de l'agent **SNMP**, es genera un error trap *warmStart* quan es torna a llegir el fitxer `/etc/snmpd.conf`. L'informació de configuració del fitxer `/etc/snmpd.conf` és per la configuració de l'agent que no té conseqüències en les bases de dades del gestor SNMP. Les èpoques de mesura no s'han de reiniciar.
linkDown	L'agent ha detectat que s'ha inhabilitat l'interfície de comunicacions coneguda.
linkUp	L'agent ha detectat que s'ha habilitat l'interfície de comunicacions coneguda.
authenticationFailure	S'ha rebut un missatge sense autenticació.
egpNeighborLoss	S'ha perdut un veïnatge **Exterior Gateway Protocol (EGP)**. Aquest valor només es genera quan l'agent s'està executant en un amfitrió que executa el daemon **gated** mitjançant **EGP**.

Element	Descripció
enterpriseSpecific	No implementat: es reserva per un ús futur.

Els errors trap *linkDown* i *linkUp* contenen una sola parella ID/Valor d'instància a la llista de vinculacions de variable. L'ID d'instància identifica l'**ifIndex** de l'adaptador que s'ha inhabilitat o habilitat i el valor és **ifIndex**. L'error trap de *egpNeighborLoss* també conté una vinculació que consisteix de l'ID i el valor d'instància de *egpNeighAddr* pel veïnatge perdut.

Suport del daemon SNMP per la família EGP de variables MIB

Si l'amfitrió de l'agent està executant el daemon **gated** amb el protocol **Exterior Gateway Protocol (EGP)** habilitat, hi haurà unes quantes variables MIB al grup **EGP** a les quals dóna suport el daemon **gated** al qual l'agent **snmpd** pot accedir.

Les variables MIB **EGP** següents tenen una sola instància única:

Element	Descripció
egpInMsgs	Nombre de missatges **EGP** rebuts sense error.
egpInErrors	Nombre de missatges **EGP** rebuts amb error.
egpOutMsgs	Nombre total de missatges **EGP** transmesos pel daemon **gated** que s'executa a l'amfitrió de l'agent.
egpOutErrors	Nombre de missatges **EGP** que no ha pogut enviar el daemon **gated** de l'amfitrió degut a limitacions dels recursos.
egpAs	Nombre del daemon **gated** d'amfitrió del sistema autònom.

Les variables MIB **EGP** següents tenen una instància per a cada similar o veí **EGP** adquirida pel daemon **gated** d'amfitrió d'agent:

Element	Descripció
egpNeighState	Estat d'aquest similar **EGP**: **1** inactiu **2** adquisició **3** desconnectat **4** connectat **5** cessat.
egpNeighAddr	Adreça IP d'aquest similar **EGP**.
egpNeighAs	Número d'aquest similar **EGP** del sistema autònom. Zero (0) indica que encara no es coneix el número del sistema autònom d'aquest similar.
egpInNeighMsgs	Nombre de missatges **EGP** rebuts sense error d'aquest similar **EGP**.
egpNeighInErrs	Nombre de missatges **EGP** rebots amb error d'aquest similar **EGP**.
egpNeighOutMsgs	Nombre de missatges **EGP** generats localment per aquest similar **EGP**.
egpNeighOutErrs	Nombre de missatges **EGP** generats localment no enviats a aquest similar **EGP** degut a limitacions de recursos.
egpNeighInErrMsgs	Nombre de missatges d'error definits per **EGP** rebuts d'aquest similar **EGP**.
egpNeighOutErrMsgs	Nombre de missatges d'error definits per **EGP** enviats a aquest similar **EGP**.
egpNeighStateUp	Nombre de transicions d'estat **EGP** a l'estat UP amb aquest similar **EGP**.
egpNeighStateDowns	Nombre de transicions d'estat **EGP** de l'estat UP a qualsevol altre estat amb aquest similar **EGP**.
egpNeighIntervalHello	Interval entre les retransmissions de l'ordre Hello **EGP** i centèssimes de segon.
egpNeighIntervalPoll	Interval entre les retransmissions de l'ordre poll **EGP** i centèssimes de segon.
egpNeighMode	Mode de sondeig d'aquest similar **EGP**. El mode pot ser actiu (1) o passiu (2).
egpNeighEventTrigger	Variable de control que desencadena incidències d'inici i aturada iniciades per operador per a aquest similar **EGP**. La variable MIB es pot establir de manera que s'inicií (1) o s'aturi (2).

Si el daemon **gated** no s'està executant o si el daemon **gated** s'està executant però no està configurat per comunicar-se amb l'agent **snmpd** o si el daemon **gated** no està configurat per **EGP**, les sol•licituds per obtenir i establir els valors d'aquestes variables retornaran el codi de resposta d'error *noSuchName*.

El fitxer de configuració **gated**, `/etc/gated.conf`, ha de contenir la sentència següent:

```
snmp      yes;
```

El daemon **gated** està configurat internament per a ser un similar de protocol de multiplexor simple (SMUX) de protocol Simple Network Management Protocol (SNMP) o un agent proxy del daemon **snmpd**. Si el daemon **gated** s'inicia, enregistrarà l'arbre de variables MIB *ipRouteTable* amb l'agent **snmpd**. Si el daemon **gated** es configura per **EGP**, el daemon **gated** també enregistra l'arbre de variables MIB de **EGP**. Un cop finalitzada la configuració, un gestor SNMP pot realitzar sol•licituds correctament a l'agent **snmpd** per les variables MIB *ipRouteTable* i **EGP** a les quals dóna suport aquest daemon **gated** d'amfitrió d'agent. Quan s'està executant el daemon **gated**, tota l'informació d'encaminament MIB s'obté mitjançant el daemon **gated**. En aquest cas, no es permet utilitzar sol•licituds d'establiment per *ipRouteTable*.

La comunicació SMUX entre el daemon **gated** i el daemon **snmpd** es produeix pel port 199 del conegut protocol de control de transmissió. Si el daemon **gated** finalitza, **snmpd** finalitza l'enregistrament dels arbres que el daemon **gated** ha enregistrar prèviament de manera immediata. Si el daemon **gated** s'inicia abans que el daemon **snmpd**, el daemon **gated** comprovarà periòdicament el daemon **snmpd** fins que es pugui establir l'associació SMUX.

Per configurar l'agent **snmpd** per reconèixer i permetre l'associació SMUX amb el client de daemon **gated**, l'usuari haurà de configurar una entrada SMUX al fitxer `/etc/snmpd.conf`. L'identificador d'objecte de client i la paraula clau especificats a l'entrada SMUX del daemon **gated** han de coincidir amb els especificats al fitxer `/etc/snmpd.peers`.

L'agent **snmpd** dóna suport a sol•licituds d'establiment per les variables MIB I i MIB II de lectura-escriptura següents:

sysContact
Identificació textual de la persona de contacte de l'amfitrió d'aquest agent. Aquesta informació inclou el nom d'aquesta persona i el mode en que s'ha de contactar. Per exemple, "Bob Smith, 555-5555, ext 5." El valor està limitat a 256 caràcters. Si, en el cas d'una sol•licitud d'establiment, la sèrie d'aquesta variable MIB és major que 256 caràcters, l'agent **snmpd** retornarà l'error *badValue* i no es durà a terme l'operació d'establiment. El valor inicial de *sysContact* es defineix a `/etc.snmp.conf`. Si no es defineix res, el valor serà una sèrie nul•la.

Instància	Valor	Acció
0	"string"	La variable MIB s'estableix en "string".

sysName
Nom d'amfitrió de l'amfitrió d'aquest agent. Normalment es tracta del nom de domini completament qualificat del node. El valor està limitat a 256 caràcters. Si, en el cas d'una sol•licitud d'establiment, la sèrie d'aquesta variable MIB és major que 256 caràcters, l'agent **snmpd** retornarà l'error *badValue* i no es durà a terme l'operació d'establiment.

Instància	Valor	Acció
0	"string"	La variable MIB s'estableix en "string".

sysLocation

Sèrie textual que indica l'ubicació física de la màquina on es troba l'agent **snmpd**: per exemple, "Austin site, building 802, lab 3C-23." El valor està limitat a 256 caràcters. Si, en el cas d'una sol•licitud d'establiment, la sèrie d'aquesta variable MIB és major que 256 caràcters, l'agent **snmpd** retornarà l'error *badValue* i no es durà a terme l'operació d'establiment. El valor inicial de *sysLocation* es defineix a `/etc/snmp.snmp.conf`. Si no es defineix res, el valor serà una sèrie nul•la.

Instància	Valor	Acció
0	"string"	La variable MIB s'estableix en "string".

ifAdminStatus

L'estat desitjat d'un adaptador d'interfície de l'amfitrió d'agent. Es dóna suport a estats en direcció ascendent i descendent. L'estat es pot establir per realitzar proves, però una acció d'aquestes característiques no té efecte en l'estat operatiu de l'interfície.

Instància	Valor	Acció
f	1	L'adaptador de l'interfície amb **ifIndex f** està habilitat.

Nota: És possible que el valor *ifAdminStatus* es pugui establir en direcció ascendent o descendent encara que el canvi operatiu de l'interfície hagi fallat. En aquest cas, una sol•licitud d'obtenció de *ifAdminStatus* pot reflectir *up* mentre que *ifOperStatus* d'aquesta interfície pot reflectir *down*. Si es produeix una situació així, l'administrador de la xarxa hauria d'emetre una altra sol•licitud d'establiment per establir *ifAdminStatus* en direcció ascendent per tornar a intentar el canvi operatiu.

atPhysAddress

Part de l'adreça de maquinari d'una taula d'adreces que es vinculen a un amfitrió d'agent (una entrada de la taula de protocol de resolució d'adreces). Aquesta és la mateixa variable MIB que *ipNetToMediaPhysAddress*.

Instància	Valor	Acció
f.1.n.n.n.n	hh:hh:hh:hh:hh:hh	Per l'interfície amb **ifIndex f,** qualsevol vinculació de taula ARP existent n.n.n.n is substituïda per la vinculació (n.n.n.n, hh:hh:hh:hh:hh:hh). Si no existeix cap vinculació, se n'afegirà una de nova. hh:hh:hh:hh:hh:hh és una adreça de maquinari de dotze dígits hexadecimals.

atN0etAddress

Adreça IP que correspon a l'adreça física o de maquinari especificada a *atPhysAddress*. Aquesta és la mateixa variable MIB que *ipNetToMediaNetAddress*.

Instància	Valor	Acció
f.1.n.n.n.n	m.m.m.m	Per l'interfície amb **ifIndex f,** l'entrada de taula ARP existent per l'adreça IP n.n.n.n es substitueix per m.m.m.m. de l'adreça IP.

ipForwarding

Indica si l'amfitrió de l'agent reenvia datagrames.

Taula 87. ipforwarding

Instància	Valor	Acció
0	1	si l'amfitrió de l'agent té més d'una interfície activa, el kernel **TCP/IP** es configura per reenviar paquets. Si l'amfitrió de l'agent només té una interfície activa, la sol•licitud d'establiment falla.
0	2	El kernel **TCP/IP** de l'amfitrió de l'agent està configurat per no reenviar paquets.

ipDefaultTTL

El valor de duració per defecte (TTL) insertat a les capçaleres IP de datagrames originat per l'amfitrió de l'agent.

Instància	Valor	Acció
0	n	El valor de duració per defecte utilitzat pel suport de protocol IP s'estableix en l'enter N.

ipRouteDest

Adreça IP de destinació d'una ruta de la taula de rutes.

Instància	Valor	Acció
n.n.n.n	m.m.m.m	la ruta de destinació de la ruta n.n.n.n s'estableix en m.m.m.m. de l'adreça IP.

ipRouteNextHop

Passarel•la per la qual es pot accedir a una adreça IP de destinació des de l'amfitrió de l'agent (una entrada de la taula de rutes).

Instància	Valor	Acció
n.n.n.n	m.m.m.m	L'entrada de la taula de rutes per arribar a la xarxa n.n.n.n mitjançant la passarel•la m.m.m.m s'afegeix a la taula de rutes. La part d'amfitrió de l'adreça IP n.n.n.n ha d'ésser 0 per indicar una adreça de xarxa.

ipRouteType

Estat de l'entrada de la taula de rutes de l'amfitrió d'agent (utilitzat per eliminar entrades).

Instància	Valor	Acció
h.h.h.h	1	Qualsevol ruta a l'adreça IP d'amfitrió h.h.h.h s'elimina.
n.n.n.n	2	Qualsevol ruta a l'adreça IP d'amfitrió n.n.n.n s'elimina.

ipNetToMediaPhysAddress

Part de l'adreça de maquinari d'una taula d'adreces que es vinculen a un amfitrió d'agent (una entrada de la taula de protocol de resolució d'adreces). Aquesta és la mateixa variable MIB que *atPhysAddress*.

Instància	Valor	Acció
f.1.n.n.n.n	hh:hh:hh:hh:hh:hh	Per l'interfície amb **ifIndex f,** qualsevol vinculació de taula ARP existent n.n.n.n is substituïda per la vinculació (n.n.n.n, hh:hh:hh:hh:hh:hh). Si no existeix cap vinculació, se n'afegirà una de nova. hh:hh:hh:hh:hh:hh és una adreça de maquinari de dotze dígits hexadecimals.

ipNetToMediaNetAddress

Adreça IP que correspon a l'adreça física o de maquinari especificada a *ipNetToMediaPhysAddress*. Aquesta és la mateixa variable MIB que *atNetAddress*.

Instància	Valor	Acció
f.1.n.n.n.n	m.m.m.m	Per l'interfície amb **ifIndex f,** l'entrada de taula ARP existent per l'adreça IP n.n.n.n es substitueix per m.m.m.m. de l'adreça IP.

ipNetToMediaType

Tipus de correlació des de l'adreça IP a l'adreça física.

Instància	Valor	Acció
f.1.n.n.n.n	1	Per l'interfície amb **ifIndex f,** per a una vinculació ARP existent d'una adreça IP a l'adreça física, el tipus de correlació s'estableix en 1, o un altre valor.
f.1.n.n.n.n	2	Per l'interfície amb **ifIndex f,** per a una vinculació ARP existent d'una adreça IP a l'adreça física, el tipus de correlació s'estableix en 2, o un valor no vàlid. Com a conseqüència, s'invalida l'entrada corresponent de **ipNetMediaTable**; és a dir, l'interfície es dissocia de la seva entrada **ipNetToMediaTable**.
f.1.n.n.n.n	3	Per l'interfície amb **ifIndex f,** per a una vinculació ARP existent d'una adreça IP a l'adreça física, el tipus de correlació s'estableix en 3, o un valor dinàmic.
f.1.n.n.n.n	4	Per l'interfície amb **ifIndex f,** per a una vinculació ARP existent d'una adreça IP a l'adreça física, el tipus de correlació s'estableix en 4, o un valor estàtic.

snmpEnableAuthenTraps

Indica si l'agent **snmpd** està configurat per generar errors trap *authenticationFailure*.

Instància	Valor	Acció
0	1	L'agent **snmpd** generarà errors trap d'anomalia d'autenticació.
0	2	L'agent **snmpd** no generarà errors trap d'anomalia d'autenticació.

smuxPstatus
Estat d'un similar de protocol SMUX (utilitzat per eliminar similars SMUX).

Instància	Valor	Acció
n	1	L'agent **snmpd** no realitza cap acció.
n	2	L'agent **snmpd** atura la comunicació amb el número de similar SMUX.

smuxTstatus
Estat d'un arbre SMUX MIB (utilitzat per eliminar muntatges d'arbre MIB).

Instància	Valor	Acció
l.m.m.m._ _ _ .p	1	L'agent **snmpd** no realitza cap acció.
l.m.m.m._ _ _ .p	2	Desmunta muntatges SMUX de l'arbre MIB m.m.m... on *l* és la longitud de l'instància de l'arbre MIB i *p* és smuxTpriority.

Les variables següents són les variables que es poden establir tal com es defineix a RFC 1229. El daemon **snmpd** permet a l'usuari establir aquestes variables. És possible que el dispositiu subjacent no permeti establir aquestes variables. Comprovi cada dispositiu per veure als elements als quals es dóna i no es dóna suport.

ifExtnsPromiscuous
Estat de modalitat de promiscuïtat d'un dispositiu determinat. Això s'utilitza per habilitar i inhabilitar la modalitat de promiscuïtat en un dispositiu determinat. L'acció **snmpd** és final i s'ha completat. Quan s'indica que s'ha de desactivar **snmpd**, la modalitat de promiscuïtat es desactiva completament, independentment de la resta d'aplicacions de la màquina.

Instància	Valor	Acció
n	1	Activa la modalitat de promiscuïtat pel dispositiu n.
n	2	Desactiva la modalitat de promiscuïtat pel dispositiu n.

ifExtnsTestType
Variable d'inici de proves. Quan s'estableix aquesta variable, s'executa la prova adient pel dispositiu en qüestió. Un identificador d'objecte és el valor de la variable. El valor especificat depèn del tipus de dispositiu i de la prova que s'ha d'executar. Actualment, l'única prova definida que **snmpd** sap executar és la prova testFullDuplexLoopBack.

Instància	Valor	Acció
n	oid	Inicia la prova especificada per oid.

ifExtnsRcvAddrStatus
Variable d'estat de l'adreça. Quan s'estableix aquesta variable, es crea l'adreça especificada amb el nivell de durada adient. **snmpd** només permet establir adreces temporals perquè no pot establir enregistraments ODM de dispositiu i només pot establir adreces de difusió o de difusió selectiva.

Instància	Valor	Acció
n.m.m.m.m.m.m	1	Afegir l'adreça de forma que no sigui una adreça temporal ni permanent.
n.m.m.m.m.m.m	2	Elimineu l'adreça per a què es deixi d'utilitzar.
n.m.m.m.m.m.m	3	Afegiu l'adreça com a adreça temporal.
n.m.m.m.m.m.m	4	Afegiu l'adreça com a adreça permanent.

Les variables llistades són les variables que es poden establir tal com es defineix a RFC 1231. El daemon **snmpd** permet a l'usuari establir aquestes variables. És possible que el dispositiu subjacent no permeti establir aquestes variables. Comproveu cada dispositiu per veure als elements als quals es dóna i no es dóna suport.

dot5Commands
L'ordre que el dispositiu token ring ha de dur a terme.

Instància	Valor	Acció
n	1	No realitza cap acció. Es retorna.
n	2	Indica al dispositiu token ring que s'obri.
n	3	Indica al dispositiu token ring que es reinicií.
n	4	Indica al dispositiu token ring que es tanqui.

dot5RingSpeed
Velocitat d'anell o d'amplada de banda actual.

Instància	Valor	Acció
n	1	Velocitat desconeguda.
n	2	1 megabit de velocitat d'anell.
n	3	4 megabits de velocitat d'anell.
n	4	16 megabits de velocitat d'anell.

dot5ActMonParticipate
L'objecte especifica si el dispositiu participa en el procés de selecció de control actiu.

Instància	Valor	Acció
n	1	Participa.
n	2	No participa.

dot5Functional
Màscara funcional que permet al dispositiu token ring especificar les adreces des de les quals rep marcs.

Instància	Valor	Acció
n	m.m.m.m.m.m	Màscara funcional que s'ha d'establir.

Les variables de temporitzador complexes següents es defineixen a RFC com a només de lectura però es recomana que facin de lectura-escriptura. Reviseu RFC per comprendre millor les seves interaccions. **snmpd** permet al usuari que ho sol•licita establir-les però el dispositiu no ho podrà fer. Comproveu la documentació del programa de control de dispositiu per obtenir més informació. Les variables són:

- dot5TimerReturnRepeat
- dot5TimerHolding
- dot5TimerQueuePDU
- dot5TimerValidTransmit

- dot5TimerNoToken
- dot5TimerActiveMon
- dot5TimerStandbyMon
- dot5TimerErrorReport
- dot5TimerBeaconTransmit
- dot5TimerBeaconReceive.

El daemon SNMP permet a l'usuari establir les variables següents. El daemon utilitza l'estàndard de protocol FDDI Station Management (SMT) 7.2 per obtenir l'informació i es determina al nivell de microcodi. Comproveu el microcodi a la documentació de FDDI per assegurar-vos que s'està utilitzen el microcodi SMT 7.2.

fddimibSMTUserData
Variable que reté 32 octets d'informació d'usuari.

Instància	Valor	Acció
n	sèrie	Emmagatzema 32 octets d'informació d'usuari.

fddimibSMTConfigPolicy
Estat de les polítiques de configuració, específicament la utilització de la política de retenció.

Instància	Valor	Acció
n	0	No utilitzeu la política de retenció.
n	1	Utilitzeu la política de retenció.

fddimibSMTConnectionPolicy
Estat de les polítiques de connexió al node FDDI. Consulteu RFC 1512 per obtenir més informació sobre els valors específics que es poden establir.

Instància	Valor	Acció
n	k	Defineix les polítiques de connexió.

fddimibSMTTNotify
El temporitzador, expressat en segons, utilitzat en el protocol de notificació de veïnatge. Té un interval de 2 a 30 segons i el seu valor per defecte és de 30 segons.

Instància	Valor	Acció
n	k	Defineix el valor del temporitzador.

fddimibSMTStatRptPolicy
Estat de la generació de marcs d'informes d'estat.

Instància	Valor	Acció
n	1	Indica que el node genera els marcs d'informes d'estat per les incidències implementades.
n	2	Indica que el node no crea marcs d'informes d'estat.

fddimibSMTTraceMaxExpiration
Aquesta variable defineix el valor de caducitat de temporitzador màxim per la traça.

Instància	Valor	Acció
n	k	Defineix la caducitat de temporitzador màxima en mil•lisegons.

fddimibSMTStationAction

Aquesta variable fa que l'entitat SMT dugui a terme una acció específica. Consulteu RFC per obtenir informació específica sobre aquesta variable.

Instància	Valor	Acció
n	k	Defineix una acció a l'entitat SMT. Les valors oscil•len entre 1 i 8.

fddimibMACRequestedPaths

Defineix els camins d'accés que el control d'accés al medi ha d'insertar.

Instància	Valor	Acció
n.n	k	Defineix el camí d'accés sol•licitat pel MAC.

fddimibMACFrameErrorThreshold

Llindar per quan es genera un informe d'estat MAC. Defineix el número d'errors que s'ha de produir per a què es generi un informe.

Instància	Valor	Acció
n.n	k	Defineix el nombre d'errors que s'han d'observar abans que es generi un informe d'estat MAC.

fddimibMACMAUnitdataEnable

Aquesta variable determina el valor del senyalador **MA_UNITDATA_Enable** a RMT. El valor per defecte i inicial d'aquest senyalador és true (1).

Instància	Valor	Acció
n.n	1	Marca el senyalador MA_UNITDATA_Enable true.
n.n	2	Marca el senyalador MA_UNITDATA_Enable false.

fddimibMACNotCopiedThreshold

Llindar per determinar quan es genera un informe de condició MAC.

Instància	Valor	Acció
n.n	k	Defineix el nombre d'errors que s'han d'observar abans que es generi un informe de condició MAC.

Les tres variables següents són variables de temporitzador que són interactives entre sí. Abans de canviar qualsevol d'aquestes variables, haureu de comprendre bé el seu significat tal com es defineix a **RFC 1512**.

- fddimibPATHTVXLowerBound
- fddimibPATHTMaxLowerBound
- fddimibPATHMaxTReq

fddimibPORTConnectionPolicies

Especifica les polítiques de connexió del port especificat.

Instància	Valor	Acció
n.n	k	Defineix les polítiques de connexió del port especificat.

fddimibPORTRequestedPaths

Aquesta variable és una llista de camins d'accés permesos on cada element de llista defineix els camins d'accés permesos de port. El primer octet correspon a `none', el segon a `tree' i el tercer a `peer'.

Instància	Valor	Acció
n.n	ccc	Defineix els camins d'accés del port.

fddimibPORTLerCutoff

Càlcul de l'índex d'errors d'enllaç en el qual s'anul•la una connexió d'enllaços. Oscil•la entre 10**-4 i 10**-15 i es considera com a valor absolut del logaritme de base 10 (valor per defecte 7).

Element	Descripció	
Instància	**Valor**	**Acció**
n.n	k	Defineix LerCutoff del port.

fddimibPORTLerAlarm

Càlcul de l'índex d'errors d'enllaç en el qual una connexió d'enllaços genera una alarma. Oscil•la entre 10**-4 i 10**-15 i es considera com a valor absolut del logaritme de base 10 del càlcul (valor per defecte 8).

Instància	Valor	Acció
n.n	k	Defineix LerAlarm del port.

fddimibPORTAction

Aquesta variable fa que l'entitat que el port dugui a terme una acció específica. Consulteu RFC per obtenir informació específica sobre aquesta variable.

Instància	Valor	Acció
n	k	Defineix una acció al port definit. Els valors oscil•len de 1 a 6.

Nota: RFC 1213 descriu totes les variables de les taules *atEntry* i *ipNetToMediaEntry* com a variables de lectura-escriptura. El suport d'establiment s'implementa per les variables *atEntry* variables *atPhysAddress* i *atNetAddress,* i les variables *ipNetToMediaEntry*, *ipNetToMediaPhysAddress, ipNetToMediaNetAddress* i *ipNetToMediaType.* Per acceptar sol•licituds d'establiment que poden especificar els atributs no suportats restants en aquestes dues taules, les sol•licituds de les variables restants s'accepten a *atIfIndex* i *ipNetToMediaIfIndex.* No es retorna cap resposta d'error a l'originador de sol•licituds d'establiment. Una sol•licitud d'obtenció posterior mostrarà els valors originals a mesura que es retenen.

A la taula *ipRouteEntry*, RFC 1213 descriu totes les variables excepte *ipRouteProto* com a lectura-escriptura. Tal com s'ha mencionat abans, el suport d'establiment només s'implementa per les variables *ipRouteDest*, *ipRouteNextHop* i *ipRouteType*. Per acceptar sol•licituds d'establiment que poden especificar diferents atributs no suportats, s'accepten sol•licitud d'establiment per les variables restants de la taula *ipRouteEntry*: *ipRouteIfIndex*, *ipRouteMetric1*, *ipRouteMetric2*, *ipRouteMetric3*, *ipRouteMetric4*, *ipRouteMetric5*, *ipRouteAge* i *ipRouteMask*. No es retorna cap resposta d'error a l'originador de sol•licituds d'establiment. Una sol•licitud d'obtenció posterior mostrarà els valors originals a mesura que es retenen. El daemon **snmpd** no coordina l'encaminat amb el daemon **routed**. Si daemon **gated** s'està executant i ha enregistrat *ipRouteTable* amb el daemon **snmpd**, no es permetran les sol•licituds d'establiment *ipRouteTable*.

RFC 1229 descriu variables que es poden establir permeses per **snmpd**. Consulteu les entrades anteriors per conèixer les desviacions reals.

Els exemples següents utilitzen l'ordre **snmpinfo**. Se suposa que el nom de comunitat per defecte **snmpinfo**, públic, té accés de lectura-escriptura pel subarbre MIB respectiu.

```
snmpinfo -m set sysContact.0="Primary contact: Bob Smith, office phone: 555-5555,
beeper: 9-123-4567. Secondary contact: John Harris, phone: 555-1234."
```

Aquesta ordre estableix el valor de `sysContact.0` per la sèrie especificada. Si ja existeix una entrada per `sysContact.0`, se substituirà.

```
snmpinfo -m set sysName.0="bears.austin.ibm.com"
```

Aquesta ordre estableix el valor de `sysName.0` per la sèrie especificada. Si ja existeix una entrada per `sysName.0`, se substituirà.

```
snmpinfo -m set sysLocation.0="Austin site, building 802, lab 3C-23, southeast
corner of the room."
```

Aquesta ordre estableix el valor de `sysLocation.0` per la sèrie especificada. Si ja existeix una entrada per `sysLocation.0`, se substituirà.

```
snmpinfo -m set ifAdminStatus.2=2
```

Aquesta ordre inhabilita l'adaptador d'interfície de xarxa que té l'ifIndex 2. Si el valor assignat és 1, s'habilita l'adaptador d'interfície.

```
snmpinfo -m set atPhysAddress.2.1.192.100.154.2=02:60:8c:2e:c2:00
snmpinfo -m set ipNetToMediaPhysAddress.2.1.192.100.154.2=02:60:8c:2e:c2:00
```

Aquestes dues ordres canvien l'adreça de maquinari de l'entrada de taula ARP de `192.100.154.2` per `02:60:8c:2e:c2:00`. Aquestes dues ordres afecten a la mateixa entrada de taula ARP. La variable MIB *atPhysAddress* és una variable desaprovada i s'està substituint per una variable MIB *ipNetToMediaPhysAddress*. D'aquesta manera, *atPhysAddress* i *ipNetToMediaPhysAddress* accedeixen a la mateixa estructura de la taula ARP del kernel TCP/IP.

```
snmpinfo -m set atNetAddress.2.1.192.100.154.2=192.100.154.3
snmpinfo -m set ipNetToMediaNetAddress.2.1.192.100.154.2=192.100.154.3
```

Aquestes ordres canvien l'adreça IP de l'entrada de taula ARP de `192.100.154.2` per `192.100.154.3`. Aquestes dues ordres afecten a la mateixa entrada de taula ARP. La variable MIB *atNetAddress* és una variable desaprovada i s'està substituint per una variable MIB *ipNetToMediaNetAddress*. D'aquesta manera, *atNetAddress* i *ipNetToMediaNetAddress* accedeixen a la mateixa estructura de la taula ARP del kernel TCP/IP.

```
snmpinfo -m set ipForwarding.0=1
```

Aquesta ordre estableix el kernel **TCP/IP** per tal que pugui reenviar paquets si l'amfitrió d'agent té més d'una interfície connectada. Si l'amfitrió només té una interfície activa, la sol•licitud d'establiment fallarà i l'agent **snmpd** retornarà un error, *badValue*.

```
snmpinfo -m set ipDefaultTTL=50
```

Aquesta ordre permet utilitzar un datagrama IP mitjançant la duració per defecte (TTL) per passar a través d'un màxim de 50 passarel•les abans de que es descarti. Quan cada passarel•la processa un datagrama, la passarel•la resta 1 del camp de duració. A més, cada passarel•la redueix el camp de duració segons el número de segons que el datagrama ha esperat pel servei a la passarel•la abans de passar el datagrama a la destinació següent.

```
snmpinfo -m set ipRouteDest.192.100.154.0=192.100.154.5
```

Aquesta ordre estableix l'adreça IP de destinació de la ruta associada amb `192.100.154.0` a l'adreça IP `192.100.154.5`, suposant que la ruta `192.100.154` ja existeix.

```
snmpinfo -m set ipRouteNextHop.192.100.154.1=129.35.38.47
```

Aquesta ordre estableix una ruta per a l'amfitrió 192.100.154.1 mitjançant l'amfitrió de passarel•la 129.35.38.47, suposant que la ruta 192.100.154.1 ja existeix.

```
snmpinfo -m set ipRouteNextHop.192.100.154.0=192.100.154.7
```

Aquesta ordre estableix una ruta per la xarxa de classe C 192.100.154 mitjançant l'amfitrió de passarel•la 192.100.154.7, suposant que la ruta 192.100.154.0 ja existeix. Tingueu en compte que la part d'amfitrió de l'adreça ha d'ésser 0 per indicar una adreça de xarxa.

```
snmpinfo -m set ipRouteType.192.100.154.5=2
```

Aquesta ordre elimina qualsevol ruta de l'amfitrió 192.100.154.5.

```
snmpinfo -m set ipRouteDest.129.35.128.1=129.35.128.1
               ipRouteType.129.35.128.1=3
            ipRouteNextHop.129.35.128.1=129.35.128.90
```

Aquesta ordre crea una nova ruta des de l'amfitrió 129.35.128.90 a 129.35.128.1 en forma de passarel•la.

```
snmpinfo -m set ipNetToMediaType.2.1.192.100.154.11=4
```

Aquesta ordre estableix l'entrada de la taula ARP per 192.100.154.11 com a estàtica.

```
snmpinfo -m set snmpEnableAuthenTraps=2
```

Aquesta ordre fa que l'agent **snmpd** de l'amfitrió especificat no generi errors trap *authenticationFailure*.

```
snmpinfo -m set smuxPstatus.1=2
```

Aquesta ordre invalida el similar SMUX 1. El resultat és que finalitza la connexió entre l'agent **snmpd** i aquest similar SMUX.

```
snmpinfo -m set smuxTstatus.8.1.3.6.1.2.1.4.21.0=2
```

Aquesta ordre invalida o elimina el muntatge de l'arbre SMUX 1.3.6.1.2.1.4.21, la taula *ipRoute*. El primer número de l'instància indica el número de nivells de l'identificador de l'arbre SMUX. El número final de l'instància indica smuxTpriority. En aquest exemple, hi ha 8 nivells de l'identificador d'arbre SMUX: 1.3.6.1.2.1.4.21. La prioritat 0 és la més alta.

```
snmpinfo -m set ifExtnsPromiscuous.1=1 ifExtnsPromiscuous.2=2
```

Aquesta ordre activa la modalitat de promiscuïtat pel primer dispositiu de la taula d'interfícies i desactiva la modalitat de promiscuïtat pel segon dispositiu de la taula d'interfícies.

```
snmpinfo -m set ifExtnsTestType.1=testFullDuplexLoopBack
```

Aquesta ordre inicia la prova testFullDuplexLoopBack a l'interfície 1.

```
snmpinfo -m set ifExtnsRcvAddrStatus.1.129.35.128.1.3.2=2
```

Aquesta ordre indica a l'interfície 1 que elimini l'adreça física 129.35.128.1.3.2 de la seva llista d'adreces acceptables.

```
snmpinfo -m set dot5Commands.1=2
```

Aquesta ordre indica a la primera interfície que s'obri.

```
snmpinfo -m set dot5RingSpeed.1=2
```

Aquesta ordre indica a la primera interfície que estableixi la velocitat d'anell a 1 megabit.

```
snmpinfo -m set dot5ActMonParticipate.1=1
```

Aquesta ordre indica a la primera interfície que participi en un procés de selecció de control actiu.

```
snmpinfo -m set dot5Functional.1=255.255.255.255.255.255
```

Aquesta ordre estableix la màscara d'adreça funcional per permetre tot tipus d'accions.

```
snmpinfo -m set fddimibSMTUserData.1="Greg's Data"
```

Aquesta ordre estableix les dades d'usuari de la primera entitat SMT en "Greg's Data".

```
snmpinfo -m set fddimibMACFrameErrorThreshold.1.1=345
```

Aquesta ordre estableix el llindar d'errors de marc a 345 al primer MAC de la primera entitat SMT.

Nota: Totes les variables descrites anteriorment s'inclouen dins d'uns dels mètodes llistats utilitzats per establir la variable.

Consulteu “Protocol de resolució d'adreces” a la pàgina 142 i “Adreces d'Internet” a la pàgina 169 per obtenir més informació sobre protocols i adreces d'Internet.

Resolució de problemes del daemon SNMP

Els consells per la resolució de problemes del daemon **SNMP** inclouen la resolució de problemes de terminació, problemes d'accés de variable MIB, accés de variable MIB en problemes d'entrada de comunitat, problemes noSuchName, problemes per no obtenció de resposta d'agent i errors de daemon.

Problema de terminació de daemon

Si l'agent **snmpd** no es comporta segons s'ha previst, seguiu un dels consells que es presenten a continuació per ajudar-vos a determinar i corregir el problema. És molt recomanable que inicieu l'agent **snmpd** amb algun tipus d'inici de sessió. Si en invocar el daemon **snmpd** es produeixen problemes, és recomanable configurar el daemon **syslogd** per l'inici de sessió al nivell del recurs del daemon i de la gravetat DEBUG. Consulteu l'ordre **snmpd** a *Commands Reference, Volume 5* i el fitxer **snmpd.conf** a *Files Reference* per obtenir més informació sobre el registre **snmpd**.

Si el daemon **snmpd** finalitza en el moment d'invocar-se, les causes possibles d'aquest error i les solucions possibles són les següents:

- El motiu pel qual el daemon **snmpd** ha finalitzen quedarà enregistrada al fitxer de registre **snmpd** o al fitxer de registre **syslogd** configurat. Comproveu el fitxer de registre per veure el missatge d'error **FATAL**.

  Solució: corregiu el problema i reinicieu el daemon **snmpd**.
- La línia d'ordres **snmpd** no s'ha utilitzat correctament. Si s'ha invocat l'ordre **snmpd** sense el controlador de recursos del sistema, la sentència d'ús necessària s'envia a la pantalla. Si s'ha invocat el daemon **snmpd** amb el control SRC, el missatge d'ús no s'envia a la pantalla. Comproveu el fitxer de registre per veure el missatge d'ús.

  Solució: invoqueu l'ordre **snmpd** amb la sentència d'ús correcte.
- L'usuari root ha d'invocar el daemon **snmpd**.

  Solució: canvieu a l'usuari root i reinicieu el daemon **snmpd**.
- El fitxer **snmpd.conf** ha d'ésser propietat de l'usuari root. L'agent **snmpd** verifica la propietat del fitxer de configuració. Si el fitxer no és propietat de l'usuari root, l'agent **snmpd** finalitzarà amb un error molt greu.

  Solució: assegureu-vos que sou l'usuari root, canvieu la propietat del fitxer de configuració a l'usuari root i reinicieu el daemon **snmpd**.
- El fitxer **snmpd.conf** ha d'existir. Si el senyalador **-c** no s'especifica al fitxer de configuració de la línia d'ordres **snmpd**, això indicarà que el fitxer **/etc/snmpd.conf** no existeix. Si el fitxer **/etc/snmpd.conf** s'elimina de forma accidental, torneu a instal•lar la imatge **bos.net.tcp.client** o torneu a construir el fitxer amb les entrades de configuració adients tal com es defineix a la pàgina de gestió del fitxer **snmpd.conf**. Si el fitxer de configuració s'ha especificat amb el senyalador **-c** de la línia d'ordres

snmpd, assegureu-vos que el fitxer existeix i que és propietat de l'usuari root. El nom complet de fitxer i de camí d'accés del fitxer de configuració s'ha d'especificar o s'utilitzarà el fitxer **/etc/snmpd.conf** per defecte.

Solució: assegureu-vos que el fitxer de configuració especificat existeix i que aquest fitxer és propietat de l'usuari root. Reinicieu el daemon **snmpd**.

- El `udp port 161` ja està vinculat. Assegureu-vos que el daemon **snmpd** no s'estigui executant. Emeteu l'ordre **ps -eaf | grep snmpd** per determinar si ja s'està executant un procés de daemon **snmpd**. Només un agent **snmpd** pot vincular-se a `udp port 161`.

  Solució: elimineu l'agent **snmpd** existent o no intenteu iniciar un altre procés de daemon **snmpd**.

Problema d'error de daemon

Si el daemon **snmpd** falla quan emeteu un senyal **refresh** o **kill -1**, les causes possibles d'aquest error i les solucions possible són les següents:

- El motiu pel qual el daemon **snmpd** ha finalitzen quedarà enregistrada al fitxer de registre **snmpd** o al fitxer de registre **syslogd** configurat. Comproveu el fitxer de registre per veure el missatge d'error FATAL.

  Solució: corregiu el problema i reinicieu el daemon **snmpd**.
- Assegureu-vos que el nom de fitxer i de camí d'accés complet del fitxer de configuració s'especifica quan s'invoca el daemon **snmpd**. El daemon **snmpd** realitza un procés fork i modifica el directori root durant l'invocació. Si no s'especifica el nom del camí d'accés complet del fitxer de configuració, l'agent **snmpd** no podrà trobar el fitxer quan es dugui a terme una renovació. Això és un error molt greu i farà que l'agent **snmpd** finalitzi.

  Solució: especifiqueu el nom de fitxer i de camí d'accés complet del fitxer de configuració **snmpd**. Assegureu-vos que el fitxer de configuració pertany a l'usuari root. Reinicieu el daemon **snmpd**.
- Assegureu-vos que el fitxer de configuració **snmpd** encara existeix. És possible que el fitxer s'hagi eliminat de forma accidental un cop s'hagi invocat l'agent **snmpd**. Si l'agent **snmpd** no pot obrir el fitxer de configuració, l'agent **snmpd** finalitzarà.

  Solució: torneu a crear el fitxer de configuració **snmpd**, assegureu-vos que el fitxer de configuració és propietat de l'usuari root i reinicieu el daemon **snmpd**.

Problema d'accés de la variable MIB

Si no es pot accedir a les variables MIB des de l'agent **snmpd**; si l'agent **snmpd** s'està executant però el temps d'espera de resposta de l'aplicació del gestor **Simple Network Management Protocol (SNMP)** finalitza des de l'agent **snmpd**, intenteu el següent:

- Comproveu la configuració de la xarxa de l'amfitrió on s'executa l'agent **snmpd** mitjançant l'ordre **netstat -in**. Verifiqueu lo0, el bucle de retorn i que el dispositiu està connectat. Si el dispositiu està desconnectat, apareixerà un asterisc (*) a l'esquerra de lo0. lo0 ha d'estar configurat per l'agent **snmpd** per sol•licituds de servei.

  Solució: emeteu l'ordre següent per iniciar l'interfície de bucle de retorn:

  ```
  ifconfig lo0 inet up
  ```
- Verifiqueu que el daemon **snmpd** té una ruta cap l'amfitrió on s'emeten les sol•licituds.

  Solució: a l'amfitrió on s'està executant el daemon **snmpd**, afegiu una ruta a l'amfitrió on s'ha emès l'ordre **route add**. Consulteu la descripció de l'ordre **route** que apareix a *Commands Reference, Volume 4* per obtenir més informació.
- Comproveu si el nom d'amfitrió i l'adreça IP d'amfitrió tenen el mateix valor.

  Solució: restabliu el nom d'amfitrió per a què coincideixi amb l'adreça IP de l'amfitrió.
- Comproveu si *localhost* s'ha definit per ser l'adreça IP de lo0.

  Solució: definiu *localhost* per tal que sigui la mateixa adreça utilitzada per l'adreça IP lo0 (normalment `127.0.0.1`).

>Problema d'entrada de comunitat d'accés de variable MIB

Si s'especifica una entrada de comunitat al fitxer de configuració amb un nom de vista MIB però no es pot accedir a les variables MIB, comproveu el següent:

- Assegureu-vos que heu especificat correctament l'entrada de la comunitat. Si heu especificat un nom de vista a l'entrada de comunitat, caldrà omplir tots els camps de la comunitat.

  Solució: especifiqueu tots els camps de l'entrada de la comunitat al fitxer de configuració. Renoveu l'agent **snmpd** i torneu a intentar la sol•licitud.
- Assegureu-vos que el mode d'accés de l'entrada de la comunitat correspon amb el vostre tipus de sol•licitud. Si emeteu una sol•licitud **get** o **get-next**, assegureu-vos que la comunitat té permisos de només lectura o d'escriptura-lectura. Si emeteu una sol•licitud **set**, assegureu-vos que la comunitat té permisos de lectura-escriptura.

  Solució: especifiqueu el mode d'accés correcte a l'entrada de la comunitat. Renoveu l'agent **snmpd** i torneu a intentar la sol•licitud.
- Assegureu-vos que s'especifica una entrada de vista del nom de vista especificat a l'entrada de la comunitat al fitxer de configuració. Si s'ha especificat un nom de vista a l'entrada de la comunitat, però no existeix una entrada de vista corresponent, l'agent **snmpd** no permetrà l'accés a aquesta comunitat. Una entrada de vista és absolutament necessària per a un nom de vista especificat en una entrada de comunitat al fitxer de configuració.

  Solució: especifiqueu una entrada de vista pel nom de vista especificat a l'entrada de la comunitat. Renoveu l'agent **snmpd** i torneu a intentar la sol•licitud.
- Si s'especifica `iso` com a subarbre MIB per l'entrada de la vista, verifiqueu que s'especifica `iso.3`. L'instància de `3` és necessària per a què l'agent **snmpd** accedeixi a la part `org` de l'arbre `iso`.

  Solució: especifiqueu el subarbre MIB com a `iso.3` a l'entrada de la vista. Renoveu l'agent **snmpd** i torneu a intentar la sol•licitud.
- Comproveu *l'adreça IP* i la *màscara de xarxa* de l'entrada de la comunitat. Verifiqueu que l'amfitrió que emet la sol•licitud SNMP s'inclou a la comunitat que s'especifica amb el nom de comunitat.

  Solució: canvieu els camps de l'*adreça IP* i la *màscara de xarxa* de l'entrada de la comunitat del fitxer de configuració per a què incloguin l'amfitrió que emet la sol•licitud SNMP.

Problema per no obtenir resposta de l'agent

Si l'*adreça IP* de la comunitat s'especifica com a 0.0.0.0, però no hi ha cap resposta de l'agent **snmpd**, intenteu el següent:

- Comproveu el camp *màscara de xarxa* de l'entrada de la comunitat. Per l'accés general al nom de la comunitat, la *màscara de xarxa* ha d'ésser **0.0.0.0**. Si la *màscara de xarxa* s'especifica per a què sigui `255.255.255.255`, l'agent **snmpd** es configura per no permetre cap sol•licitud amb el nom de comunitat especificat.

  Solució: especifiqueu la *màscara de xarxa* a l'entrada de la comunitat to 0.0.0.0. Renoveu l'agent **snmpd** i torneu a intentar la sol•licitud.
- Assegureu-vos que el mode d'accés de l'entrada de la comunitat correspon amb el vostre tipus de sol•licitud. Si emeteu una sol•licitud **get** o **get-next**, assegureu-vos que la comunitat té permisos de només lectura o d'escriptura-lectura. Si emeteu una sol•licitud **set**, assegureu-vos que la comunitat té permisos de lectura-escriptura.

  Solució: especifiqueu el mode d'accés correcte a l'entrada de la comunitat. Renoveu l'agent **snmpd** i torneu a intentar la sol•licitud.

Problema noSuchName

Si, en intentar establir una variable MIB a la qual se suposa que l'agent **snmpd** dóna suport, es retornarà un missatge `noSuchName`. La causa pot ésser la següent:

La sol•licitud d'establiment emesa no ha inclòs un nom de comunitat per a una comunitat vàlida amb accés d'escriptura. El protocol **SNMP** dicta que una sol•licitud d'establiment amb una comunitat amb privilegis d'accés inadequats, s'ha de respondre amb el missatge d'error `noSuchName`.

Solució: emeteu la sol•licitud d'establiment amb un nom de comunitat per a una comunitat que tingui privilegis d'escriptura i que inclogui l'amfitrió des del qual s'emet una sol•licitud d'establiment.

Sistema de fitxers de xarxa

El sistema de fitxers de xarxa (NFS) és un mecanisme per emmagatzemar fitxers en una xarxa. Es tracta d'un sistema de fitxers distribuïts que permet als usuaris accedir a fitxers i directoris ubicats a ordinadors remots i tractar a aquests fitxers i directoris com si fossin locals.

Per exemple, els usuaris poden utilitzar ordres del sistema operatiu per crear, eliminar, llegir, escriure i establir atributs de fitxer per fitxers i directoris remots.

El paquet de software NFS inclou ordres i daemons per NFS, el servei d'informació de la xarxa (NIS) i altres serveis. Encara que NFS i NIS estiguin instal•lats de forma conjunta com un paquet, cadascun és independent i es configura i s'administra de forma individual.

AIX 5.3 i posterior dóna suport als protocols de NFS versions 2, 3 i 4. NFS versió 4 és la versió definida més recentment de NFS i la descriu RFC 3530. Els detalls adicionals sobre el suport AIX de NFS versió 4 es tractaran més endavant en aquesta secció. Els clients NFS utilitzen el protocol de NFS versió 3 per defecte.

Serveis NFS

NFS proporciona els seus serveis a través d'una relació client-servidor.

Els ordinadors que posen a disposició el seus *sistemes de fitxers* o *directoris* i altres recursos per accés remot s'anomenen *servidors*. L'acte de fer que els sistemes de fitxers estiguin disponibles s'anomena *exportar*. Els ordinadors i els seus processos que utilitzen recursos de servidor s'anomenen *clients*. Un cop que un client munta un sistema de fitxers que un servidor exporta, el client pot accedir a fitxers de servidor individuals (l'accés a directoris exportats es pot restringir a clients específics).

Els serveis principals proporcionats per NFS són:

Taula 88. Serveis NFS

Servei	Descripció
Servei de muntatge	El muntatge es realitza a partir del daemon**/usr/sbin/rpc.mountd** daemon al servidor i l'ordre **/usr/sbin/mount** al client. Aquest servei només es troba disponible a NFS versions 2 i 3.
Accés de fitxers remot	Accessos des del daemon**/usr/sbin/nfsd** al servidor i el daemon **/usr/sbin/biod** al client.
Servei d'execució remot	S'executa des del daemon **/usr/sbin/rpc.rexd** al servidor i l'ordre **/usr/bin/on** al client.
Servei d'estadística de sistema remot	Compila a partir del daemon **/usr/sbin/rpc.rstatd** al servidor i l'ordre **/usr/bin/rup** al client.
Servei de llistat d'usuari remot	Llista a partir del daemon **/usr/lib/netsvc/rusers/rpc.rusersd** al servidor i l'ordre **/usr/bin/rusers** al client.
Servei de paràmetres d'arrencada	Proporciona paràmetres d'arrencada a clients sense disc del sistema operatiu Sun des del daemon **/usr/sbin/rpc.bootparamd** al servidor.
Servei de protecció remot	Protegeix a partir del daemon **/usr/lib/netsvc/rwall/rpc.rwalld** al servidor i l'ordre **/usr/sbin/rwall** al client.
Servei d'enviament	Envia un corrent unidireccional de paquets RPC des del daemon **/usr/lib/netsvc/spray/rpc.sprayd** al servidor i l'ordre **/usr/sbin/spray** al client.
Servei d'autenticació de PC	Proporciona un servei d'autenticació d'usuari per PC-NFS des del daemon **/usr/sbin/rpc.pcnfsd** al servidor.

Taula 88. Serveis NFS (continuació)

Servei	Descripció
Servei de seguretat ampliat	Proporciona accés a client i al servidor a serveis de seguretat més avançats com, per exemple, Kerberos 5. El daemon **/usr/sbin/gssd** proporciona NFS amb accés a serveis de seguretat proporcionats pel servei d'autenticació de xarxa. Cal instal•lar el servei d'autenticació de xarxa i els catàlegs de fitxers de biblioteca criptogràfica (`krb5.client.rte`, **krb5.server.rte**, i **modcrypt.base**). Aquests catàlegs de fitxers poden instal•lar-se des del paquet d'ampliació AIX.
Servei de conversió d'identitat	Realitza conversions entre principals de seguretat, sèries d'identitats de NFS versió 4 i els seus ID de sistema numèrics corresponents. A més, es proporciona la correlació d'informació d'entitats de dominis NFS versió 4 externs. Aquests serveis es proporcionen mitjançant el daemon **/usr/sbin/nfsrgyd**.

Nota: Un ordinador pot ser un servidor NFS i un client NFS a la vegada.

Els servidors NFS versions 2 i 3 *no tenen estat*. Això significa que el servidor no conserva cap informació de transacció sobre els seus clients. Una sola transacció NFS correspon a una sola operació de fitxer completa. NFS requereix que el client recordi qualsevol informació necessària per la utilització posterior de NFS.

Un servidor NFS versió 4 té estat perquè s'ha definit les operacions d'obertura i blocatge de fitxer al protocol de NFS versió 4.

Suport de llistes de control d'accés NFS

La implementació de AIX NFS versió 4 dóna suport a dos tipus d'ACL: NFS4 i AIXC.

L'origen autoritzar per la comprovació d'accés es basa en el sistema de fitxers subjacent exportat pel servidor NFS. El sistema de fitxers té en compte els controls d'accés del fitxer (ACL o bits de permís), les credencials de l'emissor i altres restriccions de sistema local que puguin aplicar-se. Les aplicacions i els usuaris no pressuposen que l'examinació de només bits de modalitat UNIX o ACL pugui fer-se servir per preveure l'accés de forma concloent.

Les ordres **aclget**, **aclput** i **acledit** es poden utilitzar en el client per manipular ACL de NFS o d'AIX. Per obtenir més informació, consulteu Llistes de control d'accés de *Security*.

RBAC d'NFS

NFS proporciona compatibilitat per a RBAC (Role Based Access Control). Les ordres del client i del servidor NFS estan habilitades per a RBAC.

Això permet que els usuaris que no siguin root puguin executar ordres d'NFS quan l'administrador assigna el rol RBAC de l'ordre a l'usuari. Per veure la llista de privilegis i cadenes d'autorització associada amb les ordres d'NFS, consulteu el fitxer /etc/security/privcmds del sistema.

NFS4 ACL

NFS4 ACL és la llista de control definida pel protocol NFS versió 4.

NFS4 ACL és independent de la plataforma i, per tant, pot ser suportat pels clients o servidors d'altres proveïdors. Els clients i servidors de NFS versió 4 no són necessaris per suportar NFS4 ACL.

En un servidor AIX, si una instància de sistema de fitxers físic subjacent suporta NFS4 ACL, el servidor AIX NFS4 suportarà NFS4 ACL per l'instància del sistema de fitxers en qüestió. La majoria de tipus de sistemes de fitxers físics de AIX no suporten NFS4 ACL. Aquests tipus de sistemes de fitxers inclouen, encara que no exclusivament, CFS, UDF, JFS i JFS2 amb la versió 1 d'atribut ampliada. Totes les instàncies de JFS2 amb la versió 2 d'atribut ampliada suporten NFS4 ACL.

Els sistemes de fitxers de client NFS versió 4 poden llegir i escriure NFS4 ACL si l'instància del sistema de fitxers NFS versió 4 del servidor suporta NFS4 ACL.

AIX ACL

La llista de control d'accés d'AIX és una llista de control propietat del servidors AIX.

No es defineix mitjançant el protocol NFS versió 4 i només la poden interpretar servidor i clients AIX.

En un servidor NFS versió 4, la ACL d'AIXC se suporta quan la instància de fitxers subjacent dóna suport a l'ACL d'AIX. Totes les instàncies de JFS i JFS2 donen suport a l'ACL d'AIXC.

Un client de NFS versió 4 disposa d'una opció de muntatge que habilita o inhabilita el suport per l'ACL deAIX. El valor per defecte no dóna suport a l'ACL d'AIXC. Un usuari d'un sistema de fitxers del client de NFS versió 4 pot llegir i escriure ACL d'AIXC quan el client i el servidor executen AIX, l'instància del sistema de fitxers físics subjacent del servidor dóna suport a l'ACL d'AIXC i el client d'AIX munta l'instància del sistema de fitxers amb l'ACL d'AIXC habilitada. El suport d'ACL d'AIXC a NFS versió 4 es similar al suport d'ACL d'AIXC de les implementacions de NFS versió 2 i NFS versió 3 de AIX.

Totes les instàncies del sistema de fitxers JFS2 amb la versió 2 d'atribut estès donen suport a l'ACL d'AIXC i a l'ACL de NFS4. Un fitxer d'aquest tipus de sistema de fitxers pot tenir bits de modalitat únicament (no ACL), una ACL de NFS4 o una ACL d'AIXC. No obstant això, no pot tenir l'ACL de NFS4 ni l'ACL d'AIXC a la vegada.

L'ordre **aclgettypes** pot fer-se servir per determinar el tipus d'ACL que poden llegir-se i escriu-re's en una instància del sistema de fitxers. Aquesta ordre pot retornar una sortida diferent quan s'executa contra un sistema de fitxers físic en un servidor NFS versió 4 de forma local respecte a quan s'executa contra el mateix sistema de fitxers en un client de NFS versió 4. Per exemple, una instància de sistema de fitxers de NFS versió 4 en un servidor de NFS versió 4 pot donar suport a ACL de NFS4 i a ACL d'AIXC. Tanmateix, el client només es configura per enviar i rebre ACL de NFS4. En aquest cas, quan s'executa l'ordre **aclgettypes** des d'un sistema de fitxers de client NFS versió 4, només es retorna NFS4. A més, si un usuari d'un client sol•licita una ACL d'AIX, es retorna un error.

Suport de sistema de fitxers de memòria cau

El sistema de fitxers de memòria cau (CacheFS) és un mecanisme d'emmagatzematge en memòria cau del sistema de fitxers amb finalitat general que millora el rendiment i l'escalabilitat del servidor NFS reduint la càrrega del servidor i de la xarxa.

Dissenyat com un sistema de fitxes amb capes, CacheFS permet emmagatzemar en memòria cau un sistema de fitxers en un altre. En un entorn NFS, CacheFS incrementa la proporció client per servidor, redueix les càrregues de servidor i xarxa i millora el rendiment del clients en enllaços lents com, per exemple, el protocol punt a punt (PPP).

A la màquina del client es crea una memòria cau per tal que es pugui accedir als sistemes de fitxers especificats que s'han de muntar de forma local enlloc d'accedir-hi des de la xarxa. Els fitxers es col•loquen a la memòria cau quan un usuari sol•licita l'accés a aquests per primera vegada. La memòria cau no s'omple fins que les sol•licituds de l'usuari accedeixen a un o varis fitxers. És possible que les sol•licituds de fitxer inicials siguin lentes. Tanmateix, és possible que els usos posteriors dels mateixos fitxers siguin més ràpids.

Nota:

1. A la memòria cau, no es poden emmagatzemar el sistemes de fitxers / (root) ni `/usr`.
2. Podeu muntar només sistemes de fitxers que es comparteixen. (Consulteu l'ordre **exportfs** a *Commands Reference, Volume 2*.)
3. El rendiment no es veu beneficiat si s'emmagatzema a la memòria cau el sistema de fitxers de diari local (JFS).

4. Haureu de tenir autoritat d'arrel o de sistema per realitzar les tasques de la taula següent.

Taula 89. Tasques CacheFS

Tasca	Camí d'accés ràpid de SMIT	Ordre o fitxer
Configurar una memòria cau	`cachefs_admin_create`	**cfsadmin -c** *NomDirectoriMuntatge*[1].
Especificar fitxers per al muntatge	`cachefs_mount`	**mount -F cachefs -o backfstype=***TipusSistemaFitxers*, **cachedir=** *DirectoriMemòriaCau*[,*opcions*] BackFileSystem *NomDirectoriMuntatge*[2] o edit `/etc/`**filesystems**.
Modificar la memòria cau	`cachefs_admin_change`	elimineu la memòria cau, torneu-la a crear mitjançant les opcions de l'ordre **mount** adequades.
Visualitzar informació de memòria cau	`cachefs_admin_change`	**cfsadmin -l***NomDirectoriMuntatge.*
Eliminar una memòria cau	`cachefs_admin_remove`	1. Desmunteu el sistema de fitxers: **umount** *NomDirectoriMuntatge* 2. Determineu l'ID de memòria cau: **cfsadmin -l***NomDirectoriMuntatge* 3. Suprimiu el sistema de fitxers: **cfsadmin -d** *DirMemòriaCauIDMemòriaCau*
Comprovar la integritat del sistema de fitxers	`cachefs_admin_check`	**fsck_cachefs***DirectoriMemòriaCau*[3].

Notes:

1. Un cop que hagueu creat la memòria cau, no realitzeu cap operació dins del directori de la memòria cau (`cachedir`). Això provocaria conflictes dins del programari de CacheFS.
2. Si utilitzeu l'opció de l'ordre **mount** per especificar fitxers pel muntatge, haureu de tornar a emetre l'ordre cada cop que es torni a iniciar el sistema.
3. Utilitzeu les opcions **-m** o **-o** de l'ordre **fsck_cachefs** per verificar els sistemes de fitxers sense dur a terme cap reparació.
4. Després de migrar el sistema a l'AIX versió 6.1 o posterior des de versions anteriors, el sistema de fitxers de la memòria cau antics que es crein en la versió més antiga de l'AIX s'hauran d'eliminar i tornar a crear.

Suport de fitxers correlacionats NFS

El suport de fitxers correlacionats NFS permet als programes d'un client accedir a un fitxer com si es trobés a la memòria.

Mitjançant la subrutina **shmat**, els usuaris poden mapar àrees d'un fitxer amb el seu espai d'adreces. A mesura que un programa llegeix i escriu en aquesta àrea de la memòria, el fitxer es llegeix a la memòria des del servidor o s'actualitza segons convingui al servidor.

La correlació de fitxers per NFS es limita de tres maneres:

- Els fitxers no comparteixen informació perfectament entre els clients.
- Els canvis en un fitxer d'un client mitjançant un fitxer correlacionat no es veuen en un altre client.
- El bloqueig i el desbloqueig d'àrees d'un fitxer no és un mode efectiu de coordinar dades entre clients.

Si s'ha d'utilitzar un fitxer NFS per compartir dades entre programes en clients diferents, utilitzeu el blocatge d'enregistrament i les subrutines **read** i **write** habituals.

Múltiples programes del mateix client poden compartir dades de manera efectiva mitjançant un fitxer correlacionat. El blocatge d'enregistrament d'avís pot coordinar actualitzacions pel fitxer al client, sempre que s'hagi bloquejat tot el fitxer. Múltiples clients poden compartir fitxers correlacionats mitjançant dades només si les dades no es modifiquen mai, igual que en una base de dades estàtica.

Servei de proxy NFS

AIX suporta els servidors NFS que serveixen. Un servidor AIX pot exportar concorrentment i local sistemes de fitxers i exportacions proxy. La vista de proxy exportada es pot muntar segons els clients NFS.

AIX El servei proxy NFS utilitza l'emmagatzematge en memòria cau de dades a les quals s'ha accedit per servir sol•licituds posteriors similars de forma local amb el tràfic de xarxa reduït pel servidor de fons. El servei proxy potencialment pot ampliar el accés de dades NFS per xarxes més lentes o menys segures amb una millora del rendiment i una reducció del tràfic de xarxa per el servidor principal on es troben les dades. En funció de la disponibilitat i dels requisits de gestió de contingut, el servei proxy pot proporcionar una solució per l'ampliació de l'accés NFS als límits de la xarxa sense que calgui copiar dades. Podeu configurar el servei proxy NFS AIX mitjançant l'ordre **mknfsproxy**.

L'emmagatzematge en memòria cau de proxy es pot utilitzar amb els protocols NFS versió 3 i versió 4. El protocol entre el proxy i els clients connectats pot ser NFS v3 o NFS v4 si el protocol NFS v4 s'utilitza entre el proxy i el servidor de fons. No obstant això, si s'utilitza el protocol NFS v3, el protocol entre el proxy i els clients connectats haurà d'ésser NFS v3. Les lectures i escriptures de les dades estan suportades, a més dels blocatges preventius d'interval d'octets.

Els mètodes de seguretat krb5, krb5i i krb5p es poden fer servir entre el servidor proxy i els clients connectats a aquest. Aquests mètodes també es poden utilitzar entre el servidor proxy i el servidor principal. Mitjançant la tecnologia de reenviament de tiquet a través de proxy, podeu autenticar al client i ser autenticat al servidor principal. Per treure el màxim profit d'aquesta tecnologia, utilitzeu l'ordre **kinit** amb l'opció **-f** quan dueu a terme la configuració Kerberos. Si s'utilitza la seguretat **auth_sys** entre el proxy i el servidor de fons, en accedir al servidor de fons, el servidor proxy correlacionarà accessos de client Kerberos als atributs **auth_sys**. Per obtenir millors resultats, el servidor proxy i el servidor de component de fons han de compartir les mateixes definicions d'identitat d'usuari i de grup.

Les restriccions següents s'apliquen al servei proxy:

- El servei proxy requereix clients connectats mitjançant TCP.
- Donat que el servei proxy permet als clients NFS v3 examinar l'espai de nom exportat NFS v4 sense utilitzar les ordres **mount** i **unmount**, cal que utilitzeu l'ordre **mknfsproxy** amb l'opció **mfsid** quan construïu el sistema de fitxers proxy.
- El sistema de fitxers de memòria cau utilitzat amb el servei proxy ha de ser el sistema de fitxers JFS ampliat (JFS2).
- El servei proxy executa CacheFS a sobre d'un client AIX muntat en el servidor NFS de component de fons. La funció d'E/S (CIO) concurrent, disponible amb el client NFS AIX, amplia el rendiment de CacheFS. És possible que els intents per accedir directament al muntatge de client NFS subjacent fallin degut a conflictes amb intents oberts de CIO.

Tipus de muntatges NFS

Existeixen tres tipus de muntatges NFS: predefinit, explícit i automàtic.

Els muntatges *predefinits* s'especifiquen al fitxer `/etc/filesystems`. Cada stanza (o entrada) d'aquest fitxer defineix les característiques d'un muntatge. Les dades com, per exemple, el nom d'amfitrió, el camí d'accés remot, el camí d'accés local i les opcions de muntatge es llisten en aquesta entrada. Els muntatges predefinits s'utilitzen quan determinats muntatges sempre són necessaris per tal que el funcionament d'un client sigui correcte.

Els muntatges *explícits* serveixen per satisfer les necessitats de l'usuari root. Els muntatges explícits normalment es realitzen per breus períodes de temps quan apareix la necessitat de muntatges ocasionals no planejats. Els muntatges explícits també es poden utilitzar si un muntatge és necessari per tasques especials i aquest muntatge normalment no es troba disponible al client NFS. Aquests muntatges normalment solen estar completament qualificats a la línia d'ordres mitjançant l'ordre **mount** amb tota

l'informació necessària. Per als muntatges explícits, no cal actualitzar el fitxer `/etc/filesystems`. Els sistemes de fitxers muntats explícitament resten muntats tret que s'hagin desmuntat de forma explícita amb l'ordre **umount** o fins que el sistema es reinicïi.

Els muntatges *automàtics* es controlen mitjançant l'ordre **automount**, la qual cosa fa que l'extensió del kernel **AutoFS** controli l'activitat dels directoris especificats. Si un programa o usuari intenta accedir a un directori que no es troba muntat actualment, **AutoFS** interceptarà la sol•licitud, prepararà el muntatge del sistema de fitxers i, a continuació, durà a terme la sol•licitud.

Exportació i muntatge NFS

Cal comprendre el funcionament dels directoris d'exportació i muntatge per tal d'administrar NFS.

Un servidor NFS ha d'exportar un fitxer o un directori. A continuació, un client NFS pot muntar aquest fitxer o directori. En aquesta secció, s'inclouen més detalles sobre aquests conceptes.

Exportacions de directori NFS

L'exportació d'un directori es realitza al servidor NFS. L'exportació d'un directori implica que un directori de l'espai de nom del servidor es troba disponible per a les màquines client.

Al directori exportat se'l coneix com a *export* i inclou tots els fitxers del directori que es troben al sistema de fitxers del directori exportat.

Cada exportació també defineix les restriccions d'accés. Per exemple, es poden definir les restriccions següents:

- els clients que poden accedir al directori exportat
- les versions NFS que el client ha d'utilitzar per accedir al directori
- si el client pot escriure fitxers a l'exportació
- els mètodes de seguretat que el client ha de fer servir per accedir a directoris i fitxers de l'exportació.

Per obtenir una descripció completa de les restriccions i de la semàntica de les exportacions permeses, consulteu la descripció de l'ordre **exportfs** que apareix a *Commands Reference, Volume 2* i la descripció del fitxer `/etc/exports` que apareix a *Files Reference*.

Nota: Quan es modifiquen els atributs d'exportació, el directori ha de tornar a exportar-se per tal que s'apliquin els canvis. És possible que un directori s'hagi de tornar a exportar degut als canvis a altres fitxers o canvis externs al servidor. Per exemple, si un nom de client especificat a una llista d'accés es un grup de xarxes definit al fitxer `/etc/netgroup` i la definició del grup del client s'ha modificat, totes les exportacions que utilitzin el grup de xarxes d'una llista d'accés s'hauran de tornar a exportar per tal que s'apliquin les modificacions.

De forma similar, si es canvia l'adreça IP d'un client, totes les exportacions que especifiquin aquest client a una llista d'accés hauran de tornar a exportar-se. Això es deu a què el servidor NFS manté una memòria cau de drets d'accés de client a cada exportació. La memòria cau es llança cada vegada que es cancel•la o es torna a realitzar una exportació. Si es modifiquen els drets d'accés d'una exportació, particularment si canvia l'adreça IP d'un client o si s'elimina un client de la llista d'accés, caldrà cancel•lar o tornar a realitzar l'exportació per tal que l'accés del client quedi correctament reflectit a la memòria cau. El servidor NFS crida el daemon **rpc.mountd** per obtenir els drets d'accés de cada client; per tant, el daemon **rpc.mountd** ha d'executar-se al servidor encara que el servidor només exporti sistemes de fitxers per l'accés de NFS versió 4.

Muntatges de directori NFS

Un client NFS pot muntar un directori que s'hagi exportat mitjançant un servidor NFS. En muntar un directori, els fitxers que es troben al servidor NFS es tornen disponibles per a un client NFS.

Un client pot accedir a fitxers d'un servidor si els fitxers han estat exportats pel servidor i les restriccions d'exportació permeten al client accedir als fitxers d'exportació. Un cop que el client hagi muntat correctament l'exportació d'un servidor en un punt de muntatge del seu espai de nom, els fitxers del servidor d'aquesta exportació apareixeran a l'espai de nom del client i en forma de fitxers al sistema de fitxers local.

Per exemple, suposeu que voleu exportar el directori `/tmp` al servidor `diamond` i munteu aquest directori al client `clip` en forma de directori `/mnt`. Al servidor, escriviu l'ordre següent:

```
exportfs -i -o access=clip /tmp
```

Això fa que el directori `/tmp` estigui disponible per al client.

Al client, escriviu l'ordre següent:

```
mount diamond:/tmp /mnt
```

Els directoris i els fitxers del directori `/tmp` del servidor apareixen al directori `/mnt` del client.

Nota:

1. Existeixen algunes diferències entre NFS versions 2 i 3 i NFS versió 4 pel que fa al mode en que es gestionen els muntatges. A NFS versions 2 i 3, el servidor ha exportat els directoris que ha volgut per tal de possibilitar el muntatge. A continuació, el client de NFS versió 2 o 3 ha hagut de muntar explícitament cada exportació a la qual volia accedir.

   Amb NFS versió 4, el servidor encara especifica els controls d'exportació per a cada directori de servidor o sistema de fitxers que s'ha d'exportar per l'accés NFS. A partir d'aquests controls d'exportació, el servidor representa un únic arbre de directoris de totes les dades exportades que omplen buits entre els directoris exportats. Aquest arbre es coneix com a pseudosistema de fitxers i s'inicia a la pseudoarrel del servidor de NFS versió 4. El model del pseudosistema de fitxers NFS versió 4 permet a un client de NFS versió 4, en funció de la seva implementació, realitzar un sol muntatge de la pseudoarrel del servidor per poder accedir a totes les dades exportades del servidor. El client de AIX NFS dóna suport a aquesta característica. El contingut real vist pel client depèn dels controls d'exportació del servidor.
2. NFS versió 4 no permet el muntatge entre fitxers.

Muntatge de NFS

Els clients accedeixen a fitxers del servidor muntant, en primer lloc, els directoris exportats pel servidor. Quan un client munta un directori, no fa cap copia d'aquest. Enlloc d'això, el procés de muntatge utilitza una sèrie de crides de procediment remot per habilitar un client per tal que accedeixi de forma transparent als directoris del servidor.

A continuació, es descriu el procés de muntatge:

1. Quan el servidor s'inicia, la sèrie `/etc/rc.nfs` executa l'ordre **exportfs**, la qual llegeix el fitxer `/etc/exports` del servidor i, a continuació, indica al kernel els directoris que s'han d'exportar i les restriccions d'accés que requereixen.
2. A continuació, el daemon **rpc.mountd** i diversos daemons **nfsd** s'inicien mitjançant la sèrie `/etc/rc.nfs`.
3. A continuació, la sèrie `/etc/rc.nfs` executa l'ordre **mount**, la qual llegeix els sistemes de fitxers llistats al fitxer `/etc/filesystems`.
4. L'ordre **mount** ubica un o varis servidors que exporten l'informació que el client desitja i configura la comunicació entre aquest i el servidor en qüestió. Aquest procés s'anomena *vinculació*.
5. A continuació, l'ordre **mount** sol•licita que un o varis servidors permetin al client accedir als directoris del fitxer `/etc/filesystems` del client.

6. El daemon del servidor rep les sol•licituds de muntatge del client i les atorga o les denega. Si un directori sol•licitat es troba disponible per a aquest client, el daemon del servidor envia al client el kernel i l'identificador anomenats *nansa de fitxer*.
7. A continuació, el kernel del client vincula la nansa del fitxer amb el punt de muntatge (un directori) enregistrant determinada informació en un *enregistrament de muntatge*.

La comunicació del client amb el daemon **rpc.mountd** no succeeix amb el processament de muntatge de NFS versió 4. Les operacions del protocol NFS versió 4 principal s'utilitzen per dur a terme operacions de muntatge del client. L'implementació del servidor NFS versió 4 utilitza el suport del daemon **rpc.mountd** com a part de la manipulació de l'accés de NFS versió 4.

/etc/exports file

El fitxer `/etc/exports` indica tots els directoris que un servidor exporta als seus clients.

Cada línia del fitxer especifica un sol directori. Es pot especificar un directori dues vegades al fitxer `/etc/exports`: un cop per NFS versió 2 o 3, i una altre cop per NFS versió 4. El servidor exporta automàticament els directoris llistats cada vegada que s'inicia el servidor NFS. A continuació, els clients poden muntar aquests directoris exportats. La sintaxi d'una línia del fitxer `/etc/exports` és:

directori `-`*opció*`[,`*opció*`]`

El *directori* és el nom de camí d'accés sencer del directori. Les opcions poden designar un simple senyalador com, per exemple, **ro** o una llista de noms d'amfitrió. Consulteu la documentació específica del fitxer `/etc/exports` a *Files Reference* i de l'ordre **exportfs** a la secció *Commands Reference, Volume 2* per obtenir una llista completa de les opcions i les descripcions. La seqüència `/etc/rc.nfs` no inicia daemons **nfsd** ni el daemon **rpc.mountd** si el fitxer `/etc/exports` no existeix.

L'exemple següent mostra les entrades d'un fitxer `/etc/exports`:

```
/usr/games    -ro,access=ballet:jazz:tap
/home         -root=ballet,access=ballet
/var/tmp
/usr/lib      -access=clients
/accounts/database -vers=4,sec=krb5,access=accmachines,root=accmachine1
/tmp          -vers=3,ro
/tmp          -vers=4,sec=krb5,access=accmachines,root=accmachine1
```

La primera entrada d'aquest exemple especifica que el directori `/usr/games` pot ésser muntat per sistemes anomenats `ballet`, `jazz` i `tap`. Aquests sistemes poden llegir dades i executar programes des del directori però no hi poden escriure.

La segona entrada d'aquest exemple especifica que el directori `/home` pot ésser muntat pel sistema `ballet` i que l'accés root està permès pel directori.

La tercera entrada d'aquest exemple especifica que qualsevol client pot muntar el directori `/var/tmp`. (Tingueu en compte l'absència de la llista d'accés.)

La quarta entrada d'aquest exemple especifica una llista d'accés designada pel grup de xarxes `clients`. És a dir, aquestes màquines designades com pertanyents al grup de xarxes `clients` poden muntar el directori `/usr/lib` des d'aquest servidor. (Un *grup de xarxes* és un grup que pot accedir a determinats recursos de xarxa de tota la xarxa amb finalitats de seguretat o d'organització. Els grups de xarxes es controlen mitjançant NIS.

La cinquena entrada permet accedir al directori `/accounts/database` únicament als clients del grup de xarxes `accmachines` que utilitzen el protocol de NFS versió 4 i accedeixen al directori mitjançant l'autenticació de Kerberos 5. L'accés root només es pot realitzar des de `accmachine1`.

Les entrades cinquena i setena exporten el directori /tmp mitjançant diferents versions i opcions. Si hi ha dues entrades per al mateix directori amb diferents versions NFS al fitxer /etc/exports, l'ordre **exportfs** exportarà ambdues. Si un directori té les mateixes opcions per NFS versió 4 i NFS versió 3, podreu tenir una entrada al fitxer /etc/exports que especifiqui -vers=3:4.

Fitxer /etc/xtab

El fitxer /etc/xtab té un format similar al fitxer /etc/exports i llista els directoris actualment exportats.

Sempre que s'executa l'ordre **exportfs**, canvia el fitxer /etc/xtab. Això permet exportar un directori de forma temporal sense haver de modificar el fitxer /etc/exports. Si no s'exporta el directori temporalment exportat, el directori s'eliminarà del fitxer /etc/xtab.

Nota: El fitxer /etc/xtab s'actualitza automàticament i no es pot editar.

Fitxer /etc/nfs/hostkey

Aquest fitxer l'utilitza el servidor NFS per especificar el principal d'amfitrió Kerberos i l'ubicació del fitxer keytab.

Per obtenir instruccions sobre com configurar i administrar aquest fitxer, consulteu la descripció de l'ordre **nfshostkey** que apareix a *Commands Reference, Volume 4*.

Fitxer /etc/nfs/local_domain

Aquest fitxer conté el domini NFS local del sistema.

S'entén que els sistemes que comparteixen el mateix domini local NFS també comparteixen els mateixos enregistraments de grup i d'usuari. Per obtenir instruccions sobre com configurar i administrar aquest fitxer, consulteu la descripció de l'ordre **chnfsdom** que apareix a *Commands Reference, Volume 1*.

Fitxer /etc/nfs/realm.map

Aquest fitxer l'utilitza el daemon d'enregistrament NFS per mapar principals Kerberos d'entrada amb el format *nom@kerberos-domini* amb el format *nom@nfs-domini*.

A continuació, pot resoldre *nom@nfs-domini* en una credencial UNIX local. Aquest fitxer proporciona un mode senzill de mapar principals Kerberos en l'enregistrament d'usuaris del servidor. És adequat quan els clients de diferents dominis Kerberos accedeixen al servidor. Tanmateix l'espai de nom de l'usuari es global. El fitxer hauria de contenir línies amb el format següent:

```
realm1 nfs-domini
realm2 nfs-domini
```

per tots els dominis Kerberos als quals el servidor dóna suport. Si el nom del domini Kerberos sempre coincideix amb el domini NFS del servidor, aquest fitxer no serà necessari. Si us cal la capacitat més general de mapar *usuariA@kerberos-domini* amb *usuariB@nfs-domini*, utilitzeu el servei EIM (Enterprise Identity Mapping). Per obtenir més informació, consulteu “Mapatge d'entitats” a la pàgina 533.

Per afegir, editar o eliminar entrades d'aquest fitxer, utilitzeu l'ordre **chnfsrtd**. Consulteu la descripció de l'ordre **chnfsrtd** que apareix a *Commands Reference, Volume 1* per obtenir informació més detallada.

Fitxer /etc/nfs/princmap

Aquest fitxer mapa els noms d'amfitrió amb els principals Kerberos quan el principal no és el nom de domini completament qualificat del servidor.

Consta d'un nombre qualsevol de línies del format següent:

```
<part d'amfitrió del principal> alias1 alias2 ...
```

Per afegir, editar o eliminar entrades d'aquest fitxer, utilitzeu l'ordre **nfshostmap**. Consulteu la descripció de l'ordre **nfshostmap** que apareix a *Commands Reference, Volume 4* per obtenir informació detallada al respecte.

Fitxer /etc/nfs/security_default

El fitxer `/etc/nfs/security_default` conté la llista de valors de seguretat que pot fer servir el client NFS, en l'ordre en el qual s'han de fer servir.

Utilitzeu l'ordre **chnfssec** per gestionar aquest fitxer. Consulteu la descripció de l'ordre **chnfssec** que apareix a *Commands Reference, Volume 1* per obtenir més informació.

Protocol de crida de procediment remot

NFS s'implementa en una varietat de tipus de màquina, sistemes operatius i arquitectures de xarxa. NFS aconsegueix aquesta independència mitjançant el protocol **Crida de procediment remot (RPC)**.

RPC és una biblioteca de procediments. Els procediments permeten a un procés (el procés del client) dirigir un altre procés (el procés del servidor) per executar crides de procediment com si el procés del client hagués executat les crides en el seu propi espai d'adreces. Donat que el client i el servidor són dos processos separats, no han d'existir al mateix sistema físic (encara que ho puguin fer).

NFS s'implementa com a conjunt de crides **RPC** en les quals el servidor dóna servei a determinats tipus de crides realitzades pel client. El client realitza aquestes crides basant-se en les operacions del sistema de fitxers realitzades pel procés del client. NFS, en aquest sentit, es una aplicació RPC.

Donat que els processos de servidor i client poden trobar-se en dos sistemes físics diferents que poden tenir dues arquitectures completament diferents, **RPC** ha d'incloure la possibilitat que és possible que dos sistemes no representin dades de la mateixa manera. Per aquesta raó, **RPC** utilitza tipus de dades definits pel protocol **eXternal Data Representation (XDR)**.

Protocol de representació de dades externes

El protocol **Representació de dades externes (XDR)** és l'especificació per a una representació estàndard de diferents tipus de dades.

Mitjançant una representació de tipus de dades estàndard, no hi ha cap dubte que el programa està interpretant les dades correctament, encara que l'origen de les dades sigui una màquina amb una arquitectura completament diferent.

A la pràctica, la majoria de programes no utilitzen **XDR** internament. Enlloc d'això, utilitzen la representació de tipus de dades específica per l'arquitectura de l'ordinador on s'executa el programa. Si el programa s'ha de comunicar amb un altre programa, convertirà les seves dades al format **XDR** abans d'enviar-les. A la inversa, quan rep dades, les converteix del format **XDR** a la seva representació de tipus de dades específica.

Daemon portmap

El daemon **portmap** ajuda als clients a mapar parells de números de programes i de números de versions amb el número de port d'un servidor.

Cada aplicació RPC té associat un número de programa i un número de versió. Aquests números s'utilitzen per comunicar-se amb una aplicació de servidor al sistema. Al realitzar una sol•licitud des d'un servidor, el client ha de conèixer el número de port en el qual el servidor acceptarà la sol•licitud. Aquest número de port s'associa amb amb el **User Datagram Protocol (UDP)** o amb el **protocol de control de transmissió (TCP)** que està sent utilitzat pel servei. El client coneix el número de programa, el número de versió i el nom del sistema o nom d'amfitrió on es troba el servidor. El client necessita un mode de mapar

el parell de número de programa i de número de versió amb el número de port de l'aplicació del servidor. Això es realitza amb l'ajuda del daemon **portmap**.

El daemon **portmap** s'executa en el mateix sistema que l'aplicació NFS. Quan el servidor comença a executar-se, enregistra el daemon **portmap**. Com a funció d'aquest enregistrament, el servidor proporciona el seu número de programa i de versió, així com el número de port de **UDP** o **TCP**. El daemon **portmap** conserva una taula d'aplicacions de servidor. Quan el client intenta realitzar una sol•licitud del servidor, primer es posa en contacte amb el daemon **portmap** per conèixer el port que el servidor està utilitzant. El daemon **portmap** respon al client del servidor que el client està sol•licitant. Quan rep el número de port, el client podrà realitzar totes les sol•licituds futures directament a l'aplicació del servidor.

Control i aplicacions NFS

Els daemons de NFS i NIS es controlen mitjançant el controlador de recursos del sistema (SRC).

Això significa que s'han d'emprar ordres SRC com, per exemple, **startsrc**, **stopsrc** i **lssrc** per iniciar, parar i comprovar l'estat del daemons NFS i NIS.

Alguns daemons NFS no es controlen mitjançant el controlador SRC. En concret, el controlador SRC no controla **rpc.rexd**, **rpc.rusersd**, **rpc.rwalld** ni **rpc.rsprayd**. Aquests daemons s'inicien i paren mitjançant el daemon **inetd**.

La taula següent mostra el daemons controlats pel controlador SRC i els seus noms de subsistema.

Taula 90. Daemons i els seus subsistemes

Camí d'accés del fitxer	Nom del subsistema	Nom del grup
/usr/sbin/nfsd	**nfsd**	nfs
/usr/sbin/biod	**biod**	nfs
/usr/sbin/rpc.lockd	**rpc.lockd**	nfs
/usr/sbin/rpc.statd	**rpc.statd**	nfs
/usr/sbin/rpc.mountd	**rpc.mountd**	nfs
/usr/sbin/nfsrgyd	**nfsrgyd**	nfs
/usr/sbin/gssd	**gssd**	nfs
/usr/lib/netsvc/yp/ypserv	**ypserv**	yp
/usr/lib/netsvc/yp/ypbind	**ypbind**	yp
/usr/lib/netsvc/rpc.yppasswdd	**yppasswdd**	yp
/usr/lib/netsvc/rpc.ypupdated	**ypupdated**	yp
/usr/sbin/keyserv	**keyserv**	keyserv
/usr/sbin/portmap	**portmap**	portmap

Informació relacionada:

visió general del Controlador de recursos del sistema

Canvi del nombre de daemons biod i nfsd

L'ordre **chnfs** es pot utilitzar per canviar el nombre màxim de daemons **biod** o **nfsd** que s'executaran en un sistema.

Per exemple, per establir el nombre màxim de daemons **nfsd** en 1000 i el nombre màxim de daemons **biod** en 4, executeu l'ordre següent:

```
chnfs -n 1000 -b 4
```

Nota: Aquesta ordre pararà els daemons que s'estiguin executant actualment, actualitzarà la informació de configuració SRC i, a continuació, reiniciarà els daemons. Com a conseqüència, el servei NFS no estarà

disponible temporalment.
El nombre màxim de daemons **biod** també es pot especificar segons el muntatge mitjançant la opció de muntatge `biods=n`.

Nota: Si el nombre de daemons **nfsd** no és suficient per servir al client, es retornarà un error de funcionament nonidempotent al client. Per exemple, si el client elimina un directori, es retornarà un error `ENOENT` encara que el directori del servidor s'hagi eliminat.

Modificació dels arguments de la línia d'ordres per daemons controlats per SRC

Molts daemons NFS i NIS tenen arguments de línia d'ordres que es poden especificar quan s'inicia el daemon. Donat que aquests daemons no s'inicien directament des de la línia d'ordres, haureu d'actualitzar la base de dades SRC per tal que els daemons es puguin iniciar correctament.

Per fer-ho, utilitzeu l'ordre **chssys**. L'ordre **chssys** té el format següent:

```
chssys -s Daemon -a 'ParàmetreNou'
```

Per exemple:

```
chssys -s nfsd -a '10'
```

canvia el subsistema **nfsd** per tal que quan s'iniciï el daemon, la línia d'ordres aparegui com `nfsd 10`. Els canvis realitzats mitjançant l'ordre **chssys** no s'apliquen fins que s'ha parat i reiniciat el subsistema.

Inici de daemons NFS

El límit de grandària de fitxer dels fitxers que es troben al servidor NFS es defineix mitjançant l'entorn de procés quan s'inicia **nfsd**.

Per utilitzar un valor específic, editeu el fitxer `/etc/rc.nfs`. Utilitzeu l'ordre **ulimit** amb el límit que desitgeu abans de l'ordre **startsrc** del daemon **nfsd**.

Els daemons NFS es poden iniciar individualment o tots a la vegada. Per iniciar daemons NFS de forma individual, executeu el següent:

```
startsrc -s Daemon
```

on *Daemon* és qualsevol dels daemons controlats per SRC. Per exemple, per iniciar els daemons **nfsd**, executeu:

```
startsrc -s nfsd
```

Per iniciar tots els daemons NFS, executeu:

```
startsrc -g nfs
```

Nota: Si el fitxer `/etc/exports` no existeix, no s'iniciaran els daemons **nfsd** i **rpc.mountd**. Podeu crear un fitxer `/etc/exports` buit executant l'ordre `touch /etc/exports`. Això permetrà que els daemons **nfsd** i **rpc.mountd** s'iniciïn, encara que no s'hagi exportat cap sistema de fitxers.

Aturada del daemons NFS

Els daemons NFS es poden aturar individualment o tots a la vegada.

Per aturar daemons NFS de forma individual, executeu el següent:

```
stopsrc -s Daemon
```

on *Daemon* és qualsevol dels daemons controlats per SRC. Per exemple, per aturar el daemon **rpc.lockd**, executeu:

```
stopsrc -s rpc.lockd
```

Per aturar tots els daemons NFS a la vegada, executeu:

```
stopsrc -g nfs
```

Com obtenir l'estat actual dels daemons NFS

Podeu obtenir l'estat actual dels daemons NFS de forma individual o tots a la vegada.

Per obtenir l'estat actual dels daemons NFS de forma individual, executeu:

```
lssrc -s Daemon
```

on *Daemon* és qualsevol dels daemons controlats per SRC. Per exemple, per obtenir l'estat actual del daemon **rpc.lockd**, executeu:

```
lssrc -s rpc.lockd
```

Per obtenir l'estat actual de tots els daemons NFS a la vegada, executeu:

```
lssrc -a
```

Suport de NFS versió 4

Començant amb AIX 5.3, s'inclou el suport per les funcions del protocol NFS versió 4.

Les funcions obligatòries del protocol reben suport tal com es descriu al RFC 3530 amb les excepcions següents:

- Els mecanisme de seguretat LIPKEY i SPKM-3 no reben el suport de l'autenticació RPCSEC-GSS RPC. Només es suporta el mecanisme V5 de Kerberos.
- Els requisits UTF-8 no reben un suport complet. Específicament, no es garanteix que la transmissió de noms de fitxer i de sèries de sistema de fitxers com, per exemple, el contingut d'enllaços simbòlics i els noms d'entrades de directoris es realitzi amb el format UTF-8. La transmissió de sèries d'atributs NFS com, per exemple, de propietari i de grup de propietaris, sempre es realitza en format UTF-8. El servidor i el client NFS realitzen la validació UTF-8 sobre dades de sèrie entrants, tal com es defineix a RFC 3530. Aquesta comprovació es pot inhabilitar de forma administrativa mitjançant l'ordre **nfso**. L'inhabilitació de la comprovació UTF-8 pot ser necessària per utilitzar NFS versió 4 en entorns amb configuracions i dades que no siguin UTF-8.
- El client sense disc NIM i UDP no reben suport a NFS versió 4.

Es dóna suport a les funcions opcionals següents de NFS versió 4:

- Les ACL de NFS versió 4 reben el suport del client i del servidor NFS. El client NFS dóna suport a la gestió de ACL de NFS versió 4 mitjançant els programes d'utilitat **acledit**, **aclget** i **aclput**. El servidor NFS pot emmagatzemar i recuperar ACL de NFS versió 4 a sistemes de fitxers subjacents que suportin el model SCL de NFS versió 4. Per obtenir més informació, consulteu l'apartat “Suport de llistes de control d'accés NFS” a la pàgina 509.
- Es proporciona suport per mapar atributs de principals i de propietat de fitxers del domini NFS versió 4 a un altre domini. Aquest suport està pensat principalment per utilitzar-se a servidors NFS AIX. Requereix el desplegament de LDAP. Els mapatges de NFS es gestionen mitjançant el programa d'utilitat **chnfsim**.

Existeixen diferents consideracions a l'hora d'utilitzar l'accés concurrent amb NFS versions 2 i 3 i NFS versió 4. L'accés de NFS versió 3 pot rebre errors deguts a l'estat atorgat de NFS versió 4. A més, el rendiment de NFS versió 3 es pot veure afectat quan les dades s'exporten per l'accés NFS versió 4.

Període de gràcia del servidor NFS

El protocol NFS versió 4 (NFSv4) proporciona funcions que permeten als administradors del sistema habilitar un període de gràcia al servidor NFSv4 per la gestió especial d'operacions específiques.

Dins d'aquest període de gràcia, els administradors poden gestionar el blocatge, operacions de lectura i operacions d'escriptura durant tota la duració del lloguer del servidor. Els bloqueigs i els seus estats associats poden ser recuperats per clients a través de sol•licituds de bloqueig de tipus de reclamació.

Nota: No es pot garantir que tots els estats reclamats per clients al període de gràcia siguin estats retinguts al servidor a la instància anterior. Es garanteix que l'estat que es reclama durant el període de gràcia és el correcte, segons es defineix a NFSv4 RFC.

Començant amb AIX 5L Versió 5.3 amb el nivell de tecnologia 5300-05 , els administradors poden utilitzar el període de gràcia als servidors NFSv4. El període de gràcia s'inhabilita per defecte. Per habilitar el període de gràcia al servidor, utilitzeu el menú de la SMIT o l'interficie de la línia d'ordres**chnfs**.

Si el període de gràcia està habilitat, el servidor NFSv4 enregistra l'informació d'estat al disc del fitxer `/var`. L'estat enregistrar es reclama automàticament quan es reinicia el servidor.

Suport DIO i CIO de NFS

AIX 5L Versió 5.3 amb el paquet de manteniment recomanat 5300-03 dóna suport a E/S directes i a E/S concorrents al client NFS per als protocols de les versions 3 i 4. DIO i CIO només afecten el client.

Mitjançant DIO i CIO, les càrregues de treball del centre de dades com, per exemple, bases de dades i aplicacions informàtiques d'alt rendiment, poden experimentar nivells més alts de rendiment. Això pot venir acompanyat per una reducció de la CPU del sistema i dels recursos de memòria, alhora que es mantenen els beneficis de la centralització de l'emmagatzematge basat en fitxers i de la gestió de sistemes de fons associada a aquesta.

L' E/S sovint no és seqüencial i sovint les aplicacions no es beneficien de l'emmagatzematge de dades a la memòria cau en el client NFS ni les aplicacions duen a terme totes les operacions avançades d'emmagatzematge a la memòria cau. Aquestes aplicacions es beneficien quan NFS no emmagatzema res a la memòria cau, no realitza cap predicció de lectura ni utilitza mecanismes d'enregistrament diferit. A més, algunes aplicacions, com les bases de dades, no depenen de la semàntica d'un sol indret POSIX, la qual crea sèries de lectures amb escriptures. Aquestes aplicacions emeten lectures i escriptures concorrents, sinó que són responsables de la coherència i la coordinació d'aquest tipus d'operacions.

E/S directe per NFS

DIO permet a les aplicacions realitzar lectures i escriptures directament al servidor NFS sense passar per la capa d'emmagatzematge en memòria cau del client NFS (gestor de memòria virtual) o incorrent la sobrecàrrega associada de l'emmagatzematge de dades en memòria cau.

A DIO, les sol•licituds d'E/S d'aplicació se duen a terme mitjançant crides de procediment remot (RPC) al servidor NFS. Podeu establir DIO mitjançant l'opció de muntatge AIX *dio*. Sense l'opció de muntatge, també podeu habilitar DIO per fitxer mitjançant el senyalador **AIX O_DIRECT open()**.

És possible que el servei de E/S directes requereixi múltiples RPC per al servidor, en funció de la grandària de la sol•licitud E/S i de la grandària de transferència per cable màxima permesa pel servidor i pel client. Per obtenir més informació sobre DIO, consulteu l'opció **-o** de l'ordre **mount**.

E/S concorrent per NFS

Amb CIO, les lectures i escriptures de l'aplicació que s'emeten de forma concorrent, s'executen de forma concorrent sense que les lectures bloquegin la duració de les escriptures ni a la inversa.

Quan existeixen múltiples escriptures, s'executen de forma concorrent. No es proporcionen les garanties d'atomicitat POSIX. Quan s'utilitza CIO, s'implica E/S. Utilitzeu l'opció de muntatge AIX *cio* o el senyalador **O_CIO open()** per establir CIO. Per obtenir més informació sobre CIO, consulteu l'opció **-o** de l'ordre **mount**.

A l'AIX Versió 6.1 amb el nivell de tecnologia 6100-04 i versions posteriors, podeu executar l'ordre **mount**, l'ordre **nfs4cl** o la subrutina **open()** per tal de poder obrir els fitxers de només de lectura quan aquests fitxers ja s'han obert a CIOR. L'opció de muntatge **cior** i el senyalador **O_CIOR open ()** només es poden utilitzar conjuntament amb CIO.

Informació relacionada:

ordre mount

Interacció de DIO, CIO, obertures regulars i fitxers correlacionats per NFS

Els comportaments següents es produeixen entre les diferents modalitats d'accés que es poden produir amb DIO i CIO.

Quan s'apliquen obertures DIO existents:

- Una obertura regular fa que DIO es desactivi fins que no quedin obertures regulars. Quan una tancada redueix les obertures regulars a 0, DIO es torna a activar en el cas que encara existeixin obertures DIO pendents.
- La correlació d'un fitxer amb shmat() o mmap() desactivarà DIO al fitxer fins que el nombre de mapatges es redueixi fins a 0. A continuació, si encara existeixen obertures DIO, es tornarà a activar DIO.
- Els intents d'obrir el fitxer per CIO no tindran èxit amb l'error **EINVAL**.

Quan s'apliquen obertures regulars (no CIO ni DIO):

- Tenen èxit els intents d'obertura DIO però DIO no s'activa fins que el recompte d'obertures regulars cau fins a 0.
- Les obertures per CIO fallaran amb l'error **EINVAL**.

Quan s'apliquen les obertures CIO:

- Les obertures regulars, DIO i els intents de mapar el fitxer fallaran amb l'error **EINVAL**.

Quan les obertures CIO|CIOR són efectives:

- Les obertures regulars, DIO i els intents de mapar el fitxer fallaran amb l'error **EINVAL** excepte les obertures de només de lectura i CIO|CIOR.

Nota: Quan hi ha una transició a DIO o CIO, les modificacions emmagatzemades a la memòria cau del client es tornaran a escriure al servidor NFS abans de que se suprimeixi tota l'informació emmagatzemada a la memòria cau.

Replicació NFS i espai de nom global

El protocol NFS versió 4 (NFSv4) proporciona funcions que permeten a l'usuari, com a administrador del sistema, distribuir dades per múltiples servidors de manera transparent als usuaris d'aquestes dades.

Podeu utilitzar dues funcions que comencin per AIX 5L Versió 5.3 amb el paquet de manteniment recomanat 5300-03 . La primera és una funció de espai de nom general anomenada *referència*. La segona funció és una manera d'especificar ubicacions on es poden trobar còpies de dades i que s'anomena *rèplica*.

Una *referència* és un objecte especial que es pot crear a l'espai de nom d'un servidor al qual s'adjunta informació d'ubicació. El servidor utilitza funcions del protocol NFSv4 per redireccionar clients al servidor especificat a l'informació d'ubicació. La referència forma un building block per integrar dades de múltiples servidors NFS en un sol arbre d'espai de nom de fitxer en el qual poden navegar els clients NFSv4 que coneixen la referència.

Una *rèplica* és una còpia d'un sistema de fitxers en un servidor NFS que s'ha col•locat en altres servidors NFS diferents (o en una ubicació alternativa com, per exemple, un disc diferent del mateix servidor). Si

una ubicació de rèplica determinada que utilitza un client NFSv4 que coneix la rèplica deixa d'ésser disponible, el client commutarà a una altra rèplica disponible. Per obtenir més informació sobre rèpliques, consulteu “Rèpliques NFS” a la pàgina 525.

Referències NFS

Els exemples següents proporcionen escenaris per ajudar a entendre les referències.

En els exemples següents, existeixen quatre servidors:

- El servidor anomenat `publications` conté fitxers d'informació.
- El servidor anomenat `projects` conté directoris de feina.
- El servidor anomenat `data` conté bases de dades d'informació.
- El servidor anomenat `account1` és el servidor NFS principal que exporta tota la resta de fitxers i és el servidor que tots els clients coneixen.

Permetre a tots els clients accedir a fitxers al servidor NFS principal

El servidor `account1` exporta el directori `/work` a tots els clients mitjançant la sentència següent del fitxer `/etc/exports`:

```
/work -vers=4
```

Tots els clients poden accedir als fitxers del directori remot `/work` muntant / des del servidor `account1` al directori `/mnt` mitjançant l'ordre següent:

```
mount -o vers=4 account1:/ /mnt
```

Quan l'usuari del client llista el contingut del directori `/mnt`, els usuaris veuran el directori remot`work` al camí d'accés `/mnt/work`. El contingut del directori `/mnt/work` al client és el mateix que el contingut del directori `/work` al servidor `account1`.

Permetre a un client accedir a fitxers d'un servidor específic

L'usuari del client també desitja accedir al directori `/usr/doc` al servidor `publications`.

En releases anteriors, s'ha d'exportar el directori des del servidor i muntar el directori al client.

Utilització de referències per crear un espai de nom distribuït

Podeu configurar un servidor per tal que els clients puguin accedir a les dades d'altres servidors sense que el client sàpiga on es troben les dades. Només cal que l'administrador del servidor al qual es fa referència sàpiga on es troben les dades. El servidor de referència pot redireccionar clients a l'ubicació del directori `/usr/doc` mitjançant una referència. Al servidor `publications`, és possible exportar el directori `/usr/doc` afegint la sentència següent al fitxer d'exportació:

```
/usr/doc -vers=4
```

Això fa que els directoris estiguin disponibles per als clients NFSv4.

Ara, el servidor `account1` pot utilitzar referències per fer que els directoris en qüestió estiguin disponibles als clients afegint la sentència següent al fitxer d'exportació:

```
/usr/doc -vers=4,refer=/usr/doc@publications
```

A continuació, podeu exportar el directori. En aquest punt, el client que ha muntat el directori `/mnt` a partir del directori / del servidor `account1` té accés al directori `usr` quan el client llista el directori `/mnt`. No cal que el client realitzi muntatges en altres servidors. Tampoc cal que l'usuari del client hagi de saber que els fitxers no són proporcionats pel servidor `account1`. Per exemple, podeu fer que estiguin

disponibles els directoris de /databases/db del servidor data i /home/accts del servidor projects a través de account1 exportant els directoris des dels servidors data i projects i creant referències de account1 per aquests directoris.

Donat que un usuari de client no coneix l'ubicació real de les dades, l'administrador pot redireccionar clients des d'un servidor a un altre simplement canviant la sentència de referència del fitxer d'exportacions al servidor. L'administrador s'encarrega de col•locar i corregir les dades a les quals les referències fan referència amb les seves especificacions d'ubicació.

Els administradors han d'assegurar-se que el segon servidor no farà referència a la sol•licitud del primer servidor ja que això crearia una referència circular. En l'exemple anterior, si l'administrador ha creat una referència al servidor publications a /usr/doc que ha fet referència a /usr/doc del servidor account1, la referència circular resultant no seria el resultat més desitjable.

Encara que les referències es creïn mitjançant exportfs, són diferents de les exportacions de dades. Les ubicacions especificades per les referències han de correspondre amb els directoris root del sistemes de fitxers exportats NFSv4. Podeu crear una referència dins d'espais de nom exportats o no exportats. A l'exemple anterior, es pot crear la referència /usr/doc al servidor account1 encara que /usr no s'hagi exportat. Això col•loca la referència dins del pseudoespai NFSv4. Si account1 ha exportat /usr, encara s'hauria permès l'exportació de referència, en contrast amb l'exportació d'un directori anomenat doc, la qual hagués fallat si s'hagués trobat al mateix sistema de fitxers. En qualsevol cas, l'exportació de referència hagués fallat si hi hagués hagut un fitxer o un directori a /usr/doc. No hi ha cap restricció pel que fa al nombre de referències que es poden crear dins del pseudoespai NFSv4 o del sistema de fitxers exportats.

Donat que una referència no exporta dades i només té significat pel protocol NFSv4, les referències només es troben disponibles a NSFv4. Si s'exporta una referència sense l'opció vers=4, aquesta acció no es durà a terme correctament. Encara que en aquest exemple només s'especifica una ubicació, es poden especificar fins a 8.

En crear una referència, es crea un objecte de referència especial a l'ubicació especificada pel paràmetre del directori. Donat que l'accés de client a l'objecte està determinat per l'accés del client al directori superior de l'objecte, la majoria d'opcions d'exportació no tenen significat, no estan permeses i s'ignoren. La única excepció és l'opció exname, que es comportarà de la manera prevista. Per exemple, si el servidor crea la referència /n4root/special/users -vers=4,exname=/exported/users,refer=/restricted/users@secrethost, els clients que muntin / des del servidor veuran el camí d'accés /mnt/exported/users, el qual redireccionarà els clients al directori /restricted/users de secrethost. Al servidor d'exportació, es crearia l'objecte de referència a l'espai de nom local a /n4root/special/users per tal que cap fitxer o directori no existeixi en aquest espai de nom quan es realitzi l'exportació. Un objecte especial es crea al servidor per retenir informació d'ubicació de referència. Qualsevol directori que es trobi al camí d'accés de la referència també es crearà, en el cas que encara no existeixi. Si no s'exporta la referència, l'informació de referència s'eliminarà de l'objecte, encara que l'objecte en si no s'eliminarà. El servidor NSFv4 no permetrà els clients accedir a l'objecte de referència *stale* o *orphan* resultant. Retornarà un error d'accés als clients que intentin accedir a l'objecte. L'objecte es pot eliminar mitjançant **rm**, si es desitja. És possible tornar a exportar una referència amb informació de referència nova. Això no és recomanable com a pràctica freqüent, donat que els clients que han accedit a la referència poden tardar un temps a adonar-se que l'informació de l'ubicació ha canviat. El servidor selecciona el directori superior de la referència per indicar que aquesta informació del directori ha canviat. Això ajuda als clients a adonar-se que qualsevol informació que el client hagi emmagatzemat a la memòria cau sobre el directori (i la referència dins d'aquest directori) ha canviat i que es necessari tornar a capturar-la. De tota manera, no hi ha cap garantia sobre el temps que tardaran els clients a adonar-se'n.

Per obtenir més informació sobre la utilització de l'opció **refer** per modificar l'ordre de les ubicacions especificades a la llista d'ubicacions del sistema de fitxers, vegeu Canvi de l'ordre de la llista d'ubicacions del sistema de fitxers mitjançant l'opció **scatter**.

Rèpliques NFS

La replicació permet, com a administrador NFSv4, col•locar còpies de dades en varis servidors NFSv4 i informar a clients NFSv4 on es troben les rèpliques.

En el cas que el servidor de dades principal no sigui accessible als clients, els clients poden utilitzar un dels servidors de rèplica per continuar les operacions al sistema de fitxers replicats. Se suposa que els sistemes de fitxers de rèplica són còpies exactes de les dades del servidor principal. Es pot configurar fins a 8 ubicacions de rèplica. El servidor AIX no especifica el mode en que es creen els sistemes de fitxers de rèplica des del sistema de fitxers principal ni sobre com es manté la coherència de les dades. Si voleu especificar rèpliques en forma de lectura-escriptura, haureu de mantenir la coherència de les rèpliques amb el sistema de fitxers principal.

Una rèplica és un servidor que conté una còpia d'un o varis directoris d'un altre servidor. Si el clients no poden accedir al servidor principal, el client podrà accedir als mateixos fitxers des de l'ubicació de la rèplica. A continuació, es mostra un cas d'exemple:

Si els fitxers del directori `/data` del servidor `account1` també es troben disponibles al directori `/backup/data` del servidor `inreserve`, els clients NSFv4 es podran adonar d'això especificant ubicacions de rèplica a l'exportació. En afegir una sentència semblant a la següent del fitxer d'exportació, podreu exportar el directori `/data` i especificar l'ubicació de la còpia de rèplica:

```
/data -vers=4,replicas=/data@account1:/backup/data@inreserve
```

Si el servidor `account1` està disponible, els usuaris de client que utilitzen els fitxer del directori `/data` del servidor `account1` poden començar a utilitzar fitxers del directori `/backup/data` al servidor `inreserve` sense que el client hagi canviat a un altre servidor.

Per obtenir més informació sobre la utilització de l'opció **replicas** per modificar l'ordre de les ubicacions especificades a la llista d'ubicacions del sistema de fitxers, vegeu Canvi de l'ordre de la llista d'ubicacions del sistema de fitxers mitjançant l'opció **scatter**.

Requisits de configuració NFS per permetre l'especificació de rèpliques:

Heu d'ésser un administrador per habilitar, inhabilitar o especificar rèpliques root.

Per habilitar, inhabilitar i especificar rèpliques root, utilitzeu l'ordre següent:

```
chnfs -R {on|off|host[+host]}
```

per tal d'especificar rèpliques, el servidor s'ha de configurar amb **chnfs -R** (**chnfs -R** on) per emetre nanses de fitxers NFSv4 volàtils. Una nansa de fitxer és un identificador que els servidors NFS emeten als clients per identificar un fitxer o un directori del servidor. Per defecte, el servidor emet nanses de fitxers permanents. Quan es canvia de tipus de nansa de fitxer, és possible que es produeixin errors en aplicacions en els clients NFSv4 que utilitzen activament el servidor quan es realitza la commutació. Per tal de canviar la modalitat de nansa de fitxers amb **chnfs -R**, no es pot exportar cap sistema de fitxers per l'accés de NFSv4. La configuració de la disposició de la nansa de fitxers ha de realitzar-se amb el servidor NFS que s'acaba de proporcionar o quan es pugui reduir o aturar l'activitat NFS. En el cas dels clients que estan activament connectats a servidors quan es modifica la modalitat, és possible que sigui necessari desmuntar i tornar a muntar els muntatges NFSv4 en aquests clients. Per minimitzar l'efecte d'aquesta acció, es pot reduir el nombre de muntatges de client a un nombre inferior de muntatges que munten els directoris de nivell superior de l'espai de fitxer exportat del servidor NFSv4.

El client NFSv4 no pot migrar després d'un error a rèpliques amb diferents propietats d'accés d'exportació. Els administradors han d'assegurar-se que totes les rèpliques s'especifiquen amb les mateixos controls d'accés d'exportació i la modalitat d'accés (només lectura o lectura-escriptura). Amb la possible excepció de GPFS exportat, és preveu que les dades replicades s'exportin en modalitat de només lectura. També és la responsabilitat de l'administrador mantenir el contingut de les dades a totes les

ubicacions de rèplica. Els arbres de directoris i tot el contingut de dades s'han de mantenir idèntics. Les actualitzacions del contingut de les dades s'hauran de dur a terme de la manera més compatible amb les aplicacions que utilitzaran les dades.

Amb les rèpliques, podeu utilitzar l'opció d'exportació **exname** per a què els clients de NFSv4 no puguin veure els detalls de l'espai de nom del sistema de fitxers local del servidor. Per obtenir informació detallada, consulteu la descripció de l'ordre **exportfs** que apareix a *Commands Reference, Volume 2* i la descripció del fitxer `/etc/exports` que apareix a *Files Reference*.

Podeu utilitzar l'opció **replicas** amb els sistemes de fitxers de clúster, com ara General Parallel File System (GPFS) per especificar múltiples nodes de servidor NFS que veuen la mateixa vista GPFS. Aquesta és una configuració en la qual l'exportació de dades per accés de lectura-escriptura pot ser vàlida. De tota manera, amb les rèpliques de lectura-escriptura, si es produeix una migració després d'un error d'una rèplica mentre hi ha operacions d'escriptura en progrés, és possible que les operacions que duen a terme l'escriptura es trobin errors no recuperables. De forma similar, una operació de creació de fitxer exclusiu o **mkdir** que s'executi durant una migració després d'un error pot trobar un error **EXISTS**.

Un port replicat ha d'exportar tot un sistema de fitxers. Això significa que el directori que s'està exportant ha d'ésser l'arrel del sistema de fitxers local. El servidor que exporta un sistema de fitxers replicat hauria d'especificar-se com a una de les ubicacions per l'exportació. En el cas de servidors amb múltiples interfícies, això ha d'incloure el nom d'amfitrió principal. Si el servidor que exporta un sistema de fitxers replicat no s'especifica com a una de les ubicacions per l'exportació, el servidor de l'exportació s'afegirà de forma silenciosa a la llista d'ubicacions de rèplica com a primera ubicació de rèplica. L'ordre de les ubicacions de rèplica a la llista de rèpliques especifica l'ordre de preferència que els clients han de fer servir quan es produeix una migració després d'un error. Per exemple, si l'usuari de `serverA` desitja exportar `/webpages` i hi ha una rèplica de `/webpages` a `serverB` dins del directori `/backup/webpages`, l'entrada següent del fitxer `/etc/exports` exportarà `/webpages` de `serverA` i informarà als clients que existeix una còpia del sistema de fitxers a `serverB` dins de `/backup/webpages`:

```
/webpages -vers=4,ro,replicas=/webpages@serverA:
/backup/webpages@serverB
```

Se suposa que ambdós `/webpages` de `serverA` i `/backup/webpages` de `serverB` són els directoris arrel dels seus sistemes de fitxers. Si `serverA` no s'hagués llistat a l'exportació, s'hauria afegit de forma silenciosa com a primera ubicació de rèplica. Això es deu a que se suposa que el servidor que exporta les dades és el servidor preferit de les dades que està exportant.

Les rèpliques només són utilitzades pel protocol NFSv4. L'exportació anterior podria haver especificat NFSv3 (`vers=3:4`), però l'informació de la replicació no hauria estat disponible pels clients NFSv3. Tanmateix, els clients que utilitzen NFSv3 poden accedir a l'informació de `/webpages` de `serverA` però no produiran cap migració després d'un error de la rèplica si `serverA` deixa d'ésser disponible.

Suport de client NFS per múltiples ubicacions:

Quan el client ja no pugui accedir a dades replicades des del servidor actual, el client intentarà accedir a les dades des del servidor següent més favorable.

L'ordre en el qual s'especifiquen les rèpliques a la llista de rèpliques és el que el client utilitza com a ordre de preferència.

L'administrador del client pot alterar temporalment la preferència de rèplica mitjançant la subordre **prefer** de l'ordre **nfs4cl**. L'ordre **nfs4cl** visualitza tota la informació del sistema de fitxers del client o modifica les opcions del sistema de fitxers d'un sistema de fitxers i visualitza o modifica les estadístiques i propietats de NFSv4.

Consideracions comunes de NFS per rèpliques i referències:

Si el client es troba dos camins d'accés diferents que porten a les mateixes dades (sistema de fitxers), el client tractarà el segon camí d'accés com a enllaç simbòlic al fitxer.

Per exemple, `server A` exporta:

```
/tmp/a              -vers=4,replicas=/tmp/a@B:/tmp/a@A
/tmp/b              -vers=4,refer=/tmp/a/b@B
```

I `server B` exporta:

```
/tmp/a              -vers=4
/tmp/a/b            -vers=4
```

En aquest exemple, el client munta `/` a `server A` a sobre de `/mnt` mitjançant l'ordre `mount -o vers=4 A:/ /mnt`. L'usuari client accedeix a `/tmp/a/b` de `server B` a través de `cd /mnt/tmp/a/b` o de `cd /mnt/tmp/b`. Si l'usuari canvia el directori a `cd /mnt/tmp/a/b` primer, el camí d'accés `/mnt/tmp/b` actuarà com a enllaç simbòlic per `/mnt/tmp/a/b`. En aquest cas, si l'usuari es troba a `/mnt/tmp/b` i utilitza l'ordre `/bin/pwd`, `/bin/pwd` > retornarà `/mnt/tmp/a/b`.

Nota: No és recomanable dur a terme aquesta pràctica. L'administrador ha de configurar les especificacions d'exportació que donen com a resultat un sol camí d'accés d'espai de nom possible per les dades exportades.

Podeu llistar múltiples ubicacions en referències si les dades de destinació de la referència també es repliquen. Els clients només utilitzaran les ubicacions de referència per buscar la destinació de referència en un servidor disponible. Un cop que el client estableixi l'accés a la destinació de referència, obtindrà informació de l'ubicació nova per les dades trobades.

Donat que és possible que els clients no detectin immediatament els canvis a l'informació d'ubicació de referència, no és recomana eliminar ni canviar l'ubicació de referència amb freqüència. Quan es canvia l'ubicació de la destinació d'una ubicació de referència, es recomana omplir la nova ubicació amb l'informació d'ubicació de l'especificació de la referència d'exportació. Les dades de l'antiga ubicació s'han de guardar durant algunes hores o fins i tot dies per donar als clients temps per veure i utilitzar la nova ubicació.

Tant la replicació com les referències només es poden executar a servidor que executen el kernel de 64 bits. Els clients poden executar-se en kernels de 32 i de 64 bits.

Si voleu especificar rèpliques en forma de lectura-escriptura, haureu de mantenir la coherència de les rèpliques amb el catàleg de fitxers principal.

Com els clients NFS migren després d'un error:

Una *migració després d'un error* es produeix quan el client canvia d'una ubicació de rèplica a una altra després de determinar que el servidor actual amb el qual s'està comunicant ja no és accessible.

Els factors següents influeixen el comportament de la migració després d'un error del client NFS:

Opció de muntatge NFS *timeo*
: Aquesta opció de muntatge especifica que el temps que ha d'esperar la capa TCP/IP abans que torni amb una resposta de temps d'espera.

Opció de muntatge NFS *retrans*
: Aquesta opció de muntatge especifica el nombre de vegades que la capa RCP de NFS ha d'intentar la sol•licitud del client abans de retornar un error de temps d'espera RPC (**ETIMEDOUT**).

Opció nfso *nfs_v4_fail_over_timeout*
Podeu utilitzar aquesta opció **nfso** per especificar la quantitat de temps mínima que el client ha d'esperar abans de realitzar una migració després d'un error per una altra rèplica. Aquesta opció és general al client NFS i altera temporalment el valor per defecte per comportament de muntatge. Per defecte, l'opció **nfs_v4_fail_over_timeout** no es troba activa. El seu valor és `0`.

Quan **nfs_v4_fail_over_timeout** no es troba activa, el llindar de la migració després d'un error s'estableix dues vegades el valor de l'opció **timeo** de muntatge. Si no s'ha realitzat cap crida RPC correctament durant aquest temps, el client començarà el processament de migració després d'un error per trobar una altra rèplica disponible. De tota manera, el temps real que el client haurà d'esperar està determinat per l'opció **retrans**. Si **retrans** és major que 2, és probable que el client esperi fins que rebi un temps d'espera RPC basat en el valor **retrans** multiplicat pel valor **timeo** (`retrans` × `timeo`). Per tant, la combinació de les opcions **timeo** i **retrans** es pot ajustar per controlar el comportament de migració després d'error segons el muntatge per NFS. També podeu configurar aquestes opcions en un nivell més granular mitjançant l'ordre **nfs4cl**.

Si **nfso nfs_v4_fail_over_timeout** s'ha establert en un valor diferent de zero, representarà el número de segons que el client haurà d'esperar en un servidor no disponible abans de considerar la migració després d'error de rèplica. Si les opcions **timeo** i **retrans** donen com a resultat un comportament de temps d'espera RPC més enllà del valor **nfso**, és possible que el procediment de migració després d'error no s'iniciï fins que es generi el temps d'espera RPC.

Per obtenir més informació sobre les opcions **retrans**, **timeo**, i **nfs_v4_fail_over_timeout**, consulteu les opcions específiques de NFS de les ordres **mount**, **nfs4cl**, i **nfso**.

A més de la migració després d'error de rèplica en el cas que un servidor no es trobi disponible, hi ha casos en els quals el client canviarà voluntàriament d'una ubicació de rèplica a una altra. Un cas és quan s'utilitza l'ordre **nfs4cl** per establir una rèplica preferida. En aquest cas, el client inicia un canvi al servidor preferit, en el cas que no es trobi en el servidor actual el qual està utilitzant el client. El client també tornarà a capturar l'informació d'ubicació de rèplica des del servidor NFS en intervals aproximats de 30 minuts quan hi hagi hagut activitat recent a les dades associades. Si l'ordre de les ubicacions ha canviat, el client intentarà canviar a la primera ubicació, en el cas que aquesta sigui diferent del servidor actual que el client està utilitzant i no hagi establert una preferència de rèplica amb l'ordre **nfs4cl**.

Muntatges NFS flexibles i comportament de migració després d'un error:

El model de muntatge per defecte per NFS són muntatges rígids i el comportament de la migració després d'un error de rèplica s'aplica a muntatges rígids. El comportament de migració després d'un error és diferent si s'utilitzen muntatges flexibles NFS.

Si els valor del muntatge flexible donen com a resultat un temps d'espera RPC anterior al període d'espera establert per la migració després d'un error de rèplica, el temps d'espera donarà com a resultat un error **ETIMEDOUT** per l'aplicació que s'està cridant. La utilització de muntatges flexibles amb dades replicades no és recomanable. Si s'utilitzen muntatges flexibles i s'ha establert el valor **nfso nfs_v4_fail_over_timeout**, es recomanable establir les opcions de muntatge **retrans** i **timeo** per tal que superin el valor **nfso**. Això evitarà la devolució de **ETIMEDOUT** a les aplicacions per les dades replicades.

Reordenació de la llista d'ubicacions del sistema de fitxers mitjançant l'opció scatter

L'opció **scatter** de l'ordre **exportfs** permet modificar l'ordre de les ubicacions especificades a la llista d'ubicacions del sistema de fitxers que s'estableix amb l'opció **refer** o l'opció **replicas** de l'ordre **exportfs**.

Mitjançant aquesta opció es generen diferents combinacions d'ubicacions de servidor per tal que diferents llistes tinguin diferents servidors en l'ordre de preferència. En conseqüència, diferents clients tenen diferents llistes d'ubicació de servidor diferents. Aquesta reordenació ajuda a l'equilibri de càrrega perquè

el primer servidor de la llista d'ubicacions de clients diferents és un servidor diferent. A més, si un servidor es desactiva, la càrrega de la migració després d'un error es distribueix en diversos servidors perquè el servidor de la ubicació següent de la llista d'ubicacions de servidor és diferent. L'opció **scatter** només s'aplica als directoris exportats per accés mitjançant el protocol NFS versió 4.

L'opció **scatter** pot tenir els valors següents:

- **complet** - Tots els servidors es reordenen per formar combinacions d'ubicacions alternatives. El número total de combinacions està limitada a 12 o al número de servidors, el que sigui més elevat dels dos.
- **parcial** - La primera ubicació de totes les combinacions de servidor generades és fixa pel primer servidor de la llista de servidors. La resta d'ubicacions es llisten com si s'utilitzés la reordenació completa.
- **cap** - No es realitza cap reordenació de la llista d'ubicacions del sistema de fitxers. Aquest és el valor per defecte de l'opció **scatter**. Utilitzeu aquest valor per inhabilitar les reordenacions anteriors de la llista d'ubicacions.

Nota: Si el senyalador **noauto** no està especificat quan utilitzeu l'ordre **exportfs** , l a llista d'ubicacions inclourà el nom d'amfitrió principal com a una de les ubicacions de rèplica. Per obtenir més informació sobre el senyalador **noauto**, consulteu l'ordre **exportfs** a *Commands Reference, Volume 2*.

Per especificar referències del directori `/common/documents` als amfitrions s1, s2 i s3 i reordenar-los seguidament mitjançant l'opció **full**, afegiu la línia al següent fitxer `/etc/exports` i, aleshores, exporteu el directori`/common/documents`:

```
/common/documents -ver=4, refer=/common/documents@s1:/common/document@s2a:/common/
documents@s3,scatter=full
```

Per especificar rèpliques per al directori `/common/documents` als amfitrions s1, s2, s3 i reordenar-los parcialment (el primer servidor de migració després d'un error és s1 per a totes les combinacions), afegiu la línia següent al fitxer `/etc/exports` i, aleshores, exporteu el directori `/common/documents`:

```
/common/documents -vers=4, replicas=/common/documents@s1:/common/documents@s2:/common/
   documents@s3:/common/documents@s4,scatter=partial
```

Delegació servidor-client NFS

La *delegació* és la capacitat del servidor de delegar determinades responsabilitats al client.

Començant amb AIX 5L Versió 5.3 amb el paquet de manteniment recomanat 5300-03 , es pot utilitzar la delegació. Quan el servidor atorga una delegació per a un fitxer a un client, es garanteix certa semàntica al client respecte del fet de compartir el fitxer en qüestió amb altres clients. Quan s'obre un fitxer, el servidor pot proporcionar al client una delegació de lectura per al fitxer. Si al client s'atorga una delegació de lectura, es garanteix que cap altre client podrà escriure al fitxer mentre duri la delegació. Si al client se li atorga una delegació d'escriptura, se li garanteix que cap altre client tindrà accés de lectura ni escriptura al fitxer. El servidor AIX només atorga delegacions de lectura. El servidor AIX només dóna suport a la delegació amb el kernel AIX de 64 bits. El client AIX dóna suport a les delegacions de lectura i d'escriptura.

Per tal que el servidor atorgui una delegació a un client, el client primer haurà de proporcionar una adreça de crida de retorn al servidor. Quan es torna a cridar a una delegació, el servidor enviarà una sol•licitud de crida de retorn a aquesta adreça. Per defecte, el client indicarà l'adreça IP que s'està utilitzant per a la comunicació normal amb el servidor. En el cas de clients amb múltiples interfícies de xarxa, es pot especificar una adreça específica al fitxer `/etc/nfs/nfs4_callback.conf`. El format de les entrades d'aquest fitxer és:

servidor-amfitrió adreça-ip-client

Allà on *servidor-amfitrió* sigui el nom o l'adreça d'un servidor NFSv4 i *adreça-ip-client* sigui l'adreça de client que s'ha d'utilitzar en proporcionar informació de crida de retorn del servidor. Si el nom de

servidor-amfitrió es l'adreça de IPv4 0.0.0.0 o l'adreça de IPv6 0::0, la variant *adreça-ip-client* s'utilitzarà per a tots els servidors que no estiguin llistats al fitxer. Si aquest fitxer no existeix o si no es troba l'entrada d'aquest servidor (o l'entrada per defecte), el client seleccionarà una adreça basada en la connexió existent amb el servidor.

El servidor pot tornar a cridar les delegacions. Si una altri client sol•licita l'accés al fitxer de manera que es produeixi un conflicte d'accés amb la delegació atorgada, el servidor podrà ho podrà notificar al client inicial i tornar a cridar la delegació. Això requereix que existeixi un camí d'accés de crida de retorn entre el servidor i el client. Si aquest camí d'accés de crida de retorn no existeix, no es podran atorgar delegacions. Si s'ha atorgat una delegació de fitxers, l'accés des d'altres clients NFSv4, clients NFS versions 2 i 3 i els accessos locals al fitxer del servidor de fitxers podran provocar la crida de retorn de la delegació. Si s'està exportant GPFS mitjançant NFSv4, l'accés al node GPFS de la xarxa pot fer que es torni a cridar la delegació.

L'essència de la delegació és que permet al client proporcionar operacions de forma local com, per exemple OPEN, CLOSE, LOCK, LOCKU, READ i WRITE sense l'interacció immediata amb el servidor.

La delegació del servidor es troba habilitada per defecte. La delegació del servidor es pot inhabilitar amb l'ordre `nfso -o server_delegation=0`. Els administradors poden utilitzar l'opció **exportfs deleg=yes | no** per inhabilitar o habilitar l'atorgament de delegacions segons sistema de fitxers, la qual cosa alterarà temporalment el valor **nfso**.

La delegació de client es pot inhabilitar amb l'ordre `nfso -o client_delegation=0`. La delegació de client s'ha d'establir abans de que es realitzin els muntatges al client.

Si l'administrador exporta un sistema de fitxers on molts clients escriuen a molts fitxers comuns, és possible que l'administrador desitgi inhabilitar les delegacions pel sistema de fitxers en qüestió.

Si no es pot contactar amb el client (per exemple, si la xarxa o el client experimenten una avaria), és possible que altres clients tardin a accedir a les dades.

Establiment dels amfitrions genèrics més importants per a crides de retorn protegides per Kerberos

Podeu establir un camí d'accés d'una crida de retorn per IBM Network Authentication Service (Kerberos).

El client que rep la delegació ha de ser un client complet amb el seu propi amfitrió. No obstant això, podeu establir un amfitrió genèric per tots els clients que es farà servir per a les crides de retorn.

Per tal d'establir un amfitrió genèric per tots els clients que es farà servir per a les crides de retorn, dueu a terme els passos següents:

1. Per crear un amfitrió de servei (per exemple, `nfs/client`) utilitzant el mateix mètode que per crear un amfitrió, consulteu l'apartat sobre la Creació d'un amfitrió Kerberos a *Security*.
2. Creeu una entrada keytab per aquest amfitrió de servei. Per exemple, per crear un keytab anomenat slapd_krb5.keytab, feu el següent:

```
kadmin.local: ktadd -k /etc/security/slapd_krb5.keytab ldap/plankton.austin.ibm.com
Entry for principal ldap/plankton.austin.ibm.com with kvno 2,
encryption type Triple DES cbc mode with HMAC/sha1 added to keytab
WRFILE:/etc/security/slapd_krb5.keytab.
Entry for principal ldap/plankton.austin.ibm.com with kvno 2,
encryption type ArcFour with HMAC/md5 added to keytab WRFILE:/etc/security/slapd_krb5.keytab.
Entry for principal ldap/plankton.austin.ibm.com with kvno 2,
encryption type AES-256 CTS mode with 96-bit SHA-1 HMAC added to keytab
WRFILE:/etc/security/slapd_krb5.keytab.
Entry for principal ldap/plankton.austin.ibm.com with kvno 2,
encryption type DES cbc mode with RSA-MD5 added to keytab WRFILE:/etc/security/slapd_krb5.keytab.
kadmin.local:
```

3. Distribuïu aquest keytab a tots els clients que l'hagin de fer servir.

4. Configureu els clients amb l'ordre **nfshostkey**.

Aquest procés és idèntic al procés de configurar un servidor per utilitzar-lo amb Kerberos, però l'amfitrió genèric no es pot fer servir per servidors; cada servidor ha de tenir el seu propi amfitrió amb el format `nfs/nom_sistema_principal`.

Sistemes de fitxers de xarxa de curt termini STNFS

Un sistema de fitxers STNFS és una còpia de seguretat de sistema de fitxers que fa un Network File System (NFS) i el sistema de fitxers STNFS permet modificacions locals als fitxers. Les modificacions no es desen al servidor.

Notes:

1 Molts clients d'STNFS poden compartir la mateixa imatge del sistema de fitxers d'un servidor, però les modificacions només les veurà el client que faci la modificació.

2 Totes les modificacions fetes per un client es perdran quan el sistema de fitxers es desmunti o quan el client reinicïi el sistema.

3 Les operacions d'escriptura des d'STNFS fallaran quan la memòria del sistema estigui per sota del llindar predeterminat. El llindar és intern a l'STNFS i no es pot configurar externament.

Muntatge d'un sistema de fitxers NFS a curt termini

L'ordre **mount** s'utilitza per muntar un sistema de fitxers NFS a curt termini. Per exemple, escriviu l'ordre següent:

```
mount -v stnfs -o options server:/camí-remot /camí-local
```

Les opcions disponibles són:

vers=3 Utilitza la versió 3 d'NFS per comunicar-se amb el servidor.

vers=4 Utilitza la versió 4 d'NFS per comunicar-se amb el servidor.

rsize=size
Estableix els octets de la mida de lectura.

proto=udp
Utilitza UDP per comunicar-se amb el servidor NFS.

proto=tcp
Utilitza TCP per comunicar-se amb el servidor NFS.

hard Utilitza muntatges fixos d'NFS.

soft Utilitza muntatges dinàmics d'NFS.

sec Utilitza la classificació de seguretat especificada.

Les opcions per defecte són:

vers=3

rsize=32768

proto=tcp

hard

sec=sys

Llista de control per configurar NFS

Un cop que hagueu instal•lat el programari NFS als vostres sistemes, podreu configurar NFS. Seguiu els passos per configurar NFS.

Cal instal•lar CryptoLite a la biblioteca de kernel C (CLiC) abans de configurar NFS per utilitzar els tipus de seguretat següent:

- krb5
- krb5i
- krb5p

Cada pas es descriu detalladament més endavant.

1. Determineu els sistemes de la xarxa que han de ser els servidors i els que seran els clients (un sistema es pot configurar com a servidor i com a client).
2. Determineu la versió de NFS que utilitzareu.
3. Decidiu si utilitzareu la seguretat RPCSEC-GSS. En tal cas, consulteu les consideracions que apareixen a “Configuració d'una xarxa per RPCSEC-GSS” a la pàgina 535.
4. Per a cada sistema (ja sigui client o servidor), seguiu les instruccions que apareixen a “Inici dels daemons NFS a l'engegada del sistema”.
5. Per a cada servidor NFS, seguiu les instruccions que apareixen a “Configuració d'un servidor NFS”.
6. Per a cada client NFS, seguiu les instruccions que apareixen a “Configuració d'un client NFS” a la pàgina 533.
7. Si voleu que els ordinadors personals de la vostra xarxa puguin accedir als servidors NFS (a més de poder muntar sistemes de fitxers), configureu PC-NFS seguint les instruccions que apareixen a “PC-NFS” a la pàgina 546.
8. Si voleu emprar NFS versió 4, consulteu les consideracions que apareixen a “Suport de NFS versió 4” a la pàgina 520.

Inici dels daemons NFS a l'engegada del sistema

Els daemons NFS, per defecte, no s'inicien durant l'instal•lació.

Quan s'instal•len, tots els fitxers es col•loquen al sistema però no es duen a terme els passos per activar NFS. Podeu iniciar els daemons NFS durant l'engegada del sistema mitjançant:

- El camí d'accés ràpid de la SMIT, `smit mknfs`
- L'ordre **mknfs**.

Tots aquests mètodes col•loquen una entrada al fitxer `inittab` per tal que la seqüència `/etc/rc.nfs` s'executi cada vegada que es reinicií el sistema. Per la seva banda, la seqüència inicia tots els daemons NFS necessaris per a un sistema determinat.

Configuració d'un servidor NFS

Utilitzeu aquest procediment per configurar un servidor NFS.

Per configurar un servidor NFS:

1. Creeu el fitxer `/etc/exports`. Consulteu el “/etc/exports file” a la pàgina 515.
2. Si utilitzeu Kerberos, configureu el servidor NFS com a client Kerberos. Consulteu el “Configuració d'una xarxa per RPCSEC-GSS” a la pàgina 535.
3. Si utilitzeu NFS versió 4, establiu el domini NFS versió 4 mitjançant l'ordre **chnfsdom**. Consulteu la descripció de l'ordre **chnfsdom** que apareix a *Commands Reference, Volume 1* per obtenir informació detallada al respecte.

   Inicialment, podeu especificar el domini d'internet del servidor al fitxer. No obstant, és possible definir un domini de NFS versió 4 que sigui diferent del domini d'internet del servidor. Per obtenir més informació al respecte, consulteu la documentació del daemon d'enregistrament NFS **nfsrgyd** a *Commands Reference, Volume 4*.

4. Si utilitzeu NFS versió 4 amb Kerberos, és possible que hagueu de crear el fitxer `/etc/nfs/realm.map`. Consulteu el “Fitxer /etc/nfs/realm.map” a la pàgina 516.
5. Si desitgeu utilitzar l'autenticació Kerberos al servidor, haureu d'habilitar la seguretat ampliada al servidor. Podeu habilitar la seguretat ampliada mitjançant SMIT o mitjançant l'ordre **chnfs -S -B**. Per obtenir més informació sobre **chnfs**, consulteu la descripció de l'ordre **chnfs** que apareix a *Commands Reference, Volume 1*.

Configuració d'un client NFS

Utilitzeu aquest procediment per configurar un client NFS.

1. Inicieu NFS mitjançant les instruccions que apareixen a “Inici de daemons NFS” a la pàgina 519.
2. Establiu el punt de muntatge local mitjançant l'ordre **mkdir**. Per tal que NFS completi un muntatge correctament, hi ha d'haver un directori que actuï com a punt de muntatge (o espai reservat) d'un muntatge NFS. Aquest directori ha d'estar buit. Aquest punt de muntatge es pot crear com qualsevol altre directori. No és necessari cap atribut especial.

   Nota: Amb una excepció, els punts de muntatge de tots els muntatges NFS han d'existir al sistema abans de muntar un sistema de fitxers. Si s'empra el daemon **automount**, no caldrà crear punts de muntatge. Consulteu la descripció del daemon **automount** que apareix a *Commands Reference, Volume 1* per obtenir informació detallada al respecte.
3. Si utilitzeu Kerberos, seguiu els passos següents:
   a. Configureu el client NFS dins del domini de Kerberos. Això es realitza amb l'ordre **config.krb5**. Consulteu la publicació *IBM Network Authentication Service Administrator's and User's Guide* per obtenir informació detallada sobre la configuració.
   b. Creeu els punts principals de tots els usuaris del client que accediran als fitxers a través dels muntatges de Kerberos. Això es realitza amb l'ordre **kadmin**. Consulteu la publicació *Network Authentication Service Administrator's and User's Guide* per obtenir una descripció sobre com crear els principals de Kerberos.
   c. Establir un principal de Kerberos per una màquina client en sí és opcional. Un client sense un principal es coneix com a *client prim* i un client amb un principal es coneix com a *client sencer*. Els clients prims utilitzen una seguretat NFS RPC inferior a l'hora de realitzar determinades operacions de gestió de context de client a servidor de NFS versió 4 que es fan servir per la gestió de l'estat. Un client sencer, que depèn de la configuració, pot utilitzar la seguretat RPC més robusta i basada en Kerberos. Les configuracions de clients prims requereixen menys càrrega administrativa i poden ser suficients per molts entorns. Els desplegaments que necessiten els nivells de seguretat més alts poden optar per executar configuracions de clients sencers.
4. Si utilitzeu NFS versió 4, també haureu d'establir un domini NFS versió 4 mitjançant l'ordre **chnfsdom**. Inicialment, podeu especificar el domini d'internet del client al fitxer. No obstant, és possible definir un domini de NFS versió 4 que sigui diferent del domini d'internet del client. Per obtenir més informació al respecte, consulteu la documentació del daemon d'enregistrament NFS **nfsrgyd**.
5. Si desitgeu utilitzar l'autenticació Kerberos al client, haureu d'habilitar la seguretat ampliada al client. Podeu habilitar la seguretat ampliada mitjançant SMIT o mitjançant l'ordre **chnfs -S -B**. Per obtenir més informació sobre **chnfs**, consulteu la pàgina de referència de l'ordre **chnfs**.
6. Establiu i munteu els muntatges predefinits seguint les instruccions que apareixen a “Establiment de muntages NFS predefinits” a la pàgina 541.

Mapatge d'entitats

El mapatge d'entitats proporciona un mètode per tal que el client i el servidor NFS local puguin moure usuaris i grups externs a usuaris i grups locals.

AIX utilitza la tecnologia EIM, que està basada en LDAP, per realitzar el seu mapatge d'identitats. Totes les dades del mapatge d'identitats NFS s'emmagatzemen en uns servidor LDAP.

Per configurar un client EIM, s'hauran d'instal•lar els catàlegs de fitxers `bos.eim.rte` i `ldap.client`. El servidor EIM també requereix el catàleg de fitxers `ldap.server`. Un cop s'hagin instal•lat els catàlegs de fitxers adequats, s'utilitzarà `/usr/sbin/chnfsim` per configurar EIM. Les opcions de configuració mínimes són:

```
/usr/sbin/chnfsim -c -a -t [type] -h [servidor EIM] -e [domini LDAP/EIM] -f [sufix LDAP] -w [contrasenya de l'administrador]
```

D'aquesta manera es configuren els clients i els servidors EIM per utilitzar un servidor EIM específic pel mapatge d'identitats. Si el nom de l'amfitrió especificat a l'ordre és el nom de l'amfitrió local, també es configurarà el servidor LDAP.

Un cop s'hagi completat el pas de configuració, l'administrador d'EIM podrà omplir el servidor LDAP amb dades del mapatge d'identitats NFS. Un usuari o un grup individual, com per exemple John Doe, es coneix com a identitat de mapatge. La sèrie del propietari de NFS d'aquest usuari, *johndoe@austin.ibm.com*, es coneix com a mapatge d'identitats. Per entrar al servidor LDAP amb aquestes dades, s'haurà d'executar l'ordre següent:

```
/usr/sbin/chnfsim -a -u -i "John Doe" -n johndoe -d austin.ibm.com
```

L'identitat de mapatge es el nom descriptiu de l'usuari o grup i el mapatge d'identitat és la sèrie del propietari NFS de *nom@domini*. Els mapatges de domini a domini també s'emmagatzemen al servidor LDAP. Per tal que el domini Kerberos `kerb.austin.ibm.com` realitzi un mapatge del domini NFS `austin.ibm.com`, s'haurà d'executar l'ordre següent:

```
/usr/sbin/chnfsim -a -r kerb.austin.ibm.com -d austin.ibm.com
```

Per configurar NFS per tal de fer servir les dades del mapatge a EIM, s'haurà de tornar a iniciar el daemon d'enregistrament NFS. El daemon d'enregistrament NFS comprova la disponibilitat d'un servidor EIM durant l'inici i, si se'n troba un, totes les funcions de mapatge es gestionaran a través d'EIM i no s'empraran més els mapatges locals.

Per obtenir informació sobre EIM, consulteu Mapatge d'entitats d'empresa que apareix a *Security*.

Exportació d'un sistema de fitxers NFS

Podeu exportar un sistema de fitxers de xarxa (NFS) mitjançant els procediments següents.

- Per exportar un sistema de fitxers NFS mitjançant SMIT:
  1. Comproveu que NFS ja s'està executant escrivint l'ordre `lssrc -g nfs`. La sortida hauria d'indicar que els daemons **nfsd** i **rpc.mountd** estan actius. Si no ho estan, inicieu NFS mitjançant les instruccions que apareixen a "Inici de daemons NFS" a la pàgina 519.
  2. A la línia d'ordres, escriviu el següent i feu clic a Intro:
     ```
     smit mknfsexp
     ```
  3. Especifiqueu els valors adequats a PATHNAME del directori que s'ha d'exportar, MODE per exportar el directori i EXPORT per exportar el directori ara, reinici del sistema o ambdós camps.
  4. Especifiqueu qualsevol altra característica opcional que desitgeu o accepteu els valors per defecte deixant els camps restants tal com apareixen.
  5. Quan acabeu de realitzar les modificacions, SMIT actualitzarà el fitxer `/etc/exports`. Si el fitxer `/etc/exports` no existeix, se'n crearà un.
  6. Repetiu els passos del 3 al 5 per a cada directori que desitgeu exportar.
- Per exportar un sistema de fitxers NFS mitjançant un editor de textos:
  1. Obriu el fitxer `/etc/exports` amb el vostre editor de textos preferit.
  2. Creeu una entrada per a cada directori que s'hagi d'exportar mitjançant el nom de camí d'accés sencer del directori. Llisteu cada directori que s'hagi d'exportar començant pel marge de l'esquerra. No es pot incloure cap directori dins d'un directori que ja s'hagi exportat. Consulteu el fitxer `/etc/exports` de *Files Reference* per obtenir una descripció de tota la sintaxi de les entrades del fitxer `/etc/exports`.

3. Deseu i tanqueu el fitxer /etc/exports.
4. Si s'està executant NFS, escriviu l'ordre següent i feu clic a Intro:

   ```
   /usr/sbin/exportfs -a
   ```

   L'opció **-a** indica a l'ordre **exportfs** que enviï tota la informació del fitxer /etc/exports al kernel. Si no s'està executant NFS, inicieu-lo seguint les instruccions que apareixen a "Inici de daemons NFS" a la pàgina 519.

- Per exportar temporalment un sistema de fitxers NFS (sense canviar el fitxer /etc/exports), escriviu l'ordre següent i feu clic a Intro:

  ```
  exportfs -i /nomdir
  ```

  on *nomdir* es el nom del sistema de fitxers que desitgeu exportar. L'ordre **exportfs -i** especifica que el fitxer /etc/exports no s'ha de comprovar per si conté el directori especificat i que totes les opcions es prenen directament de la línia d'ordres.

  El suport de AIX NFS versió 4 permet a l'administrador crear i controlar un espai de nom alternatiu que es representa mitjançant el servidor NFS als clients. Això es realitza mitjançant l'opció d'exportació **exname**. Aquest suport també es pot utilitzar per ocultar detalls de l'espai de nom del sistema de fitxers local del servidor respecte dels clients NFS. Per obtenir informació detallada, consulteu la descripció de l'ordre **exportfs** que apareix a *Commands Reference, Volume 2* i la descripció del fitxer /etc/exports que apareix a *Files Reference*.

Configuració d'una xarxa per RPCSEC-GSS

La xarxa que s'està configurant en aquest cas conté cinc servidors i es configura per RPCSEC-GSS.

Els cinc servidors de la xarxa són els següents:

- kdc.austin.ibm.com
- alpha.austin.ibm.com
- beta.austin.ibm.com
- gamma.austin.ibm.com
- zeta.austin.ibm.com

El sistema kdc.austin.ibm.com es configurarà com a servidor KDC i es crearà el domini Kerberos ES.IBM.COM, en el qual tots els sistemes excepte kdc.austin.ibm.com i zeta.austin.ibm.com seran servidors NFS que ofereixen sistemes de fitxers exportats amb RPCSEC-GSS.

Els sistemes alpha.austin.ibm.com i beta.austin.ibm.com tenen un enllaç addicional entre ells. En aquest enllaç, apareixen com a fast_alpha.test.austin.com i fast_beta.test.austin.ibm.com. Per aquest motiu, és necessari un pas de configuració addicional.

A més, aquesta xarxa té els usuaris següents, els quals s'han configurat en alguns dels sistemes:

- adam
- brian
- charlie
- dave
- eric

Nota: La configuració següent es proporciona només com a exemple i és possible que no sigui adient per a tots els entorns. Consulteu la Guia de l'administrador i de l'usuari del servei d'autenticació de la xarxa abans d'intentar configurar un nou domini Kerberos.

Nota: Kerberos requereix que l'hora del sistema sigui relativament propera a la de la xarxa. Abans d'intentar aquest procediment, haurà de configurar un mecanisme per sincronitzar automàticament l'hora a tota la xarxa com, per exemple, el daemon AIX **timed** o una configuració NTP.

1. Configureu el servidor KDC.

   Nota: Idealment, el servidor KDC no s'ha de fer servir per qualsevol altre finalitat. En el cas que KDC es vegi compromès, també es comprometran tots els principals de Kerberos.

   En aquest cas, `kdc.austin.ibm.com` es configurarà com a servidor KDC. La configuració següent és per **des3**. Si es prefereix utilitzar **des** per motius de rendiment, afegiu l'argument `-e des-cbc-crc:normal` a les crides `addprinc` i `ktadd` pel daemon **kadmin** següent.

   Per configurar la xarxa amb l'encriptació **aes**, afegiu l'argument `-e aes256-cts:normal` a les crides `addprinc` i `ktadd` per l'ordre **kadmin**.

   a. Instal•leu el catàleg de fitxers `krb5.server.rte` a `kdc.austin.ibm.com`.
   b. Configureu el servidor KDC. En aquest cas, s'ha utilitzat l'ordre següent:

      ```
      config.krb5 -S -d austin.ibm.com -r AUSTIN.IBM.COM
      ```

      Un cop hagueu executat aquesta ordre, el sistema sol•licitarà una paraula clau de base de dades mestra i una paraula clau pel principal administratiu.
   c. Creeu principals per a cada usuari i amfitrió executant l'ordre `/usr/krb5/sbin/kadmin.local` al servidor KDC. En aquest exemple, es creen principals de Kerberos que coincideixen amb el nom d'usuari UNIX de l'usuari associat. El nom de principal es mapejarà amb el nom d'usuari mitjançant NFS per determinar la credencial UNIX associada amb el principal. Per obtenir una descripció sobre com utilitzar mapatges més generals entre principals i noms d'usuari, consulteu “Mapatge d'entitats” a la pàgina 533. En el cas d'aquesta xarxa, hem creat els principals següents:
      - `adam`
      - `brian`
      - `charlie`
      - `dave`
      - `eric`
      - `nfs/alpha.austin.ibm.com`
      - `nfs/beta.austin.ibm.com`
      - `nfs/gamma.austin.ibm.com`

      Nota: Els noms de principal d'usuari escollits han de coincidir amb els noms d'usuari corresponents de l'enregistrament d'usuaris configurat del sistema (`/etc/passwd`, **LDAP**, **NIS**, etc.). NFS utilitza el nom de principal com a nom d'usuari per obtenir ID d'usuari i de grup al sistema local. Si els noms no coincideixen, l'accés es tractarà com si fos anònim.

   Ja s'ha configurat el servidor KDC.
2. Cada client i servidor NFS es configurarà com a clients Kerberos mitjançant l'ordre **config.krb5**. El mode en què això es realitzi dependrà de com s'hagi configurat KD. En aquest cas, s'ha executat l'ordre següent en cada sistema NFS:

   ```
   config.krb5 -C -d austin.ibm.com -r AUSTIN.IBM.COM -c kdc.austin.ibm.com -s kdc.austin.ibm.com
   ```

   Ara és possible utilitzar **kinit** com a qualsevol dels principals d'usuari en qualsevol dels sistemes configurats. Per exemple, per utilitzar **kinit** com a usuari `adam`, executeu l'ordre següent:

   ```
   /usr/krb5/bin/kinit adam
   ```

   Haureu d'especificar la paraula clau Kerberos de `adam`, no AIX.

   Aquest exemple utilitza **kinit** per autenticar l'usuari. És possible configurar AIX per utilitzar l'autenticació Kerberos durant l'inici de sessió del sistema. Per obtenir més informació, consulteu Autenticació d'AIX mitjançant Kerberos que apareix a *Security*.
3. Cada servidor NFS es configurarà amb l'entrada `keytab` adient. En aquest cas, s'ha configurat l'entrada `keytab` per `alpha.austin.ibm.com` com a exemple. El mateix procés es farà servir a `beta.austin.ibm.com` i a `gamma.austin.ibm.com`.

a. Des de alpha.austin.ibm.com, executeu l'ordre **kadmin**. A continuació, executeu l'ordre següent:
```
ktadd nfs/alpha.austin.ibm.com
```

Això crea un fitxer keytab.

b. A continuació, configureu el daemon **gssd** per utilitzar el fitxer keytab que acabeu de crear amb l'ordre **nfshostkey**. En aquest cas, s'ha executat el següent:
```
nfshostkey -p nfs/alpha.austin.ibm.com -f /etc/krb5/krb5.keytab
```

c. Configureu el daemon **gssd** per que s'iniciï automàticament executant l'ordre següent:
```
chnfs -S -B
```

Repetiu aquesta configuració per a cada sistema.

4. En aquest punt, el servidor NFS funcionarà, encara que tots els usuaris apareixeran com a nobody. És aconsellable que tots els usuaris de tots els servidors tinguin els mateixos uid i gid. Qualsevol usuari que no existeixi tindrà accés al directori exportat només com a nobody. Per obtenir els noms d'usuari que s'han de mapar correctament, haureu de configurar el daemon d'enregistrament NFS.

a. Configureu el domini mitjançant l'ordre **chnfsdom**. En aquest cas, s'ha executat l'ordre següent en tots els servidors NFS per configurar austin.ibm.com com a domini:
```
chnfsdom austin.ibm.com
```

b. Configureu el fitxer /etc/nfs/realm.map. Aquest fitxer ha de contenir una línia, amb el nom de domini seguit pel domini local. En el cas de l'exemple de xarxa, aquest dos camps han de tenir l'aspecte següent a tots els servidors NFS:
```
realm.map AUSTIN.IBM.COM   austin.ibm.com
```

L'entrada de domini d'aquest fitxer no reconeix majúscules i minúscules i, per tant, tècnicament, aquesta entrada no és necessària.

c. En el cas de zeta.austin.ibm.com, que no serà un servidor NFS, inicieu l'ordre **gssd** mitjançant l'ordre chnfs -S -B. Abans d'intentar qualsevol operació de client Kerberos, l'usuari haurà d'utilitzar **kinit** per obtenir credencials vàlides.

5. En aquest cas, s'ha configurat un enllaç de xarxa ràpid entre alpha.austin.ibm.com i beta.austin.ibm.com. En aquest enllaç, beta.austin.ibm.com veurà alpha.austin.ibm.com com a fast_alpha.test.austin.ibm.com i alpha.autsin.ibm.com veurà beta.austin.ibm.com com a fast_beta.test.austin.ibm.com. Donat que nfs/fast_alpha.test.austin.ibm.com i nfs/fast_beta.test.austin.ibm.com no són principals vàlids, no podran utilitzar aquest enllaç per realitzar muntatges.

Per corregir això, s'utilitzarà l'ordre **nfshostmap**, la qual mapejarà el principal per gestionar aquesta situació.

a. A alpha.austin.ibm.com, s'ha executat l'ordre següent:
```
nfshostmap -a beta.austin.ibm.com fast_beta.test.austin.ibm.com
```

Això indica a alpha.austin.ibm.com que el principal de fast_beta.test.austin.ibm.com es per a beta.austin.ibm.com.

b. En beta, s'ha executat l'ordre següent:
```
nfshostmap -a alpha.austin.ibm.com fast_alpha.test.austin.ibm.com
```

Els servidors poden tenir diversos principals d'amfitrió. Suposant que l'adreça IP de fast_alpha és 10.0.0.1 i l'adreça IP de fast_beta és 10.0.0.2, dueu a terme els passos següents per afegir diversos principals d'amfitrió:

a. Afegiu els principals nfs/fast_alpha.test.austin.ibm.com i nfs/fast_beta.test.austin.ibm.com als fitxers keytab adients.

b. Executeu l'ordre **nfshostkey** al servidor alpha de la manera següent:
```
nfshostkey -a -p nfs/fast_alpha.test.austin.ibm.com -i 10.0.0.1
```

c. Executeu l'ordre **nfshostkey** al servidor beta de la manera següent:

```
nfshostkey -a -p nfs/fast_beta.test.austin.ibm.com -i 10.0.0.2
```

Cancel•lació de l'exportació d'un sistema de fitxers

Podeu cancel•lar un directori NFS amb aquests procediments.

- Per cancel•lar l'exportació d'un directori NFS mitjançant la SMIT:
  1. Escriviu el següent a l'indicador d'ordres i feu clic a Intro:
     ```
     smit rmnfsexp
     ```
  2. Especifiqueu el nom de camí d'accés adient a PATHNAME, dins del camp del directori exportat que s'ha d'eliminar.

     El directori s'elimina del fitxer `/etc/exports` i es cancel•la l'exportació del mateix.

     Si el directori s'ha exportat a clients mitjançant NFS versió 4, es possible que la cancel•lació de l'exportació falli degut a l'estat dels fitxers del servidor. L'estat del fitxer fa referència a què els fitxers dels directoris exportats són oberts per un client. Podeu dur a terme accions per aturar aplicacions mitjançant aquestes dades o podeu cancel•lar l'exportació de manera obligada (**exportfs -F**) de les dades, la qual cosa pot donar lloc a que es produeixin errors a les aplicacions que utilitzen activament les dades.
- Per cancel•lar l'exportació d'un directori NFS mitjançant un editor de textos:
  1. Obriu el fitxer `/etc/exports` amb el vostre editor de textos preferit.
  2. Busqueu l'entrada del directori del qual voleu cancel•lar l'exportació i suprimiu aquesta línia.
  3. Deseu i tanqueu el fitxer `/etc/exports`.
  4. Si NFS s'està executant actualment, escriviu:
     ```
     exportfs -u dirname
     ```

     on *dirname* es el nom de camí d'accés sencer del directori que acabeu de suprimir del fitxer `/etc/exports`. Si la cancel•lació de l'exportació falla degut a l'accés de clients de NFS V4, podeu afegir una opció -F per forçar la cancel•lació del directori.

Modificació del sistema de fitxers exportats

Canvieu un sistema de fitxers NFS exportats mitjançant els procediments següents.

- Per canviar un sistema de fitxers exportats mitjançant SMIT:
  1. Per cancel•lar l'exportació del sistema de fitxers, escriviu:
     ```
     exportfs -u /dirname
     ```

     on *dirname* és el nom del sistema de fitxers que desitgeu canviar.
  2. Escriviu:
     ```
     smit chnfsexp
     ```
  3. Especifiqueu el nom de camí d'accés adequat a PATHNAME, dins del camp del directori exportat.
  4. Realitzeu tots els canvis que desitgeu.
  5. Sortiu de SMIT.
  6. Torneu a exportar el sistema de fitxers especificant el següent:
     ```
     exportfs /dirname
     ```

     on *dirname* és el nom del sistema de fitxers que acabeu de modificar.
- Per canviar un sistema de fitxers NFS exportats mitjançant un editor de textos:
  1. Per cancel•lar l'exportació del sistema de fitxers, escriviu:
     ```
     exportfs -u /dirname
     ```

     on *dirname* és el nom del sistema de fitxers que desitgeu canviar.
  2. Obriu el fitxer `/etc/exports` amb el vostre editor de textos preferit.

3. Realitzeu tots els canvis que desitgeu.
4. Deseu i tanqueu el fitxer `/etc/exports`.
5. Torneu a exportar el sistema de fitxers especificant el següent:
   ```
   exportfs /dirname
   ```

   on *dirname* és el nom del sistema de fitxers que acabeu de modificar.

Accés d'usuari root a un sistema de fitxers exportats

Quan s'exporta un sistema de fitxers, per defecte, no s'otorga accés root a l'usuari root per accedir als sistemes de fitxers exportats.

Quan un usuari root d'un amfitrió sol•licita accés a un fitxer particular des de NFS, l'ID d'usuari del peticionari es mapat per NFS a l'ID d'usuari de l'usuari `nobody` (`nobody` és un dels noms d'usuari col•locat al fitxer `/etc/password` per defecte). Els drets d'accés de l'usuari `nobody` són els mateixos que els que es proporcionen al públic (*others*) per un fitxer determinat. Per exemple, si *others* només té permís d'execució per un fitxer, l'usuari `nobody` només podrà executar el fitxer.

Per habilitar l'accés d'usuari root a un sistema de fitxers exportats, segueixi les instruccions de "Modificació del sistema de fitxers exportats" a la pàgina 538. Si utilitza el mètode SMIT, especifiqui el nom de l'amfitrió al qual desitja atorgar accés root al camp d'accés root permès HOSTS. Si edita el fitxer amb un editor de textos, afegeixi el qualificador `-root=hostname` a l'entrada del sistema de fitxers. Per exemple,

```
/usr/tps -root=hermes
```

especifica que l'usuari root de l'amfitrió `hermes` pot accedir al directori `/usr/tps` amb privilegis root.

Muntatge d'un sistema de fitxers NFS de forma explícita

Per muntar un directori NFS de forma explícita, utilitzeu el procediment següent:

1. Comproveu que el servidor NFS ha exportat el directori:
   ```
   showmount -e >NomServidor
   ```

   on *NomServidor* és el nom del servidor NFS. Aquesta ordre mostra els noms dels directoris que actualment s'han exportat del servidor NFS. Si el directori que desitja muntar no apareix a la llista, exporteu el directori des del servidor.

   Nota: L'ordre **showmount** no funcionarà per sistemes de fitxers que s'hagin exportat només en forma de sistemes de fitxers de NFS versió 4. En el cas de NFS versió 4, el client pot muntar el sistema de fitxers d'arrel pel servidor i travessar l'estructura de directoris exportats. No cal muntar explícitament els sistemes de fitxers exportats individuals per tal que el client hi accedeixi.
2. Establiu el punt de muntatge local mitjançant l'ordre **mkdir**. Un direcotri nul (buit) que actua com a punt de muntatge (o espai reservat) d'un muntatge NFS ha d'ésser present per tal que NFS completi un muntatge de forma correcta. Aquest punt de muntatge es pot crear com qualsevol altre directori. No és necessari cap atribut especial.
3. Escriviu:
   ```
   mount NomServidor:/remote/directori /local/directori
   ```

   on *NomServidor* és el nom del servidor NFS, `/remote/`*directori* és el directori del servidor NFS que desitgeu muntar i `/local/`*directori* és el punt de muntatge del client NFS.
4. A la màquina del client, escriviu el camí d'accés ràpid de SMIT següent:
   ```
   smit mknfsmnt
   ```
5. Realitzeu modificacions als camps següents que siguin apropiades per la configuració de xarxa. És possible que la vostra configuració no requereixi que es completin totes les entrades de la pantalla.

Nota: Si s'està utilitzant la interfície SMIT, feu clic a la tecla del tabulador per canviar el valor correcte per a cada camp, però *no* feu clic a Intro fins que no hagueu completat el pas 7.

- NOM DE VIA D'ACCÉS del punt de muntatge.
- NOM DE VIA D'ACCÉS del directori remot.
- AMFITRIÓ on es troba el directori remot.
- MUNTAR ara, afegir entrada a `/etc/filesystems` o ambdós?
- L'entrada `/etc/filesystems` no muntarà el directori durant el reinici del sistema.
- MODALITAT per aquest sistema de fitxers NFS.

6. Canvieu o utilitzeu els valors per defecte per les entrades restants, en funció de la configuració NFS.
7. Quan acabeu de realitzar tots els canvis a la pantalla, SMIT muntarà el sistema de fitxers NFS.
8. Quan el camp **Command:** mostri l'estat OK, sortiu de SMIT.

El sistema de fitxers NFS està llest per ésser utilitzat.

Subsistema de muntatge automàtic

El subsistema **automount** permet als usuaris que no són root muntar sistemes de fitxers remots un cop que el punts de muntatge han estat especificats per l'usuari root.

El fitxer `/etc/auto_master` especifica aquesta informació. Aquests punts de muntatge, coneguts com a claus, tenen mapatges corresponents que determinen el sistema de fitxers remot que s'hi ha de muntar a sobre. El format del fitxer `/etc/auto_master` és el següent:

```
/key map
```

Nota: El fitxer `/etc/auto_master` es llegeix quan l'ordre **automount** s'executa inicialment i els canvis produïts en aquest no s'aplicaran fins que es torni a executar l'ordre **automount**.

Els mapatges més comuns son els directes, indirectes i d'amfitrió.

Mapatges directes

Els mapatges directes requereixen una clau especial (`/-`) al fitxer `/etc/auto_master`.

El mapatge és un fitxer amb el format següent:

```
/claudirecta [-opcions] servidor:/dir
```

Si un usuari accedeix al directori */directkey*, el daemon **automount** muntarà *servidor*:*/dir* a sobre de */claudirecta*.

Mapatges indirectes

Un altre tipus de mapatge que determina el sistema de fitxers remot que s'ha de muntar a sobre d'un punt de muntatge és el mapatge indirecte.

Els mapatges indirectes tenen el format següent:

```
clauindirecta [-opcions] servidor:/dir
```

Quan un usuari accedeix al directori `/key/`*clauindirecta*, el daemon **automount** muntarà *servidor*:*/dir* a sobre de `/key/`*clauindirecta*.

Mapatges d'amfitrió

Els mapatges d'amfitrió requereixen un mapatge especial (`-hosts`) al fitxer `/etc/auto_master`.

El daemon **automount** crearà un subdirectori al directori `/key` per a cada servidor llistat al fitxer`/etc/hosts`. Quan un usuari accedeix al directori `/key/server`, el daemon **automount** muntarà els directoris exportats del servidor al directori `/key/server`.

Utilització d'AutoFS per muntar un sistema de fitxers de forma automàtica

AutoFS confia en l'ús de l'ordre **automount** per propagar la informació de configuració de muntatge automàtic a l'extensió del kernel **AutoFS** i iniciar el daemon **automountd**.

A través la propagació d'aquesta configuració, l'extensió munta de forma automàtica i transparent el sistemes de fitxers cada vegada que s'obri un fitxer o un directori dins d'un sistema de fitxers. L'extensió informa al daemon **automountd** de les sol•licituds de muntatge i desmuntatge i el daemon **automountd** duu a terme realment el servei sol•licitat.

Donat que la vinculacío nom-ubicació es dinàmica dins del daemon **automountd**, les actualitzacions d'un mapatge del servei d'informació de xarxa emprades pel daemon **automountd** són transparents per l'usuari. A més, no cal muntar prèviament el sistemes de fitxers compartits per aplicacions que tenen referències codificades amb fitxers i directoris. Tampoc cal conservar enregistraments dels quals cal muntar amfitrions per aplicacions determinades.

AutoFS permet muntar els sistemes de fitxers segons calgui. Amb aquest mètode de muntatge de directoris, no cal muntar tots els sistemes de fitxers sempre; només es munten els que s'estan utilitzant.

Per exemple, per muntar un directori NFS automàticament:

1. Verifiqueu que el servidor NFS ha exportat el directori entrant el següent:

   ```
   showmount -e NomServidor
   ```

   on *NomServidor* és el nom del servidor NFS. Aquesta ordre mostra els noms dels directoris que actualment s'han exportat del servidor NFS.
2. Creeu un fitxer mestre **AutoFS** i un fitxer de mapatges. **AutoFS** munta i desmunta els directoris especificats en aquests fitxers de mapatges. Per exemple, suposi que desitja que **AutoFS** munti els directoris `/local/dir1` i `/local/dir2` segons convingui al servidor **serve1** en els directoris `/remote/dir1` i `/remote/dir2` respectivament. L'entrada de fitxer `auto_master` tindria l'aspecte següent:

   ```
   /remote  /tmp/mount.map
   ```

   L'entrada del fitxer `/tmp/mount.map` tindria l'aspecte següent:

   ```
   dir1 -rw serve1:/local/dir1
   dir2 -rw serve1:/local/dir2
   ```
3. Asegureu-vos que l'extensió del kernel **AutoFS** es carrega i que el daemon **automountd** s'executa. Això es pot dur a terme de dues maneres:
   a. Mitjançant l'ordre **automount**: executeu `/usr/bin/automount -v`.
   b. Mitjançant **SRC**: executeu `lssrc -s automountd`. Si el subsistema **automountd** no s'està executant, executeu `startsrc -s automountd`.

      Nota: Si inicieu el daemon **automountd** amb l'ordre **startsrc**, s'ignoraran tots els canvis que s'hagin realitzat al fitxer `auto_master`.
4. Per parar el daemon **automount**, executeu l'ordre `stopsrc -s automountd`.

   Si, per algun motiu, el daemon **automountd** s'ha iniciat sense utilitzar el controlador **SRC**, executeu el següent:

   ```
   kill PID_automountd
   ```

   on *PID_automountd* es l'ID de procés del daemon **automountd**. (En executar l'ordre **ps -e** es mostra l'ID de procés del daemon **automountd**.) L'ordre **kill** envia una senyal SIGTERM al daemon **automountd**.

Establiment de muntages NFS predefinits

Podeu establir muntatges NFS predefinits mitjançant un d'aquests procediments.

Nota: Definiu les opcions **bg** (segon pla) i **intr** (interrumpibles) al fitxer `/etc/filesystems` en establir un muntatge predefinit que es munta durant l'inici del sistema. Els muntatges són ininterrumplibles i quan s'executen en primer pla poden bloquejar el client si la xarxa o el servidor estan desconnectats quan s'inicia el sistema del client. Si un client no pot accedir a la xarxa o al servidor, l'usuari haurà de tornar a iniciar la màquina en la modalitat de manteniment i editar les sol•licituds de muntatge adequades.

- Per establir muntatges predefinits a través de la SMIT:
  1. Escriviu:
     ```
     smit mknfsmnt
     ```
  2. Especifiqueu valors en aquesta pantalla per a cada muntatge que desitgeu predefinir. Especifiqueu un valor per a cada camp obligatori (els que apareixen marcats amb un asterisc (*) al marge esquerre). Especifiqueu també valors per a altres camps o accepteu els valors per defecte. Aquest mètode crea una entrada al fitxer `/etc/filesystems` pel muntatge que desitgeu i intenta realitzar el muntatge.
- Per establir els muntatges per defecte NFS mitjançant l'edició del fitxer `/etc/filesystems`:
  1. Obriu el fitxer `/etc/filesystems` amb un editor de textos.
  2. Afegiu entrades per a cada un dels sistemes de fitxers remots que s'han de muntar quan s'iniciï el sistema. Per exemple:
     ```
     /home/jdoe:
     dev = /home/jdoe
     mount = false
     vfs = nfs
     nodename = mach2
     options = ro,soft
     type = nfs_mount
     ```
     La stanza dirigeix el sistema per tal que munti el directori remot `/home/jdoe` a sobre del punt de muntatge local del mateix nom. El sistema de fitxers se munta en modalitat de només de lectura (`ro`). Donat que també es munta com a `soft`, es retorna un error en el cas que el servidor no respongui. En especificar el paràmetre *type* com a `nfs_mount`, el sistema intenta muntar el fitxer `/home/jdoe` (junt amb qualsevol altre sistema de fitxers especificat al grup `type = nfs_mount`) quan s'emet l'ordre **mount -t nfs_mount**.

     L'exemple de stanza següent dirigeix el sistema per tal que munti el sistema de fitxers `/usr/games` durant el reinici del sistema. Si el muntatge falla, el sistema continua intentant realitzar el muntatge en segon pla.
     ```
     /usr/games:
     dev = /usr/games
     mount = true
     vfs = nfs
     nodename = gameserver
     options = ro,soft,bg
     type = nfs_mount
     ```
     Els paràmetres següents són necessaris per les stanzas que pertanyen a muntages NFS:

Element	Descripció
`dev=`*`nome_sistema_fitxers`*	Especifica el nom de via del sistema de fitxers remot que s'està muntant.
`mount=[true|false]`	Si se selecciona `true`, el sistema de fitxers NFS es munta quan s'inicia el sistema. Si se selecciona `false`, el sistema de fitxers NFS no es muntarà quan s'iniciï el sistema.
`nodename=`*`nom_sistema_principal`*	Especifica la màquina de l'amfitrió on es troba el sistema de fitxers remot.
`vfs=nfs`	Especifica que el sistema de fitxers virtual que s'està muntant és un sistema de fitxers NFS.

     Els paràmetres següents són opcionals per les stanza que pertanyen a muntatges NFS:

Element	Descripció
type=*nom_tipus*	Defineix el sistema de fitxers que s'està muntant com a part del grup de muntatge *nom_tipus*. Aquest paràmetre s'utilitza amb l'ordre **mount -t**, la qual munta grups de sistemes de fitxers específics a la vegada.
options=*opcions*	Especifica un o varis paràmetres *d'opcions* següents: **biods=***N* Especifica el nombre màxim de daemons **biod** que s'han d'utilitzar. El valor per defecte és set per NFS versió 2 i quatre per NFS versió 3 i versió 4. **bg** Especifica que s'ha de tornar a intentar el muntatge en segon pla si el primer intent de muntatge no funciona. **fg** Especifica que s'ha de tornar a intentar el muntatge en primer pla si el primer intent de muntatge no funciona. **noacl** Inhabilita, només per aquest muntatge, el suport de la llista de control d'accés proporcionat pel sistema de fitxers de diari NFS. Quan es fa servir entre dos sistemes, NFS suporta les llistes de control d'accés. Si s'utilitza l'opció `noacl` al muntar un sistema de fitxers, NFS no utilitzarà llistes de control d'accés. L'efecte de l'opció `noacl` equival a allò que succeeix quan es munta un client NFS d'un sistema des d'un servidor NFS que no suporta llistes de control d'accés. Per obtenir més informació sobre llistes de control d'accés, consulteu "Suport de llistes de control d'accés NFS" a la pàgina 509. **retry=***n* Estableix el nombre de vegades que s'intenta realitzar el muntatge. **rsize=***n* Estableix la grandària de buffer de lectura en el número d'octets especificats per *n*. **wsize=***n* Estableix la grandària de buffer d'escriptura en el número d'octets especificats per *n*. **timeo=***n* Estableix el temps d'espera NFS en les dècimes parts d'un segon especificades per *n*. Utilitzeu aquesta variable per evitar situacions que poden succeir en xarxes en les quals la càrrega del servidor pot fer que el temps de resposta sigui inadequat. **retrans=***n* Estableix el nombre de retransmissions NFS en el nombre especificat per *n*. **port=***n* Estableix el port del servidor en el número especificat per *n*. **soft** Retorna un error si el servidor no respon. **hard** Continua intentant la sol•licitud fins que el servidor respon. **Nota:** Quan s'especifica un muntatge `hard`, és possible que el procés es bloquegi mentre s'espera una resposta. Per poder interrompre el procés i finalitzar-lo des del teclat, utilitzeu la variable `intr` en les variables de muntatge. **intr** Permet interrupcions de teclat en muntatges fixos. **ro** Estableix la variable de només de lectura.

Element	Descripció
	rw Estableix la variable de lectura-escriptura. Utilitza la variable `hard` amb aquesta variable per evitar condicions d'error que poden entrar en conflicte amb aplicacions si s'intenta realitzar el muntatge `flexible` com a lectura-escriptura. Consulteu "Resolució de problemes NFS" a la pàgina 552 per obtenir informació sobre problemes de muntatges fixos i flexibles. **secure** Especifica l'ús d'un protocol més segur per transaccions NFS. **sec** L'opció **sec** especifica la llista de valors de seguretat pel muntatge NFS. Els valors disponibles són **des**, **unix**, **sys**, **krb5**, **krb5i** i **krb5p**. Aquesta opció només s'aplica a AIX 5.3 o posterior. **actimeo=***n* Amplia el temps de llançament en *n* segons per fitxers i directoris normals. **Nota:** La memòria cau d'atributs conserva els atributs de fitxer al client. Per als atributs d'un fitxer, s'assigna un temps en el qual s'han d'eliminar. Si el fitxer es modifica abans del temps de llançament, aquest temps s'haurà ampliat des de la modificació anterior (suposant que és probable que els fitxers que s'han modificat recentment tornin a canviar aviat). Existeixen ampliacions de temps de llançament màximes i mínimes per fitxers normals i directoris. **vers** Especifica la versió NFS. El valor per defecte es la versió del protocol NFS utilitzada entre el client i el servidor i és la més elevada disponible en ambdós sistemes. Si el servidor NFS no suporta NFS Versió 3, el muntatge NFS utilitzarà NFS Versió 2. Utilitzeu l'opció **vers** per seleccionar la versió NFS. Per defecte, el muntatge NFS no utilitzarà mai NFS Versió 4 tret que s'especifiqui. **acregmin=***n* Reté atributs emmagatzemats a la memòria cau durant al menys *n* segons després de la modificació del fitxer. **acregmax=***n* Reté atributs emmagatzemats a la memòria cau durant més de *n* segons després de la modificació del fitxer. **acdirmin=***n* Reté atributs emmagatzemats a la memòria cau durant al menys *n* segons després de l'actualització de directoris. **acdirmax=***n* Reté atributs emmagatzemats a la memòria cau durant més de *n* segons després de l'actualització de directoris. **cio** Especifica el sistema de fitxers que s'ha de muntar per lectors i escriptors concurrents. L'entrada/sortida de fitxers en aquest sistema de fitxers es comportarà com si s'haguessin obert amb **O_CIO** especificat a la crida del sistema **open()**. Mitjançant aquesta opció, evitareu l'accés de qualsevol altra manera que no sigui amb CIO. És impossible utilitzar E/S emmagatzemades en memòria cau en un sistema de fitxers muntat amb l'opció **cio**. Això significa que ordres de correlació com, per exemple **mmap()** i **shmat()** fallaran amb **EINVAL** quan s'utilitzin en qualsevol fitxer d'un sistema de fitxers muntat amb l'opció **cio**. Un efecte secundari d'això es que és impossible executar binaris a partir d'un sistema de fitxers muntat amb **cio**, donat que el carregador pot utilitzar **mmap()**. **dio** Especifica que l'entrada/sortida del sistema de fitxers es comportin com si tots els fitxers s'haguessin obert amb **O_DIRECT** especificat a la crida del sistema **open()**. **Nota:** La utilització dels senyaladors **-odio** o **-ocio** pot contribuir favorablement en el rendiment de determinades càrregues de treball. No obstant això, els usuaris han de saber que el fet d'utilitzar aquests senyaladors evitarà que es dugui a terme l'emmagatzematge de fitxers d'aquests sistemes de fitxers. Donat que la lectura per avançat està inhabilitada per a aquests sistemes de fitxers, això pot reduir el rendiment per lectures seqüencials de gran capacitat.

Element	Descripció

	maxpout=*n*
	Especifica el nivell extern de pàgina per fitxers del sistema de fitxers en el qual s'ha de mantenir els fils adormits. Si s'especifica **maxpout**, també haureu d'especificar **minpout**. Aquest valor no pot ésser negatiu ni major que **minpout**. El valor per defecte és el nivell **maxpout** del kernel.
	minpout=*n*
	Especifica el nivell extern de pàgina per fitxers del sistema de fitxers en el qual s'ha de llegir els fils. Si s'especifica **minpout**, haureu d'especificar també **maxpout**. Aquest valor no pot ésser negatiu. El valor per defecte és el nivell **minpout** del kernel.
	rbr Utilitza la capacitat d'alliberar darrere mentre es llegeix. Quan es detecta la lectura seqüencial d'un fitxer en aquest sistema de fitxers, les pàgines de memòria reals utilitzades pel fitxer s'alliberen un cop que les pàgines es copien en buffers interns.
	Nota: Si no establiu les opcions següents, el kernel les establirà automàticament en els valors per defecte:
	`fg`
	`retry=10000`
	`rsize=8192`
	`wsize=8192`
	`timeo=7`
	`retrans=5`
	`port=NFS_PORT`
	`hard`
	`secure=off`
	`acregmin=3`
	`acregmax=60`
	`acdirmin=30`
	`acdirmax=60`

3. Elimineu totes les entrades de directori que no desitgeu muntar automàticament durant l'engegada del sistema.
4. Deseu i tanqueu el fitxer.
5. Executeu l'ordre **mount -a** per muntar tots els directoris especificats al fitxer `/etc/filesystems`.

Desmuntatge d'un sistema de fitxers muntat de forma explícita o automàtica

El procediment següent es pot emprar per desmuntar un directori NFS muntat de forma explícita o automàtica.

Per desmuntar un directori NFS muntat de forma explícita o automàtica, escriviu:

```
umount /directory/to/unmount
```

Eliminació de muntatges NFS predefinits

Podeu eliminar muntatges NFS predefinits mitjançant els procediments següents.

- Per eliminar un muntatge NFS predefinit a través de la SMIT:
  1. Escriviu:

     ```
     smit rmnfsmnt
     ```
- Per eliminar un muntatge NFS predefinit mitjançant l'edició del fitxer `/etc/filesystems`:
  1. Escriviu l'ordre: `umount /directory/to/unmount`.
  2. Obriu el fitxer `/etc/filesystems` amb el vostre editor preferit.
  3. Busqueu l'entrada del directori que acabeu de desmuntar i, a continuació, elimineu-la.
  4. Deseu i tanqueu el fitxer.

PC-NFS

PC-NFS és un programa per ordinadors personals que permet al ordinadors personals muntar sistemes de fitxers exportats mitjançant un sistema de fitxers de xarxa.

L'ordinador personal també pot sol•licitar adreces de xarxa i noms d'amfitrions des del servidor NFS. A més, si el servidor NFS està executant el daemon **rpc.pcnfsd**, l'ordinador personal podrà accedir a serveis d'autenticació i de enviament a cua d'impressió.

És aconsellable configurar el daemon **rpc.pcnfsd** als llocs següents:

- Sistemes que duen a terme serveis d'autenticació d'usuari
- Sistemes que ofereixen enviament a cua d'impressió
- Tots els servidors mestre i esclau del servei d'informació de la xarxa (NIS).

Nota: Donat que les xarxes NIS normalment es configuren per tal que PC-NFS puguin seleccionar qualsevol servidor NIS com a servidor per defecte, és important que tots els servidor tinguin el daemon **rpc.pcnfsd** executant-se. Si l'execució d'aquest daemon a tots els servidors NIS no és pràctica o si voleu limitar les sol•licituds a un servidor específic, afegiu una ordre **net pcnfsd** al fitxer `autoexec.bat` de cada ordinador personal per obligar-lo a utilitzar un servidor NIS específic.

Informació relacionada:

Network Information Services (NIS)

Servei d'autenticació PC-NFS

Per defecte, PC-NFS es presenta en servidors NFS com a usuari `nobody`. Amb els privilegis `nobody`, tots els fitxers d'usuari d'ordinador personals apareixen tal com n'en disposa `nobody`i, en conseqüència, no es pot distingir entre diferents usuaris d'ordinador personal.

La capacitat d'autenticació del daemon **rpc.pcnfsd** permet controlar la seguretat i els recursos del sistema reconeixent usuaris individuals i assignant-los diferents privilegis.

Amb el daemon **rpc.pcnfsd** executant-se, un usuari PC-NFS pot emetre l'ordre **net name** des d'un ordinador personal per iniciar sessió a PC-NFS de la mateixa manera que un usuari pot iniciar sessió en aquest sistema operatiu. El nom d'usuari i la paraula clau són verificats pel daemon **rpc.pcnfsd**. Aquest procediment d'autenticació no fa que un servidor sigui més segur, sinó que proporciona més control sobre l'accés als fitxers que estan disponibles a través de NFS.

Servei d'enviament a cua d'impressió PC-NFS

El servei d'enviament a cua d'impressió del daemon **rpc.pcnfsd** permet a qualsevol ordinador personal que executi PC-NFS imprimir a impressores que no estan directament connectades a l'ordinador personal.

Especificament, PC-NFS redirecciona els fitxers que en principi s'havien d'enviar a impressores d'ordinadors personals a un fitxer en un servidor NFS. Aquest fitxer es col•loca en un directori d'enviament a cua al servidor NFS. A continuació, el daemon **rpc.pcnfsd** invoca el recurs d'impressió del servidor. (El directori d'enviament a cua ha d'estar en un sistema de fitxers exportats per tal que els clients PC-NFS el puguin muntar.) Quan PC-NFS sol•licita que el daemon **rpc.pcnfsd** imprimeixi el fitxer, proporcionarà l'informació següent:

- Nom del fitxer que s'ha d'imprimir.
- ID d'inici de sessió de l'usuari al client.
- Nom de l'impressora que s'ha de fer servir.

Configuració del daemon rpc.pcnfsd

Per obtenir un rendiment òptim, configureu el daemon **rpc.pcnfsd** seguint els passos següents.

Per configurar el daemon **rpc.pcnfsd**:

1. Instal•leu el programa PC-NFS al vostre ordinador personal.
2. Seleccioneu una ubicació pel directori de cues al servidor NFS. El directori de cues per defecte és `/var/tmp`. El directori de cues ha de tenir al menys 100 kilobytes d'espai lliure.
3. Exporteu el directori de cues. No col•loqueu restriccions al directori exportat que puguin causar problemes d'accés a la xarxa. Per obtenir detalls sobre aquest procediment, consulteu "Exportació d'un sistema de fitxers NFS" a la pàgina 534.
4. Inicieu el daemon **rpc.pcnfsd** seguint les instruccions que apareixen a "Inici del daemon rpc.pcnfsd".
5. Comproveu que el daemon **rpc.pcnfsd** sigui accessible seguint les instruccions que apareixen a "Comprovació de l'accessibilitat del daemon rpc.pcnfsd".

Nota: Donat que les sol•licituds de redirecció d'impressora a vegades fan que quedin llistats de fitxers de longitud zero als directoris de cues PC-NFS, netegeu periòdicament els directoris d'enviaments a la cua d'aquestes entrades.

Inici del daemon rpc.pcnfsd

Per iniciar el daemon **rpc.pcnfsd** mitjançant el directori d'enviament a cua per defecte, utilitzeu el procediment següent.

1. Amb un editor de textos, elimineu els comentaris de l'entrada següent al fitxer `/etc/inetd.conf`:
   ```
   pcnfsd sunrpc_udp udp wait root /usr/sbin/rpc.pcnfsd pcnfsd 150001 1
   ```
2. Deseu el fitxer i sortiu de l'editor de textos.

Per iniciar el daemon **rpc.pcnfsd** mitjançant un directori que no és l'establert per defecte:

1. Utilitzeu un editor de textos per afegir l'entrada següent al fitxer `/etc/rc.nfs`:
   ```
   if [ -f /usr/sbin/rpc.pcnfsd ] ; then
   /usr/sbin/rpc.pcnfsd -s spooldir ; echo ' rpc.pcnfsd\c'
   fi
   ```

   on *spooldir* especifica el nom de camí d'accés sencer del directori d'enviament a cua.
2. Deseu el fitxer i sortiu de l'editor de textos.
3. Amb un editor de textos, comenteu l'entrada següent al fitxer `/etc/inetd.conf`:
   ```
   #pcnfsd sunrpc_udp udp wait root /usr/sbin/rpc.pcnfsd pcnfsd 150001 1
   ```

   Si col•loqueu el signe # al principi de la línia, s'evita que el daemon **inetd** iniciï el daemon **rpc.pcnfsd** mitjançant el directori d'enviament a cua per defecte.
4. Inicieu el gestor de cues d'impressió del daemon **rpc.pcnfsd** escrivint el següent a la línia d'ordres:
   ```
   /usr/sbin/rpc.pcnfsd -s spooldir
   ```

   on *spooldir* especifica el nom de camí d'accés sencer del directori d'enviament a cua.

Per obtenir més informació sobre l'actualització de la base de dades de configuració **inetd**, consulteu "Configuració del daemon inetd" a la pàgina 354.

Nota: El directori per defecte que el daemon **rpc.pcnfsd** utilitza no pot modificar-se des del fitxer `inetd.conf`.

Comprovació de l'accessibilitat del daemon rpc.pcnfsd

Seguiu el procediment següent per determinar si es pot accedir al daemon **rpc.pcnfsd**.

Per comprovar l'accessibilitat del daemon **rpc.pcnfsd**, escriviu:

```
rpcinfo -u host 150001
```

on *host* especifica el nom d'amfitrió del sistema en el qual s'està configurant **rpc.pcnfsd** i 15001 és el número de programa RPC del daemon **rpc.pcnfsd**. Un cop que hagueu introduït l'ordre, rebreu un missatge informant-vos que el programa està preparat i esperant.

Mapatges de muntatge automàtic de LDAP

Podeu configurar el subsistema de muntatge automàtic per recuperar els mapatges des d'un servidor LDAP.

Per administrar mapatges de muntatge automàtic a LDAP, afegiu la línia següent al fitxer `/etc/irs.conf`:

```
automount nis_ldap
```

Per tal d'administrar mapatges de muntatge automàtic a LDAP, haureu de crear fitxers LDIF adequats. Podeu convertir fitxers de correlació de muntatge automàtic locals en format LDIF mitjançant l'ordre **nistoldif**. Com a exemple, si el servidor LDAP s'anomena `ldapserver`, el seu sufix base serà `dc=suffix` i el fitxer de correlació `/etc/auto_home` contindrà les línies següents:

```
user1   server1:/home/user1
user2   server1:/home/user2
user3   server1:/home/user3
```

Utilizeu les ordres següents per crear un fitxer LDIF pel fitxer de correlació `/etc/auto_home` i afegiu-lo al servidor LDAP:

```
nistoldif -d dc=suffix -sa -f /etc/auto_home > /tmp/auto_home.ldif
ldapadd -D cn=admin -w passwd -h ldapserver -f /tmp/auto_home.ldif
```

Per tal d'editar o eliminar entrades de muntatge automàtic existents del servidor LDAP, caldrà crear els fitxers LDIF de forma manual. Per exemple, si el directori d'inici `user2` es troba a `server2`, caldrà crear el fitxer LDIF següent:

```
# cat /tmp/ch_user2.ldif
dn: automountKey=user2,automountMapName=auto_home,dc=suffix
changetype: modify
replace: automountInformation
automountInformation: server2:/home/user2
```

Després que hagueu creat el LDIF anterior, executeu l'ordre següent:

```
ldapmodify -D cn=admin -w passwd -h ldapserver -f /tmp/ch_user2.ldif
```

També haureu de crear un fitxer LDIF per eliminar l'usuari. Per exemple, per eliminar `user3`, creeeu el LDIF següent:

```
# cat /tmp/rm_user3.ldif
dn: automountKey=user3,automountMapName=auto_home,dc=suffix
changetype: delete
```

Després que hagueu creat el LDIF anterior, executeu l'ordre següent:

```
ldapmodify -D cn=admin -w passwd -h ldapserver -f /tmp/rm_user3.ldif
```

WebNFS

El sistema operatiu proporciona capacitat de servidor NFS per WebNFS.

Definit per Oracle, WebNFS és una extensió simple del protocol NFS que permet accedir més fàcilment a servidors i clients a través dels tallafocs d'Internet.

Un navegador web WebNFS millorat pot utilitzar l'URL per accedir a les dades directament des del servidor. Un exemple d'URL de NFS és:

```
nfs://www.YourCompany.com/
```

WebNFS funciona juntament amb els protocols basats en web existents per proporcionar dades als clients.

WebNFS també s'aprofita de l'escalabilitat del servidors NFS.

Gestor de bloqueig de la xarxa

El gestor de bloqueig de la xarxa és un recurs que funciona junt amb el sistema de fitxers de la xarxa per proporcionar un estil System V de blocatge d'enregistrament i de fitxer d'avís per la xarxa.

El gestor de bloqueig de la xarxa (**rpc.lockd**) i el monitor d'estat de la xarxa (**rpc.statd**) són daemons de servei de xarxa. El daemon **rpc.statd** és un procés de nivell d'usuari que es duu a terme mentre el daemon **rpc.lockd** s'implementa com a conjunt de fils de kernel (similars al servidor NFS). Ambdós daemons són essencials per tal que el kernel pugui proporcionar serveis de xarxa fonamentals.

Nota:

1. NFS no dóna suport a bloqueigs obligatoris ni obligats.
2. El gestor de bloqueig de la xarxa és específic de NFS versions 2 i 3.

Arquitectura del gestor de bloqueig de la xarxa

El gestor de bloqueig de la xarxa conté funcions de servidor i de client.

Les funcions de client són responsables del processament de sol•licituds des de les aplicacions i de l'enviament de sol•licituds al gestor de bloqueig de la xarxa al servidor. Les funcions del servidor són responsables d'acceptar so.licituds de bloqueig de clients i de generar les crides de bloqueig adequades en el servidor. A continuació, el servidor respondrà a la sol•licitud de bloqueig del client.

En contrast amb NFS, que no té estat, el gestor de bloqueig de la xarxa té un estat implícit. En altres paraules, el gestor de bloqueig de la xarxa ha de recordar si el client té actualment un bloqueig. El monitor d'estat de la xarxa, **rpc.statd**, implementa un protocol simple que permet al gestor de bloqueig de la xarxa supervisar l'estat d'altres màquines de la xarxa. Donat que disposa d'informació d'estat precisa, el gestor de bloqueig de la xarxa pot mantenir un estat coherent dins de l'entorn NFS sense estat.

Procés de blocatge de fitxers de xarxa

Quan una aplicació desitja obtenir un blocatge en un fitxer local, envia una sol•licitud al kernel mitjançant les subrutines **lockf**, **fcntl** o **flock**.

A continuació, el kernel processa la sol•licitud de blocatge. De tota manera, si una aplicació d'un client NFS realitza una sol•licitud de blocatge per a un fitxer remot, el client del gestor de blocatge de la xarxa genera una crida de procediment remot (RPC) al servidor per manipular la sol•licitud.

Quan el client rep una sol•licitud de blocatge remot inicial, enregistra l'interès en el servidor amb el daemon **rpc.statd** del client. El mateix s'aplica pel gestor de blocatge de la xarxa al servidor. En la sol•licitud inicial d'un client, enregistra l'interès en el client amb el monitor d'estat de la xarxa local.

Procés de recuperació de caiguda

El daemon **rpc.statd** de cada màquina notifica al daemon **rpc.statd** de la resta de màquines les seves activitats. Si el daemon **rpc.statd** rep un avís que una altra màquina s'ha bloquejat o recuperat, ho notificarà al seu daemon **rpc.lockd**.

Si un servidor cau, els clients amb els fitxers bloquejats hauran de poder recuperar-se del blocatge. Si un client cau, els seus servidors hauran de contenir els bloqueigs del client mentre es recupera. A més, per conservar la transparència general de NFS, la recuperació de caiguda haurà de produir-se sense que calgui l'intervenció de les aplicacions en sí.

El procediment de recuperació de caiguda és senzill. Si es detecta un error d'un client, el servidor alliberarà els bloqueigs del client que ha fallat suposant que l'aplicació d'aquest client tornarà a sol•licitar

els bloqueigs quan sigui necessari. Si es detecta la caiguda i la recuperació d'un servidor, el gestor de bloqueig del client tornarà a transmetre totes les sol•licituds de bloqueig otorgades anteriorment pel servidor. Aquesta informació retransmesa és utilitzada pel servidor per reconstruir el seu estat de blocatge durant un període de gràcia. (El període de gràcia, de 45 segons per defecte, és un període de temps dins del qual un servidor permet als clients reclamar els seus bloqueigs.)

El dimoni **rpc.statd** utilitza noms de sistema principal desats a `/var/statmon/sm` i `/var/statmon/sm.bak` per fer un seguiment de quins sistemes principals s'han d'informar quan la màquina hagi recuperar operacions.

Inici del gestor de bloqueig de la xarxa

Per defecte, la sèrie `/etc/rc.nfs` inicia els daemons **rpc.lockd** i **rpc.statd** junt amb altres daemons NFS.

Si NFS ja s'està executant, podeu verificar que els daemons **rpc.lockd** i **rpc.statd** s'estan executant seguint les instruccions que apareixen a "Com obtenir l'estat actual dels daemons NFS" a la pàgina 520. L'estat d'aquests dos daemons hauria de ser *actiu*. Si els daemons **rpc.lockd** i **rpc.statd** no estan actius i, per tant no s'estan executant, realitzeu el següent:

1. Mitjançant el vostre editor de textos preferit, obriu el fitxer `/etc/rc.nfs`.
2. Busqueu les línies següents:

```
if [ -x /usr/sbin/rpc.statd ]; then
              startsrc -s rpc.statd
fi
if [ -x /usr/sbin/rpc.lockd ]; then
              startsrc -s rpc.lockd
fi
```

3. Si apareix el signe # al principi de qualsevol d'aquestes línies, suprimiu el caràcter, deseu i sortiu del fitxer. A continuació, inicieu els daemons **rpc.statd** i **rpc.lockd** seguint les instruccions que apareixen a "Inici de daemons NFS" a la pàgina 519.

   Nota: La seqüència és important. Sempre inicieu el daemon **statd** en primer lloc.
4. Si NFS s'està executant i les entrades del fitxer `/etc/rc.nfs` són correctes, atureu i reinicieu els daemons **rpc.statd** i **rpc.lockd** seguint les instruccions que apareixen a "Aturada del daemons NFS" a la pàgina 519 i a "Inici de daemons NFS" a la pàgina 519.

   Nota: La seqüència és important. Sempre inicieu el daemon **statd** en primer lloc.

Si els daemons **rpc.statd** i **rpc.lockd** encara no s'estan executant, consulteu "Resolució de problemes del gestor de bloqueig de la xarxa".

Resolució de problemes del gestor de bloqueig de la xarxa

Alguns dels problemes del gestor de bloqueig de la xarxa que apareixen es poden solucionar seguint els consells següents.

Si rebeu un missatge en un client similar a:

```
clnttcp_create: RPC: Remote System error - Connection refused
rpc.statd:cannot talk to statd at {server}
```

llavors la màquina interpretarà que hi ha una altra màquina a la qual s'ha d'informar que és possible que s'hagin de prendre mesures de recuperació. Quan una màquina es reinicia o quan els dimonis **rpc.lockd** i **rpc.statd** s'aturen i es reinicien, els noms de la màquina es mouen de `/var/statmon/sm` a `/var/statmon/sm.bak` i el dimoni **rpc.statd** intenta informar a cada màquina corresponent a cada entrada de `/var/statmon/sm.bak` que es necessiten procediments de recuperació.

Si el dimoni **rpc.statd** pot arribar a la màquina, s'elimina la seva entrada a `/var/statmon/sm.bak`. Si el daemon **rpc.statd** no pot arribar a la màquina, continuarà intentant-ho a intervals regulars. Cada vegada que la màquina no pugui respondre, el temps d'espera generarà el missatge anterior. En interès de

l'integritat del blocatge, el daemon continuarà intentant-ho; de tota manera, això pot tenir un efecte contrari pel que fa al rendiment del blocatge. La manipulació es diferent, en funció de si la màquina de destinació no respon o si es troba fora de producció temporalment. Per eliminar el missatge:

1. Copmproveu que els daemons **statd** i **lockd** del servidor s'estan executant seguint les instruccions que apareixen a "Com obtenir l'estat actual dels daemons NFS" a la pàgina 520. (L'estat d'aquests dos daemons hauria de ser *actiu*.)
2. Si aquests daemons no s'estan executant, inicieu els daemons **rpc.statd** i **rpc.lockd** al servidor seguint les instruccions que apareixen a "Inici de daemons NFS" a la pàgina 519.

   Nota: La seqüència és important. Sempre inicieu el daemon **statd** en primer lloc.

   Un cop que hagueu reiniciat els daemons, recordeu-vos que existeix un període de gràcia. Durant aquest temps, els daemons **lockd** permeten reclamar sol•licituds per tal que vinguin d'altres clients que anteriorment disposaven de bloqueigs amb el servidor. D'aquesta manera, és possible que no obtingueu un bloqueig nou just després d'iniciar els daemons.

Com alternativa, elimineu el missatge fent el següent:

1. Atureu els daemons **rpc.statd** i **rpc.lockd** al client seguint les instruccions que apareixen a "Aturada del daemons NFS" a la pàgina 519.
2. Al client, elimineu l'entrada de màquina de destinació del fitxer `/var/statmon/sm.bak` especificant:

   ```
   rm /var/statmon/sm.bak/NomMàquinaDestinació
   ```

   Aquesta acció evita que la màquina de destinació detecti que probablement necessiti participar en la recuperació de blocatge. Només s'hauria de fer servir quan es pot determinar que la màquina no té cap aplicació executant-se que participi en el bloqueig de xarxa amb la màquina afectada.
3. Inicieu els daemons **rpc.statd** i **rpc.lockd** al client seguint les instruccions que apareixen a "Inici de daemons NFS" a la pàgina 519.

Si no podeu obtenir un bloqueig d'un client, realitzeu el següent:

1. Utilitzeu l'ordre **ping** per comprovar que el client i el servidor poden arribar i reconèixer-se entre sí. Si ambdues màquines s'estan executant i la xarxa està intacta, comproveu els noms de sistema principal llistats al fitxer `/var/statmon/hosts` de cada màquina. Els noms d'amfitrió han de coincidir exactament entre el servidor i el client per tal que es reconegui la màquina. Si s'utilitza un servidor de noms per a la resolució de noms de sistema principal, assegureu-vos que la informació de sistema principal és exactament igual que la que apareix al fitxer `/var/statmon/hosts`.
2. Comproveu que els daemons **rpc.lockd** i **rpc.statd** s'estan executant al client i al servidor seguint les instruccions que apareixen a "Com obtenir l'estat actual dels daemons NFS" a la pàgina 520. L'estat d'aquests dos daemons hauria de ser *actiu*.
3. Si no es troben actius, inicieu els daemons **rpc.statd** i **rpc.lockd** seguint les instruccions que apareixen a "Inici de daemons NFS" a la pàgina 519.
4. Si estan actius, és possible que hagueu de restablir-los tant als clients com als servidors. Per fer-ho, atureu totes les aplicacions que sol•licitin bloqueigs.
5. A continuació, atureu els daemons **rpc.statd** i **rpc.lockd** tant al client com al servidor seguint les instruccions que apareixen a "Aturada del daemons NFS" a la pàgina 519.
6. Ara, reinicieu els daemons **rpc.statd** i **rpc.lockd** al client seguint les instruccions que apareixen a "Inici de daemons NFS" a la pàgina 519.

   Nota: La seqüència és important. Sempre inicieu el daemon **statd** en primer lloc.

Si el procediment no soluciona el problema de bloqueig, executeu el daemon **lockd** en la modalitat de depuració fent el següent:

1. Atureu els daemons **rpc.statd** i **rpc.lockd** tant al client com al servidor seguint les instruccions que apareixen a "Aturada del daemons NFS" a la pàgina 519.

2. Inicieu el daemon **rpc.statd** al client i al servidor seguint les instruccions que apareixen a "Inici de daemons NFS" a la pàgina 519.
3. Inicieu el daemon **rpc.lockd** al client i al servidor escrivint el següent:

   ```
   /usr/sbin/rpc.lockd -d1
   ```

   Quan s'invoqui amb el senyalador **-d1**, el daemon **lockd** proporcionarà missatges de diagnòstic per syslog. Al principi, hi haurà un nombre de missatges que s'inclouran dins del període de gràcia. Espereu a què el seu temps d'espera finalitzi. Un cop el període de gràcia hagi finalitzat tant al servidor com als clients, executeu l'aplicació que té problemes de bloqueig i comproveu que la sol•licitud de bloqueig s'estigui transmetent des del client al servidor i l'inversa.

Podeu limitar l'interval de nombre de ports IP utilitzats pel client NFS per comunicar-se amb el servidor NFS establint la variable **INTERVAL_PORT_NFS** al fitxer `/var/statmon/environment`.

Intervals de port NFS

La variable d'entorn **INTERVAL_PORT_NFS** es pot utilitzar per limitar el port d'origen de les crides de xarxa que el client realitza al servidor.

Si s'utilitza, aquesta variable d'entorn ha d'afegir-se al fitxer `/etc/environment`. El format de la variable d'entorn és el següent:

```
INTERVAL_PORT_NFS=udp[4000-5000]:tcp[7000-8000]
```

En aquest exemple, els paquets UDP enviats pel client tenen un port d'origen en l'interval de 4000 a 5000 i les connexions TCP tenen un port d'origen en l'interval de 7000 a 8000.Per evitar problemes de reutilització de ports, els números de port que s'especifiquen en aquest interval no han d'utilitzar-se com a números de port fixes per cap dels dimonis del sistema de fitxers de xarxa (NFS) en el fitxer `/etc/services`.

Seguretat NFS

Es pot trobar informació sobre la seguretat NFS a diferents llocs.

El tema Seguretat del sistema de fitxers de la xarxa a *Security* explica els detalls sobre la seguretat DES. Per obtenir informació sobre la seguretat Kerberos, consulteu "Configuració d'una xarxa per RPCSEC-GSS" a la pàgina 535.

Resolució de problemes NFS

Igual que amb altres serveis de la xarxa, es poden produir problemes a màquines que utilitzen el sistema de fitxers de xarxa (NFS). La resolució d'aquests problemes implica la comprensió d'estratègies per realitzar un seguiment dels problemes NFS, el reconeixement de missatges d'error relacionats amb NFS i la selecció de les solucions adients.

Al realitzar un seguiment d'un problema NFS, aïlleu cadascun d'aquests tres punts principals d'error per determinar quin dels elements següents no està funcionant: el servidor, el client o la xarxa.

Nota: Consulteu "Resolució de problemes del gestor de bloqueig de la xarxa" a la pàgina 550 per obtenir informació sobre problemes de bloqueig de fitxers.

Problemes amb fitxers rígids i flexibles

Quan la xarxa o el servidor experimenta problemes, els errors que experimenten els programes que accedeixen a fitxers remots rígids són diferents del que s'experimenten al accedir fitxers remots flexibles.

Si un servidor no pot respondre a una sol•licitud rígida, NFS imprimirà el missatge:

```
NFS server hostname not responding, still trying
```

Els sistemes de fitxers remots rígids fan que els programes es bloquegin fins que el servidor respongui, donat que el client torna a intentar muntar la sol•licitud fins que ho aconsegueix. Utilitzeu el senyalador **-bg** amb l'ordre **mount** quan realitzeu un muntatge rígid per tal que si el servidor no respon, el client torni a intentar el muntatge en segon pla.

Si un servidor no pot respondre a una sol•licitud flexible, NFS imprimirà el missatge següent:

```
Connection  timed  out
```

Els sistemes de fitxers remots flexibles retornen un error després que s'hagi intentat el muntatge sense èxit. Malauradament, molts programes no comproven les condicions de devolució de les operacions del sistema de fitxers i, per tant, el missatge d'error no apareix quan s'accedeix als fitxers flexibles. No obstant això, aquest missatge d'error s'imprimeix a la consola.

Identificació de problemes NFS

Si us trobeu amb problemes NFS, seguiu els passos següents.

Si un client té problemes amb NFS, feu el següent:

1. Comproveu que la connexió de la xarxa sigui bona.
2. Comproveu que els daemons **inetd**, **portmap** i **biod** s'estiguin executant al client seguint les instruccions que apareixen a "Com obtenir l'estat actual dels daemons NFS" a la pàgina 520.
3. Comproveu que existeix un punt de muntatge vàlid per al sistema de fitxers que s'està muntant. Per obtenir més informació, consulteu l'apartat "Configuració d'un client NFS" a la pàgina 533.
4. Comproveu que el servidor està actiu i executant-se mitjançant l'execució de l'ordre següent a l'indicador de l'intèrpret d'ordres del client:

   ```
   /usr/bin/rpcinfo  -p  nom_servidor
   ```

   Si el servidor està actiu, s'imprimirà una llista de programes, versions, protocols i números de port semblant a la següent:

   ```
   program    vers  proto      port
   100000        2      tcp       111    portmapper
   100000        2      udp       111    portmapper
   100005        1      udp      1025    mountd
   100001        1      udp      1030    rstatd
   100001        2      udp      1030    rstatd
   100001        3      udp      1030    rstatd
   100002        1      udp      1036    rusersd
   100002        2      udp      1036    rusersd
   100008        1      udp      1040    walld
   100012        1      udp      1043    sprayd
   100005        1      tcp       694    mountd
   100003        2      udp      2049    nfs
   100024        1      udp       713    status
   100024        1      tcp       715    status
   100021        1      tcp       716    nlockmgr
   100021        1      udp       718    nlockmgr
   100021        3      tcp       721    nlockmgr
   100021        3      udp       723    nlockmgr
   100020        1      udp       726    llockmgr
   100020        1      tcp       728    llockmgr
   100021        2      tcp       731    nlockmgr
   ```

   Si no es retorna una resposta semblant, inicieu sessió al servidor a la consola del servidor i comproveu l'estat del daemon **inetd** seguint les instruccions que apareixen a "Com obtenir l'estat actual dels daemons NFS" a la pàgina 520.
5. Comproveu que els daemons **mountd**, **portmap** i **nfsd** s'estan executant al servidor NFS entrant les ordres següents a l'indicador de l'intèrpret d'ordres del client:

```
/usr/bin/rpcinfo  -u  nom_servidor  mount
/usr/bin/rpcinfo  -u  nom_servidor  portmap
/usr/bin/rpcinfo  -u  nom_servidor  nfs
```

Si els daemons s'estan executant al servidor, es retornaran les respostes següents:

```
program  100005  version  1  ready  and  waiting
program  100000  version  2  ready  and  waiting
program  100003  version  2  ready  and  waiting
```

Els números de programa corresponen amb les ordres, respectivament, tal com es mostra a l'exemple anterior. Si no es retorna una resposta semblant, inicieu sessió al servidor a la consola del servidor i comproveu l'estat dels daemons seguint les instruccions que apareixen a "Com obtenir l'estat actual dels daemons NFS" a la pàgina 520.

6. Comproveu que el fitxer `/etc/exports` del servidor inclou a la llista el nom del sistema de fitxers que el client desitja muntar i que el sistema de fitxers s'ha exportat. Per fer-ho, escriviu l'ordre següent:

   ```
   showmount -e nom_servidor
   ```

   Aquesta ordre llista tots els sistemes de fitxers exportats per *nom_servidor*.
7. En el cas de NFS versió 4, comproveu que el domini NFSv4 s'hagi configurat correctament.
8. En el cas de NFS versió 4, comproveu que el daemon **nfsrgyd** s'estigui executant.
9. Si utilitzeu seguretat ampliada, consulteu "Determinació de problemes de RPCSEC-GSS" a la pàgina 560.

Errors d'escriptura asíncrons

Quan un programa d'aplicació escriu dades en un fitxer d'un sistema de fitxers muntat per NFS, l'operació d'escriptura es programa pel processament asíncron mitjançant el daemon **biod**.

Si es produeix un error al servidor NFS al mateix temps que les dades s'escriuen al disc, l'error es retornarà al client NFS i el daemon **biod** desarà l'error internament a les estructures de dades NFS. Més endavant, l'error emmagatzemat es retorna al programa d'aplicació la propera vegada que cridi les funcions **fsync** o **close**. Com a conseqüència d'aquests errors, no s'informa a l'aplicació sobre l'error d'escriptura fins que el programa tanca el fitxer. Un exemple típic d'aquest cas és quan un sistema de fitxer del servidor està ple i això fa que els intents d'escriptura del client no es realitzin correctament.

Missatge d'error nfs_server

Quan el buffer de transmissió és massa petit, es retorna un missatge d'error.

Si no existeixen suficients buffers de transmissió a la xarxa, és possible que aparegui el missatge d'error següent:

```
nfs_server:  bad  sendreply
```

Per augmentar els buffers de transmissió, utilitzeu el camí d'accés ràpid de la System Management Interface Tool (SMIT), `smit commodev`. A continuació, seleccioneu el tipus d'adaptador i augmenteu el nombre de buffers de transmissió.

Missatges d'error de muntatge

Un procés de muntatge remot pot fallar de diverses maneres. Els missatges d'error associats amb errors de muntatge es descriuen en aquest apartat.

mount: ... already mounted
: El sistema de fitxers que està intentant muntar ja està muntat.

muntar: ... no trobat a /etc/filesystems
: No és possible trobar una correspondència amb el sistema de fitxers o el nom de directori especificat.

Si emeteu l'ordre **mount** amb un nom de directori o de sistema de fitxers però no ambdós, l'ordre buscarà al fitxer `/etc/filesystems` una entrada el camp de directori o de sistema de fitxers de la qual coincideixi amb l'argument. Si l'ordre **mount** troba una entrada com la següent:

```
/dancer.src:
          dev=/usr/src
          nodename  =  d61server
          type  =  nfs
          mount  =  false
```

llavors realitzarà el muntatge com si haguéssiu introduït el següent a la línia d'ordres:

```
/usr/sbin/mount -n dancer -o rw,hard /usr/src /dancer.src
```

... no trobat a la base de dades d'hosts

En una xarxa sense el servei d'informació de la xarxa, aquest missatge indica que l'amfitrió especificat a l'ordre **mount** no es troba al fitxer `/etc/hosts`. A una xarxa que executa NIS, el missatge indica que NIS no ha pogut trobar el nom de l'amfitrió a la base de dades `/etc/hosts` o que el daemon **ypbind** de NIS de la màquina ja no existeix. Si el fitxer `/etc/resolv.conf` existeix per tal que el servidor del nom es faci servir per la resolució de noms d'amfitrió, és possible que hi hagi un problema a la base de dades **named**. Consulteu el "Resolució de noms de l'amfitrió en un servidor NFS" a la pàgina 559.

Comproveu l'ortografia i la sintaxi de l'ordre **mount**. Si l'ordre és correcta, la xarxa no executarà NIS i només apareixerà aquest missatge per aquest nom d'amfitrió. Comproveu l'entrada al fitxer `/etc/hosts`.

Si la xarxa està executant NIS, assegureu-vos que el daemon **ypbind** s'està executant introduint el següent a la línia d'ordres:

```
ps  -ef
```

El daemon **ypbind** hauria d'aparèixer a la llista. Intenteu utilitzar l'ordre **rlogin** per iniciar sessió de forma remota a una altra màquina o utilitzeu l'ordre **rcp** per copiar de forma remota quelcom a una altra màquina. Si això també falla, és probable que el daemon **ypbind** s'hagi aturat o bloquejat.

Si només apareix aquest missatge per aquest nom d'amfitrió, comproveu l'entrada `/etc/hosts` al servidor NIS.

mount: ... server not responding: port mapper failure - RPC timed out

El servidor des del qual esteu intentant realitzar el muntatge està desconnectat o el seu correlacionador de ports està aturat o bloquejat. Intenteu reiniciar el servidor per activar els daemons **inetd**, **portmap** i **ypbind**.

Si no podeu iniciar sessió al servidor de forma remota amb l'ordre **rlogin** i el servidor està connectat, comproveu la connexió de xarxa intentant iniciar sessió de forma remota en una altra màquina. Comproveu també la connexió de la xarxa del servidor.

mount: ... server not responding: program not registered

Això significa que l'ordre **mount** ha travessat el correlacionador de ports. Tanmateix, el daemon de muntatge NFS **rpc.mountd** no s'ha enregistrat.

mount: access denied ...

El nom de la màquina no es troba a la llista d'exportació del sistema de fitxers que esteu intentant muntar des del servidor.

Podeu obtenir una llista del sistemes de fitxers exportats de servidor executant l'ordre següent a la línia d'ordres:

```
showmount  -e  hostname
```

Si el sistema de fitxers que desitgeu no es troba a la llista o el nom de la màquina o del grup de xarxes no es troba a la llista d'usuaris del sistema de fitxers, inicieu sessió al servidor i comproveu que el fitxer `/etc/exports` conté l'entrada del sistema de fitxers correcta. Un nom de sistema de fitxers que apareix al fitxer `/etc/exports` però no a la sortida a partir de l'ordre

showmount, indica un error al daemon **mountd**. És possible que el daemon no pogués analitzar aquesta línia al fitxer, no podia trobar el directori, o que el nom del directori no es tractés d'un directori muntat de forma local. Si el fitxer `/etc/exports` sembla correcte i la xarxa executa NIS, comproveu el daemon **ypbind** al servidor. És possible que s'hagi aturat o bloquejat.

mount: ...: Permission denied
Aquest missatge és una indicació genèrica que una part de l'autenticació ha fallat al servidor. Podria ser que, a l'exemple anterior, no us trobéssiu a la llista d'exportació, el servidor no reconegués el daemon **ypbind** de la màquina o que el servidor no acceptés l'identitat que heu proporcionat.

Comproveu el fitxer `/etc/exports` al servidor i, si convé, el daemon **ypbind**. En aquest cas, només cal que canvieu el nom d'amfitrió per l'ordre **hostname** i torneu a intentar l'ordre **mount**.

mount: ...: Not a directory
El camí d'accés remot o local no és un directori. Comproveu l'ortografia de l'ordre i intenteu executar-la a ambdós directoris.

mount: ...: You are not allowed
Heu de comptar amb autorització root o ser membre del grup de sistemes per executar l'ordre **mount** a la màquina perquè això afecta al sistema de fitxers de tots els usuaris de la màquina en qüestió. Els muntatges i els desmuntatges NFS només els poden realitzar membres i usuaris root del grup de sistemes.

Informació relacionada:

Network Information Services (NIS)

Causes de temps d'accés lents per NFS

Si l'accés als fitxers remots sembla que es produeixi de forma lenta, assegureu-vos que el temps d'accés no està afectat per un daemon runaway, una línia **tty** o un problema similar.

Connexions de xarxa:

Utilitzeu l'ordre **nfsstat** per recopilar informació sobre les connexions de xarxa.

L'ordre **nfsstat** determina si es deixaran anar paquets. Utilitzeu les ordres **nfsstat -c** i **nfsstat -s** per determinar si el client o el servidor estan restransmetent grans bloqueigs. Les retransmissions sempre són una possibilitat degut a que es perden paquets o que els servidors estan ocupats. Un índex de retransmissió del cinc per cent o més es considera elevat.

La probabilitat de retransmissions es pot reduir canviant els paràmetres de cua de transmissió de l'adaptador de comunicació. La SMIT es pot fer servir per canviar aquests paràmetres. Per obtenir més informació, consulteu Available system management interfaces a *Operating system and device management*.

Es recomana utilitzar els valors següents pels servidors NFS.

Nota:

1. Apliqueu aquests valors a clients NFS si les retransmissions continuen.
2. Tots els nodes d'una xarxa han d'utilitzar la mateixa grandària de MTU.

Taula 91. L'unitat de transmissió màxima i les grandàries de cua de transmissió de l'adaptador de comunicació

Adaptador	MTU	Cua de transmissió
Token Ring		
4 Mb	1500 3900	50 40 (augmenteu si finalitza el temps d'espera de l'ordre **nfsstat**.)
16 Mb	1500 8500	40 (augmenteu si finalitza el temps d'espera de l'ordre **nfsstat**.) 40 (augmenteu si finalitza el temps d'espera de l'ordre **nfsstat**.)
Ethernet	1500	40 (augmenteu si finalitza el temps d'espera de l'ordre **nfsstat**.)

Les grandàries de la MTU més grans de la velocitat de cada token ring redueixen l'ús de processador i milloren significativament les operacions de lectura/escriptura.

Configuració de grandàries de la MTU:

Per establir la grandària de la MTU, utilitzeu el camí d'accés ràpid de la SMIT `smit chif`.

Seleccioneu l'adaptador adequat i escriviu un valor MTU al camp de grandària màxima de paquet IP.

L'ordre **ifconfig** es pot utilitzar per establir la grandària de la MTU (i *és obligatori* fer-la servir per establir la grandària de la MTU a 8500). El format de l'ordre **ifconfig** és:

```
ifconfig trn NomNode up mtu GrandàriaMTU
```

on `trn` és el nom de l'adaptador, per exemple, `tr0`.

Un altre mètode d'establir grandàries de la MTU combina l'ordre **ifconfig** amb la SMIT.

1. Afegiu l'ordre **ifconfig** per les opcions de menú Token Ring, tal com es mostra en l'exemple anterior, al fitxer `/etc/rc.bsdnet`.
2. Especifiqueu el camí d'accés ràpid `smit setbootup_option`. Commuteu el camp **Utilitzar estil BSD** a **yes**.

Grandàries de cua de transmissió:

Les grandàries de cua de transmissió de l'adaptador de comunicació s'estableixen amb la SMIT.

Escriviu el camí d'accés ràpida `smit chgtok`, seleccioneu l'adaptador adequat i escriviu la grandària de cua al camp de transmissió.

Bloqueig de programes:

Si els programes es bloquegen mentre es realitza una tasca relacionada amb fitxers, és possible que el servidor NFS s'hagi aturat.

En aquest cas, és possible que aparegui el missatge d'error següent:

```
NFS server hostname not responding, still trying
```

The NFS server (*hostname*) is down. Això indica que existeix un problema amb el servidor, la connexió de xarxa o amb el servidor NIS.

Comproveu els servidors des dels quals heu muntat els sistemes de fitxers en el cas que la vostra màquina s'hagi bloquejat completament. Si un o varis servidors estan desconnectats, no us preocupeu. Quan el servidor es torni a connectar, els programes continuaran automàticament. No es destrueix cap fitxer.

Si un servidor muntat de forma flexible deixa de funcionar, la resta de tasques no es veuran afectades. El temps d'espera dels programes que hagi finalitzat en intentar accedir a fitxers remots muntats de forma flexible, no funcionaran correctament amb el missatge `errno`. De tota manera, encara podreu accedir a altres sistemes de fitxers.

Si s'estan executant tots els servidors, determineu si altres usuaris que estan utilitzant els mateixos servidors estan tenint problemes. Si més d'una màquina experimenta problemes de servei, això significarà que existeix un problema amb els daemons **nfsd** al servidor. En aquest cas, inicieu sessió al servidor i executeu l'ordre **ps** per veure si el daemon **nfsd** s'està executant i si està acumulant temps d'UCP. En cas contrari, és possible que podeu aturar el daemon **nfsd** i, a continuació, reiniciar-lo. Si això no funciona, haureu de reiniciar el servidor.

Comproveu la connexió de la xarxa i la connexió del servidor si sembla que la resta de sistemes estan connectats i funcionen.

Esquemes de permisos i d'autenticació:

De vegades, un cop els muntatges s'han establert correctament, existeixen problemes a l'hora de llegir, escriure o crear fitxers o directoris remots. Aquestes dificultats solen succeir per causa de problemes de permisos o d'autenticació.

Els problemes de permisos i d'autenticació poden variar pel que fa a la seva causa en funció de si NIS s'està utilitzant i si s'estan especificant muntatges segurs.

El cas més simple succeeix quan els muntatges que s'especifiquen no són segurs i quan el NIS no s'està utilitzant. En aquest cas, els ID d'usuari (UID) i els ID de grup (GID) només es correlacionen a través del fitxer `/etc/passwd` del servidor i del fitxer `/etc/group` del client. En aquest esquema, per tal que l'usuari anomenat `B` s'identifiqui al client i al servidor com a `B`, l'usuari `B` haurà de tenir el mateix número UID al fitxer `/etc/passwd`. A continuació, es mostra un exemple de com això pot causar problemes:

```
User  B  is  uid  200  on  client  foo.
User  B  is  uid  250  on  server  bar.
User  G  is  uid  200  on  server  bar.
```

El directori `/home/bar` es munta des del servidor `bar` al client `foo`. Si l'usuari `B` està editant fitxers al sistema de fitxers remots `/home/bar` en el client `foo`, es confondrà a l'hora de desar fitxers.

El servidor `bar` creu que els fitxers pertanyen a `user G`, perquè `G` és UID `200` a `bar`. Si `B` inicia sessió directament a `bar` mitjançant l'ordre **rlogin**, és possible que no pugui accedir als fitxers que acaba de crear mentre treballava al sistema de fitxers muntats de forma remota. No obstant això, `G`, pot fer-ho perquè les màquines assignen permisos de forma arbitrària segons UID, no segons nom.

La única solució definitiva per això es reassignar UID coherents a les dues màquines. Per exemple, assigneu `B` UID 200 al servidor `bar` o 250 al client `foo`. Per als fitxers que són propietat de `B` s'hauria d'executar l'ordre **chown** per tal que coincidissin amb el nou ID de la màquina adequada.

Degut als problemes amb el manteniment de mapatges UID i GID coherents a totes les màquines de la xarxa, sovint s'utilitza NIS per realitzar els mapatges adequades per tal d'evitar aquest tipus de problema.

Resolució de noms de l'amfitrió en un servidor NFS:

Quan un servidor NFS ofereix serveis a una sol•licitud de muntatge, busca el nom del client que realitza la sol•licitud. El servidor utilitza l'adreça IP del client i busca el nom d'amfitrió corresponent que coincideix amb l'adreça.

Un cop s'ha trobat el nom d'amfitrió, el servidor busca el directori sol•licitat a la llista d'exportacions i comprova l'existència del nom del client a la llista d'accés del directori. Si existeix una entrada pel client i aquesta coincideix exactament amb l'entrada que s'ha retornat per la resolució de noms, llavors es passa aquesta part de l'autenticació del muntatge.

Si el servidor no pot realitzar la resolució d'adreça IP a nom d'amfitrió, el servidor denegarà la sol•licitud de muntatge. El servidor ha de poder trobar alguna correspondència per l'adreça IP del client en realitzar la sol•licitud de muntatge. Si el directori s'exporta amb l'accés habilitat per a tots els clients, el servidor continuarà podent realitzar la cerca de noms invertits per permetre la sol•licitud de muntatge.

El servidor també ha de poder buscar el nom correcte del client. Per exemple, si existeix una entrada al fitxer `/etc/exports` com la següent:

```
/tmp      -access=silly:funny
```

al fitxer `/etc/hosts` existiran les entrades corresponents següents:

```
150.102.23.21        silly.domain.name.com
150.102.23.52        funny.domain.name.com
```

Tingueu en compte que els noms no coincideixen exactament. Quan el servidor busca correspondències d'adreça IP i nom d'amfitrió dels amfitrions `silly` i `funny`, els noms de sèrie no coincideixen exactament amb les entrades de la llista d'accés de l'exportació. Aquest tipus de problema de resolució de noms normalment succeeix quan s'utilitza el daemon **named** per la resolució de noms. La majoria de les bases de dades de daemon **named** tenen àlies pels noms de domini complets dels amfitrions per tal que els usuaris no tinguin que especificar noms sencers a l'hora de fer referència a amfitrions. Encara que aquestes entrades de nom d'amfitrió a adreça IP existeixen per a tots els àlies, és possible que la cerca inversa no existeixi. La base de dades per la cerca de noms de dominis invertida (d'adreça IP a nom d'amfitrió) normalment té entrades que contenen l'adreça IP i el nom de domini complet (no l'àlies) de l'amfitrió en qüestió. De vegades, les entrades d'exportació es creen amb un àlies més breu, amb la qual cosa es creen problemes quan els clients intenten realitzar un muntatge.

Limitacions sobre el nombre de grups dins de l'estructura NFS:

En sistemes que utilitzen NFS versió 2 o 3, els usuaris no poden ser membres de més de 16 grups sense complicacions.

Els grups es defineixen mitjançant l'ordre **groups**. Si un usuari forma part de 17 grups o més i intenta accedir a fitxers que són propietat del dissetè grup (o un grup més gran), el sistema no deixarà que es llegeixi ni es copiï el fitxer. Per permetre que l'usuari accedeixi als fitxers, torneu a ordenar els grups.

La informació anterior descriu un comportament per defecte. Vegeu el paràmetre **maxgroups** de l'ordre **mount** per obtenir més detalls.

Servidors NFS amb versions anteriors de NFS:

Un client de NFS Versió 3 no pot muntar-se en un servidor NFS Versió 4.

En muntar un sistema de fitxers des de un servidor NFS amb una versió anterior a la versió 3 en un client NFS de versió 3, succeirà un problema si l'usuari del client que executa el muntatge forma part de més de vuit grups. Alguns servidors no poden gestionar correctament aquesta situació i deneguen la

sol•licitud pel muntatge. La solució és canviar la pertinença al grup de l'usuari per un nombre inferior a vuit i, a continuació, torna a intentar el muntatge. El missatge d'error següent és característic d'aquest problema de grup:

```
RPC:    Authentication  error;  why=Invalid  client  credential
```

Determinació de problemes de RPCSEC-GSS:

Considereu les instruccions següents si teniu problemes amb RPCSEC-GSS.

- Utilitzeu l'ordre **klist** del client per assegurar-vos que les vostres credencials són vàlides i actuals.
- Assegureu-vos que els rellotges del client, del servidor i de KDC estan sincronitzats. Es recomana utilitzar NTP o una configuració equivalent per garantir que l'hora és coherent en tot el domini de Kerberos.
- Assegureu-vos que el servidor té un fitxer `keytab` vàlid i un principal d'amfitrió. Si l'ordre següent falla, el servidor no funcionarà:

  ```
  kinit -kt 'tail -n 1 /etc/nfs/hostkey' 'head -n 1 /etc/nfs/hostkey'
  ```

- Assegureu-vos que el daemon **gssd** s'està executant i que respon al client i al servidor amb l'ordre següent:

  ```
  rpcinfo -u localhost 400234
  ```

  Si el daemon **gssd** no respon, RPCSEC-GSS fallarà. Per corregir aquest problema, atureu i reinicieu el daemon **gssd**.
- Si rebeu errors d'escriptura amb integritat o privacitat, assegureu-vos que esteu utilitzant la modalitat de kernel. L'integritat i la privacitat no estan suportades sense el mòdul del kernel. (El mòdul del kernel és el mòdul de kernel de Kerberos `/usr/lib/drivers/nfs.ext`. S'instal•la amb el fitxer `modcrypt.base` establert des del paquet d'extensió.)
- Si usuaris específics reben denegacions al accedir a les dades a les que haurien de poder accedir, verifiqueu que els principals implicats a KDC estan sincronitzats correctament amb el nom de compte d'AIX de l'usuari.
- Activeu el enregistrament del sistema. La majoria dels errors RPCSEC-GSS s'enregistraran. Els errors tenen dues parts: la primera és el codi d'error GSS (consulteu RFC 2744 per obtenir informació detallada al respecte) i la segona es un codi d'error kerberos.

  Nota: L'activació de l'enregistrament del sistema pot afectar al rendiment del sistema i, per tant, el enregistrament s'hauria de desactivar després que s'hagi completat la determinació de problemes.
  A continuació, es presenten alguns codis d'error comuns i les seves solucions:

  KRB5_CC_NOTFOUND
  No s'han pogut trobar credencials kerberos vàlides. L'ordre **kinit** pot corregir aquest problema.

  KRB5_KDC_UNREACH
  No es pot arribar a KDC. Assegureu-vos que KDC funciona i que no existeixen problemes de xarxa entre el client o el servidor i KDC.

  KRB5_KT_NOTFOUND
  No s'ha trobat l'entrada `keytab` del principal del servidor. Utilitzeu l'ordre **nfshostkey -l** per assegurar-vos que esteu utilitzant el principal correcte (hauria de ser `nfs/<nom de domini completament qualificat>`) i el fitxer `keytab`. Utilitzeu **klist -ke** per comprovar que el fitxer `keytab` del servidor té l'entrada adient.

  KRB5KRB_AP_ERR_TKT_NYV
  El més probable és que indiqui un problema amb el rellotge.

  KRB5KRB_AP_WRONG_PRINC i KRB5KDC_ERR_S_PRINCIPAL_UNKNOWN
  Ambdós errors indiquen que el principal que utilitza el client pel client no coincideix amb el principal de l'amfitrió del servidor.

KRB5KRB_AP_WRONG_PRINC
Indica que el client ha resolt correctament el nom d'amfitrió del servidor en un principal existent amb el format nfs/<*nom de domini completament qualificat*> però el principal de l'amfitrió del servidor no coincideix amb aquest principal.

KRB5KDC_ERR_S_PRINCIPAL_UNKNOWN
Indica que el client no ha pogut resoldre el nom d'amfitrió del servidor en un principal existent. Utilitzeu l'ordre **nfshostkey -l** per comprovar el servidor i assegurar-vos que té el principal correcte. En cas afirmatiu, és probable que s'hagi d'actualitzar la taula de correlació d'amfitrió del client. Consulteu l'ordre **nfshostmap** a *Commands Reference, Volume 4* per obtenir més informació detallada al respecte.

Determinació de problemes d'EIM:

Al solucionar problemes EIM, tingueu en compte els consells següents.

Tingueu en compte el següent quan tingueu problemes amb EIM:

- Si les ordres **nfsrgyd** o **chnfsim** no poden connectar-se amb el servidor LDAP d'EIM, assegureu-vos que el procés **ibmslapd** s'està executant al servidor LDAP d'EIM escrivint l'ordres següent:
  ```
  ps -ef | grep ibmslapd
  ```
  Si el procés **ibmslapd** no s'està executant, escriviu l'ordre següent per activar-lo:
  ```
  /usr/sbin/ibmslapd
  ```
- Si les ordres **nfsrgyd** o **chnfsim** poden connectar-se amb el servidor LDAP d'EIM però no poden realitzar cap de les operacions de correlació d'entitat, assegureu-vos que el procés **ibmslapd** no s'està executant en la modalitat de només configuració. Això pot succeir si la base de dades **ldapdb2** no s'està executant quan s'inicia el servidor **ibmslapd**. Seguiu els passos següents:
  1. Inicieu sessió en el servidor LDAP d'EIM com a usuari root.
  2. Vegeu el fitxer /var/ldap/ibmslapd.log. Comproveu quan s'ha iniciat el procés **ibmslapd** per última vegada. Comproveu també si el servidor s'ha iniciat en la modalitat de només configuració perquè no es podia connectar amb la base de dades **ldapdb2**.

  Si el servidor no s'ha pogut connectar amb la base de dades **ldapdb2**, caldrà iniciar-la. Seguiu els passos següents per iniciar la base de dades **ldapdb2**:
  1. Inicieu sessió al servidor LDAP d'EIM com a usuari root.
  2. Escriviu l'ordre següent per comprovar si el procés **ibmslapd** està actiu:
     ```
     ps -ef | grep ibmslapd
     ```
     Si està actiu, inhabiliteu-lo executant l'ordre següent:
     ```
     kill ibmslapd pid
     ```
     on *pid* és l'ID de procés que s'ha retornat de l'ordre **ps -ef**.
  3. Un cop que el procés **ibmslapd** s'hagi inhabilitat, inicieu la base de dades **ldapdb2**:
     a. Inicieu sessió al servidor LDAP d'EIM com a usuari **ldapdb2**.
     b. Escriviu db2start.
  4. Un cop que inicieu la base de dades **ldapdb2**, activeu el procés **ibmslapd**:
     a. Inicieu sessió en el servidor LDAP d'EIM com a usuari root.
     b. Escriviu ibmslapd.

Problemes que succeeixen si no es carrega l'extensió del kernel NFS:

Algunes ordres NFS no s'executen correctament si no es carrega l'extensió del kernel NFS. Algunes ordres amb aquesta dependència són: **nfsstat**, **exportfs**, **mountd**, **nfsd** i **biod**.

Quan s'instal•la NFS al sistema, l'extensió del kernel es col•loca al fitxer /usr/lib/drivers/nfs.ext. A continuació, aquest fitxer es carrega com a extensió de kernel NFS quan es configura el sistema. La seqüència que realitza l'extensió d'aquest kernel carrega el fitxer /etc/rc.net. Es realitzen altres procediments en aquesta seqüència, una de les quals és la càrrega de l'extensió de kernel NFS. És important tenir en compte que l'extensió del kernel de **Transmission Control Protocol/Internet Protocol (TCP/IP)** i el fitxer **nfs_kdes_null.ext** s'haurien de carregar abans que es carregui l'extensió de kernel NFS.

Nota: L'ordre **gfsinstall** s'utilitza per carregar l'extensió de kernel NFS al kernel quan el sistema s'acaba d'iniciar. Aquesta ordre es pot executar més d'un cop per engegada del sistema i no causarà cap problema. El sistema s'entrega actualment amb l'ordre **gfsinstall** que s'utilitza als fitxers /etc/rc.net i /etc/rc.nfs. No hi ha cap necessitat d'eliminar cap d'aquestes crides.

Problemes que succeeixen si el suport de Kerberos no està instal•lat.:

Si el suport de Kerberos no està instal•lat, el daemon **gssd** no s'iniciarà.

Assegureu-vos que els catàlegs de fitxers krb5.client.rte i modcrypt.base estan instal•lats. Si cap dels dos està instal•lat, no s'executarà el daemon **gssd**.

Elements que s'ha de comprovar si el daemon d'enregistrament no s'està executant:

El daemon **nfsrgyd** no s'executarà si el domini de NFS versió 4 no s'ha configurat.

Per obtenir informació sobre la configuració del domini NFS versió 4, consulteu “Fitxer /etc/nfs/local_domain” a la pàgina 516.

Fitxers NFS

Aquí es pot trobar una referència als fitxers NFS i a les seves descripcions.

Element	Descripció
bootparams	Llista els clients que els clients sense disc poden fer servir per arrencar.
exports	Llista els directoris que es poden exportar a clients NFS.
filesystems	Llista tots els sistemes de fitxers que es munten al reinici del sistema.
hostkey	Especifica el principal d'amfitrió Kerberos i l'ubicació del fitxer keytab.
local_domain	Conté el domini NFS local del sistema.
networks	Conté informació sobre les xarxes de la xarxa d'Internet.
pcnfsd.conf	Proporciona opcions de configuració pel daemon **rpc.pcnfsd**.
princmap	Mapa noms d'amfitrió amb principals Kerberos quan el principal no és el nom de domini completament qualificat del servidor.
realm.map	Utilitzat pel daemon d'enregistrament NFS per mapar principals Kerberos d'entrada.
rpc	Conté informació de base de dades per programes de crida de procediment remot.
security_default	Conté valors per defecte de seguretat NFS.
xtab	Llista directoris que actualment estan exportats.

Ordres NFS

A continuació, es pot trobar una referència a les ordres NFS i les seves descripcions.

Element	Descripció
chnfs	Inicia un nombre específic de daemons **biod** i **nfsd**.
chnfsdom	Canvia el domini NFS local.
chnfsim	Canvia els mapatges d'identitat externes de NFS.
chnfssec	Canvia el valor de seguretat per defecte utilitzar pel client NFS.
chnfsrtd	Canvia els mapatges de domini a domini NFS locals.
mknfs	Configura el sistema per tal que executi NFS i inicia damenos NFS.
nfso	Configura les opcions de xarxa NFS.
automount	Munta un sistema de fitxers NFS de forma automàtica.
chnfsexp	Canvia els atributs d'un directori exportat per NFS.
chnfsmnt	Canvia els atributs d'un directori muntat per NFS.
exportfs	Exporta i cancel•la l'exportació de directoris a clients NFS.
lsnfsexp	Visualitza les característiques dels directoris que s'exporten amb NFS.
lsnfsmnt	Visualitza les característiques dels sistemes NFS muntats.
mknfsexp	Exporta un directori mitjançant NFS.
mknfsmnt	Munta un directori mitjançant NFS.
nfshostkey	Configura la clau d'amfitrió per a un servidor NFS.
nfs4cl	Visualitza informació sobre sistemes de fitxers a la qual un client està accedint mitjançant NFS versió 4.
nfs4smctl	Administra la revocació de l'estat de NFS versió 4.
rmnfs	Atura els daemons NFS.
rmnfsexp	Elimina els directoris exportats per NFS des d'una llista d'exportacions de servidor.
rmnfsmnt	Elimina sistemes de fitxers muntats per NFS des d'una llista de muntatges de client.

Daemons NFS

A continuació, es pot trobar una referència als daemons NFS i les seves descripcions.

Bloqueig de daemons

Element	Descripció
lockd	Processa les sol•licituds de bloqueig pel paquet RPC.
statd	Proporciona funcions de caiguda i recuperació pels serveis de bloqueig a NFS.

Daemons i programes d'utilitat de servei de xarxa

Element	Descripció
biod	Envia les sol•licituds de lectura i escriptura del client al servidor.
mountd	Respon a les sol•licituds de clients dels muntatges del sistema de fitxers.
nfsrgyd	Realitza conversions entre principals de seguretat, sèries d'identitats de NFS versió 4 i els seus ID de sistema numèrics corresponents. A més, es proporciona la correlació d'informació d'entitats de dominis NFS versió 4 externs.
nfsd	Inicia els daemons que manipulen les sol•licituds de client per a operacions del sistema de fitxers.
nfsstat	Visualitza informació sobre la capacitat de recuperar crides per a una màquina determinada.
on	Executa ordres en màquines remotes.
pcnfsd	Manipula sol•licituds de servei de clients PC-NFS.
portmap	Mapa números de programa RPC amb números de port d'Internet.
rexd	Accepta sol•licituds per executar programes des de màquines remotes.
rpcgen	Genera codi C per implementar un protocol RPC.
rpcinfo	Informa sobre l'estat dels servidors RPC.
rstatd	Retorna estadístiques de rendiment obtingudes del kernel.
rup	Mostra l'estat d'un amfitrió remot a la xarxa local.
rusers	Informa sobre una llista d'usuaris connectats a les màquines remotes.
rusersd	Respon a les consultes de l'ordre **rusers**.
rwall	Envia missatges a tots els usuaris de la xarxa.
rwalld	Manipula les sol•licituds de l'ordre **rwall**.
showmount	Visualitza una llista de tots els clients que han muntat sistemes de fitxers remots.
spray	Envia un número específic de paquets a un amfitrió.
sprayd	Rep paquets enviats per l'ordre **spray**.

Daemons i programes d'utilitat de xarxa segurs

Element	Descripció
chkey	Canvia la clau d'encriptació de l'usuari.
gssd	Proporciona NFS amb accés a serveis de seguretat proporcionats per serveis d'autenticació de xarxa.
keyenvoy	Proporciona un intermediari entre processos d'usuari i el servidor clau.
keylogin	Desencripta i emmagatzema la clau secreta de l'usuari.
keyserv	Emmagatzema claus públiques i privades.
mkkeyserv	Inicia el daemon **keyserv** i elimina els comentaris de les entrades adequades del fitxer `/etc/rc.nfs`.
newkey	Crea una clau nova al fitxer `publickey`.
rmkeyserv	Atura el daemon **keyserv** i comenta l'entrada del daemon **keyserv** al fitxer `/etc/rc.nfs`.
ypupdated	Actualitza l'informació dels mapatges del servei d'informació de la xarxa (NIS).

Per obtenir més informació sobre la seguretat NFS, consulteu Seguretat del sistema de fitxers de la xarxa a *Security*.

Suport de client sense disc de Sun

Element	Descripció
bootparamd	Proporciona l'informació necessària per arrencar els clients sense disc.

Subrutines NFS

En aquest apartat, es descriuen les subrutines NFS.

Element	Descripció
cbc_crypt, **des_setparity** o **ecb_crypt**	Implementa les rutines d'estàndard d'encriptació de dades.

Sistema de fitxers de bloqueig de missatges de servidor

El sistema SMBFS permet accedir a recursos compartits de servidors SMB com a sistemes de fitxers a AIX.

En aquest sistema de fitxers, l'usuari pot crear, eliminar, llegir, escriure i modifica les hores d'accés dels fitxers i dels directoris. No és possible modificar el mode de propietari ni d'accés.

SMBFS es pot utilitzar per accedir a fitxers en un servidor SMB. El servidor SMB és un servidor que executa Samba o un servidor o estació de treball Windows XP, Windows NT o Windows 2000. Cadascun d'aquests tipus de servidors permet exportar directoris com a recursos compartits. A continuació, aquest recurs compartit es pot muntar en un sistema AIX mitjançant SMBFS.

Instal•lació de SMBFS

Per instal•lar SMBFS en un sistema AIX, instal•leu el paquet `bos.cifs_fs`.

Quan s'hagi instal•lat el paquet `bos.cifs_fs`, es crearà el dispositiu `nsmb0`. Aquest dispositiu permet a l'ordre **mount** establir una connexió entre el servidor SMB i el client.

Muntatge SMBFS

El sistema SMBFS es pot muntar d'una de les dues maneres següents.

Es pot realitzar a través de l'ordre AIX **mount**. Per exemple:

```
mount -v cifs -n pezman/user1/pass1 -o uid=201,fmode=750 /home /mnt
```

Per obtenir més informació sobre l'ordre **mount** i explicacions dels senyaladors utilitzats, consulteu l'ordre **mount** que apareix a *Commands Reference, Volume 3*.

Podeu especificar opcions de muntatge mitjançant el senyalador
`-o`

. Les opcions de la línia d'ordres s'ha de separar només amb comes, no una coma i un espai. Les opcions del sistema de fitxers són:

Element	Descripció
`fmode`	Estableix un fitxer o un directori en el mode d'octets. El valor per defecte és 755.
`uid`	Assigna un UID als fitxer durant el muntatge. El valor per defecte és **root**.
`gid`	Assigna un GID als fitxer durant el muntatge. El valor per defecte és **sistema**.
`wrkgrp`	Grup de feina al qual pertany el servidor SMB.
`op`	Estableu el valor en 1 si utilitzeu el bloqueig oportú. Estableu el valor en 0 si no utilitzeu el bloqueig oportú.
`opfs`	Nom del sistema de fitxers de memòria cau que s'ha d'utilitzar per emmagatzemar fitxers de memòria cau de bloqueig.
`opsz`	Grandària dels fitxers de memòria cau individuals utilitzada pel bloqueig oportú.
`opfssz`	Grandària del sistema de fitxers de memòria cau utilitzat en un bloqueig oportú.

També podeu muntar el sistema de fitxers utilitzant el programa d'utilitat SMIT, `smit cifs_fs`, el qual executa l'ordre **mount** després de recopilar tota l'informació necessària.

Per muntar un sistema de fitxers SMBFS, cal proporcionar un nom d'usuari i una paraula clau per autenticar-se al servidor. Aquest nom d'usuari i aquesta paraula clau s'utilitzaran per realitzar totes les operacions de fitxer necessàries al servidor. El camp **Password** del panell smit no està marcat com a obligatori. Si el camp de la paraula clau no s'omple, es buscaran credencials al fitxer `cifscred` que coincideixin per l'usuari o el servidor que es proporciona. Si hi ha una coincidència, s'utilitzarà la paraula clau emmagatzemada del fitxer `cifscred`; en cas contrari, es demanarà una paraula clau a l'usuari a través de la sol•licitud de paraula clau AIX estàndard. D'aquesta manera, l'usuari pot proporcionar una paraula clau sense que sigui visible.

Nota: La contrasenya utilitzada per muntar l'SMBFS pot tenir 14 caràcters de longitud com a màxim i incloure caràcters especials.

Sempre que s'invoqui una ordre de sistema de fitxers com, per exemple, read en un fitxer dins del punt de muntatge SMBFS, s'envia una sol•licitud al servidor per a què llegeixi el fitxer. El nom d'usuari i la paraula clau s'envien com a part d'aquesta sol•licitud per a què el servidor pugui determinar si l'usuari té permisos al servidor per realitzar una operació de lectura al fitxer en qüestió. Per tant, l'última paraula pel que fa a si es pot realitzar una operació en un fitxer, la té el servidor.

De tota manera, l'opció `fmode` de l'ordre **mount** proporciona un mode a l'usuari root del sistema client de controlar l'accés als fitxers del servidor abans de que es realitzi una consulta al servidor. Si l'usuari no proporciona l'opció `fmode`, s'utilitzarà l'opció per defecte `755`. La taula següent il•lustra el mode en què l'opció `fmode` funciona mitjançant la sol•licitud d'escriptura:

Taula 92. A continuació, es proporcionen cinc casos en els quals als usuaris se'ls permet o no accedir al servidor segons els permisos dels quals disposen.

Número de cas	Usuari autenticat al servidor	Usuari al costat del client que vol accés d'escriptura	Propietari, grup o mode de muntatge	Propietari, grup o mode al servidor	Accés permès
Cas 1	user1	user2	user1, staff rwxr-xr-x	user1, staff rwxrwxr-x	no
Cas 2	user1	root	user1, staff rwxr-xr-x	user2, staff rwxr-xr-x	no
Cas 3	user1	user1	user1, staff rwxr-xr-x	user2, staff rwxrwxr-x	sí
Cas 4	user1	user1	user, staff rwxr-xr-x	root, system rwx------	no
Cas 5	user1	user1	user1, staff rwxr-xr-x	root, system rwxrwxrwx	sí

Al cas 1, l'accés es denega perquè el propietari, el grup i el mode del muntatge al client no han permès l'accés d'escriptura a `user2`.

Al cas 2, l'accés es denega perquè, encara que `root` tingui accés a totes les dades del costat del client, l'usuari autenticat pel servidor, `user1`, no té accés al fitxer al servidor.

Al cas 3, s'atorga l'accés perquè `user1` era el propietari al muntatge i `user1`, membre del grup `staff` al servidor, tenia accés al fitxer del servidor.

Al cas 4, l'accés es denega perquè, encara que `user1` era el propietari al muntatge, el fitxer es propietat de `root` al servidor, sense que hi pugui accedir cap grup ni qualsevol altre element.

Al cas 5, s'atorga l'accés perquè `user1` era el propietari al muntatge i `user1` tenia accés al fitxer del servidor a través d'altres permisos.

Notes:

1. Al sistema de fitxers muntat, una operació de còpia d'un fitxer a un altre es duu a terme correctament per a un fitxer amb una grandària de 4 GB + 4096 bytes o menys. En el cas dels fitxers que superin aquesta grandària, s'imprimeix un missatge d'avís i 4 GB + 4096 bytes del fitxer original es copien a la destinació.
2. Al sistema de fitxers muntat, els caràcters següents no es poden utilitzar en el nom de fitxer: barra inversa {\}, barra inclinada {/}, dos punts {:}, asterisc {*}, interrogant {?}, menor que {< }, major que {>}, barra vertical { | }.

Paraules clau emmagatzemades

SMBFS pot emmagatzemar credencials `server/user/password` al fitxer `/etc/cifs_fs/cifscred` per permetre la recuperació automàtica de paraules clau en muntar SMBFS.

És possible afegir, canviar i eliminar credencials d'aquest fitxer amb les ordres **mkcifscred**, **chcifscred** i **rmcifscred** (que es troben al fitxer `/usr/sbin`). Les paraules clau que s'afegeixen a aquest fitxer s'encripten. Quan s'intenta realitzar el muntatge sense proporcionar una paraula clau, es busquen

credencials corresponents al fitxer `cifscred`. Si hi ha una coincidència, s'utilitzarà la paraula clau emmagatzemada del fitxer `cifscred`; en cas contrari, es demanarà una paraula clau a l'usuari a través de la sol•licitud de paraula clau AIX estàndard.

El suport per les paraules clau emmagatzemades té les limitacions següents:

- Per a què la recuperació de paraules clau funcioni correctament, la convenció de denominació del servidor ha d'ésser coherent. Per exemple, si les credencials s'afegeixen amb una adreça IP enlloc de un nom d'amfitrió o un nom de domini completament qualificat, només es podran recuperar paraules clau quan es realitzin muntatges segons l'adreça IP.
- L'autenticació de paraules clau de text pla no és compatible amb el mètode de recuperació de paraules clau emmagatzemades. Si el servidor requereix paraules clau de text pla, l'autenticació no funcionarà.

/etc/filesystems support

L'SMBFS dóna suport a `/etc/filesystems` per permetre un muntatge automatitzat durant l'engegada del sistema.

El suport per `/etc/filesystems` també proporciona accés al servidor, usuari, paraula clau i dades d'opcions emmagatzemats durant el muntatge. Utilitzeu les ordre **mkcifsmnt**, **chcifsmnt**, **rmcifsmnt** i **lscifsmnt** (que es troben a `/usr/sbin`) per afegir, canviar, eliminar i llistar, respectivament, stanzas cifs a `/etc/filesystems`. Les credencials s'han d'emmagatzemar al fitxer `cifscred`.

Resolució de problemes SMBFS

Seguiu els passos següents quan us trobeu amb problemes amb SMBFS.

Si l'ordre **mount** o el camí d'accés ràpid `smit cifs_fs` retornen un error, tingueu en compte el següent:

1. Assegureu-vos que el nom d'usuari i la paraula clau siguin correctes. El nom d'usuari i la paraula clau han de permetre l'accés al recurs compartir al servidor.
2. Assegureu-vos que el nom de servidor és correcte. Si el nom del servidor és correcte, utilitzeu el nom completament qualificat de sistema en el cas que el servidor no formi part de la mateixa subxarxa que el client. També podeu intentar utilitzar l'adreça IP del servidor.
3. Assegureu-vos que l'ordre `lsdev -L|grep nsmb` retorna un nom de dispositiu. Si no es troba disponible cap dispositiu `nsmb`, el client AIX no podrà establir una connexió amb el servidor SMB.
4. Assegureu-vos que el nom del recurs compartit sigui correcte. Si el recurs compartit no existeix al servidor o no s'hi pot accedir amb el nom d'usuari i la paraula clau proporcionats, el servidor SMB rebutjarà la sol•licitud de connexió.
5. Utilitzeu l'ID d'incidència 525 per recopilar les dades de traça per SMBFS.
6. Assegureu-vos que el servidor està configurat per acceptar paraules clau NTLM, LM o de text pla. Aquests són els únics tipus d'encriptació de paraula clau als quals dóna suport SMBFS.
7. Si voleu autenticar-vos en un domini, haureu d'especificar el nom de domini amb l'opció **wrkgrp**. Sense aquesta opció, el servidor gestionarà l'autenticació de forma local.

Comunicacions asíncrones

L'AIX proporciona les següents categories de programes de control de dispositius asíncrons, també anomenats programes de control de dispositius tty.

- Programes de control per als ports en sèrie de la placa del sistema
- Programes de control per als ports en sèrie connectats al sistema mitjançant un adaptador
- Programes de control de pseudo-tty

Els controlados de la primera categoria són els adaptadors PCI. Inclouen adaptadors de 2, 8 i 128 ports.

En la segona categoria, els adaptadors PCI de 8 i 128 ports s'anomenen adaptadors intel•ligents, perquè utilitzen un processador Intel 8086 per descarregar una part considerable del processament de caràcters de la CPU de l'amfitrió. Aquests adaptadors estan controlats per un sondejador de 20 ms en comptes d'interrupcions de maquinari i proporcionen característiques de rendiment que s'adapten bé a la majoria d'aplicacions i dispositius sèrie. A mesura que s'afegeixen més dispositius al sistema, la càrrega de treball del sistema augmenta molt poc i, per tant, aquests adaptadors poden donar suport a un nombre molt gran de dispositius sèrie, molts més del que seria possible utilitzant interrupcions de maquinari. A més, com que aquests adaptadors utilitzen una millora patentada de rendiment de programari, poden enviar i rebre grans quantitats de dades més de pressa i de manera més eficient que els ports del sistema nadius, sempre i quan les dades es transfereixin en blocs grans. Per a obtenir més informació, consulteu la descripció de wantio al fitxer `/usr/include/sys/pse/README.pse`.

Nota: Els *ports del sistema* POWER5 integrats són semblants als ports en sèrie, tret que els ports del sistema només estan disponibles per a funcions suportades específicament. Consulteu l'apartat “Diferències funcionals entre els ports del sistema i els ports en sèrie” a la pàgina 575 per obtenir més informació.

No obstant això, alguns dispositius i aplicacions esperen o necessiten una latència molt baixa per al processament d'un únic caràcter, per la qual cosa és possible que tingueu problemes de temporització en la connexió amb aquests adaptadors intel•ligents. La latència de caràcter, o eco de caràcter, pot definir-se com el temps que es triga en rebre un únic caràcter en un port en sèrie, lliurar aquest caràcter a una aplicació i després fer eco al caràcter per tornar-lo a enviar al mateix port en sèrie.

Com que utilitzen la interrupció amb la prioritat més alta del sistema (INTCLASS0), els ports controlats per interrupcions proporcionen valors de latència compresos entre 0,10 ms i 0,20 ms en un sistema inactiu. Els adaptadors PCI de 8 ports proporcionen valors de latència que de mitjana estan al voltant de 10 a 12 ms, amb temps individuals que varien en més o menys 10 ms a causa del sondejador de 20 ms. Els adaptadors PCI de 128 ports tenen el mateix sondejador de 20 ms, que es comunica a través d'un enllaç de comunicacions amb els nodes d'accés remot (RAN). Els RAN permeten a un programa de control de sondeig controlar els ports en sèrie. Els valors de latència en aquests ports estan al voltant dels 30 ms de mitjana, però poden sobrepassar els 60 ms.

Els valors de latència en els adaptadors PCI de 8 i 128 ports es poden sintonitzar per a aplicacions especials utilitzant el paràmetre EDELY (retard d'incidència). Per obtenir una capacitat de resposta màxima en rebre un únic caràcter, reduïu el valor del paràmetre EDELAY. Això minimitza el temps necessari per enviar un únic caràcter des del port en sèrie a l'aplicació, però pot reduir la productivitat i el rendiment global del sistema quan es reben múltiples caràcters en una ràfega.

L'adaptador PCI EIA-32 de 2 ports és un adaptador de comunicacions en sèrie asíncron que es basa en l'UART dual Exar 17D152 Universal PC. L'adaptador de 2 ports dóna suport a dos connectors DB-9 i proporciona connectivitat a dispositius EIA-32 asíncrons, com ara mòdems i terminals tty.

A la plataforma IBM eServer p5 no hi ha ports del sistema nadius disponibles per a l'AIX. Malgrat que la interfície del terminal virtual s'ha millorat per donar suport a ports en sèrie físics que es troben a l'FSP a través de l'hipervisor, aquesta interfície només dóna suport a un conjunt específic de dispositius sèrie i no és un recanvi adequat per a un port en sèrie físic d'ús general. L'adaptador de 2 ports es comporta en certa manera com un port del sistema nadiu. El programa de control de dispositius adaptadors està controlat per interrupcions i dóna suport al trànsit programable i rep nivells de desencadenament FIFO. És un adaptador PCI; per tant, el programa de control de dispositius dóna suport a consultes VPD, connexió dinàmica i EEH. L'adaptador de 2 ports no dóna suport a les característiques de port del sistema nadiu quan s'utilitza el terminal virtual, com per exemple durant l'engegada, la instal•lació i el suport KDB.

Els programes de control pseudo-tty s'utilitzen quan s'accedeix a un sistema a través d'una xarxa que utilitza les ordres **rlogin** o **telnet** o quan s'accedeix a un sistema que utilitza un sistema de finestres en un monitor de gràfics. El programa de control pseudo-tty proporciona una forma d'executar aplicacions

antigues basades en caràcters, com ara l'editor de textos **vi**, a través d'un suport de comunicacions que no és un suport en sèrie. El que és important destacar dels programes de control pseudo-tty és que no són simètrics. L'extrem esclau proporciona una interfície compatible amb l'estàndard POSIX per a les aplicacions anteriors. L'extrem mestre es controla mitjançant una entitat, com ara el daemon **rlogin** o **telnet** o X-windows, que ha de proporcionar una emulació d'un dispositiu de terminal en sèrie al programa de control pseudo-tty. L'AIX pot donar suport de manera eficient a un nombre molt gran de dispositius pseudo-tty.

Velocitats de línia no POSIX

La interfície amb els dispositius sèrie que especifica POSIX i els estàndards UNIX posteriors, com per exemple X/OPEN, depèn de l'estructura de dades **termios** definida a `/usr/include/termios.h`. Malauradament, aquesta estructura de dades no pot utilitzar-se per especificar velocitats de línia superiors a 38.400 bits per segon. La majoria del maquinari en sèrie que s'utilitza actualment pot admetre velocitats de fins a 230.000 bps. Per utilitzar aquestes velocitats de línia més altes a l'AIX, la velocitat desitjada s'ha d'especificar en el moment de configurar el port utilitzant la SMIT. Si el maquinari del port en sèrie (UART) pot admetre la velocitat de línia que heu especificat, el port es podrà configurar.

L'atribut get ioctls utilitzant l'estructura **termio** o **termios** indicarà que la velocitat de línia és de 50 bps. El port utilitzarà la velocitat de línia no POSIX fins que es canviï, de manera que les aplicacions que utilitzen l'atribut set ioctls amb l'estructura **termio** i **termios** no han de modificar els senyaladors CBAUD a no ser que realment tinguin la intenció de canviar la velocitat de línia. Si el maquinari del port en sèrie (UART) no pot admetre la velocitat de línia sol•licitada, el port no es podrà configurar i es tornarà un error.

Nota: Els adaptadors PCI de 8 i 128 ports només admeten velocitats de línia no POSIX de 115.200 i 230.000 bps. L'adaptador PCI de 128 ports té una restricció addicional pel que fa a l'amplada de banda agregada de 2,5 Mbps (amb el cable de 8 fils), ja que es consumiria completament amb 11 dispositius transferint a una velocitat sostinguda de 230.000 bps cadascun. Aquesta restricció es troba a la línia que connecta l'adaptador als RAN, de manera que un sol adaptador es pot consumir completament amb 22 dispositius d'aquest tipus.

Adaptadors asíncrons

Els productes de comunicacions asíncrones ofereixen els avantatges de les comunicacions de dispositius i terminals de baix cost, multiusuaris i amb un rendiment mitjà a alt.

L'AIX permet a molts usuaris accedir a recursos i aplicacions del sistema. Cada usuari ha d'estar connectat mitjançant una sessió de terminal. La connexió pot ser local o remota a través d'un port en sèrie.

Cada sistema té com a mínim un port en sèrie estàndard disponible (alguns sistemes tenen tres ports en sèrie). Aquests ports poden donar suport a la comunicació asíncrona i a l'adjunció de dispositius.

Els ports asíncrons permeten l'adjunció de dispositius perifèrics asíncrons que compleixen els estàndards EIA 232, EIA 422 o RS-423, com per exemple:

- Mòdems asíncrons
- Escàners de codi de barres
- Impressores de gràfics i caràcters
- Terminals de pantalla i teclat
- Ordinadors personals
- Traçadors i impressores
- Terminals de punt de venda
- Sensors i dispositius de control
- Escàners de text

- Rellotges

Opcions de comunicacions asíncrones

Es pot afegir capacitat asíncrona ampliada a la unitat del sistema amb adaptadors que utilitzen busos PCI (Peripheral Component Interconnect).

Diversos factors poden influir en el tipus de connectivitat asíncrona que escolliu. A la taula següent trobareu un resum d'aquests productes.

Taula 93. Productes de comunicació asíncrona

Connexió asíncrona	Basat en processadors POWER	Basat en Itanium	Tipus de bus	Codi de dispositiu o tipus de màquina (model)	Velocitat màxima de dades per port (kbps)	Característiques destacades
Port en sèrie estàndard	X	X	Placa del sistema	n/d	Seleccionable en funció de la velocitat del rellotge generador de velocitat en bauds de l'UART (universal asynchronous receiver and transmitter).	Característica estàndard
RAN 232	X	X		8130	57,6	Capacitat remota
RAN 232 ampliat	X	X		8137	230	Capacitat remota
RAN EIA 422 de 16 ports	X	X		8138	230	Capacitat remota
Controlador de 128 ports	X			8128	230	Eficiència, recomptes de dispositiu més alts
Controlador de 128 ports	X			2933	230	Eficiència, recomptes de dispositiu més alts
Controlador de 128 ports	X	X	PCI	2944	230	Eficiència, recomptes de dispositiu més alts

Nota: El codi de dispositiu del RAN muntat sobre bastidor és 8136.

Nota: La velocitat màxima de dades per port està limitada per l'amplada de banda de la línia (1.2 Mbps per al RAN estàndard o 2.4 Mbps per al RAN ampliada).

La primera característica d'aquesta taula representa els ports en sèrie adjuntats a la placa que són estàndard amb cada unitat del sistema. Les característiques següents són els adaptadors. El subsistema asíncron de 128 ports inclou els nodes asíncrons remots (RAN) que s'hi adjunten.

Ports asíncrons adjuntats a la placa

La majoria de models de la unitat del sistema tenen dos ports en sèrie asíncrons EIA 232 (estàndard) integrats. Els dispositius sèrie asíncrons EIA 232 poden adjuntar-se directament als ports en sèrie estàndard utilitzant cables sèrie estàndard amb connectors d'intèrpret d'ordres D de 9 potes.

Alguns sistemes de multiprocessador tenen un tercer port en sèrie que s'utilitza per a la comunicació amb el centre de servei remot.

Nota: Els sistemes basats en Itanium tenen un o dos ports en sèrie integrats. Els models d'estacions de treball inicials tenen un port, mentre que els models de classes de servidor inicials tenen dos ports.

Ports asíncrons adjuntats a adaptadors

Cadascun dels adaptadors necessita una ranura de bus i només es poden utilitzar en sistemes que donen suport al tipus de bus necessari.

Els adaptadors ISA de 8 i 128 ports i els adaptadors PCI de 8 ports són adaptadors intel•ligents que proporcionen una descàrrega significativa del processador de l'amfitrió.

EIA 232 és l'estàndard de comunicacions més habitual, però l'EIA 422A (utilitzat quan es necessita una distància de cable més llarga) també està suportat. La implementació EIA 422A no inclou la capacitat de detecció de l'estat del dispositiu ni els senyals de control de mòdem RS 232.

Nota: La plataforma basada en Itanium només dóna suport als adaptadors PCI de 8 i 128 ports.

Ports asíncrons adjuntats a nodes

L'adaptador de 128 ports, disponible per al bus Micro Channel, ISA o PCI, permet adjuntar d'un a vuit nodes asíncrons remots (RAN).

Cada RAN té 16 ports asíncrons per a la connexió amb dispositius i són unitats alimentades per separat. Es poden connectar en margarita fins a quatre RAN des de cadascuna de les dues connexions de la targeta adaptadora de 128 ports. Els RAN poden admetre 16 dispositius EIA 232 o 16 dispositius EIA 422. El controlador de 128 ports és un adaptador intel•ligent que augmenta el nombre de sessions asíncrones possibles a un determinat nivell d'ús de la UCP.

A continuació s'indiquen característiques addicionals del dispositiu de 128 ports:

- Els RAN poden estar situats a una distància de 300 metres del processador del sistema utilitzant cablatge protegit de 8 fils i mantenir al mateix temps tots els valors de rendiment.
- La distància es pot ampliar a 1200 metres reduint la velocitat de dades entre els RAN i el processador del sistema.
- Els RAN poden estar situats en ubicacions remotes del processador del sistema utilitzat els mòdems síncrons EIA 232 i EIA 422. A cada connexió en margarita de quatre RAN només se li permet una parella de mòdems en algun punt de la connexió.
- Es millora el rendiment del sistema descarregant el processament de caràcters tty del processador del sistema.

Consideracions sobre la selecció del producte

El producte asíncron adequat sovint depèn d'una situació en concret.

Les següents preguntes us ajudaran a escollir el producte que necessiteu instal•lar.

Ampliabilitat

Quants ports asíncrons es necessiten?

Quants ports es necessitaran en el futur?

Topologia

Hi haurà dispositius en altres edificis o ubicacions remotes?

On es realitzarà l'administració de xarxa/sistema?

Hi ha un clúster HACMP?

Quin tipus de cablatge es necessita o ja existeix?

Rendiment

L'aplicació fa un ús intens de la UCP?

Quins tipus de dispositius s'adjuntaran?

Quina és la demanda d'amplada de banda asíncrona relativa per a la suma agregada dels dispositius?

Taula 94. Demanda d'amplada de banda relativa dels dispositius

Demanda baixa	Demanda moderada	Demanda alta
Terminals ASCII, terminals punt de venda, mòdems asíncrons	Impressores, FAX/mòdems de baixa velocitat, escàners de codi de barres	Terminals X en sèrie, FAX/mòdems d'alta velocitat, impressores d'alta velocitat, aplicacions de transferència de fitxers.

Requisit per a la interfície de dispositiu

Quina interfície asíncrona es necessita, per exemple, EIA 232, EIA 422A, EIA 423?

Els dispositius o aplicacions necessiten la interfície EIA 232 completa?

Seguretat

És necessari el kernel de seguretat del sistema (SAK)? (només ports adjuntats a la placa)

A la taula següent es mostren les característiques detallades dels productes.

Taula 95. Característiques dels productes de connexió asíncrona

Característica	Ports en sèrie nadius	PCI de 2 ports	PCI de 8 ports	PCI de 128 ports amb RAN
Nombre de ports asíncrons per adaptador	n/d	2	8	128
Nombre màxim d'adaptadors	n/d	sense límit	20	20
Nombre màxim de ports asíncrons	2 ó 3	2	160	2560
Nombre de ports asíncrons per RAN	n/d	n/d	n/d	16
Nombre màxim de RAN	n/d	n/d	n/d	160
Velocitat màxima (KBits/seg)	Seleccionable en funció de la velocitat del rellotge generador de velocitat en bauds de l'UART.	230	230	230
Mètode d'adjunció	placa	directa	directa	node
Interfícies elèctriques asíncrones suportades	EIA 232	EIA 232	EIA 232 EIA 422A	EIA 232 EIA 422
Connector estàndard	DB9	DB9	DB25M	RJ-45 (10 potes o 8 potes)
Opcions de cable DB25	n/d	n/d	n/d	RJ-45-DB25
Opció muntada sobre bastidor	n/d	n/d	n/d	sí
Font d'alimentació	n/d	n/d	n/d	externa
Senyals suportats (EIA 232)	TxD RxD RTS CTS DTR DSR DCD RI	TxD RxD RTS CTS DTR DSR DCD RI	TxD RxD RTS CTS DTR DSR DCD RI	TxD RxD RTS CTS DTR DSR DCD RI

Aplicacions d'adaptadors asíncrons

Cada oferta de productes està caracteritzada per un cas pràctic representatiu dels seus punts forts. Els adaptadors descrits en aquest tema s'enumeren juntament amb les seves especificacions per tal que pugueu seleccionar per cada cas específic.

Element	Descripció
EIA 232 de bus PCI de 2 ports	• Ranura PCI disponible. • Fins a dos ports per adaptador. • Necessita tots els ports EIA 232. • Velocitats asíncrones de fins a 230 Kbps.
EIA 232/EIA 422 de bus PCI de 8 ports	• Ranura PCI disponible. • Es necessiten menys de vuit ports amb poca expansió o sense expansió. • Necessita tots els ports EIA 232, tots els ports EIA 422 o una combinació de ports EIA 232 i EIA 422. • Descàrrega del processament d'E/S de terminal i interrupció de caràcters de la UCP principal. • Velocitats asíncrones de fins a 230 Kbps. • Rendiment màxim per a mòdems d'alta velocitat (33,6 Kbps) amb compressió de dades.
Adaptador (PCI) de 128 ports	• Una ranura de bus Micro Channel, ISA o PCI disponible per a E/S asíncrona. (Per obtenir més informació sobre Micro Channel o ISA, consulteu l'apartat "Adaptador de 128 ports (Micro Channel, ISA)" a la pàgina 661.) • Setze ports actualment, amb possibilitat d'expansió fins a 128 ports sense ranures addicionals. • Terminal més distant situat a uns 90 metres (300 peus) del sistema a una velocitat màxima de dades de 230 Kbps. • Terminals planificats: pròxims o al mateix local, distants al mateix local, i remots. • Necessiten alta productivitat asíncrona amb baixa demanda de processador. • Necessiten capacitat d'impressora adjuntada a terminal. • Necessiten connexió amb locals remots a través de fibra òptica o mòdems síncrons.

Casos pràctics per a solucions asíncrones

Els casos pràctics de clients que es descriuen a continuació es van resoldre amb un PCI de 8 ports i un programa de control asíncron de 128 ports.

Element	Descripció
Oficina immobiliària	• La simplicitat i el cost són prioritaris. • Sistema operatiu i servidor. • De sis a deu dispositius connectats al servidor que accedeix a la base de dades. • Una ranura està disponible per a la comunicació asíncrona. • Els dispositius estan a menys de 61 metres (200 peus) del servidor. **Solució:** PCI de 8 ports.
Punt de venda al detall	• El cost per seient és d'alta prioritat. • Sistema operatiu i servidor. • 20 o més terminals ASCII: per exemple, caixes registradores. • Una ranura està disponible per a la comunicació asíncrona. • Es preveu una futura expansió amb terminals addicionals. **Solució:** Controlador asíncron de 128 ports amb dos RAN. Futura expansió amb RAN addicionals.

Consideracions sobre topologia

La família d'adaptadors asíncrons ofereix un ampli ventall d'opcions pel que fa a la topologia de distància.

Les longituds màximes de cable des dels adaptadors d'adjunció directa i a la placa normalment corresponen a la distància entre el port i el dispositiu asíncron, que funciona a la velocitat de dades màxima especificada. L'adaptador de 128 ports es mesura des de la targeta adaptadora al RAN connectat en margarida adjuntat a ell. Amb l'adaptador de 128 ports, es poden assolir de manera efectiva distàncies il•limitades utilitzant mòdems síncrons EIA 422 per adjuntar els RAN a l'adaptador.

El cablatge correcte és de vital importància i és exclusiu de cada entorn.

Comunicació en sèrie

En aquesta secció es descriuen els conceptes, la terminologia, el maquinari i els estàndards de la comunicació asíncrona.

Els ports en sèrie s'utilitzen per connectar físicament dispositius asíncrons a un ordinador. Estan situats a la part posterior de la unitat del sistema, ja sigui integrats o utilitzant un adaptador multiport, com ara els adaptadors asíncrons de 2 ports, 8 ports, 16 ports i 128 ports.

Nota: Els ports del sistema integrats POWER5 no són ports en sèrie de funcions completes i ús general. Vegeu l'apartat "Diferències funcionals entre els ports del sistema i els ports en sèrie" a la pàgina 575 per obtenir més informació.

Per entendre el funcionament d'un port en sèrie, primer cal examinar les comunicacions en paral•lel. Un port en paral•lel estàndard utilitza vuit potes, o fils, per transmetre simultàniament els bits de dades que formen un únic caràcter. A la il•lustració següent es mostra la transmissió en paral•lel de la lletra a.

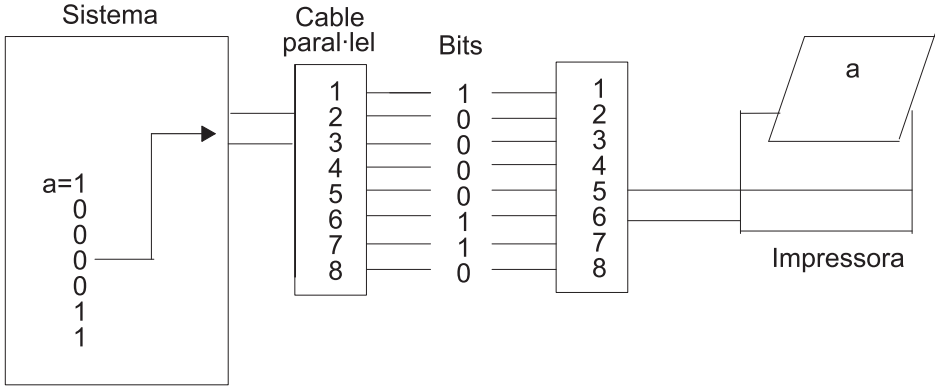


Figura 29. Port de comunicacions en paral•lel

Els ports en sèries només necessiten una única pota, o fil, per enviar el mateix caràcter de dades al dispositiu. Per a aconseguir-ho, les dades es converteixen d'un format en paral•lel (que envia l'ordinador) a un format seqüencial, en el qual els bits s'organitzen un rera l'altre en una sèrie. A continuació, les dades es transmeten al dispositiu enviant en primer lloc el bit menys important (o bit zero). Un cop el dispositiu remot ha rebut les dades, aquestes es tornen a convertir al format en paral•lel. A la il•lustració següent es mostra la transmissió en sèrie de la lletra a.

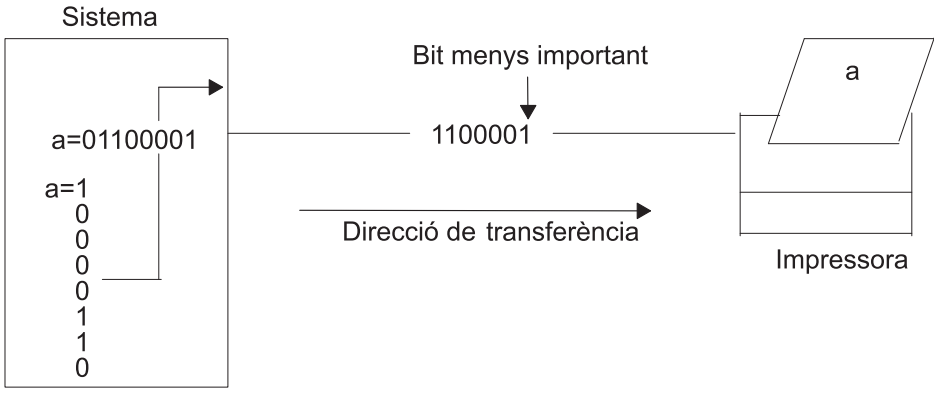


Figura 30. Port de comunicacions en sèrie

Les transmissions en sèrie d'un únic caràcter són senzilles i directes; no obstant això, surten complicacions quan un gran nombre de caràcters es transmeten en sèrie tal com es mostra a la il•lustració següent. El sistema receptor no sap on acaba un caràcter i on comença l'altre. Per solucionar aquest problema, els dos extrems de l'enllaç de comunicacions s'han de sincronitzar o temporitzar.

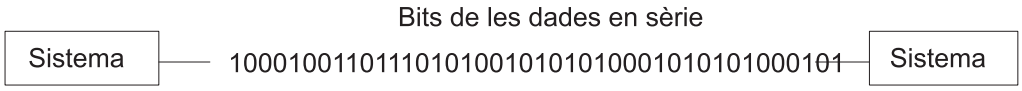


Figura 31. Transmissió en sèrie

Diferències funcionals entre els ports del sistema i els ports en sèrie

Els *ports del sistema* POWER5 integrats són semblants als ports en sèrie, tret que els ports del sistema només estan disponibles per a funcions suportades específicament.

Els ports del sistema estan inhabilitats quan un port de la consola de gestió del maquinari (HMC) està connectat a una HMC. Es poden utilitzar els ports de l'HMC o els ports del sistema, però no tots alhora.

Fins i tot quan no hi ha cap HMC adjuntada, els ports del sistema integrats es limiten a la funció de la consols TTY connectada en sèrie. Només funcionen correctament amb mòdems homologats de crida automàtica, terminals asíncrons i determinats UPS. L'adjunció d'altres dispositius sèrie (incloses les connexions de sistema a sistema per a l'HACMP) requereix un adaptador de port en sèrie en una ranura PCI.

Sincronització

La sincronització és el procés de temporitzar la transmissió en sèrie per identificar correctament les dades que s'estan enviant.

Els dos modes més comuns són el síncron i l'asíncron.

Transmissió síncrona:

El terme *síncron* s'utilitza per descriure una transferència contínua i uniforme de blocs de dades.

Aquests tipus de connexions s'utilitzen quan s'han de transferir molt de pressa grans quantitats de dades des d'una ubicació a una altra. La velocitat de la connexió síncrona s'aconsegueix mitjançant la transferència de dades en blocs grans en comptes de caràcters individuals.

Els blocs de dades s'agrupen i s'espaien a intervals regulars i van precedits de caràcters especials anomenats syn o caràcters inactius síncrons. Vegeu la il•lustració següent.

Figura 32. Transmissió síncrona

Un cop el dispositiu remot ha rebut els caràcters syn, aquests es descodifiquen i s'utilitzen per sincronitzar la connexió. Quan la connexió s'ha sincronitzat correctament, la transmissió de dades pot començar.

Una analogia d'aquest tipus de connexió seria la transmissió d'un document de text gran. Abans de transferir el document per la línia síncrona, primer es descomposa en blocs de frases o paràgrafs. A continuació, els blocs s'envien a través de l'enllaç de comunicacions a l'indret remot. Amb altres modes de transmissió, el text s'organitza en sèries llargues de lletres (o caràcters) que formen les paraules dins de frases i paràgrafs. Aquests caràcters s'envien d'un en un a través de l'enllaç de comunicacions i es tornen a ajuntar a la ubicació remota.

La temporització necessària per a les connexions síncrones s'obté dels dispositius que es troben a l'enllaç de comunicacions. Tots els dispositius de l'enllaç síncron s'han d'establir en la mateixa sincronització.

La llista següent enumera les característiques que són específiques de la comunicació síncrona:

- No hi ha espais buits entre els caràcters que es transmeten.
- La temporització la proporcionen els mòdems o altres dispositius que es troben a cada extrem de la connexió.
- Els caràcters especials syn precedeixen a les dades que es transmeten.
- Els caràcters syn s'utilitzen entre blocs de dades a efectes de temporització.

Transmissió asíncrona:

El terme *asíncron* s'utilitza per descriure el procés mitjançant el qual les dades transmeses estan codificades amb bits d'inici i d'aturada, que especifiquen el començament i el final de cada caràcter.

A la figura següent es mostra un exemple de transmissió asíncrona.

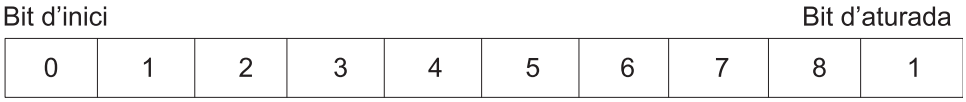


Figura 33. Transmissió asíncrona

Aquests bits addicionals proporcionen la temporització o sincronització de la connexió indicant quan s'ha enviat o rebut un caràcter complet; així doncs, la temporització de cada caràcter comença amb el bit d'inici i s'acaba amb el bit d'aturada.

Quan apareixen espais buits entre les transmissions de caràcters, es diu que la línia està en un estat de marca. Una marca és un 1 binari (o voltatge negatiu) que s'envia durant els períodes d'inactivitat de la línia, tal com es mostra a la figura següent.

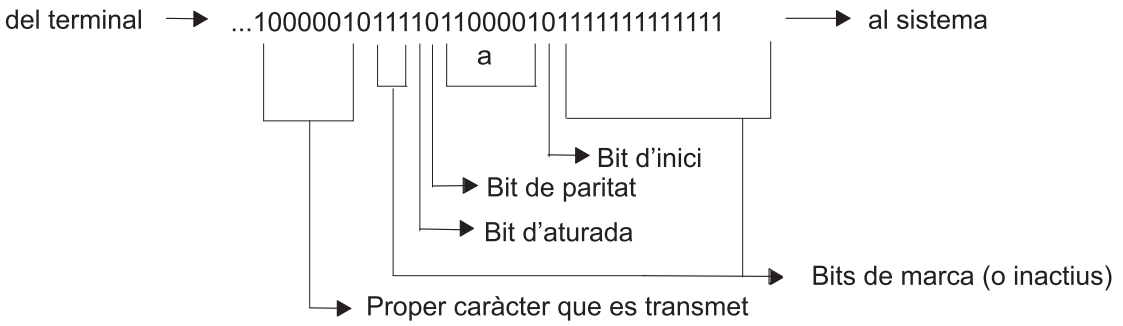


Figura 34. Bits de marca (inactivitat) al corrent de dades

Quan l'estat de marca s'interromp per un voltatge positiu (un 0 binari), el sistema receptor sap que a continuació vindran caràcters de dades. Per aquest motiu, el bit d'inici, que precedeix al caràcter de dades, és sempre un bit d'espai (0 binari) i el bit d'aturada, que senyala el final d'un caràcter, és sempre un bit de marca (1 binari).

La llista següent enumera les característiques específiques de la comunicació asíncrona:

- Cada caràcter va precedit per un bit d'inici i va seguit d'un o més bits d'aturada.
- Poden existir espais buits entre els caràcters.

Paràmetres de la comunicació en sèrie

Els paràmetres que s'utilitzen durant la comunicació en sèrie inclouen els bits per caràcter, els bits per segon (bps), la velocitat en bauds, la paritat i els bits d'inici, aturada i marca.

Bits per caràcter:

El número de bits per caràcter (bpc) indica el nombre de bits utilitzats per representar un únic caràcter de dades durant la comunicació en sèrie.

Aquest número no reflecteix la quantitat total de bits de paritat, d'inici o d'aturada inclosos amb el caràcter. Dos possibles valors per a bpc són 7 i 8.

Quan s'utilitza el valor de set bits per caràcter, només és possible enviar els primers 128 caràcters (0-127) del joc de caràcters ASCII estàndard. Cadascun d'aquests caràcters es representa mitjançant set bits de dades. El valor de vuit bits per caràcter s'ha d'utilitzar per enviar el joc de caràcters ampliats ASCII (128-255). Cadascun d'aquests caràcters només es pot representar utilitzant vuit bits de dades.

Bits per segon (bps):

Proporciona una descripció de l'estadística bits per segon.

Bits per segon (bps) és el nombre de bits de dades (1 i 0 binaris) que es transmeten per segon a través de la línia de comunicacions.

Velocitat en bauds:

La velocitat en bauds és el nombre de vegades per segon que un senyal de comunicacions en sèrie canvia d'estat; un estat pot ser un nivell de voltatge, una freqüència o un angle de fase de freqüència.

Si el senyal canvia una vegada per a cada bit de dades, aleshores un bps és igual a un baud. Per exemple, un mòdem de 300 bauds canvia d'estat 300 vegades per segon.

Bits de paritat:

El bit de paritat, a diferència dels bits d'inici i aturada, és un paràmetre opcional que s'utilitza a les comunicacions en sèrie per determinar si el dispositiu remot rep correctament el caràcter de dades que s'està transmetent.

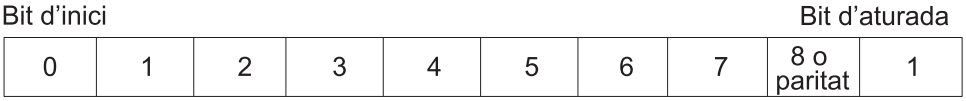


Figura 35. Paritat

El bit de paritat pot tenir una de les cinc especificacions següents:

Element	Descripció
cap	Especifica que el sistema local no ha de crear un bit de paritat per als caràcters de dades que s'estan transmetent. També indica que el sistema local no comprova si hi ha un bit de paritat a les dades rebudes des d'un sistema remot.
parell	Especifica que el nombre total d'1 binaris, d'un sol caràcter, suma un número parell. Si no és així, el bit de paritat ha de ser un 1 per tal de garantir que el nombre total d'1 binaris es parell. Per exemple, si la lletra a (1100001 binari) es transmet sota paritat parell, el sistema emissor suma el nombre d'1 binaris, que en aquest cas és tres, i fa que el bit de paritat sigui un 1 per tal de mantenir un número parell d'1 binaris. Si la lletra A (1000001 binari) es transmet sota les mateixes circumstàncies, el bit de paritat seria un 0, mantenint així el nombre total d'1 binaris com un número parell.
senar	Funciona sota les mateixes directrius que la paritat parell, excepte que el nombre total d'1 binaris ha de ser un número senar.
espai	Especifica que el bit de paritat sempre serà un zero binari. Un altre terme utilitzat per a la paritat d'espai és el paritat d'emplenar amb bits, ja que s'utilitza per emplenar dades de set bits que es transmeten a un dispositiu que només pot acceptar dades de vuit bits. Aquests dispositius consideren el bit de paritat d'espai com un bit de dades addicional per al caràcter transmès.
marca	Funciona sota les mateixes directrius que la paritat d'espai, excepte que el bit de paritat és sempre un 1 binari. El bit de paritat de marca només actua per emplenar.

Bits d'inici, aturada i marca:

Els bits d'inici i aturada s'utilitzen a la comunicació asíncrona com a mitjà per temporitzar o sincronitzar els caràcters de dades que es transmeten.

Sense la utilització d'aquests bits, els sistemes emissor i receptor no sabran quan acaba un caràcter i comença un altre.

Un altre bit utilitzat per separar els caràcters de dades durant la transmissió és el bit RS de marca (o inactivitat). Aquest bit, un 1 binari, es transmet quan la línia de comunicacions està inactiva i no s'estan enviant ni rebent caràcters.

Quan el sistema rep un un bit d'inici (binari 0) s'entén que un número fixe de bit de caràcter (determinat pel paràmetre **bits per character**) i, fins i tot, un bit de paritat (determinat pel paràmetre**parity**), segueixen a aquest bit d'inici. A continuació, el sistema rep un bit d'aturada (binari 1). A l'exemple següent, el bit **parity** està present i el **bits per character** és 7.

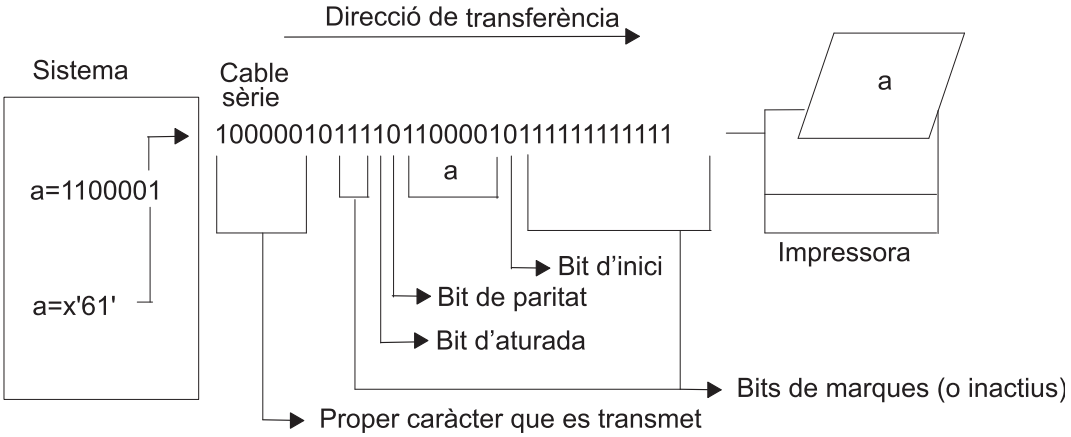


Figura 36. Bits d'inici, aturada i marca

L'estàndard EIA 232D

L'estàndard EIA 232D va ser desenvolupat el 1969 per tal d'especificar les connexions entre un ordinador i un mòdem.

El propi terme és un acrònim que significa el següent:

Estàndard acceptat per l'EIA (Associació d'indústries electròniques), número d'ID 232 revisió D

L'EIA 232D especifica les característiques de les connexions físiques i elèctriques entre dos dispositius. S'assignen noms i abreviatures a cada pota o cable necessari per a les comunicacions en sèrie, com per exemple:

Taula 96. Connexions EIA 232D

Senyal	Tipus d'equip	Símbol	Pota
Dades de transmissió	DCE	TxD	2
Dades de recepció	DTE	RxD	3
Sol•licitud per enviar	DCE	RTS	4
Preparat per emetre	DTE	CTS	5
Conjunt de dades preparat	DTE	DSR	6
Senyal de terra		SG	7
Detecció de portadora	DTE	CD	8
Terminal de dades preparat	DCE	DTR	20
Indicador de timbre	DTE	RI	22

A l'EIA 232D, els dispositius que utilitzen la pota 2 (TxD) per a la sortida (per exemple, ordinadors i terminals) reben el nom de DTE (Data Terminal Equipment). Els dispositius que utilitzen la pota 2 (TxD) per a l'entrada (per exemple, mòdems) reben el nom de DCE (Data Communication Equipment).

L'EIA 232D també especifica els connectors. Un dispositiu DTE normalment té connectors mascle mentre que els dispositius DCE tenen connectors femella. Els fabricants no sempre compleixen aquest estàndard; per tant, s'aconsella als usuaris que llegeixin sempre la documentació del dispositiu abans de connectar els cables.

Mètodes de comunicació asíncrona

Aquest tema descriu les dues formes de comunicació asíncrona, la unidireccional i la bidireccional (que inclou semidúplex i dúplex).

La comunicació símplex, o unidireccional, és la forma de connexió més simple entre dos dispositius. Aquest mode de comunicació permet transmetre dades en només una direcció i només requereix connectar dues línies, com per exemple TxD (o RxD) i SG.

Hi ha dues formes de comunicacions bidireccionals: semidúplex i dúplex. Una connexió en mode semidúplex permet transmetre dades en dues direccions però no simultàniament. Una analogia de semidúplex seria la utilització d'una ràdio CB on és possible la comunicació bidireccional però només pot parlar una persona a la vegada.

En el mode dúplex, la comunicació de dades pot tenir lloc en dues direccions simultàniament. Una analogia de comunicació dúplex és una conversa telefònica en què dues persones parlen al mateix temps.

Control de flux

El dispositiu sèrie necessita algun tipus de control de flux de dades per limitar la quantitat de dades que transmet el sistema.

Els dispositius sèrie, com ara impressores i mòdems, no processen les dades tan de pressa o de manera tan eficient com ho fan els ordinadors als que estan connectats.

El terme *control de flux* s'utilitza per descriure el mètode mitjançant el qual un dispositiu sèrie controla la quantitat de dades que es transmeten a si mateix.

Flux de maquinari RTS/CTS:

Sol•licitud per enviar/preparat per emetre (RTS/CTS) a vegades s'anomena "pacing" o conformitat de connexió de maquinari en comptes de control de flux.

El terme conformitat de connexió de maquinari prové de la utilització de cables i voltatges com a mètode de control de la transmissió de dades. A diferència de XON/XOFF, que envia caràcters de control al corrent de dades, RTS/CTS utilitza voltatges positius i negatius juntament amb potes i fils dedicats en el cablatge del dispositiu.

Un voltatge positiu significa que es permet la transmissió de dades, mentre que un voltatge negatiu significa que s'ha de suspendre la transmissió de dades.

Flux de maquinari DTR/DSR:

El senyal DTR (terminal de dades preparat), una altra forma de control de flux de maquinari, normalment es generat per dispositius, com ara impressores, per indicar que estan preparats per comunicar-se amb el sistema. Aquest senyal normalment s'utilitza conjuntament amb el senyal DSR (conjunt de dades preparat) que genera el sistema per controlar el flux de dades.

Un voltatge positiu significa que es permet la transmissió de dades, mentre que un voltatge negatiu significa que s'ha de suspendre la transmissió de dades.

Flux de programari XON/XOFF:

El control de flux XON/XOFF (transmitter on/transmitter off) implica l'enviament de caràcters de control de transmissió de dades juntament amb el corrent de dades (TxD i RxD). Per aquest motiu, se l'anomena control de flux de programari.

Quan les dades s'envien a un mòdem, es col•loquen a un buffer. Una mica abans de que aquest buffer arribi a la seva capacitat màxima, el mòdem enviarà un caràcter XOFF al sistema i el sistema aturarà la transmissió de les dades. Quan el buffer del mòdem està gairebé buit i preparat per rebre més dades, enviarà un caràcter XON de tornada al sistema la qual cosa farà que s'enviïn més dades.

Configuració d'un port per a la conformitat de connexió de maquinari RTS/CTS:

S'aconsella que els mòdems adjuntats al servidor que funciona a una velocitat de 9600 o superior utilitzin la conformitat de connexió de maquinari RTS/CTS en comptes del control de flux XON/XOFF.

D'aquesta manera s'evitarà sobrepassar el límit de buffer en un sistema amb recursos limitats. RTS no és un valor per defecte en cap port tty i, per tant, l'haurà d'establir l'administrador del sistema.

`Prerequisits`

Cal utilitzar com a mínim un cable de cinc fils per donar suport a RTS/CTS.

Per habilitar RTS/CTS per a un port, cal dur a terme els passos següents:

1. Utilitzeu el camí d'accés ràpid `smit tty`.
2. Seleccioneu **Canviar/mostrar característiques d'un TTY**.
3. Seleccioneu el tty en el que s'ha d'habilitar RTS/CTS.
4. Establiu el camp CONTROL DE FLUX a utilitzar en **rts**.
5. Seleccioneu **Realitzar**.
6. Sortiu de la SMIT.

Dispositiu de terminal TTY

Un dispositiu de terminal tty és un dispositiu de caràcter que realitza l'entrada i sortida caràcter a caràcter.

La comunicació entre els dispositius de terminal i el programes que llegeixen i escriuen en ells es controla mitjançant la interfície tty. Exemples de dispositius tty són els següents:

- Mòdems
- Terminals ASCII
- Consola del sistema (LFT)
- **aixterm** sota AIXwindows

Els dispositius tty poden afegir-se, suprimir-se, llistar-se i canviar-se com qualsevol altre dispositiu del sistema utilitzant l'eina SMIT o les ordres específiques del dispositiu.

Valors TERM per a diferents pantalles i terminals

La informació sobre les possibilitats dels terminals s'emmagatzema a la base de dades `terminfo`.

El valor de la variable d'entorn **TERM** identifica la descripció del terminal específic de la base de dades `terminfo`. Proporciona tota la informació que un programa necessita per comunicar-se de forma efectiva amb el dispositiu tty actual.

Taula 97. Valors TERM per diferents terminals

Pantalla/terminal	Valor
Terminal ASCII 3161	ibm3161
Terminal ASCII 3163	ibm3161
DEC VT100 (terminal)	vt100
DECVT220	vt220
Estació de pantalla ASCII 3151 amb cartutx o estació de pantalla ASCII 3161 amb cartutx	ibm3161-C
Estació de pantalla ASCII 3162	ibm3161
Estació de pantalla ASCII 3162 amb cartutx	ibm3162
Pantalla 6091	lft

Taula 97. Valors TERM per diferents terminals (continuació)

Pantalla/terminal	Valor
AIXwindows	aixterm

Per obtenir més informació sobre les entrades en la base de dades `terminfo`, consulteu e l format de fitxer `terminfo` a *Files Reference*. Per convertir les entrades `termcap` a entrades `terminfo`, consulteu l'ordre **captoinfo** a *Commands Reference, Volume 1*. (El fitxer `termcap` conté les descripcions de terminal per als sistemes Berkeley més antics).

Característiques de TTY

La *disciplina de línia* proporciona la interfície d'usuari independent del maquinari per la comunicació entre l'ordinador i un dispositiu asíncron.

Per exemple, un usuari pot esborrar una sola línia o interrompre un procés que s'està executant actualment escrivint una seqüència determinada de caràcters. Podeu definir el significat d'aquestes seqüències de caràcters així com establir altres característiques del terminal, com ara la velocitat de la comunicació, utilitzant l'ordre **chdev**, la System Management Interface Tool (SMIT) o l'ordre **stty**.

Requisits d'atributs per al dispositiu TTY connectat.

Una comunicació correcta entre l'amfitrió i un dispositiu tty connectat ha de tenir els requisits següents.

- Un cable de comunicacions correctament connectat.
- Valors de comunicacions coincidents (velocitat de línia, grandària dels caràcters, paritat, bit d'aturada i interfície) entre l'amfitrió i el dispositiu tty connectat.

Gestió de dispositius TTY

En aquest tema es descriuen les tasques de gestió de dispositius així com les ordres i camins d'accés ràpid de la SMIT associats.

Taula 98. Tasques de gestió de dispositius TTY

Tasca	Camí d'accés ràpid de la SMIT	Ordre o fitxer
Llistar dispositius TTY definits	`smit lsdtty`	**lsdev -C -c tty -H**
Afegir un TTY	`smit mktty`	**mkdev -t tty**[1,2]
Moure un TTY a un altre port[3]	`smit movtty`	**chdev -l** *Nom* **-p** *NomPare* **-w** *UbicacióConnexió*[2,4]
Canviar/mostrar característiques d'un TTY	`smit chtty`	**lsattr -l***Nom* **-E** (per mostrar); **chdev -l** *Nom* (per canviar)[4,5]
Eliminar un TTY[3]	`smit rmtty`	**rmdev -l** *Nom*
Configurar un TTY definit (Fer disponible per a l'ús)	`smit mktty`	**mkdev -l** *Nom*

Nota:

1. Es poden utilitzar altres senyaladors per especificar amb més detall el nou dispositiu tty. Per exemple, per definir i configurar un dispositiu tty RS-232 connectat al port `0` de l'adaptador asíncron de 8 ports `sa3` amb l'atribut `speed` establert en `19200` i altres atributs establerts en els valors recuperats del fitxer `foo`:

   ```
   mkdev -t tty -s rs232 -p sa3 -w 0 -a speed=19200 -f foo
   ```

2. Les ordres **mkdev** i **chdev** admeten opcions que no són possibles amb la SMIT.
3. Inhabiliteu el tty abans de dur a terme aquesta tasca. Consulteu l'ordre **pdisable** a *Commands Reference, Volume 4*.
4. Utilitzeu senyaladors per canviar característiques específiques d'un tty des de la línia d'ordres.

5. Podeu seleccionar una velocitat en bauds Posix de la funció Llista, o bé podeu escriure la velocitat en bauds no Posix directament en el camp. Si el maquinari del mòdem no pot donar suport a la velocitat en bauds seleccionada, el sistema visualitza un missatge d'error.

Si afegiu o canvieu un tty des de la línia d'ordres, consulteu la llista següent per saber el nom de l'*Atribut* que heu d'especificar al senyalador **-a** *Atribut*=*Valor* per a la característica que voleu establir. Per exemple, especifiqueu `-a speed=Value` per establir la velocitat en bauds d'un dispositiu tty.

Taula 99. Atributs TTY

Característica	**Nom de l'atribut**
Habilitar INICI DE SESSIÓ	login
Velocitat en BAUDS	speed
PARITAT	parity
BITS per caràcter	bpc
Nombre de BITS D'ATURADA	stops
TEMPS abans d'avançar al següent valor de port	timeout
Conformitat de connexió XON-XOFF	xon
Tipus de TERMINAL	term
CONTROL DE FLUX a utilitzar	flow_disp
DISCIPLINA OBERTA a utilitzar	open_disp
Atributs STTY per al temps d'EXECUCIÓ	runmodes
Atributs STTY per a l'INICI DE SESSIÓ	logmodes
Gestor d'activitat de l'intèrpret d'ordres d'EXECUCIÓ	intèrpret d'ordres
Nom de GESTOR DE CONNEXIONS	logger
ESTAT del dispositiu en el moment d'ENGEGAR	autoconfig
Recompte de buffers de TRANSMISSIÓ	tbc
Nivell de desencadenament de RECEPCIÓ	rtrig
Mòduls STREAMS que s'han de transferir en obert.	modules
Fitxer de mapatge d'ENTRADA	imap
Fitxer de mapatge de SORTIDA	omap
Fitxer de mapatge de CONJUNT DE CODIS	csmap
Caràcter d'INTERRUPCIÓ	intr
Caràcter de SORTIR	quit
Caràcter d'ESBORRAT	erase
Caràcter d'ELIMINACIÓ D'UN PROCÉS AMB L'ORDRE KILL	kill
Caràcter de FINAL DE FITXER	eof
Caràcter de FINAL DE LÍNIA	eol
2n caràcter de FINAL DE LÍNIA	eol2
Caràcter DSUSP (RETARDAR SUSPENSIÓ DE PROCÉS)	dsusp
Caràcter de SUSPENSIÓ DE PROCÉS	susp
Caràcter de LITERAL SEGÜENT	lnext
Caràcter d'INICI	start
Caràcter d'ATURADA	stop
Caràcter d'ESBORRAT DE PARAULA	werase
Caràcter de REIMPRESSIÓ DE LÍNIA	reprint
Caràcter de DESCARTAR	discard

Resolució de problemes de TTY

Hi ha diversos casos pràctics de resolució de problemes comuns de TTY.

El casos pràctics de resolució de problemes comuns de TTY inclouen els errors de `Regeneració massa ràpida`, els ports TTY bloquejats, i els fitxers de registre d'errors comuns, les ordres, i els missatges d'informes d'errors.

Errors de regeneració massa ràpida:

El sistema enregistra el nombre de processos **getty** creats per a un determinat tty en un curt període de temps. Si el nombre de processos **getty** creats en aquest període de temps es superior a 5, es visualitza l'error `Regeneració massa ràpida` a la consola i el sistema inhabilita el port.

El tty resta inhabilitat durant uns 19 minuts o fins que l'administrador del sistema torna a habilitar el port. Al final dels 19 minuts, el sistema habilita automàticament el port, donant com a resultat la creació d'un nou procés **getty**.

Entre les causes possibles s'inclouen les següents:
- Configuració incorrecta del mòdem
- Un port està definit i habilitat però no hi ha cap cable o dispositiu adjuntat a ell.
- Cable erroni o connexió fluixa
- Soroll a la línia de comunicacions
- Fitxers `/etc/environment` o `/etc/inittab` malmesos o falsificats
- La configuració del tty està malmesa
- El maquinari és defectuós

Dels següents procediments de recuperació, utilitzeu el que s'apliqui a la vostra situació.
- Configuració incorrecta del mòdem:

  Assegureu-vos que la detecció de portadora del mòdem *no* estigui forçada a un estat activat.

  Nota: Les instruccions següents s'apliquen als mòdems compatibles amb Hayes.
  1. Estabiu una connexió amb el mòdem i examineu el perfil actiu.
  2. Estabiu la detecció de portadora del mòdem en **&C1** en comptes de **&C0** (forçada a un estat activat). Utilitzeu les següents ordres AT del mòdem per establir i canviar l'atribut de portadora:
     ```
     AT&C1
     AT&W
     ```

     Nota:
     a. Consulteu l'apartat “Enviament d'ordres AT amb l'ordre cu” a la pàgina 596
     b. Consulteu la documentació del mòdem per obtenir més informació.
- Inhabilitar el tty, eliminar la definició de tty o adjuntar un dispositiu al port:
  – Per inhabilitar la definició de tty, utilitzeu l'ordre **chdev** tal com s'indica a continuació:
    ```
    chdev -l nom_tty -a Login=disable
    ```

    Després d'executar aquesta ordre el tty *no* s'habilita després d'un reinici del sistema.
  – Per eliminar la definició de tty:
    1. Inhabiliteu el port tty utilitzant l'ordre **pdisable**:
       ```
       pdisable nom_tty
       ```
    2. Elimineu la definició de tty del sistema. Vegeu l'apartat “Gestió de dispositius TTY” a la pàgina 582 per obtenir més informació.
- Comprovar si els cables són incorrectes o si les connexions estan fluixes:
  1. Comproveu el cablatge. Estrenyeu les connexions fluixes i substituïu el connectors malmesos o incorrectes.

2. Verifiqueu que el cablatge sospitós sigui un cable sèrie d'IBM P/N 6323741 o que el cable compleixi el mateix estàndard. Substituïu el cables malmesos o incorrectes.

- Eliminar el soroll de la línia de comunicacions:
  1. Verifiqueu que el cablatge té una longitud i una impedància correctes.
  2. Assegureu-vos que els anells toroides estan col•locats on calgui en els cables més llargs.
  3. Comproveu la disposició dels cables; no han d'estar a prop de llums fluorescents ni de motors.
- Comprovar si els fitxers `/etc/environment` o `/etc/inittab` estan malmesos o falsificats:
  1. Si és possible, compareu aquests fitxers amb còpies bones conegudes.
  2. Feu una còpia de seguretat dels fitxers i realitzeu els canvis que calguin.
  3. Al fitxer `/etc/environment`, elimineu les línies que *no* siguin:
     - línies en blanc
     - línies de comentaris
     - *variable=valor*
  4. Al fitxer `/etc/inittab`, examineu les línies dels dispositius tty. Si el tty està establert en off (desactivat), probablement el port tty no s'està utilitzant. Si no s'està utilitzant, elimineu la definició de tty o adjunteu un dispositiu al port.
- Eliminar la configuració de tty malmesa:
  1. Elimineu la definició de tty. Vegeu l'apartat “Gestió de dispositius TTY” a la pàgina 582 per obtenir més informació.
  2. Si voleu un enregistrament en còpia impresa de la definició de tty abans d'eliminar-la, feu clic a la tecla Imatge (F8 o Esc+8). Es capturarà la imatge de la pantalla actual i la copiarà al fitxer `smit.log` del directori `$HOME`.
  3. Llegiu la definició de tty. Consulteu les instruccions per afegir un tty a l'apartat “Gestió de dispositius TTY” a la pàgina 582.
- Localitzar el maquinari defectuós:
  1. Executeu els diagnòstics utilitzant l'ordre **diag**.
  2. Si es detecten problemes de maquinari, seguiu els procediments de resolució de problemes locals.

Informació d'enregistraments d'errors i identificadors d'enregistraments TTY:

Les ordres i els fitxers de registre següents estan relacionats amb els TTY

Ordre: **errclear**

Aquesta ordre suprimeix entrades de l'enregistrament d'errors. Es pot esborrar tot l'enregistrament amb `errclear 0` o bé es poden eliminar entrades amb tipus, classes o números d'ID d'error especificats.

Ordre: **errpt**

Aquesta ordre genera un informe d'errors a partir de les entrades de l'enregistrament d'errors del sistema. El format més utilitzat per a aquesta ordre és `errpt -a | pg`, que genera un informe detallat que comença amb els errors més actuals.

Fitxer: `/var/adm/ras/errlog`

Aquest fitxer emmagatzema instàncies d'errors i anomalies que troba el sistema. El fitxer `errlog` sol fer-se bastant gran. Si no s'esborra periòdicament, pot arribar a ocupar molt espai del disc dur. Utilitzeu l'ordre **errclear** mencionada anteriorment per esborrar aquest fitxer.

Fitxer: `/usr/include/sys/errids.h`

El fitxer de capçalera `errids.h` correlaciona els ID d'error amb les etiquetes d'error.

Els següents missatges d'informes d'errors comuns estan relacionats amb TTY:

Taula 100. Missatges d'error TTY

Missatge	Descripció	Comentaris
Core Dump	El programari ha finalitzat de forma anòmala	Aquest error s'enregistra quan un programari finalitza de forma anòmala i produeix una imatge de memòria buidada. És possible que els usuaris no surtin correctament de les aplicacions, que el sistema hagi estat aturat mentre els usuaris treballaven a l'aplicació o que el terminal de l'usuari s'hagi bloquejat i l'aplicació s'hagi aturat.
Errlog On	Errdaemon activat	El daemon **error** enregistra aquest error quan s'inicia l'enregistrament d'errors. El sistema desactiva automàticament l'enregistrament d'errors durant l'aturada del sistema.
Lion Box Died	S'ha perdut la comunicació amb el concentrador de 64 ports	El programa de control del concentrador de 64 ports enregistra aquest error si es perden les comunicacions amb el concentrador. Si rebeu aquest error, comproveu la data i la indicació de l'hora per veure si l'usuari hagués pogut provocar l'aparició d'aquest missatge. Una sèrie d'aquests errors pot indicar un problema amb l'adaptador de 64 ports o el seu maquinari associat.
Lion Buffero	Límit del buffer sobrepassat: Concentrador de 64 ports	Aquest error es produeix quan se sobrepassa el límit del buffer de maquinari en un concentrador de 64 ports. Si el dispositiu i el cablatge ho permeten, proveu d'afegir la conformitat de connexió RTS (Sol•licitud per enviar) a port i dispositiu. A més, proveu de baixar la velocitat en bauds.
Lion Chunknumc	Recompte de fragments erroni: Controlador de 64 ports	Aquest error es produeix quan el valor per al nombre de caràcters d'un fragment no coincideix amb els valors reals del buffer. Aquest error pot indicar un problema amb el maquinari; proveu d'executar els diagnòstics en els dispositius.
Lion Hrdwre	No es pot accedir a la memòria del controlador de 64 ports	El programa de control del concentrador de 64 ports enregistra aquest error si no pot accedir a la memòria del controlador de 64 ports.
Lion Mem ADAP	No es pot assignar memòria: Estructura ADAP	El programa de control del concentrador de 64 ports enregistra aquest error si la rutina **malloc** per a l'estructura adap no s'executa satisfactòriament.
Lion Mem List	No es pot assignar memòria: Llista TTYP_T	El programa de control del concentrador de 64 ports enregistra aquest error si la rutina **malloc** per a l'estructura de la llista *ttyp_t* no s'executa satisfactòriament.
Lion Pin ADAP	No es pot reservar memòria: Estructura ADAP	El programa de control del concentrador de 64 ports enregistra aquest error si la rutina **pin** per a l'estructura adap no s'executa satisfactòriament.

Taula 100. Missatges d'error TTY (continuació)

Missatge	Descripció	Comentaris
SRC	Error de programari	El daemon SRC (Controlador de recursos del sistema) enregistra aquest error en cas de què es produeixi alguna condició anòmala. Les condicions anormals es divideixen en tres àrees: subsistemes anòmals, anomalies en les comunicacions i altres anomalies.
Lion Unkchunk	Codi d'error desconegut del concentrador de 64 ports	Codi d'error: Nombre de caràcters del fragment rebut.
TTY Badinput	Cable o connexió erronis	El port genera entrades més de pressa del que el sistema pot consumir-les, i una part d'aquestes entrades es descarta. Normalment, les entrades errònies estan produïdes per un o més senyals RS-232 que canvien el seu estat de forma ràpida i repetida en un curt període de temps, la qual cosa fa que el sistema passi molt de temps al gestor d'interrupcions. Els errors de senyals normalment estan produïts per un connector fluix o trencat; per un cable erroni, no connectat a terra o no protegit; o bé per un enllaç de comunicacions "sorollós".
TTY Overrun	Límit de receptor sobrepassat a l'entrada	La majoria de ports TTY tenen un FIFO d'entrada de 16 caràcters, i el valor per defecte especifica que una interrupció s'envia després de que s'hagin rebut 14 caràcters. Aquest error es notifica quan el gestor d'interrupcions del programa de control ha esborrat el FIFO d'entrada i les dades s'han perdut. Les possibles solucions depenen del maquinari que estigueu utilitzant: • Adaptadors de 8 i 128 ports Verifiqueu que el control de flux està configurat correctament. Si és així, executeu els diagnòstics i substituïu el maquinari segons calgui. • Ports nadius Si el problema es produeix en un sistema inactiu, desplaceu la càrrega de treball a un altre port. Si aquesta acció corregeix el problema, actualitzeu el microprogramari del sistema. • Solucions generals – Reduïu el "Nivell de desencadenament de RECEPCIÓ" d'aquest port de 3 a 2 ó 1. – Reduïu la velocitat de línia en aquest port. – Examineu altres dispositius i processos per intentar reduir el temps que el sistema passa amb les interrupcions inhabilitades.

Taula 100. Missatges d'error TTY (continuació)

Missatge	Descripció	Comentaris
TTY TTYHOG	Límit de TTYHOG sobrepassat	Aquest error normalment es produeix per una discrepància en el mètode de control de flux que s'utilitza entre el transmissor i el receptor. El programa de control TTY ha intentat diverses vegades demanar al transmissor que faci una pausa, però l'entrada no s'ha aturat, la qual cosa ha fet que les dades s'hagin descartat. Comproveu els mètodes de control de flux configurats en cada extrem per tal d'assegurar-vos que s'utilitza el mateix mètode en cadascun d'ells.
TTY Parerr	Error de paritat/trama a l'entrada	Aquest error indica errors de paritat en les dades d'entrada als port asíncrons caràcter a caràcter. Normalment es produeix per una discrepància en els paràmetres de control de línia (paritat, velocitat de línia, grandària dels caràcters o nombre de bits d'aturada) entre el transmissor i el receptor. Els paràmetres de control de línia s'han d'establir de la mateixa manera en ambdós costats per tal que es puguin comunicar.
TTY Prog PTR	Error intern de programa de control	El programa de control tty enregistra aquest error si el punter *t_hptr* és nul.

Eliminació d'un port TTY bloquejat:

En aquest exemple d'eliminació d'un port bloquejat, se pressuposa que el port tty bloquejat és `tty0`.

Cal disposar d'autorització root per poder dur a terme aquest procediment.

1. Determineu si el tty actualment gestiona processos escrivint el següent:

   ```
   ps -lt tty0
   ```

   S'haurien de tornar resultats semblants al següent.

   ```
        F S UID   PID  PPID   C PRI NI ADDR    SZ    WCHAN    TTY  TIME CMD
   240001 S 202 22566  3608   0  60 20 781a   444 70201e44   tty0  0:00 ksh
   ```

   Aquí l'identificador de procés (PID) és 22566. Per eliminar aquest procés amb l'ordre kill, escriviu el següent:

   ```
   kill 22566
   ```

   Assegureu-vos que el procés s'ha eliminat satisfactòriament escrivint l'ordre `ps -lt tty0`. Si el procés encara existeix, afegiu el senyalador `-9` a l'ordre kill, tal com s'indica a l'exemple següent.

   Nota: No utilitzeu l'opció -9 per eliminar un procés slattach amb l'ordre kill. L'eliminació d'un procés slattach amb l'ordre kill amb el senyalador `-9` podria fer que un bloqueig slip romangués al fitxer `/etc/locks`. Suprimiu aquest fitxer de bloqueig per netejar després del procés slattach.

   ```
   kill -9 22566
   ```

2. Determineu si algun procés intenta utilitzar el tty escrivint el següent:

   ```
   ps -ef | grep tty0
   ```

   Nota: Si l'ordre **ps -ef | grep tty** torna alguna cosa semblant al següent resultat:

   ```
   root 19050      1    0    Mar 06       -  0:00 /usr/sbin/getty /dev/tty
   ```

   on "-" es visualitza entre la data (`Mar 06`) i l'hora (`0:00`), aquest tty no té el cable correcte. Aquest estat indica que el procés d'inici de sessió del sistema (getty) intenta obrir aquest tty i el procés d'obertura

es bloqueja perquè el senyal RS-232 Detecció de portadora de dades (DCD) no s'ha confirmat. Podeu corregir aquesta condició utilitzant l'adaptador de mòdem nul al cablatge. Quan getty pot obrir el port tty, "-" es substitueix pel número de tty. Per obtenir més informació sobre cables, consulteu l'apartat “Adjunció del mòdem amb els cables apropiats” a la pàgina 595.

Nota: L'ordre següent es pot utilitzar per inhabilitar el procés d'inici de sessió a `tty0`.

```
pdisable tty0
```

Si el procés s'ha eliminat satisfactòriament però el tty encara no respon, continueu en el pas següent.

3. Escriviu l'ordre següent:

   ```
   fuser -k /dev/tty0
   ```

   Aquesta ordre eliminarà qualsevol procés que es pugui trobar executant-se en el port i visualitzarà el PID. Si el tty encara no es pot utilitzar, continueu en el pas següent.

4. Utilitzeu l'ordre **strreset** per llançar les dades de sortida del port que està bloquejat a causa de les dades que no es poden lliurar perquè s'ha perdut la connexió amb l'extrem remot.

   Nota: Si l'ordre **strreset** arregla el port bloquejat, el port té un problema de cable o configuració perquè la pèrdua de la connexió amb l'extrem remot hauria fet que les dades col•locades al buffer s'haguessin llançat automàticament.

   Primer heu de determinar els números de dispositiu principal i secundari per al tty escrivint el següent:

   ```
   ls -al /dev/tty0
   ```

   Els resultats haurien de ser semblants als següents:

   ```
   crw-rw-rw-    1 root     system    18,   0 Nov  7  06:19 /dev/tty0
   ```

   Això indica que `tty0` té un número de dispositiu principal de 18 i un número de dispositiu secundari de 0. Especifiqueu aquests números quan utilitzeu l'ordre **strreset**, tal com s'indica a continuació:

   ```
   /usr/sbin/strreset -M 18 -m 0
   ```

   Si el tty encara no es pot utilitzar, continueu en el pas següent.

5. Desconnecteu el cable del port tty bloquejat i torneu-lo a adjuntar. L'AIX utilitza el senyal DCD (Detecció de portadora de dades) per determinar la presència d'un dispositiu adjuntat al port. Si s'elimina el senyal DCD, el fet de desconnectar i tornar a connectar el cable eliminarà en molts casos els processos bloquejats.

   Per determinar la ubicació del port on està configurat el tty, escriviu l'ordre següent:

   ```
   lsdev -Cl tty0
   ```

   Els resultats haurien de ser semblants als següents:

   ```
   tty0    Available   00-00-S1-00  Asynchronous Terminal
   ```

   La tercera columna de la sortida anterior indica el codi d'ubicació del tty. En aquest exemple, `S1` indica que el port en sèrie està configurat per al port en sèrie nadiu 1. Per obtenir més informació sobre com interpretar els codis d'ubicació, consulteu Codis d'ubicació de dispositius a *Operating system and device management*.

   Si el tty encara no es pot utilitzar, continueu en el pas següent.

6. Llanceu el port utilitzant **stty-cxma**. Escriviu el següent:

   ```
   /usr/lbin/tty/stty-cxma flush tty0
   ```

   Aquesta ordre està pensada per als tty configurats als ports dels adaptadors de 8 i 128 ports. No obstant això, en alguns casos pot utilitzar-se satisfactòriament per llançar altres ports tty.

   Si el tty encara no es pot utilitzar, continueu en el pas següent.

7. Al teclat del terminal bloquejat, mantingueu premuda la tecla `Control` i feu clic a `Q`. La sortida que estigui suspesa es reprendrà enviant un caràcter **Xon**.

   Si el tty encara no es pot utilitzar, continueu en el pas següent.
8. A vegades un programa obrirà un port tty, modificarà alguns atributs i tancarà el port sense restablir els atributs en els seus estats originals. Per corregir-ho, dugueu el tty a un estat DEFINIT i després féu que estigui disponible escrivint el següent:

   ```
   rmdev -l tty0
   ```

   Aquesta ordre deixa la informació sobre el tty a la base de dades però fa que el tty no estigui disponible al sistema.

   L'ordre següent reactiva el tty:

   ```
   mkdev -l tty0
   ```

   Si el tty encara no es pot utilitzar, considereu la possibilitat de desplaçar el dispositiu a un altre port i de configurar un tty en aquesta ubicació fins que el sistema es pugui tornar a engegar. Si l'acció de tornar a engegar no elimina el port, el més probable és que tingueu un problema de maquinari. Consulteu l'informe d'errors per veure els problemes de maquinari del port escrivint el següent:

   ```
   errpt -a | pg
   ```

Algunes de les ordres anteriors no funcionaran i donaran un error de mètode que indica que el dispositiu està ocupat. Això és a causa del procés que s'executa al tty. Si cap dels passos anteriors no allibera el tty bloquejat, com a últim recurs, reengegueu el sistema AIX i llanceu el kernel per què el procés desaparegui.

Mòdems

Els mòdems proporcionen comunicacions en sèrie a través de línies telefòniques normals. Els conceptes sobre els mòdems inclouen els estàndards, la configuració general del mòdem i els consells de configuració específics per als mòdems populars.

Un *mòdem* és un dispositiu que permet connectar un ordinador amb un altre a través de línies telefòniques normals. El sistema telefònic actual no té capacitat per portar els canvis de voltatge necessaris per a una connexió digital directa. Un mòdem vença aquesta limitació modulant la informació digital en tons d'àudio que es transmeten a través de la línia telefònica i desmodulant aquests tons en informació digital a la recepció. Els mòdems normalment s'utilitzen amb els BNU (Basic Network Utilities) o altres implementacions del Programa de còpia UNIX a UNIX (UUCP). Un mòdem d'alta velocitat (14.400 bps o superior) també pot utilitzar-se amb el Protocol d'interfície de línia sèrie (SLIP) per proporcionar connectivitat TCP/IP (Transmission Control Protocol/Internet Protocol).

Sovint, el terme *baud* s'utilitza per indicar la velocitat del mòdem en comptes de bps. De fet, baud és una mesura de la velocitat de modulació. En el mòdems més antics, només es codificava 1 bit en cada canvi de senyal, amb la qual cosa la velocitat en bauds era igual a la velocitat del mòdem. No obstant això, els mòdems que funcionen a velocitats més altes, encara funcionen generalment a 2.400 (o fins i tot 1.200) bauds i codifiquen dos o més bits per canvi de senyal. La velocitat en bps del mòdem es calcula multiplicant els bauds pel nombre de bits de dades per senyal (per exemple, 2.400 bauds x 6 bits per canvi de senyal = 14.400 bits per segon). Els mòdems més moderns es poden comunicar a diferents velocitats (per exemple, 28.800, 14.400, 9.600, 7.800, 4.800 i 2.400 bps).

Estàndards de telecomunicacions

Les velocitats més antigues de 300, 1.200 i 2.400 bps estaven ben definides. No obstant això, a mesura que els fabricants de mòdems van començar a dissenyar mètodes per aconseguir velocitats més altes, cada fabricant va començar a utilitzar el seu propi mètode propietari incompatible amb els mòdems d'altres fabricants. Actualment, la ITU-TSS (anteriorment el Comitè Consultiu de les Nacions Unides per a la Telefonia i Telegrafia Internacional, CCITT) defineix estàndards per a la majoria de comunicacions d'alta velocitat.

Fins i tot els mòdems d'alta velocitat són molt més lents que altres mètodes de comunicació informàtica. Un mòdem d'alta velocitat pot funcionar a 28.800 bps, però una connexió Ethernet funciona a 10.000.000 bps. Per augmentar la productivitat de les dades, els mòdems d'alta velocitat normalment ofereixen un o més algorismes de compressió de dades. Aquests algorismes poden augmentar la productivitat d'un mòdem d'alta velocitat a velocitats de 57.600 bps (si la velocitat de dades és de 14.400 bps) o de 115.200 bps (si la velocitat de dades és de 28.800 bps). Cal tenir en compte que aquests algorismes de compressió són sensibles a les dades que s'estan transmeten. Si les dades ja s'han comprimit (per exemple, amb l'ordre **compress**), els mètodes de compressió de dades dels mòdems d'alta velocitat ofereixen pocs avantatges o no cap, i fins i tot poden reduir la productivitat de les dades. Quan s'utilitza un mòdem amb tecnologia de compressió de dades, la velocitat de la connexió DTE/DCE (data terminal equipment/data circuit-terminating equipment) entre l'ordinador i el mòdem és igual o superior a la velocitat nominal de dades de la connexió entre mòdems. Per exemple, amb un mòdem V.32*bis* amb compressió de dades V.42*bis*, la velocitat de dades del mòdem (la velocitat a la que el mòdem es comunica a través de línies telefòniques) és de 14.400 bps. Quan la compressió V.42*bis* està activa, la productivitat real de les dades pot arribar a 57.600 bps. Per acomodar la major productivitat que ofereix la compressió de dades, la velocitat de l'enllaç entre l'ordinador i el mòdem s'ha d'establir en 57.600 bps.

La ITU-TSS defineix estàndards per a les comunicacions d'alta velocitat, inclosos els algorismes de compressió de dades. Els estàndards ITU-TSS normalment s'anomenen V.*nn*, on *nn* és un número. Un altre estàndard una mica menys comú és el Microcom Networking Protocol (MNP). Disponible en les versions (anomenades classes) 1-9, l'MNP és un protocol d'alt rendiment i alta velocitat que va aparèixer relativament aviat i va esdevenir com una espècie d'estàndard de facto abans de l'aparició dels estàndards ITU-TSS.

Transmissions semidúplex i dúplex:

Quan s'estudien els estàndards de telecomunicacions, és important entendre les diferències entre les transmissions semidúplex i dúplex.

En una transmissió *semidúplex* (HDX), un sistema envia un paquet de dades i l'altre sistema el rep. No es pot enviar un altre paquet de dades fins que el sistema receptor envia una confirmació de tornada a l'emissor.

En una transmissió *dúplex* (FDX), tant el sistema emissor com el sistema receptor es poden comunicar entre sí simultàniament; és a dir, els dos mòdems poden enviar i rebre dades al mateix temps. Això significa que un mòdem pot estar rebent un paquet de dades mentre confirma la recepció d'un altre.

Estàndards de comunicacions ITU-TSS:

A continuació es descriuen alguns estàndards de comunicacions comuns definits pels ITU-TSS.

Tingueu en compte que aquesta llista només es una llista parcial. Per obtenir una llista completa, consulteu el lloc web d'Internet de la International Telecommunication Union.

Element	Descripció
V.29	Estàndard ITU-TSS per a comunicacions semidúplex a 9600 bps.
V.32	Estàndard ITU-TSS per a comunicacions dúplex a 9600 bps.
V.32*bis*	Estàndard ITU-TSS per a comunicacions a 14.400. V.32*bis* és una revisió de l'estàndard V.32.
V.34	Estàndard ITU-TSS per a comunicacions a 33.600 bps. Tingueu en compte que aquest estàndard arriba a velocitats de dades de 33.600 bps mitjançant codificacions de varis bits, enlloc de l'esquema de compressió de dades utilitzat per NNP Class 9. S'ha fet referència anteriorment a aquest estàndard com a V.*fast*.
V.42	Procediments de correcció d'errors ITU-TSS per DCE mitjançant la conversió d'asíncron a síncron.
V.42*bis*	Estàndard de compressió de dades ITU-TSS revisat.

Microcom Networking Protocol (MNP):

Un altre estàndard de facto és el **Microcom Networking Protocol (MNP)**, que originàriament va ser desenvolupat per l'empresa Microcom, Inc.

Disponible en les versions (anomenades classes) 1-9, **MNP** és un protocol d'alt rendiment i alta velocitat que ja existia abans de l'aparició dels estàndards ITU-TSS. Amb l'**MNP**, el mòdem remot detecta els errors en els paquets de dades transmesos i sol•licita una retransmissió del paquet de dades erroni. La seva capacitat de reconèixer i corregir ràpidament els errors en les dades fa que l'**MNP** sigui actualment un dels protocols més comuns.

La taula següent especifica els estàndards de comunicacions **MNP**.

Element	Descripció
MNP Classe 1	Un mètode orientat a octets, semidúplex i asíncron que permet transferir dades a una eficiència del 70%. Aquest estàndard no és comú en els mòdems moderns.
MNP Classe 2	És la versió dúplex de l'**MNP Classe 1** que tampoc és comuna en els mòdems moderns.
MNP Classe 3	Un mètode dúplex, orientat a bits i síncron que permet transferir dades a una eficiència del 108%. S'aconsegueix una eficiència superior al 100% perquè s'eliminen els bits d'inici/aturada necessaris per a una connexió asíncrona. Les DTE/DCE entre el mòdem i el sistema encara són asíncrones.
MNP Classe 4	Una millora de l'**MNP Classe 3** que inclou un mecanisme per variar la grandària dels paquets (acoblament de paquets adaptatiu) i un sistema d'eliminar la sobrecàrrega administrativa redundant (optimització de fase de dades). Un mòdem **MNP Classe 4** ofereix una eficiència aproximada del 120%.
MNP Classe 5	Inclou la compressió de dades a més de les característiques de la Classe 4. Un mòdem **MNP Classe 5** ofereix una eficiència del 200%.
MNP Classe 6	Permet la incorporació de diverses tècniques de modulació incompatibles en un mòdem (negociació d'enllaç universal). Això permet als mòdems **MNP Classe 6** iniciar la comunicació a una velocitat més lenta i negociar una transició a una velocitat més alta. La **Classe 6** també inclou un esquema de duplicació estadística que assigna dinàmicament la utilització de la modulació semidúplex per simular el servei dúplex. Totes les característiques de l'**MNP Classe 5** estan suportades.
MNP Classe 7	Incorpora la compressió de dades millorada. En combinació amb la Classe 4, es poden assolir eficiències del 300%.
MNP Classe 8	No aplicable.
MNP Classe 9	Combina la compressió de dades millorada amb la tecnologia V.32 per a assolir velocitats de dades de fins a 28.800 bps.

Consideracions sobre el mòdem

Els requisits de la interfície del mòdem per a l'usuari general poden variar.

La configuració d'un mòdem connectat a aquest sistema operatiu és diferent de la d'un ordinador personal (PC) o estació de treball.

Mòdems suportats:

Qualsevol mòdem que sigui compatible amb l'EIA 232 i pugui tornar resultats com a resposta a una ordre pot connectar-se a aquest sistema operatiu.

Utilització del senyal DCF (Detecció de portadora de dades):

El servidor utilitza el senyal DCD (Detecció de portadora de dades) per supervisar l'estat real d'un mòdem.

Si el senyal DCD en el port del mòdem està "activat", el servidor creu que el mòdem està sent utilitzat. Per tant, és important conèixer les circumstàncies que fan que aquest senyal es vegi forçat a un estat "activat". El senyal DCD es pot activar pels següents motius:

- La utilització de **clocal** als atributs stty per al camp de temps d'execució del panell **Configuració de TTY** de la SMIT.

- Tenir el camp Ignorar detecció de portadora establert en **enable** al panell **Configuració de TTY** de la SMIT per als tty connectats a un adaptador de 128 ports.
- El mòdem força l'activació del senyal DCD amb ordres AT o commutadors.
- El port tty ja està sent utilitzat per una aplicació.

  Nota: Quan els mòdems estableixen una connexió amb un altre mòdem, el mòdem activa el senyal CD. La majoria de valors per defecte del mòdem mantenen sempre "activat" aquest senyal fins i tot quan el mòdem està inactiu. El senyal CD no s'ha de forçar a un estat "activat".

Velocitats DTE (Data Terminating Equipment) or DCE (Data Circuit-Terminating Equipment):

Les velocitats DTE (Data Terminating Equipment) i DCE (Data Communication Equipment) s'utilitzen per descriure dos grups diferents de maquinari.

El terme DTE s'utilitza principalment per als dispositius que mostren informació de l'usuari. També inclou els dispositius que emmagatzemen o generen dades per a l'usuari. Tant les unitats del sistema com els terminals i les impressores estan dins de la categoria DTE.

DCE inclou qualsevol dispositiu que pot utilitzar-se per accedir a un sistema a través de línies de telecomunicacions. Les formes més habituals de DCE són els mòdems i els multiplexors.

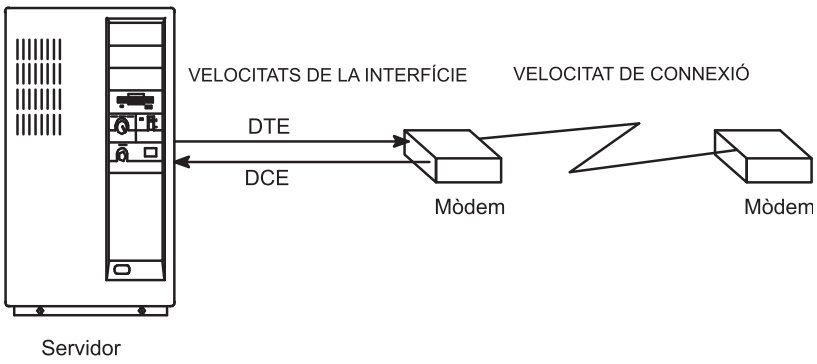


Figura 37. Consideracions sobre la velocitat del mòdem

Amb la comunicació en sèrie d'aquest sistema operatiu que implica mòdems, tal com es mostra a la il•lustració anterior, cal fer tres consideracions importants:
- Velocitat de la interfície DTE (servidor a mòdem). És la velocitat a la que el servidor es comunica amb el mòdem.
- Velocitat de la interfície DCE (mòdem a servidor), a vegades anomenada "velocitat de la interfície de port en sèrie". És la velocitat a la que el mòdem es comunica amb el servidor.
- Velocitat de la connexió (mòdem a mòdem). És la velocitat a la que un mòdem es comunica o "parla" amb un altre mòdem.

La majoria de mòdems moderns d'alta velocitat permeten que la velocitat de la interfície DCE sigui diferent de la velocitat de la connexió. D'aquesta manera, la velocitat DTE es pot bloquejar a una única velocitat en bauds mentre que la velocitat de la connexió pot fluctuar, amunt o avall segons calgui, per permetre la comunicació correcta entre els mòdems.

Els mòdems moderns d'alta velocitat retenen a un buffer les dades que s'han de transmetre al servidor i les envien quan el sistema pot acceptar-les. També poden retenir a un buffer les dades que s'han de transmetre a l'altre mòdem i enviar-les quan el mòdem remot pot acceptar-les. Per a aquest tipus de transmissió de dades cal que el mòdem i el servidor utilitzin un *control de flux*.

Senyals de control del mòdem:

Sovint els mòdems s'utilitzen per iniciar i rebre crides. Per això és important programar el mòdem per què negociï una connexió a la velocitat més alta possible i es reinicialitzi a un estat conegut després de que s'hagi aturat una connexió.

El servidor commutarà el senyal DTR (Terminal de dades preparat) d'activat a desactivat per indicar al mòdem que finalitzi la connexió. La majoria de mòdems es poden configurar per què es reinicialitzin quan es produeix aquesta transició d'activat a desactivat del senyal DTR.

Nota: El tty es pot configurar per no eliminar el senyal DTR inhabilitant el senyalador **hupcl** en els atributs de temps d'execució stty.

Per tal que la connexió entre el servidor i el mòdem sigui completament funcional, el cablatge ha de tenir les següents qualificacions:

- Ha de complir les especificacions.
- Ha d'estar degudament protegit.
- S'han de proporcionar el següents senyals: RxD, TxD, RTS, CTS, SG, DCD i DTR.

  Nota: L'adaptador asíncron de 16 ports no proporciona suport per als senyals RTC i CTS. Per tant, és impossible utilitzar el control de flux de maquinari RTS/CTS amb aquest adaptador.

Si s'han de transferir dades binàries amb un mòdem d'aquest adaptador, cal utilitzar un protocol de transferència de fitxers que detecti les dades incorrectes i reenviï les dades que falten (per exemple, Xmodem, zmodem, Kermit i UUCP).

A continuació es descriuen els senyals que utilitza el servidor:

Senyal	Descripció
FG	Trama de terra. Pota 1 de l'especificació EIA 232D que proporciona una protecció de cable. Utilitzat correctament, el senyal s'adjunta a la pota 1 només d'un costat del cable i es connecta a una beina metàl•lica que protegeix el cable.
TxD	Dades de transmissió. Pota 2 de l'especificació EIA 232D. Les dades es transmeten en aquest senyal. Està controlat pel servidor.
RxD	Dades de recepció. Pota 3 de l'especificació EIA 232D. Les dades enviades pel mòdem es reben en aquest senyal, que està controlat pel mòdem.
RTS	Sol•licitud per enviar. Pota 4 de l'especificació EIA 232D. S'utilitza quan el control de flux RTS/CTS està habilitat. Aquest senyal s'activa quan el sistema està preparat per enviar dades i s'elimina quan el sistema vol que el mòdem aturi l'enviament de dades.
CTS	Preparat per emetre. Pota 5 de l'especificació EIA 232D. S'utilitza quan el control de flux RTS/CTS està habilitat. Aquest senyal s'activarà quan el mòdem estigui preparat per enviar o rebre dades. S'eliminarà quan el mòdem vulgui que el servidor aturi l'enviament de dades. Està controlat pel mòdem.
DSR	Conjunt de dades preparat. Pota 6 de l'especificació EIA 232D. Senyal que indica al servidor que el mòdem es troba en un estat preparat per a l'ús. Està controlat pel mòdem.
SG	Senyal de terra. Pota 7 de l'especificació EIA 232D. Aquest senyal proporciona un voltatge de referència per als altres senyals.
DCD	Detecció de portadora de dades. Pota 8 de l'especificació EIA 232D. Proporciona un senyal al servidor que indica que el mòdem està connectat amb un altre mòdem. Quan s'activa aquest senyal, els programes que s'executen al servidor poden obrir el port. Està controlat pel mòdem.
DTR	Terminal de dades preparat. Pota 20 de l'especificació EIA 232D. Proporciona un senyal al mòdem que indica que el servidor està encès i preparat per acceptar una connexió. Aquest senyal s'elimina quan el servidor vol que el mòdem elimini la connexió amb un altre mòdem. S'activa quan s'està obrint el port. Està controlat pel servidor.
RI	Indicador de timbre. Pota 22 de l'especificació EIA 232D. Proporciona un senyal al servidor que indica que el mòdem està rebent una crida. S'utilitza molt poc i no és necessari per a les operacions més comuns. Està controlat pel mòdem.

Cablatge del mòdem

A les taules següents es mostra un resum de la informació de cables necessària per adjuntar correctament un mòdem a qualsevol dels controladors en sèrie.

Adaptador/controlador	Número(s) de peça d'IBM
Sèrie nadiu (S1 o S2)	00G0943*, 6326741
Controlador de 2 ports	00G0943*, 6326741
Controlador de 8 ports	6323741
Controlador de 128 ports	43G0935, 6323741

Número de peça d'IBM	Descripció	Longitud en peus
00G0943*	Pont del port en sèrie (en espiral)	0,33
6323741	Asíncron	10
43G0935	Cable convertidor RJ-45 a DB25	2

*Aquest número de peça no és obligatori en alguns tipus de màquines.

Configuració del dispositiu TTY al sistema operatiu

Utilitzeu la SMIT (System Management Interface Tool) per definir un port tty per a l'adjunció del dispositiu.

La majoria de camps són per al tipus de dispositiu general. L'únic camp que pot afectar el mòdem és el camp Habilitar INICI DE SESSIÓ amb els següents valors:

Element	Descripció
DISABLE	No s'executa cap procés getty al port. Utilitzeu aquest valor només per a ports de mòdem de marcatge de sortida.
ENABLE	S'executa un procés getty al port. Utilitzeu aquest valor només per a mòdems de marcatge d'entrada.
SHARE	S'executa un procés getty al port, però el procés getty permet als programes fer marcartges d'entrada i sortida d'aquest port sense canviar manualment als valors disable o enable. Utilitzeu aquest valor per a un ús bidireccional del port.
DELAY	S'executa un procés getty al port en mode bidireccional, però no s'envia cap indicador fins que el procés getty rep una pulsació de tecla de l'usuari.

Camps específics de l'adaptador asíncron de 128 ports:

Element	Descripció
Forçar portadora o ignorar detecció de portadora	disable*
Realitzar un processament preparat a l'adaptador	disable

Nota: Aquest valor indicat amb un asterisc (*) s'estableix en inhabilitat si s'utilitza el connector RJ-45 de 10 potes. Aquest valor ha d'estar habilitat si s'utilitza el connector RJ-45 de 8 potes.

Adjunció del mòdem amb els cables apropiats

El primer pas a l'hora de configurar un mòdem és adjuntar el mòdem amb els cables apropiats.

A continuació es mostra una llista amb els números de peça i les seves descripcions.

6323741
Cable asíncron, EIA-232; s'utilitza per adjuntar tots els dispositius asíncrons; a vegades s'utilitza amb altres acoblaments de cables.

59F3740
Connector d'intèrpret d'ordres D de 10 a 25 potes que s'utilitza per adjuntar el cable asíncron 6323741 al ports en sèrie nadius S1 i S2 tal com es mostra a la figura següent.

Figura 38. Connector de 10 a 25 potes

Aquesta il•lustració mostra un connector de 10 a 25 potes.

A continuació es mostren alguns exemples de connexions de cables:

1. Per adjuntar un mòdem al port en sèrie nadiu S1, utilitzeu els següents cables:

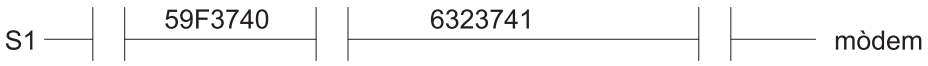


Figura 39. Mòdem a l'acoblament de cables del port en sèrie nadiu

   Aquesta il•lustració mostra un cable 59F3740 a l'extrem del port en sèrie i un cable 6323741 a l'extrem del mòdem.

2. Per adjuntar un mòdem a un acoblament de cables de la interfície de l'adaptador asíncron de 8 ports (EIA-232), utilitzeu els cables següents:

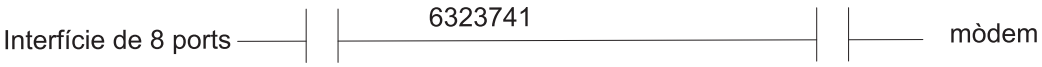


Figura 40. Acoblament de cables de la interfície de 8 ports al mòdem

   Aquesta il•lustració mostra una interfície de 8 ports connectada a un mòdem amb un cable 6323741.

Addició d'un TTY per al mòdem

Utilitzeu aquesta informació a l'hora d'afegir un tty per a un mòdem.

En primer lloc, assegureu-vos que el sistema està encès i que el mòdem està apagat. Utilitzeu el camí d'accés ràpid de la SMIT `smit mktty`.

Configuració del mòdem

Utilitzeu només un dels dos mètodes que es presenten a continuació per configurar el mòdem.

Si teniu instal•lats els BNU (Basic Networking Utilities), consulteu l'apartat "Enviament d'ordres AT amb l'ordre cu". Si no teniu instal•lats els BNU, consulteu l'apartat "Enviament d'ordres AT utilitzant un programa C" a la pàgina 597. Per obtenir informació sobre com instal•lar els BNU, consulteu l'apartat "Basic Networking Utilities (BNU)" a la pàgina 432.

Enviament d'ordres AT amb l'ordre cu:

Si teniu instal•lats els BNU (Basic Network Utilities) (BNU), utilitzeu l'ordre **cu** per configurar un mòdem tal com s'explica a continuació.

Les ordres i els valors que es descriuen en aquesta secció configuren un mòdem compatible amb Hayes amb els paràmetres bàsics necessaris per al funcionament en els ports en sèrie del servidor.

1. Afegiu la línia següent al fitxer **/usr/lib/uucp/Devices**. No afegiu la línia si ja existeix al fitxer. (Substituïu # pel numero del port).

   ```
   Direct tty# - Any direct
   ```

2. Verifiqueu que tty està inhabilitat escrivint el següent:

   ```
   pdisable tty#
   ```

3. Escriviu l'ordre següent:

```
cu -ml tty#
```

Hauríeu de veure un missatge que diu `Connectat`.

4. Verifiqueu que teniu l'atenció del mòdem escrivint el següent:
   ```
   AT
   ```

   El mòdem hauria de respondre amb `OK`. Si no ho fa, consulteu l'apartat "Resolució de problemes del mòdem" a la pàgina 599.

   Per obtenir més informació sobre les ordres **AT** i les seves descripcions, consulteu l'apartat "Ordres AT" a la pàgina 601.
5. En funció de l'opció getty que hagueu seleccionat, especifiqueu una de les següents ordres: Substitutiu el dispositiu tty per *n*.
   - `penable tty`*n*
   - `pshare tty`*n*
   - `pdelay tty`*n*
   - `pdisplay tty`*n*

Ara el mòdem està configurat amb les ordres bàsiques necessàries per satisfer la majoria de les demandes de comunicacions en sèrie del sistema operatiu. Si teniu problemes, invoqueu l'ordre **cu -dl** per iniciar una traça de diagnòstic a la connexió.

Enviament d'ordres AT utilitzant un programa C:

Si no heu pogut configurar el mòdem utilitzant l'ordre **cu**, o si no teniu instal•lats els BNU, intenteu executar el següent programa C.

Creeu un fitxer anomenat `motalk.c` que contingui el següent codi. Deseu el fitxer. Compileu-lo i executeu-lo seguint les instruccions especificades en els comentaris del programa.

```
/*************************************************************/
/*  MoTalk - Un programa "C" per a la configuració del mòdem. */
/*           Aquest programa només pretén ser una ajuda i   */
/*           no està suportat per IBM. */
/*                  compileu:  cc -o motalk motalk.c       */
/*                  Utilització:  motalk /dev/tty? [speed]      */
/*************************************************************/
#include <errno.h>
#include <stdio.h>
#include <signal.h>
#include <fcntl.h>
#include <termio.h>
FILE *fdr, *fdw;
int fd;
struct termio term_save, stdin_save;
void Exit(int sig)
{
   if (fdr) fclose(fdr);
   if (fdw) fclose(fdw);
   ioctl(fd, TCSETA, &term_save);
   close(fd);
   ioctl(fileno(stdin), TCSETA, &stdin_save);
   exit(sig);
}
main(int argc, char *argv[])
{
   char *b, buffer[80];
   int baud=0, num;
   struct termio term, tstdin;
   if (argc < 2 || !strcmp(argv[1], "-?"))
   {
```

```
   fprintf(stderr, "Usage: motalk /dev/tty? [speed]\n");
   exit(1);
}
if ((fd = open(argv[1], O_RDWR | O_NDELAY)) < 0)
{
   perror(argv[1]);
   exit(errno);
}
if (argc > 2)
{
   switch(atoi(argv[2]))
   {
      case   300: baud = B300;
                  break;
      case  1200: baud = B1200;
                  break;
      case  2400: baud = B2400;
                  break;
      case  4800: baud = B4800;
                  break;
      case  9600: baud = B9600;
                  break;
      case 19200: baud = B19200;
                  break;
      case 38400: baud = B38400;
                  break;
      default:    baud = 0;
                  fprintf(stderr, "%s: %s is an unsupported baud\n", argv[0],argv[2]);
                  exit(1);
      }
   }
/* Deseu l'entrada estàndard i l'estat tty i intercepteu alguns senyals */
ioctl(fd, TCGETA, &term_save);
ioctl(fileno(stdin), TCGETA, &stdin_save);
signal(SIGHUP, Exit);
signal(SIGINT, Exit);
signal(SIGQUIT, Exit);
signal(SIGTERM, Exit);
/*  Estabiu l'entrada estàndard en mode sense format, sense eco */
ioctl(fileno(stdin), TCGETA, &tstdin);
tstdin.c_iflag = 0;
tstdin.c_lflag &= ~(ICANON | ECHO);
tstdin.c_cc[VMIN] = 0;
tstdin.c_cc[VTIME] = 0;
ioctl(fileno(stdin), TCSETA, &tstdin);
/*  Estabiu l'estat tty */
ioctl(fd, TCGETA, &term);
term.c_cflag |= CLOCAL|HUPCL;
if (baud > 0)
{
   term.c_cflag &= ~CBAUD;
   term.c_cflag |= baud;
}
term.c_lflag &= ~(ICANON | ECHO); /* per forçar el mode sense format */
term.c_iflag &= ~ICRNL; /* per evitar línies en blanc no necessàries */
term.c_cc[VMIN] = 0;
term.c_cc[VTIME] = 10;
ioctl(fd, TCSETA, &term);
fcntl(fd, F_SETFL, fcntl(fd, F_GETFL, 0) & ~O_NDELAY);
/*  Obriu tty per a lectura i escriptura */
if ((fdr = fopen(argv[1], "r")) == NULL )
{
   perror(argv[1]);
   exit(errno);
}
if ((fdw = fopen(argv[1], "w")) == NULL )
{
```

```
      perror(argv[1]);
      exit(errno);
   }
   /*  Comuniqueu-se amb el mòdem */
   puts("Ready... ^C to exit");
   while (1)
   {
      if ((num = read(fileno(stdin), buffer, 80)) > 0)
         write(fileno(fdw), buffer, num);
      if ((num = read(fileno(fdr), buffer, 80)) > 0)
         write(fileno(stdout), buffer, num);
      Exit (0);
   }
}
```

Utilització de mòdems Hayes i compatibles amb Hayes

Utilitzeu aquest procediment per a mòdems Hayes i compatibles amb Hayes.

1. Canvieu els valors tty, si és necessari, utilitzant el camí d'accés ràpid de la SMIT, `smit chtty`. Per exemple, us pot interessar canviar el camp Habilitar INICI DE SESSIÓ a **Compartir** o **Habilitar**.
2. Afegiu la línia següent al fitxer `/usr/lib/uucp/Systems`:

   ```
   hayes Nvr HAYESPROG 2400
   ```
3. Afegiu la línia següent al fitxer `/usr/lib/uucp/Devices`:

   ```
   # Només per programar el mòdem Hayes:
   HAYESPROG tty0 - 2400 HayesProgrm2400
   #entrada ACU normal:
   ACU tty0 - Any hayes
   ```
4. Afegiu la línia següent al fitxer `/usr/lib/uucp/Dialers`:

   ```
   # Aquesta entrada NOMÉS s'utilitza per PROGRAMAR el mòdem:
   # les 3 línies següents s'han de convertir en una sola:
   HayesProgrm2400     =,-,     "" \d\dAT\r\c OK AT&F\r\c OK ATM1\r\c OK
   AT&D3\r\c OK AT&K3&C1\r\c OK ATL0E0Q2\r\c OK ATS0=1\r\c OK AT&W\r\c
   OK
   hayes     =,-,     "" \dAT\r\c OK ATDT\T\d\r\c CONNECT
   ```
5. Per programar el mòdem, especifiqueu l'ordre `cu -d hayes`. Aquesta ordre utilitza l'ordre **cu** per programar el mòdem. Com que no s'estableix cap connexió amb un altre sistema, l'ordre no s'executarà correctament. El mòdem es programa si a la sortida es visualitza `sendthem AT&W` i després `OK got it`.

   Si no realitzeu transferències de fitxers binaris ni utilitzeu els BNU, deixeu de banda l'ordre **&K3** i establiu XON com el control de flux a utilitzar. No obstant això, resulta més eficaç utilitzar el control de flux de maquinari (en comptes de la conformitat de connexió XON-XOFF). Per fer-ho, utilitzeu els valors i les entrades `Dialers` del pas següent.
6. Un cop programat el mòdem, podeu configurar el programa de control de dispositius del sistema per què utilitzi el control de flux de maquinari. S'està utilitzant la SMIT (camí d'accés ràpid `smit chtty`), canvieu el control de flux a RTS. Consulteu els manuals del mòdem per esbrinar si el mòdem dóna suport al control de flux de maquinari.

Resolució de problemes del mòdem

Si teniu problemes quan utilitzeu un mòdem amb el vostre ordinador, tingueu en compte els punts següents:

- Alguns mòdems són sensibles a les majúscules i minúscules. Utilitzeu lletres majúscules per a les ordres **AT**.
- Durant l'operació normal, és preferible reinicialitzar el mòdem quan s'elimini el senyal DTR (valor &D3). No obstant això, quan es configura el mòdem per primera vegada, s'aconsella no reinicialitzar el mòdem si s'elimina el senyal DTR (valor &D2). Si el mòdem es reinicialitza ell mateix, es perdran tots els valors programats que no s'han desat a la memòria del mòdem.

No reinicialitzar el mòdem també protegeix els canvis quan s'estableix &C1. Canviar l'estat del senyal Detecció de portadora (CD) pot fer que la línia de detecció de portadora commuti en alguns mòdems, la qual cosa fa que l'ordre **cu** elimini la línia. És possible que us interessi configurar el mòdem a &D3 un cop s'ha realitzat la configuració final.

- Malgrat que les ordres descrites en aquesta col•lecció de temes són estàndard per a la majoria de mòdems compatibles amb Hayes, no hi ha cap garantia que siguin estàndard per al vostre mòdem. Compareu les ordres amb la documentació del vostre mòdem abans de continuar.

Una manera còmoda de depurar qualsevol problema amb el mòdem és extreure el mòdem i connectar un terminal ASCII (amb un adaptador o mòdem nul) al mateix port i cablatge que el mòdem. Configureu el terminal amb la mateixa velocitat de línia, bits per caràcter i paritat que el mòdem. Si el port està habilitat per a iniciar la sessió, s'hauria de visualitzar un indicador d'inici de sessió a la pantalla. Si l'indicador es visualitza a la pantalla del terminal, el problema queda aïllat ràpidament a la configuració del mòdem.

Els consells següents l'ajudaran a solucionar els problemes relacions amb les connexions via mòdem:

Taula 101. Problemes i solucions del mòdem

Problema	Resolució
Regeneració massa ràpida	**init** regenera el programa **getty**.
Missatges a la consola o errpt	Si **init** veu que ha de regenerar un programa més de cinc vegades en 225 segons, mostrarà el missatge a la consola i no el regenerarà durant un període de temps. La solució passa per esbrinar per què s'està morint el programa **getty**. Pot haver-hi diverses causes: • Valors incorrectes del mòdem, normalment com a conseqüència de tenir activat el senyal CD al mòdem o cablatge i també de tenir activada la funció "eco" o "resposta a ordres". (El senyal CD també es pot pressuposar que està activat afegint clocal als modes d'execució (runmodes) i/o als modes d'inici de sessió (logmodes) de la configuració del port o també es pot forçar al port 128). • Commutació del senyal CD. El procés **getty** es detindrà cada vegada que el senyal CD commuti d'un estat activat a un estat desactivat. (Aquesta acció podria estar causada per diversos motius. Assegureu-vos que el cable està correctament protegit. Iniciar i finalitzar una sessió diverses vegades en una successió ràpida podria provocar-ho).
No es visualitza cap indicador d'inici de sessió després de la connexió amb el mòdem	Assegureu-vos que **getty** s'executa al port. En cas afirmatiu, verifiqueu que la connexió de detecció de portadora amb el senyal del mòdem s'activa després de que la part remota s'hagi connectat amb el mòdem. Si el senyal CD es confirma correctament, verifiqueu que el mòdem està connectat al port correcte. Si encara no veieu l'inici de sessió, adjunteu un terminal amb adaptador al cable en comptes del mòdem i comproveu si apareix un indicador d'inici de sessió. Si encara no veieu un indicador, intenteu fer eco als caràcters per enviar-los a la pantalla del terminal per verificar que el cable i el maquinari funcionen correctament.
Quan un mòdem remot es connecta, tot seguit es desconnecta	Verifiqueu que el mòdem es comunica amb el servidor a la mateixa velocitat a la que el servidor escolta el mòdem. Proveu diferents velocitats en bauds per al tty, o bé programeu el mòdem per què bloquegi la velocitat DTE per tal que coincideixi amb la velocitat del port tty. Verifiqueu que el mòdem o el port no mantingui activat el senyal de detecció de portadora (CD) o que un altre procés ja estigui utilitzant el port.
S'obtenen caràcters inservibles en comptes d'un indicador d'inici de sessió	Això és a causa d'una diferència en els protocols. Verifiqueu que el mòdem i el port tty es posen d'acord sobre la mateixa paritat, velocitat en bauds, control de flux i grandària de caràcters.
De vegades, després una sessió satisfactòria, ningú no pot iniciar una sessió.	La causa podria ser que el mòdem no es reinicialitza després de la desconnexió. Consulteu el manual del mòdem per veure com es pot configurar el mòdem per què es reinicialitzi després d'una transició del senyal DTR d'activat a desactivat.
El buffer receptor sobrepassa el límit a errpt	El buffer del xip UART està sobrepassant el límit. Disminuïu el valor del desencadenament de recepció a la SMIT per al tty. Aquesta solució només és vàlida per als adaptadors asíncrons nadius de 8 o 16 ports. Comproveu que el mòdem i el port tty utilitzen el mateix control de flux.
Errors ttyhog a errpt	El mòdem i tty no es posen d'acord sobre el control de flux, o bé no s'està realitzant cap control de flux.

Qüestionari del mòdem per a serveis de programari:

Abans de demanar ajuda per resoldre els problemes del mòdem, recopileu informació bàsica per accelerar el servei.

La informació que teniu disponible inclou la següent:

- Nivell del sistema operatiu. Quant temps heu estat en aquest nivell del sistema operatiu?
- Funcionava bé el mòdem abans?
- Quin tipus de mòdem esteu utilitzant? Quin tipus de mòdem hi ha a l'altre extrem de la connexió telefònica?
- A quin tipus d'adaptador està connectat el mòdem?
- A quin número de port està connectat el mòdem?
- A quin número de tty està connectat el mòdem?
- Quin tipus de cablatge esteu utilitzant?
- Quin és el valor d'inici de sessió (share, delay, enable)?
- El mòdem pot connectar-se amb altres mòdems?
- Altres mòdems poden connectar-se amb el vostre mòdem?
- Quins són els següents valors a la SMIT, el mòdem o el port?
  - XON/XOFF?
  - RTS/CTS?
  - Velocitat en BPS?
- Inclogueu la següent informació a la descripció del problema:
  - El port es bloqueja de manera intermitent?
  - Podeu fer marcatges de sortida? Els altres usuaris poden fer marcatges d'entrada?
  - Qualsevol altra condició d'error específica i descriptiva.
- Hi ha errors a la consola? Quins són?
- Hi ha errors a l'informe d'errors? (**errpt** o **errpt -a**)
- Quina ordre utilitzeu per fer un marcatge sortida?
- Quin programari es fa servir al sistema?

Ordres AT:

El conjunt d'ordres de l'Hayes Smartmodem inclou el conjunt d'ordres AT que utilitzen molts mòdems populars.

Aquesta informació s'ha obtingut de la Targeta de referència ràpida (*Quick Reference Card*) de l'Hayes Smartmodem 2400, publicada per l'empresa Hayes Microcomputer Products, Inc. Consulteu la documentació del mòdem per veure una llista d'ordres AT pertinents.

Element	Descripció
AT	Prefix d'ordre - precedeix a la línia d'ordres
<CR>	Caràcter de retorn de carro (nova línia) - finalitza la línia d'ordres.
A	Despenjar, romandre en mode d'ordres.
A/	Repetir la línia d'ordres anterior. Aquesta ordre no va precedida d'**AT** ni va seguida de **<CR>**/.
B0	Seleccionar l'estàndard CCITT V.22 per a comunicacions de 1200 bps.
B1	Seleccionar l'estàndard Bell 212A per a comunicacions de 1200 bps.
D	Entrar en mode d'originar, marcar el número que segueix i intentar connectar-se. D va seguida de T per to; també es pot utilitzar P per pulsació.
DS=*n*	Marcar el número emmagatzemant a la ubicació *n*
E0	Inhabilitar l'eco de caràcter a l'estat d'ordres.
E1	Habilitar l'eco de caràcter a l'estat d'ordres.

Element	Descripció
H0	Penjar (penjar el telèfon)
H1	Operar enganxament commutador i retransmissió auxiliar.
I0	Tornar codi d'identificació de producte.
I1	Realitzar suma de comprovació a la ROM de microprogramari; tornar suma de comprovació.
I2	Realitzar suma de comprovació a la ROM de microprogramari; torna `OK` o `ERROR` com a resultat.
L0	Altaveu apagat.
L1	Volum baix d'altaveu.
L2	Volum mitjà d'altaveu.
L3	Volum alt d'altaveu.
M0	Altaveu apagat.
M1	Altaveu encès fins detecció de portadora.
M2	Altaveu sempre encès.
M3	Altaveu encès fins detecció de portadora, menys durant el marcatge.
O0	Entrar en estat connectat.
O1	Entrar en estat connectat i iniciar reciclatge de compensació.
Q0	El mòdem torna codis de resultats.
Q1	El mòdem no torna codis de resultats.
Sr	Establir punter en l'enregistrament r.
Sr=*n*	Establir enregistrament r en el valor *n*.
V0	Visualitzar codis de resultats en format numèric.
V1	Visualitzar codis de resultats en format detallat (en paraules).
X0	Habilitar les característiques representades pels codis de resultats 0-4.
X1	Habilitar les característiques representades pels codis de resultats 0-5, 10.
X2	Habilitar les característiques representades pels codis de resultats 0-6, 10.
X3	Habilitar les característiques representades pels codis de resultats 0-5, 7, 10.
X4	Habilitar les característiques representades pels codis de resultats 0-7, 10.
Y0	Inhabilitar desconnexió d'espai llarg.
Y1	Habilitar desconnexió d'espai llarg.
Z	Reinicialitzar el mòdem.
&C0	Pressuposar que la portadora de dades està sempre present.
&C1	Fer un seguiment de la presència de la portadora de dades.
&D0	Ignorar el senyal DTR.
&D1	Pressuposar estat d'ordres quan es produeix una transició d'activat a desactivat del senyal DTR.
&D2	Penjar i pressuposar estat d'ordres quan es produeix una transició d'activat a desactivat del senyal DTR.
&D3	Reinicialitzar quan es produeix una transició d'activat a desactivat del senyal DTR.
&F	Recuperar els valors de fàbrica com a configuració activa.
&G0	Sense to de protecció.
&G1	To de protecció de 500 Hz.
&G2	To de protecció de 1800 Hz.
&J0	Connector telco RJ-11/RJ41/RJ45S.
&J1	Connector telco RJ-11/RJ-13.
&P0	Marcatge per pulsacions amb una relació make/break de 39/61.
&P1	Marcatge per pulsacions amb una relació make/break de 33/67.
&Q0	Operar en mode asíncron.
&Qn	Operar en mode síncron *n*
&R0	Fer un seguiment de CTS segons RTS.
&R1	Ignorar RTS; pressuposar sempre la presència de CTS.
&S0	Pressuposar la presència del senyal DSR.
&S1	Fer un seguiment de la presència del senyal DSR.
&T0	Prova de finalització en curs.
&T1	Inicia bucle de retorn analògic local.
&T3	Iniciar bucle de retorn digital.
&T4	Atorgar sol•licitud del mòdem remot per a enllaç de dades remotes (RDL).
&T5	Denegar sol•licitud del mòdem remot per a RDL.
&T6	Inicia bucle de retorn digital.
&T7	Inicia bucle de retorn digital remot amb autoprova.
&T8	Inicia bucle de retorn analògic local amb autoprova.
&V	Veure configuració activa, perfils d'usuari i números emmagatzemats.

Element	Descripció
&Wn	Desar paràmetres emmagatzemables de la configuració activa com a perfil d'usuari *n*.
&X0	El mòdem proporciona senyal de rellotge de transmissió.
&X1	El terminal de dades proporciona senyal de rellotge de transmissió.
&X2	La portadora de recepció proporciona senyal de rellotge de transmissió.
&Yn	Recuperar perfil d'usuari *n*.
&Zn=*x*	Emmagatzemar número de telèfon *x* a la ubicació *n*.

Resum d'enregistraments S:

A la taula següent trobareu una llista d'enregistraments S, els seus intervals i les seves descripcions.

Taula 102. Descripcions de registre S

Registre	Interval	Descripció
S0	0-255	Seleccionar nombre de timbres abans de contestar.
S1	0-255	Recompte de timbres (s'incrementa amb cada timbre).
S2	0-127	Definir caràcter de seqüència d'escapament (ASCII).
S3	0-127	Definir caràcter de retorn de carro (ASCII).
S4	0-127	Definir caràcter de salt de línia (ASCII).
S5	0-32, 127	Definir caràcter de retrocés (ASCII).
S6	2-255	Seleccionar temps d'espera en segons abans de marcatge ocult.
S7	1-55	Seleccionar temps d'espera en segons per a portadora/to de marcatge.
S8	0-255	Seleccionar durada en segons de la coma.
S9	1-255	Temps de resposta de detecció de portadora en increments de 0,1 segons (10 = 1 segon).
S10	1-255	Retard entre pèrdua de portadora i acció de penjar en increments de 0,1 segons.
S11	50-255	Durada/espaiat dels tons en mil•lisegons.
S12	50-255	Temps de protecció de la seqüència d'escapament a intervals de 0,2 segons.
S13	—	Reservat.
S14	—	Reservat.
S15	—	Reservat.
S16	—	Reservat (les funcions per a aquest enregistrament es controlen mitjançant les ordres **&T**).
S17	—	Reservat.
S18	0-255	Provar durada de temporitzador en segons
S19	—	Reservat.
S20	—	Reservat.
S21	—	Reservat.
S22	—	Reservat.
S23	—	Reservat.
S24	—	Reservat.

Taula 102. Descripcions de registre S (continuació)

Registre	Interval	Descripció
S25	0-255	Seleccionar temps de detecció de canvi de DTR a intervals de 0.01 segons.
S26	0-255	Retard de RTS a CTS a intervals de 0,01 segons.
S27	—	Reservat.

Codis de resultats dels adaptadors asíncrons:

A la taula següent s'identifiquen els codis de resultats que tornen els adaptadors asíncrons, inclosos els números, les paraules i les descripcions.

Taula 103. Codis de resultat d'adaptadors asíncrons

Número	Paraula	Descripció
0	OK	Ordre executada.
1	CONNECT	Connexió establerta a 0-300 bps.
2	RING	Timbre detectat
3	NO CARRIER	Senyal de portadora perdut o no detectat.
4	ERROR	Ordre no vàlida, suma de comprovació, error a la línia d'ordres o línia d'ordres massa llarga.
5	CONNECT 1200	Connexió establerta a 1200 bps.
6	NO DIALTONE	No s'ha detectat to de marcatge
7	BUSY	S'ha detectat senyal d'ocupat.
8	NO ANSWER	Cap resposta en marcar un sistema.
9	CONNECT 2400	Connexió establerta a 2400 bps.

Modificadors de marcatge:

A continuació es mostren els modificadors de marcatge i les seves descripcions.

Element	Descripció
0-9 # * A-D	Dígits i caràcters per marcar.
P	Marcatge per pulsacions.
T	Marcatge per tons.
,	Retardar el processament del següent caràcter.
!	Flaix d'engaxament.
@	Esperar silenci.
W	Esperar to de marcatge.
;	Tornar a l'estat d'ordres després de marcar.
R	Invertir mode.
S=*n*	Marcar el número emmagatzemat a la ubicació *n*.

Ajuda per al mòdem:

Quan tingueu problemes amb el mòdem, podeu trobar ajuda en els següents llocs.

- El vostre representant d'àrea local us pot ajudar a realitzar la configuració del mòdem.
- Existeixen moltes opcions diferents de suport que estan a l'abast dels clients als Serveis de suport oferts, entre les que s'inclouen l'assistència in situ o el suport telefònic. Poseu-vos en contacte amb el representant de servei més proper per obtenir ajuda.

- Potser una font d'ajuda que sovint no es té en compte és el propi fabricant. La majoria de fabricants tenen algun tipus d'ajuda en línia per als seus productes.

Entrades del fitxer /usr/lib/uucp/Dialers.samples:

Aquestes entrades del fitxer d'exemple es proporcionen sense cap garantia i funcionaran "tal qual" per als models mencionats, però podrien no satisfer les vostres necessitats específiques.

És possible que calgui fer algunes modificacions per satisfer les vostres necessitats individuals. Consulteu el manual del mòdem per veure una explicació més detallada dels valors.

Per poder utilitzar els valors per programar el mòdem, necessitareu una entrada del fitxer /usr/lib/uucp/Systems, com per exemple:

```
hayes Nvr HayesPRGM Any
```

El fitxer /usr/lib/uucp/Devices ha de tenir una entrada com ara la següent:

```
HayesPRGM tty0 - 2400 HayesProgrm2400
```

Amb les dues entrades anteriors realitzades, utilitzeu l'ordre **cu** següent per programar el mòdem:

```
cu -d hayes
```

```
# COMPONENT_NAME: cmduucp
#
#
# (C) COPYRIGHT International Business Machines Corp. 1994
# Materials sota llicència - Propietat d'IBM
# Drets restringits als usuaris del governs dels EUA - L'ús, la duplicació o
# la divulgació estan limitats d'acord amb les restriccions del contracte
# GSA ADP Schedule Contract amb IBM Corp.
################################################################
# Mòdem UDS Motorola
#
# Utilitzeu udsmodemPROGRAM per programar el mòdem.
# El port ha de tenir establert rts/cts.
# Utilitzeu un marcador uds o hayes.
#
# La línia "udsmodemPROGRAM" ha de ser una única línia contínua
#
################################################################
udsmodemPROGRAM =,-, "" \dAT&FQ2\r\c OK
ATE0Y0&C1&D2&S1%B5%E0*LC\r\c OKAT&K3&W\r\c OK

uds =,-, "" \dAT\r\c OK\r ATDT\T\d\r\c CONNECT

################################################################
#
# IBM 7855 Model 10
# Utilitzeu IBMProgrm per programar el mòdem.
# Estableix el control de flux rts/cts, desactiva
# xon/xoff i estableix la velocitat DTE a 19.200 bps.
# El mòdem es connectarà a la velocitat i control de
# flux apropiats amb el servidor.
# El port ha de tenir establert rts/cts.
#
# La línia "IBMProgrm" ha de ser una única línia contínua
#
################################################################
IBMProgrm =,-, "" \dATQ0\r\c OK AT&F\r\c OK ATM1\r\c OK
AT&D3\r\c OK AT&C1\R2\Q2\M14\r\c OK AT&B8N1L0E0\A0\r\c OK
ATS0=1\r\c OK ATQ1&W0&Y0\r\c ""

#####################################################
# Les següents entrades s'usen per fer un marcatge de sortida en
```

```
# un dispositiu ACU normal 7855. Hem d'activar els codis de
# resultats (Q0) perquè es desactiven quan el
# programem. (Impedeix que es produeixi un inici de sessió
# tot en majúscules quan s'intenta marcar.)
# Hem de tenir un caràcter "\" addicional abans de "\N" perquè
# el programa dels BNU el treuen si està davant d'una "N".
#####################################################
ibm =,-, "" \dATQ0\r\c OK ATDT\T\d\r\c CONNECT

# IBM 7855 ECL (sense compressió)
ibmecl =,-, "" \dAT\\N3%C0Q0\r\c OK ATDT\T\d\r\c CONNECT

# IBM 7855 ECLC (compressió)
ibmeclc =,-, "" \dAT\\N3%C1Q0\r\c OK ATDT\T\d\r\c CONNECT

# IBM 7855 ECLC Compressió amb grandària de bloc de 256 octets
ibmeclc256 =,-, "" \dAT\\N3%C1Q0\A3\r\c OK ATDT\T\d\r\c CONNECT

# IBM 7855 1200bps sense compressió
ibm_ne12 =,-, "" \dATQ0\\N0&A2%C0\r\c OK ATDT\T\d\r\c CONNECT

# IBM 7855 2400bps sense compressió
ibm_ne24 =,-, "" \dATQ0\\N0&A3%C0\r\c OK ATDT\T\d\r\c CONNECT

# IBM 7855 9600bps sense compressió
ibm_ne96 =,-, "" \dATQ0\\N0&A6%C0\r\c OK ATDT\T\d\r\c CONNECT

# IBM 7855 19200bps sense compressió
ibm_ne192 =,-, "" \dATQ0\\N0%C0\r\c OK ATDT\T\d\r\c CONNECT

# IBM 7855 12000bps sense compressió
ibm_ne120 =,-, "" \dATQ0\\N3%C0&AL8\r\c OK ATDT\T\d\r\c CONNECT

# IBM 7855 1200bps sense compressió (marcatge silenciós)
ibmq12 =,-, "" \dATQ0\r\c OK AT&A2M0DT\T\d\r\c CONNECT

# IBM 7855 2400bps sense compressió (marcatge silenciós)
ibmq24 =,-, "" \dATQ0\r\c OK AT&A3M0DT\T\d\r\c CONNECT

# IBM 7855 9600bps sense compressió (marcatge silenciós)
ibmq96 =,-, "" \dATQ0\r\c OK AT&A6M0DT\T\d\r\c CONNECT

# IBM 7855 19200bps sense compressió (marcatge silenciós)
ibmq192 =,-, "" \dATQ0\r\c OK ATM0DT\T\d\r\c CONNECT

#############################################################
#
# Mòdem Intel 9600EX
# Utilitzeu IntelProgram per programar el mòdem.
# Estableix el control de flux rts/cts i desactiva
# xon/xoff.
# El port ha de tenir establert rts/cts. (Utilitzeu el marcador hayes)
#
# La línia "IntelProgram" ha de ser una única línia contínua
#
#############################################################
#IntelProgram =,-, "" \d\dAT\r\c OK AT&F\r\c OK AT&S1M1\r\c OK
AT&D3\r\c OKAT&C1\r\c OK ATL0E0Y0&Y0\X1\r\c OK ATS0=1\r\c OK
AT&W\r\c OK

#############################################################
# Mòdem Practical Peripherals 1440FXMT
# Utilitzeu PracPerProgram144 per programar el mòdem.
# Estableix el control de flux rts/cts i desactiva
# xon/xoff. (Utilitzeu el marcador hayes)
# La velocitat DTE es bloquejarà a la velocitat de connexió quan
# es programi el mòdem. (Suggeriment: 38400 bauds)
```

```
#
# La línia "PracPerProgram144" ha de ser una única línia
# contínua
################################################################
PracPerProgram144 =,-, "" \d\dAT\r\c OK AT&F\r\c OK ATM1\r\c OK
AT&D3\r\c OKAT&C1&K3\r\c OK ATQ2E1&Q9\r\c OK ATS0=1S9=20\r\c OK
AT&W\r\c OK

################################################################
# Mòdem Practical Peripherals 9600 bps
# Utilitzeu PracPerProgram9600 per programar el mòdem.
# Estableix el control de flux rts/cts i desactiva
# xon/xoff. (Utilitzeu el marcador hayes)
#
# La línia "PracPerProgram144" ha de ser una única línia
# contínua
################################################################
PracPerProgram9600 =,-, "" \d\dAT\r\c OK AT&F\r\c OK ATM1\r\c OK
AT&D3\r\c OKAT&C1&K3\r\c OK ATL0E0\r\c OK ATS0=1S9=20\r\c OK
AT&W\r\c OK

################################################################
# Mòdem Practical Peripherals 2400 bps
# Utilitzeu PracPerProgram per programar el mòdem
#
# La línia "PracPerProgram2400" ha de ser una única línia
# contínua
################################################################
PracPerProgram2400 =,-, "" \d\dAT\r\c OK AT&F\r\c OK ATM1\r\c OK
AT&D3\r\c OKAT&C1\r\c OK ATL0E0\r\c OK ATS0=1S9=20\r\c OK AT&W\r\c OK

################################################################
# Mòdem Hayes 2400 bps
# Utilitzeu HayesProgrm2400 per programar el mòdem.
# (Utilitzeu el marcador hayes per marcar)
#
# La línia "HayesProgrm2400" ha de ser una única línia contínua
#
################################################################
HayesProgrm2400 =,-, "" \d\dAT\r\c OK AT&F\r\c OK ATM1\r\c OK
AT&D3\r\c OKAT&C1\r\c OK ATL0E0\r\c OK AT S0=1\r\c OK AT&W\r\c OK

################################################################
# Telebit t2000 Trailblazer Plus
# Utilitzeu TelebitProgrm per programar el mòdem
# Estableix el control de flux rts/cts i desactiva
# xon/xoff i estableix la velocitat DTE per defecte a
# 19.200 bps.
# El port ha de tenir establert rts/cts.
# Això fa que el mòdem enviï els tons PEP al final ja que
# es poden confondre amb altres mòdems.
#
# La línia "TelebitProgram" ha de ser una única línia contínua
#
################################################################
TelebitProgram =,-, "" \dAT&F\r\c OK
ats2=255s7=60s11=50s41=2s45=255s51=254s52=2s54=3s58=2s64=1s66=1\r\c OK
ATs69=1s92=1s96=0s105=0s110=1s111=30s130=3s131=1F1M0Q6TV1W0X3Y0\r\c OK
ATE0&W\r\c OK
# Entrades del marcadors Telebit T2000:
# Força una connexió PEP:
tbfast =,-, "" \dATs50=255s7=60\r\c OK\r ATDT\T\r\c
CONNECT-\d\c-CONNECT

# Connexió a 2400bps:

#tb2400 =,-, "" \dATs50=3\r\c OK\r ATDT\T\r\c CONNECT
```

```
# 2400 MNP:
tb24mnp =,-, "" \dAT\r\c OK ATS0=0S95=2S50=3S41=0\r\c OK
ATDT\T\r\c CONNECT

# Connexió a 1200bps:#tb1200 =,-, "" \dATs50=2\r\c OK\r
ATDT\T\r\c CONNECT

# 1200 MNP:
tb12mnp =,-, "" \dAT\r\c OK ATS0=0S95=2S50=2S41=0\r\c OK
ATDT\T\r\c CONNECT

#############################################################
# Telebit WorldBlazer
# WORLDBLAZERProgram estableix la velocitat DTE a 38400, però
# podeu establir-la més alta si la connexió DTE pot
# admetre-la. Contestem amb tons PEP al final per tal que
# no es confonguin amb altres mòdems. Això desactiva xon/xoff
# i activa el control de flux RTS/CTS. El port ha d'estar
# bloquejat a 38400 amb aquests valors i ha de tenir
# activat RTS/CTS.
#
# La línia "WORLDBLAZERProgram" ha de ser una única línia
# contínua
#############################################################
WORLDBLAZERProgram =,-, "" \dAT\r\c AT AT&F3M0\r\c AT
ATs51=253s92=1\r\c ATAT&W\r\c AT

#####################################################
# Marcadors ACU per diverses velocitats en BAUDS per al
# WorldBlazer - cadascun configura el mòdem per què intenti
# connectar a una velocitat específica i més baixes. WBlazer
# acceptarà tot el que el mòdem remot pugui
# fer. Us interessarà utilitzar PEP per altres Telebits;
# per tant, utilitzeu WBlazer38400 o WBlazer19200 per aquests
#####################################################
# WBlazer =,-, "" \dAT\r\c OK ATDT\T\d\r\c CONNECT
WBlazer38400 =,-, "" \dATs50=255\r\c OK ATDT\T\d\r\c CONNECT
WBlazer19200 =,-, "" \dATs50=255\r\c OK ATDT\T\d\r\c CONNECT
# WBlazer14400 intenta negociar una connexió V.42bis.
WBlazer14400 =,-, "" \dATs50=7\r\c OK ATDT\T\d\r\c CONNECT

# Per a una connexió V.32:
WBlazer9600 =,-, "" \dATs50=6\r\c OK ATDT\T\d\r\c CONNECT

# Per a una connexió V.22:
WBlazer2400 =,-, "" \dATs50=3\r\c OK ATDT\T\d\r\c CONNECT

# Per a una connexió a 1200 bps:
WBlazer1200 =,-, "" \dATs50=2\r\c OK ATDT\T\d\r\c CONNECT
```

Consideracions sobre el cablatge del mòdem de 128 ports:

Aquest sistema operatiu no necessita DSR a les aplicacions de control de mòdem, i com que gairebé tots el mòdems actuals tenen capacitat de resposta automàtica, el senyal Indicador de timbre normalment no és necessari.

Els endolls RJ-45 de 10 potes no són el subsistema de cablatge predominant i poden ser difícils de trobar en el mercat al detall. El subsistema TTY d'aquest sistema operatiu proporciona una característica opcional anomenada ALTPIN, que intercanvia les funcions lògiques de DSR (Conjunt de dades preparat) amb DCD (Detecció de portadora de dades) per a un port. Quan s'habilita ALTPIN, DCD passa a estar disponible a la pota 1 d'un connector RJ-45 de 8 potes (equivalent a la pota 2 d'un connector de 10 potes).

Si desitgeu crear un cable de mòdem de 8 fils per a un RAN de 128 ports, utilitzeu l'endoll RJ-45 de 8 potes connectat tal com es descriu a la taula següent:

Taula 104. Cablatge del mòdem de 128 ports

Element	Descripció	Mòdem
CONNECTOR DE L'EXTREM DEL SISTEMA RJ-45 de 8 potes	FI DE DISPOSITIURI	22
1	DSR	6
2	RTS	4
3 (xassís)	GND	SHELL
4	TxD	2
5	TxD	3
6 (senyal)	GND	7
7	CTS	5
8	DTR	20
	CD	8

Nota: La ubicació física de DSR i CD pot intercanviar-se amb el paràmetre ALTPIN quan s'habilita utilitzant l'ordre stty-cmxa.

La taula següent mostra la comunicació de senyals asíncrons entre la unitat del sistema i un mòdem adjuntat. Aquí, les dades s'envien des de la unitat del sistema a un sistema remot.

Taula 105. Comunicació de senyals asíncrons

DISPOSITIU	SENYAL	ENCÉS/APAGAT	SIGNIFICAT
Ordinador	DTR	+	Ei, mòdem, estàs preparat per connectar-te amb un altre sistema?
Mòdem	DSR	+	Sí, estic preparat. Endavant, ja pots marcar.
Mòdem	DCD	+	Tinc un altre sistema al telèfon.
Ordinador	RTS	+	D'acord, puc enviar les dades ara?
Mòdem	CTS	+	Sí, endavant
Ordinador	TxD		Enviant dades al mòdem.
Mòdem	RxD		He rebut les dades.
Mòdem	CTS	–	No m'enviïs més dades, les estic enviant fora...
Mòdem	CTS	+	D'acord, estic preparat per rebre més dades, envia-me-les!
Els passos de transmissió de dades es poden repetir fins... Ordinador	DTR	–	HE ACABAT! Ja pots penjar.
Mòdem	DCD	–	D'acord.
Aquí, la comunicació de senyals és entre un RS/6000 i un mòdem sobre com rebre una crida d'entrada d'un altre sistema. Ordinador	DTR	+	Estic preparat i he "habilitat" el port per fer marcatges d'entrada.
Mòdem	DSR	+	Jo també estic preparat però estic esperant una crida.
Algú crida!Mòdem	DCD	+	Algú ha cridat i el tinc a la línia.

Taula 105. Comunicació de senyals asíncrons (continuació)

DISPOSITIU	SENYAL	ENCÉS/APAGAT	SIGNIFICAT
Mòdem	CTS	+	Tinc dades d'una altra safata, et puc enviar les dades ara?
Ordinador	RTS	+	Estic preparat per rebre-les. Endavant, ja les pots enviar.
Mòdem	RxD		Aquí van!
El mòdem continua enviant dades fins... Ordinador	RTS	–	ESPERA! El meu buffer és ple, no enviïs més dades.
Ordinador	RTS	+	Ja torno a estar preparat. Envia'm més dades.
Mòdem	DCD	–	La crida ha finalitzat.
Ordinador	DTR	–	D'acord, ja pots penjar.

Opcions de terminal d'stty-cxma

stty-cxma és un programa d'utilitats que estableix i mostra les opcions de terminal per als adaptadors PCI de 2, 8 i 128 ports, i es troba al directori `/usr/lbin/tty`.

El format és:

```
stty-cxma [-a] [opció(ns)] [ttyname]
```

Sense cap opció, **stty-cxma** mostra tots els valors especials del programa de control, el senyals del mòdem i tots els paràmetres estàndard que visualitza **stty(1)** per al dispositiu tty al que fa referència l'entrada estàndard. S'inclouen opcions d'ordres per canviar els valors de control de flux, establir opcions d'impressió transparent, forçar línies de control de mòdem i visualitzar tots els valors tty. Les opcions no reconegudes es passen a **stty(1)** per ser interpretades. Les opcions són:

-a Mostra tots els valors d'opcions d'adaptador exclusius, així com tots els valors tty estàndard sobre el quals informa l'ordre **stty -a**.

ttyname
Estableix i visualitza opcions per al dispositiu tty especificat, en comptes de l'entrada estàndard. Aquest format pot utilitzar-se amb un nom de camí d'accés tty prefixat amb **/dev/** o amb un nom tty simple que comença per tty. Aquesta opció pot utilitzar-se en una línia de control de mòdem quan no hi cap portadora present.

Les opcions següents especifiquen accions transitòries que s'han de realitzar immediatament:

break Envia un senyal d'interrupció de 250 ms a la línia tty.

flush Indica un llançament (rebuig) immediat de l'entrada i sortida tty.

flushin
Només llança l'entrada tty.

flushout
Només llança la sortida tty.

Les opcions següents especifiquen accions que es restableixen quan es tanca el dispositiu. El dispositiu utilitzarà els valors per defecte la propera vegada que s'obri.

stopout
Atura la sortida exactament de la mateixa manera que si s'hagués rebut un caràcter XOF.

startout
Reinicia la sortida aturada exactament de la mateixa manera que si s'hagués rebut un caràcter XON.

stopin Activa el control de flux per aturar l'entrada.

startin Allibera el control de flux per reprendre l'entrada aturada.

[-]dtr [drop]
Activa la línia de control de mòdem DTR, si no s'ha seleccionat el control de flux de maquinari DTR.

[-]rts [drop]
Activa la línia de control de mòdem RTS, si no s'ha seleccionat el control de flux de maquinari RTS.

Les opcions següents romanen en vigor fins que es reengega el sistema o fins que es canvien les opcions.

[-]fastcook
Realitza un processament preparat de la sortida a la targeta intel•ligent per reduir l'ús d'UCP de l'amfitrió i augmentar el rendiment de l'entrada en mode sense format.

[-]fastbaud
Modifica les taules de velocitats en bauds, de manera que 50 bauds passa a ser 57.600 bauds, 75 bauds passa a ser 76.800 bauds, 110 bauds passa a ser 115.200 bauds i 200 bauds passa a ser 230.000 bauds per als dispositius suportats.

[-]rtspace
Habilita/inhabilita el control de flux d'entrada de maquinari del senyal RTS, de manera que l'RTA s'elimina per fer una pausa en la transmissió remota.

[-]ctspace
Habilita/inhabilita el control de flux de sortida de maquinari del senyal CTS, de manera que la transmissió local fa una pausa quan s'elimina el CTS.

[-]dsrpace
Habilita/inhabilita el control de flux de sortida de maquinari del senyal DSR, de manera que la transmissió local fa una pausa quan s'elimina el DSR.

[-]dcdpace
Habilita/inhabilita el control de flux de sortida de maquinari del senyal DCD, de manera que la transmissió local fa una pausa quan s'elimina el DCD.

[-]dtrpace
Habilita/inhabilita el control de flux d'entrada de maquinari del senyal DTR, de manera que el DTR s'elimina per fer una pausa en la transmissió remota.

[-]forcedcd
Inhabilita [torna a habilitar] la portadora sensible, de manera que el tty es pot obrir i utilitzar fins i tot quan la portadora no està present.

[-]altpin
Mapeja els passadors del connector RJ-45 amb els valors del connector de 10 potes per defecte o el valors del connector de 8 potes. Quan aquest paràmetre està **habilitat**, la ubicació de DSR i DCD es commuta de manera que DCD està disponible quan s'utilitza un connector RJ-45 de 8 potes en comptes del connector RJ-45 de 10 potes. (Valor per defecte=**inhabilitar**.)

Valors possibles:

habilitat (especifica els valors del connector de 8 potes)

inhabilitar (especifica els valors del connector de 10 potes)

startc *c*
Estableix el caràcter de control de flux XON. El caràcter es pot expressar com a número decimal, octal o hexadecimal. Els números octals es reconeixen per la presència d'un zero inicial i els números hexadecimals s'indiquen mitjançant un 0x inicial. Per exemple, el caràcter XON estàndard, CONTROL-Q, pot especificar-se com a 17 (decimal), 021 (octal) o 0x11 (hexadecimal).

stopc*c* Estableix el caràcter de control de flux XOFF. El caràcter es pot expressar com a número decimal, octal o hexadecimal (consulteu **startc** per veure el format dels números octals i hexadecimals).

astartc*c*
Estableix el caràcter de control de flux XON auxiliar. El caràcter es pot expressar com a número decimal, octal o hexadecimal (consulteu **startc** per veure el format dels números octals i hexadecimals).

astopc*c*
Estableix el caràcter de control de flux XOFF auxiliar. El caràcter es pot expressar com a número decimal, octal o hexadecimal (consulteu **startc** per veure el format dels números octals i hexadecimals).

[-]aixon
Habilita el control de flux auxiliar, de manera que s'utilitzen dos caràcters exclusius per a XON i XOFF. Si es reben els dos caràcters XOFF, la transmissió no es reprendrà fins que es rebin els dos caràcters XON.

[-]2200flow
Utilitza el control de flux d'estil de 2200 al port. Els terminals 2200 donen suport a una impressora adjuntada i utilitzen quatre caràcters de control de flux: XON de terminal (0xF8), XON d'impressora (0xF9), XOFF de terminal (0xFA) i XOFF d'impressora (0xFB).

[-]2200print
Determina com s'interpreten aquests caràcters de control de flux. Si 2200print està establert, s'executen controls de flux independents per als dispositius de terminal i d'impressió transparent. En cas contrari, els controls de flux de terminal i impressora estan units de manera lògica. Si es rep el caràcter XOFF, es fa una pausa en tota la sortida fins que es rep el caràcter XON.

maxcps*n*
Estableix la velocitat màxima en caràcters per segons (cps) a la que els caràcters s'envien al dispositiu d'impressió transparent. La velocitat escollida ha de ser just per sota de la velocitat mitja d'impressió. Si el número és massa baix, es reduirà la velocitat d'impressió. Si el número és massa alt, la impressora utilitza el control de flux, i es redueix el temps d'entrada de l'usuari. El valor per defecte és 100 cps.

maxchar*n*
Estableix el nombre màxim de caràcters d'impressió transparent que el programa de control col•loca a la cua de sortida. Si es redueix aquest número augmenta la sobrecàrrega del sistema; si s'augmenta aquest número es retarden els temps d'eco de les pulsacions de tecles de l'operador quan s'està utilitzant la impressora transparent. El valor per defecte és 50 caràcters.

bufsize*n*
Estableix l'estimació del programa de control pel que fa a la grandària del buffer d'entrada de la impressora transparent. Després d'un període d'inactivitat, el programa de control envia en una ràfega aquests caràcters múltiples a la impressora transparent abans de reduir la velocitat maxcps. El valor per defecte és 100 caràcters.

onstr*s*
Estableix la seqüència d'escapament del terminal per activar la impressió transparent. Les sèries poden estar formades per caràcters imprimibles i no imprimibles ASCII estàndard. Els caràcters de control (no imprimibles) s'han d'especificar segons els seus valors octals i han d'estar formats per tres dígits precedits d'un caràcter de barra inversa. Per exemple, el caràcter d'escapament, 33 octal, s'ha d'especificar com \033. Si la impressió transparent s'activa mitjançant la sèrie <Esc>[5i (estàndard ANSI), s'especificaria com: \033[5i.

offstr*s*
Estableix la seqüència d'escapament del terminal per desactivar la impressió transparent. Consulteu **onstr***s* per veure el format de les sèries.

term*t* Estableix les sèries d'activació/desactivació de la impressora transparent en els valors trobats a la

taula de valors per defecte interns. Els valors per defecte interns s'utilitzen per als següents terminals: adm31, ansi, dg200, dg210, hz1500, mc5, microterm, multiterm, pcterm, tvi, vp-a2, vp-60, vt52, vt100, vt220, wyse30, wyse50, wyse60 o wyse75. Si el tipus de terminal no es troba a la taula de valors per defecte interns, ditty llegeix l'entrada terminfo corresponent al tipus de terminal i estableix les sèries d'activació/desactivació de la impressió transparent en els valors que proporcionen els atributs mc5/mc4 que es troben a les entrades terminfo.

Subsistema Protocol punt a punt asíncron

El subsistema **Protocol punt a punt (PPP) asíncron** proporciona una alternativa a SLIP.

PPP proporciona un mètode estàndard per transportar datagrames de multiprotocol a través d'un suport punt a punt. **PPP** es composa de tres capes principals:

1. Un mètode per encapsular datagrames de multiprotocol. **PPP** dóna suport als protocols de capa de xarxa TCP/IP.
2. Un **Protocol de control d'enllaços (LCP)** per establir, configurar i provar la connexió d'enllaç de dades. **PPP** ho implementa mitjançant extensions del kernel streams.
3. Una família de **Protocols de control de xarxa (NCP)** per establir i configurar diferents protocols de capa de xarxa. **PPP** dóna suport a **Internet Protocol Control Protocol (IPCP/IPv6CP)** per negociar una connexió TCP/IP.

Aquesta implementació de **PPP** dóna suport a les següents Sol•licituds de comentaris (RFC):

- RFC 1661, *El Protocol punt a punt, LCP*
- RFC 1332, *L'Internet Protocol Control Protocol (IPCP) PPP*
- RFC 1662, *PPP en trames semblants a HDLC*
- RFC 1334, *Protocols d'autenticació PPP*
- RFC 1990, *Multienllaç PPP*
- RFC 2472, *IP Versió 6 sobre PPP*

PPP distingeix entre client i servidor. Aquest sistema operatiu pot actuar com a client i com a servidor. La distinció es fa per simplificar la configuració. Els servidors **PPP** solen assignar una agrupació d'adreces IP/IPv6CP entre les connexions que es realitzen. Existeix una certa correlació entre els dispositius de suport d'emmagatzematge. Aquesta implementació de **PPP** trenca aquesta correlació. Totes les connexions **PPP** de servidor s'assignen a partir de la primera que està disponible. Això facilita la separació de **PPP** del suport d'emmagatzematge. El procés d'adjunció ha de sol•licitar ser enllaçat al tipus d'enllaç correcte.

Processos a nivell d'usuari PPP

El **Protocol punt a punt asíncron** d'aquest sistema operatiu utilitza tres processos a nivell d'usuari.

1. Un daemon de control (**pppcontrold**) que executa l'usuari root sota el Controlador de recursos del sistema (**startsrc -s pppcontrold**). La funció del daemon de control inclou la càrrega i la configuració de totes les extensions del kernel associades amb el subsistema. S'està executant mentre el sistema operatiu necessiti la funció **PPP**.
2. Un procés d'adjunció (**pppattachd**) que uneix un corrent TTY a una instància del **Protocol de control d'enllaços (LCP)**, **Protocol de control de xarxa (NCP)** i un protocol de datagrama. Existeix una instància de **pppattachd** per a cada connexió **PPP** activa del sistema. Qualsevol usuari del procés d'adjunció ha de pertànyer al grup **uucp** i ha de contenir `/usr/sbin` dins de la seva variable d'entorn**PATH**.
3. Un procés de marcador (**pppdial**) que estableix una connexió de sortida. El marcador està previst ser executar per **pppattachd** com a programa connector. La seva finalitat és interactuar a través del dispositiu asíncron abans de la negociació **PPP**. Aquesta interacció es defineix de manera semblant al format del diàleg chat de l'UUCP. La capacitat de marcador es proporciona per ajudar a establir una connexió amb un sistema remot. L'establiment de sessió real està fora de l'àmbit de **PPP**.

Configuració del Protocol punt a punt asíncron

Podeu utilitzar la SMIT per configurar el **Protocol punt a punt asíncron**.

La taula següent mostra totes les tasques que possiblement haureu de dur a terme quan configureu el vostre sistema. Heu de tenir privilegis d'usuari root per dur a terme les tasques d'aquesta taula.

Com a mínim, quan configureu inicialment el sistema, haureu d'escollir les tasques següents de la taula:

- Afegir una configuració d'enllaç
- Afegir una interfície del servidor (si configureu la màquina com a servidor PPP)
- Afegir una interfície de demanda (si voleu que la màquina doni suport a connexions de demanda)
- Manipular usuaris/paraules clau PAP o CHAP (si voleu que la màquina doni suport a l'autenticació **PPP**)
- Iniciar **PPP** per què els canvis entrin en vigor (o be aturar i després iniciar **PPP**, si **PPP** s'està executant actualment).

Taula 106. Configuració de les tasques del PPP asíncron

Tasca	**Camí d'accés ràpid de la SMIT**
Crear una configuració de control d'enllaços	`smit ppplcp`
Afegir una configuració d'enllaç	`smit addlcp`
Canviar/mostrar una configuració d'enllaç	`smit chglcp`
Eliminar una configuració d'enllaç[1]	`smit rmlcp`
Crear interfícies IP PPP	`smit pppip`
Afegir una interfície del servidor	`smit addpppserver`
Canviar/mostrar una interfície del servidor	`smit listserver`
Eliminar una interfície del servidor[1]	`smit rmlistserver`
Afegir una interfície de demanda	`smit addpppdemand`
Canviar/mostrar una interfície de demanda	`smit listdemand`
Eliminar una interfície de demanda[1]	`smit rmlistdemand`
Manipular usuaris/paraules clau PAP	`smit ppppap`
Afegir un usuari PAP	`smit addpapuser`
Canviar/mostrar un usuari PAP	`smit listpapuser`
Eliminar un usuari PAP	`smit rmpapuser`
Manipular usuaris/paraules clau CHAP	`smit pppchap`
Afegir un usuari CHAP	`smit addchapuser`
Canviar/mostrar un usuari CHAP	`smit listchapuser`
Eliminar un usuari CHAP	`smit rmchapuser`
Iniciar **PPP**[2]	`smit startppp`
Aturar **PPP**[3]	`smit stopppp`
Interfícies IPv6 **PPP**	`smit pppipv6`
Afegir una interfície del servidor IPv6 **PPP**	`smit addpppv6server`
Mostrar o canviar una interfície IPv6 **PPP**.	`smit listv6server`
Eliminar una interfície IPv6 **PPP**.	`smit rmlistv6server`
Afegir una interfície del client IPv6 **PPP**.	`smit addpppv6client`
Mostrar o canviar una interfície del client IPv6 **PPP**.	`smit listpppv6client`
Eliminar una interfície del client IPv6 **PPP**.	`smit rmlistpppv6client`
Afegir una interfície de demanda IPv6 **PPP**	`smit addpppv6demand`
Mostrar o canviar una interfície de demanda IPv6 **PPP**.	`smit listpppv6demand`
Eliminar una interfície de demanda IPv6 **PPP**.	`smit rmlistpppv6demand`

Taula 106. Configuració de les tasques del PPP asíncron (continuació)

Tasca	Camí d'accés ràpid de la SMIT
Interfícies IP i IPv6 **PPP**	`smit pppipv4_6`
Afegir una interfície del servidor IP/IPv6 **PPP**	`smit addpppv4_6server`
Mostrar o canviar una interfície IP/IPv6 **PPP**.	`smit listv4_6server`
Eliminar una interfície IP/IPv6 **PPP**.	`smit rmlistv4_6server`
Afegir una interfície del client IP/IPv6 **PPP**.	`smit addpppv4_6client`
Mostrar o canviar una interfície del client IP/IPv6 **PPP**.	`smit listpppv4_6client`
Eliminar una interfície del client IP/IPv6 **PPP**.	`smit rmlistpppv4_6client`
Afegir una interfície de demanda IP/IPv6 **PPP**	`smit addpppv4_6demand`
Mostrar o canviar una interfície de demanda IP/IPv6 **PPP**.	`smit listpppv4_6demand`
Eliminar una interfície de demanda IP/IPv6 **PPP**.	`smit rmlistpppv4_6demand`

Nota:

1. Quan se selecciona aquest tasca es destrueix la informació existent.
2. Una forma alternativa d'iniciar **PPP** és executant l'ordre **startsrc -s pppcontrold**. No obstant això, la interfície SMIT també permet definir **PPP** per què s'inicïi en el moment d'engegar.
3. Una forma alternativa d'aturar **PPP** és executant l'ordre **stopsrc -s pppcontrold**. No obstant això, la interfície SMIT també permet que **PPP** no s'inicïi en el moment d'engegar.

Habilitació de l'SNMP PPP

PPP pot interactuar amb el daemon SNMP TCP/IP per notificar informació sobre la configuració de capa d'enllaços PPP així com informació sobre les interfícies **Protocol de control d'enllaços (LCP)** actives.

Sempre que l'SNMP TCP/IP i el programari de gestió de l'SNMP estiguin configurats correctament, l'SNMP **PPP** habilita:

- la recuperació de la informació sobre Configuració d'enllaços **PPP** (com per exemple la grandària de la Unitat de recepció màxima (MRU) i el mapatge de caràcters asíncrons).
- la definició de la informació sobre Configuració d'enllaços **PPP**
- la recuperació de la informació sobre la interfície LCP per als enllaços LCP actius
- el canvi de l'estat dels enllaços LCP actius pot canviar-se a "inactiu" definint l'objecte MIB (base d'informació de gestió) **ifAdminStatus** apropiat.

No tots els objectes que defineix l'RFC1471 per a l'MIB **PPP** estan suportats. Només la taula **pppLink** s'aplica al subsistema **PPP** i, per tant, les parts **pppLqr** i **pppTests** no estan suportades. La part **pppLink** està suportada amb les següents excepcions:

- L'objecte **pppLinkConfigMagicNumber** és només de lectura. A **PPP**, la negociació de número màgic sempre es duu a terme i no es pot inhabilitar.
- L'objecte **pppLinkConfigFcsSize** és només de lectura. **PPP** només dóna suport a grandàries FCS de 16 amb aquest sistema operatiu.

Per defecte, l'SNMP per a **PPP** està inhabilitat. Per habilitar l'SNMP **PPP**, podeu utilitzar el següent procediment. Heu de tenir privilegis d'usuari root per dur a terme aquest procediment.

Nota: El següent procediment pressuposa que la Configuració d'enllaços **PPP** ja s'ha definit. De no ser així, realitzeu el procediment descrit a l'apartat “Configuració del Protocol punt a punt asíncron” a la pàgina 614 abans d'habilitar l'SNMP **PPP**.

1. Inicieu la interfície SMIT i visualitzeu la pantalla Canviar/mostrar una configuració d'enllaços escrivint:
   ```
   smit chglcp
   ```

2. Commuteu el camp Habilitar subagent de l'SNMP **PPP** a sí.
3. Accepteu els canvis i sortiu de la SMIT.

L'SNMP **PPP** no s'habilita fins que es reinicia **PPP**.

- Si **PPP** s'està executant actualment:
  1. Atureu **PPP** utilitzant el camí d'accés ràpid `smit stopppp` (vegeu la taula de l'apartat "Configuració del Protocol punt a punt asíncron" a la pàgina 614).
  2. Comproveu periòdicament si el subsistema ha completat l'aturada escrivint:
     ```
     lssrc -s pppcontrold
     ```
     La quantitat de temps que es triga en aturar completament el subsistema depèn del nombre d'enllaços definits a la configuració **PPP**. El subsistema està completament aturat quan la sortida d'aquesta ordre mostra un estat d'`inoperatiu`.
  3. Inicieu **PPP** utilitzant el camí d'accés ràpid `smit startppp` (vegeu la taula de l'apartat "Configuració del Protocol punt a punt asíncron" a la pàgina 614).
- Si **PPP** no s'està executant actualment, inicieu **PPP** utilitzant el camí d'accés ràpid `smit startppp` (vegeu la taula de l'apartat "Configuració del Protocol punt a punt asíncron" a la pàgina 614).

Protocol d'Internet de línia sèrie

El **Protocol d'Internet de línia sèrie (SLIP)** és el protocol que TCP/IP utilitza quan funciona a través d'una connexió en sèrie.

Normalment s'utilitza en enllaços sèrie dedicats i connexions de marcatge que funcionen a velocitats entre 1200 bps i 19,2 Kbps o superiors.

Nota: Per utilitzar velocitats en bauds superiors a 38400, especifiqueu una velocitat en bauds de 50 al fitxer `/etc/uucp/Devices` per al tty desitjat i, a continuació, canvieu la configuració de la SMIT per aquest tty per tal que reflecteixi la velocitat en bauds real desitjada.

Per exemple, per executar l'ordre **cu** al tty0 amb una velocitat en bauds de 115200, utilitzeu el següent procediment:

1. Assegureu-vos que el maquinari admet la velocitat en bauds.
2. Editeu `/etc/uucp/Devices` per incloure la línia següent:
   ```
   Direct tty0 - 50 direct
   ```
3. Especifiqueu el camí d'accés ràpid `smit chtty`.
4. Seleccioneu tty0.
5. Canvieu la velocitat en bauds a 115200.
6. Sortiu de la SMIT.

Configuració d'SLIP

Es recomana seguir dos passos durant la configuració d'**SLIP**.

La utilització d'aquest enfoc de dos passos separa els requisits de configuració dependents de la màquina i de maquinari dels problemes de sintaxi d'ordres i del programari SLIP.

1. Utilitzeu l'ATE o la utilitat **cu** per dur a terme un inici de sessió satisfactori al sistema remot. D'aquesta manera es demostrarà la usabilitat de l'enllaç físic i si aquest és correcte.

   És important verificar l'operabilitat dels mòdems que intervenen en un enllaç **SLIP** ja que són la causa més freqüent de problemes durant la fase de configuració.
2. Després d'establir un inici de sessió sense errors al sistema remot mitjançant l'ATE o l'ordre **cu**, podeu iniciar la configuració d'**SLIP**.

Consideracions sobre el mòdem SLIP

A l'hora de configurar mòdems per a **SLIP**, és important que aquests canvis es facin en els dos extrems de l'enllaç de comunicacions.

Tant el mòdem local com el mòdem remot s'han de configurar exactament de la mateixa manera.

1. El mòdem ha de confirmar la presència del senyal DTR.

   Pel que fa al mòdem local, si es pressuposa o s'ignora el senyal DTR, el mòdem no pot realitzar mai una acció de penjar. Només pot tancar la línia o penjar quan reconeix la pèrdua de portadora de l'altre extrem. Això significa que les desconnexions només es poden produir quan estan instigades per l'altre extrem. Les ordres AT &D2 o &D3 són valors adequats per a la majoria de mòdems compatibles amb Hayes.

2. El mòdem no ha de forçar, pressuposar ni ignorar mai el senyal DCD (Detecció de portadora de dades).

   DCD ha de seguir o fer un seguiment de la condició real. Això significa que la portadora existirà després d'una connexió autèntica amb l'altre extrem (mòdem) d'una línia telefònica commutada. Això també s'aplica a una línia dedicada. &C1 és el valor recomanat per a la majoria de mòdems compatibles amb Hayes.

3. El mòdem no ha de forçar, pressuposar ni ignorar un senyal CTS (Preparat per emetre).

   CTS ha de fer un seguiment o seguir el senyal RTS (Sol•licitud per enviar). Si es força un senyal CTS, no es podrà obrir el port sempre que s'executi un procés **getty** en el port o quan el protocol de control de flux RTS s'afegeixi al port.

4. Els mòdems s'han de configurar de manera que desactivin el codis ARQ (sol•licitud de repetició automàtica) si surten problemes durant els intents de marcatge **slattach**.

   Si, en repetides ocasions, els mòdems no aconsegueixen establir una connexió durant els intents de fer un marcatge d'entrada **slattach**, l'usuari ha de comprovar les configuracions dels mòdems i desactivar els codis ARQ si actualment estan activats. A la majoria de mòdems compatibles amb Hayes, es tracta del valor &A0.

   El fet d'inhabilitar els codis de resultats ARQ no afecta les connexions controlades per errors ni tampoc impedeix que el mòdem torni missatges CONNECT estàndard (si els codis de resultats estan habilitats) segons calgui per a la sèrie de marcatge **slattach**.

5. ECL (Comprovació d'errors a l'enllaç) és fonamental.

   Pot ser utilitzar per AMBDÓS mòdems o per CAP dels mòdems. Normalment, ambdós mòdems s'han de posar d'acord sobre la seva utilització durant la sessió de connexió. Si s'escull ECL, la línia telefònica física ha de ser suficientment bona per permetre una recuperació d'un error de dades abans que caduquin els temporitzadors TCP/IP mentre s'espera un paquet de confirmació de les darreres dades enviades a través de l'enllaç **SLIP**.

6. Compressió de dades a través de l'enllaç.

   S'accepta utilitzar la compressió de dades a través de l'enllaç sempre i quan la duguin a terme exclusivament els mòdems. **SLIP** no realitza cap tipus de compressió. Si s'invoca la compressió de dades, és molt millor que els dos mòdems siguin exactament del mateix tipus; així s'assegura que cadascun d'ells realitzarà la compressió de la mateixa manera i en el mateix interval de temps.

Programació manual de mòdems utilitzant l'ordre cu

Utilitzeu el següent procediment per programar manualment els mòdems adjuntats a la unitat del sistema.

- El Programa de còpia UNIX a UNIX (UUCP) ha d'estar instal•lat al sistema. Utilitzeu l'ordre **lslpp -f | grep bos.net.UUCP** per verificar la instal•lació.
- Un mòdem ha d'estar adjuntat al sistema i ha d'estar encès.
- Cal autorització d'usuari root per canviar els fitxers apropiats.

1. Afegiu la línia següent al fitxer `/etc/uucp/Devices` si encara no existeix (substituïu # pel número del vostre port).

```
Direct tty# - Any direct
```

Nota: Les línies del fitxer `Devices` que comencen amb un signe # a la columna situada més a l'esquerra són comentaris.

2. Deseu el fitxer i sortiu.
3. Escriviu la següent ordre a la línia d'ordres:
   ```
   cu -ml tty#
   ```
4. Ha d'aparèixer un missatge de connectat a la pantalla que indiqui que el mòdem està connectat i preparat per ser programat.
5. Escriviu `AT` i feu clic a Intro. El mòdem respondrà amb `OK`. Si no hi ha cap resposta del mòdem o si els caràcters escrits no apareixen a la pantalla, comproveu el següent:
   - Verifiqueu les connexions de cablatge del mòdem.
   - Verifiqueu que el mòdem està encès.
   - Observeu els llums del panell frontal del mòdem quan feu clic a Intro. Si els llums RD (Dades de recepció) i SD (Dades d'enviament) parpellegen, el mòdem s'està comunicant amb el sistema i el problema podria raure en els valors actuals del mòdem. Si els llums no parpellegen, el problema està amb la connexió del mòdem.
   - Escriviu el següent i mireu si la condició canvia:
     ```
     ATE1 <intro>
     ATQ0 <intro>
     ```

     ATE1 activa el mode d'eco que visualitza tots els caràcters escrits a la pantalla. ATQ0 habilita la visualització dels codis de resultats.
6. Programeu el mòdem utilitzant els valors indicats a l'apartat anterior, "Consideracions sobre el mòdem". L'exemple següent mostra com programar i desar els valors bàsics per a un mòdem compatible amb Hayes. Especifiqueu:
   ```
   AT&F    <intro>
   AT&D2   <intro>
   ATS0=1  <intro>
   ATS9=12 <intro>
   AT&C1   <intro>
   AT&W    <intro>
   ~.      <intro>
   ```
   On `&F` s'utilitza per reinicialitzar el mòdem en els valors per defecte de fàbrica, `&D2` estableix el senyal DTR, `S0` i `S9` estableixen els valors d'enregistrament, `&C1` estableix la portadora i `&W` escriu els valors al mòdem. La titlla i el punt finalitzen la connexió.

Configuració de mòdems automatitzats

Els usuaris poden personalitzar els mòdems manualment o bé utilitzar la utilitat **cu** amb els seus fitxers associats per crear una seqüència de configuració de mòdem automatitzada.

- L'UUCP ha d'estar instal•lat al sistema. Utilitzeu l'ordre **lslpp -f | grep bos.net.UUCP** per verificar la instal•lació.
- Un mòdem ha d'estar adjuntat al sistema i ha d'estar encès.
- La sèrie d'ordres AT del mòdem ja ha d'existir (per exemple, `at&f&c1&d3`). Els usuaris no han d'intentar la configuració automatitzada del mòdem fins que la sèrie d'ordres s'hagi intentat manualment utilitzant l'ordre **cu**.
- Cal autorització d'usuari root per canviar els fitxers apropiats.

L'exemple següent mostra com configurar automàticament un mòdem Telebit T3000 adjuntat a tty0.

1. Editeu el fitxer `/etc/uucp/Systems`.
2. Afegiu la línia següent al final del fitxer. L'entrada ha de començar a la columna situada més a l'esquerra del fitxer.
   ```
   telebit Nvr TELEPROG 19200
   ```

3. Deseu el fitxer i sortiu.
4. Editeu el fitxer `/etc/uucp/Devices`.
5. Afegiu la línia següent al final del fitxer. L'entrada ha de començar a la columna situada més a l'esquerra del fitxer.

   ```
   TELEPROG tty0 - 19200 TelebitProgram
   ```
6. Deseu el fitxer i sortiu.
7. Editeu el fitxer `/etc/uucp/Dialers`.
8. Afegiu les línies següents al final del fitxer. Les entrades han de començar a la columna situada més a l'esquerra del fitxer.

   Nota: Les quatre línies següents s'han de convertir en una sola línia llarga:

   ```
   TelebitProgram  =,-,    "" \dAT&F\r\c OK
   ats0=1s2=255s7=60s11=50s41=2s45=255s51=252s63=1s58=2s64=1\r\c OK
   ATs69=2s105=0s111=30s255=0M0&C1Q2&D3&Q0&R3&S1&T5\r\c OK
   ATE0X12&W\r\c OK
   ```
9. Deseu el fitxer i sortiu.
10. Per començar la configuració automatitzada, escriviu l'ordre següent:

    ```
    cu -d telebit
    ```

    L'ordre no s'executarà satisfactòriament perquè no esteu connectant amb un sistema. Examineu la sortida de depuració de l'ordre per veure si `ATE0X12&W` s'ha enviat al mòdem i si s'ha rebut un OK. En cas afirmatiu, el mòdem s'ha programat satisfactòriament.

Poden aparèixer problemes a causa de la col•locació de valors incorrectes al fitxer `Dialers` o a causa de la configuració existent del mòdem. En aquest cas, proveu de programar manualment el mòdem i especifiqueu les sèries dels marcadors (del pas 8) d'una en una.

Configuració d'SLIP a través d'un mòdem

Per configurar el **Protocol d'interfície de línia sèrie (SLIP)** entre dos sistemes que es comuniquen a través d'un mòdem, podeu utilitzar aquest procediment, que alterna entre la interfície SMIT (System Management Interface Tool) i la línia d'ordres per completar la configuració.

Per claredat, les instruccions següents utilitzen els noms bronze i gold per als dos amfitrions.

1. Connecteu físicament els mòdems a bronze i a gold.
2. Per crear un tty a bronze utilitzant la SMIT, seguiu aquests passos:
   a. Escriviu:

      ```
      smit maktty
      ```
   b. Seleccioneu **rs232** com el tipus de tty que voleu crear.
   c. Seleccioneu un port en sèrie disponible, per exemple `sa0` (port en sèrie 1 del sistema).
   d. Seleccioneu de la llista un número de port per a aquest tty.
   e. Establiu la velocitat en BAUDS en la velocitat en bauds del vostre mòdem.
   f. Establiu Habilitar INICI DE SESSIÓ en disable.
   g. Sortiu de la SMIT.
3. Creeu un tty a gold.

   Seguiu el mateix procediments que heu seguit per a bronze (al pas 2), tret que heu d'establir Habilitar INICI DE SESSIÓ en **enable**.

   La resta d'aquestes instruccions pressuposen que el número de tty tant a bronze com a gold és tty1.
4. Proveu la connexió física amb l'ATE.
   a. A bronze, escriviu:

      ```
      ate
      ```

b. A Unconnected Main Menu, seleccioneu la subordre **Alter**. Estabiu la velocitat (Rate) en la velocitat en bauds del vostre mòdem i el dispositiu (Device) en tty1.
c. A Unconnected Main Menu, seleccioneu la subordre **Connect**. Quan l'ATE sol•liciti un número de telèfon, especifiqueu el número de telèfon de gold i feu clic a Intro.
d. En aquest punt, hauríeu de rebre un indicador d'inici de sessió per a gold. Inicieu una sessió.
e. Torneu a la pantalla connectada, finalitzeu la sessió de gold, feu clic Control-v (per anar a l'ATE CONNECTED MAIN MENU), feu clic a la tecla T per finalitzar la connexió i feu clic a la tecla Q per sortir de l'ATE.

Nota: Si no rebeu un indicador d'inici de sessió, torneu al pas 1 i comproveu que la configuració és correcta. No continueu fins que pugueu iniciar una sessió a gold.

5. Com que la configuració de tty que s'utilitza amb l'ATE és lleugerament diferent de la configuració que s'utilitza amb SLIP, heu de realitzar els següents canvis:
   a. A bronze, escriviu:
      ```
      smit chgtty
      ```
   b. A gold, escriviu:
      ```
      smit chgtty-pdisable tty1
      ```
   c. Seleccioneu **tty1** i, a continuació, seleccioneu **Canviar/mostrar programa TTY**.
   d. Estabiu Habilitar INICI DE SESSIÓ en disable i, a continuació, sortiu de la SMIT.
6. Afegiu la línia següent al fitxer `/usr/lib/uucp/Devices` tant de bronze com de gold.
   ```
   Direct tty1 - 9600 direct
   ```
   o bé substituïu `9600` per la velocitat del vostre mòdem.
7. Creeu una interfície de xarxa **SLIP** a bronze.
   a. Escriviu:
      ```
      smit mkinet1sl
      ```
   b. Per al PORT TTY de la interfície de xarxa SLIP, seleccioneu **tty1**.
   c. Especifiqueu una ADREÇA D'INTERNET, com per exemple 130.130.130.1.
   d. Especifiqueu l'adreça de DESTINACIÓ (de gold), com per exemple 130.130.130.2.
   e. Especifiqueu la VELOCITAT EN BAUDS del vostre mòdem.
   f. Especifiqueu la SÈRIE DE MARCATGE; per exemple:
      - "" AT OK ATDT555-1234 CONNECT ""
      - El significat d'aquesta ordre és: Utilitzeu **tty1** a 9600 bauds. Envieu AT al mòdem. El mòdem hauria de respondre amb OK. Marqueu el número de telèfon `555-1234`. El mòdem hauria de respondre amb `CONNECT`. Els espais abans i després dels caràcters `""` són necessaris.
   g. Sortiu de la SMIT.
8. Creeu una interfície de xarxa **SLIP** a gold. Seguiu el mateix procediment que heu seguit per a bronze (al pas 5), tret que heu d'intercanviar l'ADREÇA D'INTERNET i l'adreça de DESTINACIÓ.
9. Afegiu les dues entrades següents al fitxer **/etc/hosts** tant de bronze com de gold.
   ```
   130.130.130.1   bronze
   130.130.130.2   gold
   ```
   El nom que assigneu ha de ser exclusiu. És a dir, si la interfície Token-Ring de bronze ja té assignat el nom `bronze`, assigneu a la interfície **SLIP** un nom com ara `bronze_slip`.

   Nota: Per tal d'establir una interfície simplificada amb l'ordre **slattach**, podríeu utilitzar la seqüència `/usr/sbin/slipcall`.
10. Proveu la connexió **SLIP**.
    a. A bronze, escriviu:
       ```
       ping gold
       ```
    b. A gold, escriviu:

```
ping bronze
```

Si les dues proves son satisfactòries, la connexió **SLIP** està preparada per a l'ús. En cas contrari, torneu al pas 5 i verifiqueu que la configuració tant a bronze com a gold és correcta.

Configuració d'SLIP a través d'un cable de mòdem nul

Per configurar **SLIP** entre dos sistemes que estan connectats utilitzant un cable de mòdem nul, podeu utilitzar aquest procediment, que alterna entre la interfície SMIT (System Management Interface Tool) i la línia d'ordres per completar la configuració.

Per claredat, aquestes instruccions utilitzen els noms bronze i gold per als dos amfitrions.

1. Connecteu físicament bronze i gold utilitzant el cable de mòdem nul. Es necessiten els següents cables. (Els cables s'enumeren seguint l'ordre en què es connectaran des de bronze a gold).
   a. Cable B (número de peça 00G0943). Cable de pont del port en sèrie; se'n proporcionen dos amb cada sistema, tret dels models 220, 340 i 350 que no els necessiten.
   b. Cable D (número de peça 6323741, codi de dispositiu 2936). Cable asíncron EIA-232/V.24.
   c. Cable E (número de peça 59F2861, codi de dispositiu 2937). Adaptador d'impressora/terminal EIA-232 (cable de mòdem nul).
   d. Adaptador canviador (els dos costats de l'adaptador són sòcols).
2. Creeu un tty a bronze.
   a. Escriviu:
      ```
      smit maktty
      ```
   b. Seleccioneu **rs232** com el tipus de tty que voleu crear.
   c. Seleccioneu un port en sèrie disponible, per exemple **sa0** (port en sèrie 1 del sistema).
   d. Seleccioneu de la llista un número de port per a aquest tty.
   e. Establiu la velocitat en BAUDS en 19200. (Més tard canviareu aquest valor a 38400. Però, de moment, utilitzeu 19200.)
   f. Establiu Habilitar INICI DE SESSIÓ en disable i, a continuació, sortiu de la SMIT.
3. Creeu un tty a gold. Seguiu els mateixos passos que heu seguit per a bronze (al pas 2), tret que heu d'establir Habilitar INICI DE SESSIÓ en **enable**.

   Nota: La resta d'aquestes instruccions pressuposen que el número de tty tant a bronze com a gold és tty1.
4. Proveu la connexió física amb l'ATE.
   a. A bronze, escriviu:
      ```
      ate
      ```
   b. A Unconnected Main Menu, seleccioneu la subordre **Alter**. Establiu la velocitat (Rate) en 19200 i el dispositiu (Device) en tty1.
   c. A Unconnected Main Menu, seleccioneu la subordre **Connect**. Quan l'ATE sol•liciti un número de telèfon, feu clic a Intro. Hauríeu de rebre el següent missatge:
      ```
      ate: 0828-010 L'ordre Connect ha establert una connexió a través del port tty1
      ```
   d. Premeu Intro. Hauríeu de rebre un indicador d'inici de sessió per a gold. Inicieu una sessió a gold.
   e. Finalment, torneu a la pantalla connectada, finalitzeu la sessió de gold, feu clic a Control-v (per anar a l'ATE CONNECTED MAIN MENU), feu clic a la tecla T per finalitzar la connexió i feu clic a la tecla Q per sortir de l'ATE.

      Nota: Si no rebeu un indicador d'inici de sessió, torneu al pas 1 i comproveu que la configuració és correcta. No continueu fins que pugueu iniciar una sessió a gold.
5. Com que la configuració de tty que s'utilitza amb l'ATE és lleugerament diferent de la configuració que s'utilitza amb **SLIP**, heu de realitzar els següents canvis:

a. A bronze, escriviu:
   ```
   smit chgtty
   ```
b. Seleccioneu **tty1**. Estabiu la velocitat en BAUDS en `38400` i, a continuació, sortiu de la SMIT.
c. A gold, escriviu:
   ```
   pdisable tty1
   ```
d. A gold, escriviu:
   ```
   smit chgtty
   ```
e. Seleccioneu **tty1**. Estabiu Habilitar INICI DE SESSIÓ en disable, estabiu la velocitat en BAUDS en `38400` i, a continuació, sortiu de la SMIT.

6. Afegiu la línia següent al fitxer `/usr/lib/uucp/Devices` tant de bronze com de gold.
   ```
   Direct tty1 - 38400 direct
   ```
7. Creeu una interfície de xarxa **SLIP** a **bronze**.
   a. Escriviu:
      ```
      smit mkinet1sl
      ```
   b. Per al PORT TTY de la interfície de xarxa SLIP, seleccioneu **tty1**.
   c. Especifiqueu una ADREÇA D'INTERNET, com per exemple 130.130.130.1.
   d. Especifiqueu l'adreça de DESTINACIÓ (de gold), com per exemple `130.130.130.2`, i després seleccioneu D'acord o Intro.
   e.
8. Creeu una interfície de xarxa **SLIP** a gold. Seguiu el mateix procediment que heu seguit per a bronze (al pas 5), tret que heu d'intercanviar l'ADREÇA D'INTERNET i l'adreça de DESTINACIÓ.
9. Afegiu les dues entrades següents al fitxer `/etc/hosts` tant de bronze com de gold.
   ```
   130.130.130.1   bronze
   130.130.130.2   gold
   ```
   El nom que assigneu ha de ser exclusiu. És a dir, si la interfície Token-Ring de bronze ja té assignat el nom `bronze`, assigneu a la interfície **SLIP** un nom com ara `bronze_slip`.
10. Inicieu **SLIP** tant a bronze com a gold. Escriviu:
    ```
    slattach tty1
    ```
11. Proveu la connexió **SLIP**.
    a. A bronze, escriviu:
       ```
       ping gold
       ```
    b. A gold, escriviu:
       ```
       ping bronze
       ```

Si les dues proves son satisfactòries, la connexió **SLIP** està preparada per a l'ús. En cas contrari, torneu al pas 5 i verifiqueu que la configuració tant a bronze com a gold és correcta.

Desactivació d'una connexió SLIP

Per desactivar una connexió **SLIP**, utilitzeu aquest procediment.

1. Escriviu:
   ```
   ps -ef | grep slatt
   ```
   Observeu els números dels processos associats amb l'ordre **slattach**.
2. Per a cada número de procés, escriviu:
   ```
   kill número_procés
   ```
   No utilitzeu el senyalador **-9** de l'ordre **kill**.

   Si el procés **slattach** s'elimina amb l'ordre kill de manera accidental amb un senyalador **-9**, un bloqueig slip podria romandre a /etc/locks. Suprimiu aquest fitxer de bloqueig per netejar després del procés **slattach**.

Per desactivar temporalment una connexió **SLIP**, efectueu aquests passos tant al sistema local com al sistema remot:

1. Escriviu:
   ```
   ifconfig sl# down
   ```
2. Llisteu els processos **slattach** que actualment estan en execució utilitzant l'ordre:
   ```
   ps -ef | grep slat
   ```
   La sortida podria ser semblant a la següent:
   ```
   root  1269  1    0   Jun 25  ... slattach
   ```
3. Elimineu el procés **slattach** amb l'ordre kill utilitzant el seu ID de procés. Per exemple, per eliminar amb l'ordre kill el procés **slattach** que es mostra a l'exemple anterior, escriviu:
   ```
   kill 1269
   ```
   on 1269 es l'ID de procés d'**slattach**. *No* elimineu el procés **slattach** utilitzant el senyalador **-9** de l'ordre **kill**.

   La connexió **SLIP** ara està inhabilitada.

Activació d'una connexió SLIP

Utilitzeu aquestes instruccions per activar una connexió **SLIP** que està temporalment inhabilitada.

Executeu les següents ordres tant al sistema local com al sistema remot.

1. Escriviu:
   ```
   ifconfig sl# up
   ```
2. Torneu a executar l'ordre **slattach** utilitzada inicialment.

Eliminació d'una interfície SLIP

Utilitzeu les següents instruccions per eliminar completament una interfície **SLIP**.

Un cop s'han executat aquestes instruccions, s'eliminen la interfície sl# i el seu procés **slattach** associat. Les entrades realitzades al fitxer `/etc/hosts` romandran i s'hauran d'eliminar manualment.

1. Per eliminar la interfície **SLIP** i el seu procés **slattach** associat, utilitzeu el camí d'accés ràpid `smit rminet` per accedir a la pantalla **Interfícies de xarxa disponibles**.
2. Seleccioneu l'entrada apropiada a la pantalla **Interfícies de xarxa disponibles** i seleccioneu **Realitzar**.

   Nota: Les entrades realitzades al fitxer `/etc/hosts` romandran i s'hauran d'eliminar manualment.

Resolució de problemes d'SLIP

Aquestes ordres són necessàries per depurar problemes d'**SLIP**.

Cada ordre ve amb un exemple de com s'utilitza l'ordre per a resoldre problemes d'**SLIP**.

A més, es proporciona una llista de problemes i missatges d'error més freqüents que us servirà de referència.

Ordre netstat:

L'ordre **netstat** funciona conjuntament amb l'ordre **ifconfig** per proporcionar una condició d'estat de la interfície de xarxa TCP/IP.

L'ordre **netstat -in**, per exemple, utilitza el senyalador **-i** per presentar informació sobre les interfícies de xarxa mentre que el senyalador **-n** imprimeix les adreces IP en comptes dels noms d'amfitrió. Utilitzeu aquesta ordre per verificar les interfícies SLIP, les adreces i els noms d'amfitrió. La secció següent descriu la sortida de **netstat -in**.

Programeu el mòdem utilitzant els valors que apareixen a l'apartat "Consideracions sobre el mòdem SLIP" a la pàgina 617. L'exemple següent mostra com programar i desar els valors bàsics per a un mòdem compatible amb Hayes. Especifiqueu:

```
Nom  Mtu   Xarxa    Adreça             Ipkts     Ierrs Opkts Oerrs  Col
lo0   1536  <Link>                         2462       0    2462   0     0
lo0   1536  127        localhost.austi     2462       0    2462   0     0
tr0   1492  <Link>                         1914560    0   21000   0     0
tr0   1492  129.35.16  glad.austin.ibm     1914560    0   21000   0     0
sl0   552   1.1.1.0    1.1.1.1             48035      0   54963   0     0
sl1*  552   140.252.1  140.252.1.5         48035      0   54963   0     0
```

Observeu l'asterisc (*) al costat de la interfície sl1. Indica que la interfície de xarxa no està funcionant o que no està disponible per a l'ús. L'usuari ho pot corregir executant l'ordre **ifconfig sl1 up** si es tracta d'una interfície **SLIP** vàlida.

netstat proporciona estadístiques sobre els recomptes de paquets d'entrada i sortida, així com els errors d'entrada i sortida que són útils a l'hora de resoldre problemes de les connexions **SLIP**.

Per exemple, un usuari especifica una ordre **ping** en un amfitrió remot a través d'un enllaç **SLIP** i l'ordre **ping** sembla bloquejar-se. L'usuari executa ràpidament una ordre **netstat -in** des d'un altre intèrpret d'ordres i observa que augmenten els valors Opkts però que no hi ha valors Ipkts de l'amfitrió remot. Això indica que el sistema remot no torna (o no rep) la informació. L'usuari ha d'executar la mateixa ordre **netstat** al sistema remot per verificar la recepció dels paquets **ping** o l'augment en el recompte d'errors.

La conversió de noms d'amfitrió en números d'Internet és relativa a la resolució de noms i, per tant, crítica per al funcionament correcte d'una línia **SLIP**. Per depurar problemes de noms d'amfitrió, d'àlies i d'encaminament, utilitzeu l'ordre **netstat -rn**. El nom base de l'amfitrió o el nom d'amfitrió és l'únic nom que s'ha de tornar del fitxer **/etc/hosts**. Si la màquina rep servei tècnic d'un servidor de noms (és a dir, `/etc/resolv.conf` existeix), aleshores el servidor de noms tornarà el nom de domini completament qualificat en aquest ordre.

Ordre ifconfig:

L'ordre **ifconfig** és l'eina de configuració d'interfície de xarxa que permet crear o suprimir dinàmicament la interfície de xarxa STRUCTURE de la memòria del kernel.

Aquesta ordre accepta les dades de la línia d'ordres i, a continuació, munta una estructura de memòria que s'adapta als paràmetres. Per motius de depuració, l'ordre **ifconfig** s'utilitza per examinar l'estat d'una interfície de comunicacions.

Nota: Qualsevol canvi realitzat als atributs d'una interfície mitjançant l'ordre **ifconfig** es perdrà quan es reengegui el sistema.

Per exemple, per examinar l'estat actual de la interfície sl1:

1. Especifiqueu l'ordre **netstat -i** i examineu la sortida seleccionant la interfície sl# apropiada. Per exemple, sl0, sl1, sl2, i així successivament.
2. Especifiqueu l'ordre **ifconfig sl#** i examineu la sortida d'ifconfig per al següents camps clau:

Element	Descripció
Senyalador POINTTOPOINT	Aquest senyalador ha d'estar present sempre en un enllaç SLIP operatiu. En cas contrari, l'enllaç podria estar en un estar inactiu o desconnectat. Proveu de tornar a executar les ordres **ifconfig sl# up** i **ifconfig sl#** per veure si canvia la seva condició.
Senyalador UP	Indica que la interfície sl# de xarxa està activada i hauria d'estar operativa.
Senyalador RUNNING	Indica que l'ordre **slattach** s'ha executat satisfactòriament. De fet, s'ha accedit a l'enllaç, s'ha realitzat un marcatge, l'altre extrem ha contestat i l'extrem remot ha tornat l'estat DETECCIÓ DE PORTADORA (CD). Quan apareix l'estat CD, els senyaladors s'actualitzen amb el bit en execució.

Ordres pdisable i lsdev:

Qualsevol port tty que s'utilitza per a connexions **SLIP** ha de trobar-se en estat inhabilitat o no disponible.

Per verificar que el port per tty1 està inhabilitat, obtingueu l'autorització d'usuari root i especifiqueu una de les ordres següents:

- `lsattr -El tty1  -a login`

  Aquesta ordre mostra l'estat permanent del port tty tal com s'ha enregistrat al Gestor de base de dades d'objectes (ODM). Si la sortida és diferent de `login disable`, utilitzeu la SMIT per canviar el camp Habilitar INICI DE SESSIÓ a **disable**.
- `pdisable | grep tty1`

  Aquesta ordre, quan s'utilitza sense paràmetres, mostra tots els ports tty que es troben en estat inhabilitat. En aquest exemple, **pdisable** es connectarà amb l'ordre **grep** per eliminar la sortida innecessària. Si tty1 no es visualitza després d'executar aquesta ordre, el port no està inhabilitat.

Ordre ps:

L'ordre **ps** mostra informació sobre els processos actius a la sortida estàndard.

Utilitzeu aquesta ordre per verificar l'existència (o no existència) de processos **slattach** que s'utilitzen per assignar una línia tty a les interfícies de xarxa.

Si **netstat -in** mostra que la interfície no està funcionant, l'usuari ha d'executar l'ordre **ps -ef | grep slat** per veure si un procés **slattach** s'està executant actualment al port tty associat. Cal tenir en compte que per a una interfície **SLIP** connectada directament, les connexions trencades es reintenten automàticament sense intervenció manual. Per a una interfície **SLIP** connectada via mòdem, les connexions trencades s'han de tornar a marcar manualment. Si un usuari especifica una sèrie de marcatge a la línia d'ordres **slattach**, l'usuari ha de tornar a escriure l'ordre i la sèrie de marcatge per restaurar una connexió trencada.

Ordre ping i llums del mòdem:

L'ordre **ping** i les llums del mòdem s'utilitzen per depurar els problemes de les comunicacions **SLIP**.

Un ping és un paquet de sol•licitud d'eco, que s'envia fora de la màquina i es retorna un paquet de resposta d'eco. Aquesta seqüència d'incidències és útil si l'administrador pot veure els llums del mòdem.

Per exemple, un sistema local construeix el paquet de sol•licitud d'econ i l'envia al sistema remot. El llum SD (Dades d'enviament) del mòdem local s'encén. Això significa que el TCP/IP local, **slattach**, i tty han pogut agrupar la informació i enviar-la fora del mòdem fins al sistema remot.

El mòdem remot rep el paquet i el llum de dades de recepció parpelleja però el llum SD no. Això significa que el sistema remot no ha pogut enviar (o retornar) la sol•licitud de ping del sistema local. Com a conseqüència, l'usuari del sistema local pot veure que l'ordre **ping** es bloqueja, per la qual cosa cal fer Control-C per sortir de la condició.

La causa més habitual d'aquest problema és la utilització del control de flux XON/XOFF en un o els dos mòdems; no obstant això, l'usuari no ha de descartar la possibilitat d'encaminar o adreçar els conflictes en els sistemes.

Problemes i missatges d'error comuns d'SLIP:

Aquest tema descriu els problemes i missatges d'error comuns d'**SLIP**, les seves causes possibles i les accions d'usuari suggerides.

Missatge: 0821-296 No es pot establir la disciplina de línia per a `/dev/tty#` en slip.ioctl(TXSETLD). Una crida del sistema ha rebut un paràmetre que no és vàlid.

Causes possibles: Aquest tipus d'error normalment es produeix quan s'inicia el procés **slattach** i és atribuïble a una configuració incorrecta d'SLIP. Probablement la causa del problema és una discrepància entre el número de dispositiu tty i el número d'interfície sl. Això també explica per què el sistema ha informat que ifconfig no s'havia executat abans d'**slattach**.

Aquest problema també es pot produir quan els processos **slattach** s'eliminen incorrectament amb l'ordre kill o bé quan l'usuari intenta desplaçar una connexió **SLIP** a un altre port tty i s'oblida de tornar a configurar la interfície sl# per tal que coincideixi amb el tty. Comproveu els processos **slattach** en execució que encara poden estar executant-se (per exemple, `ps -ef | grep slat`).

Acció: El dispositiu tty per a SLIP és **/dev/tty24** i l'usuari ha creat una interfície sl0. Això és incorrecte. L'usuari ha de crear una interfície sl24 que coincideixi amb el número de tty (tty24 i sl24). Si el problema continua, l'usuari ha d'aturar la interfície sl (vegeu "Aturada d'una interfície SLIP") i torneu a configurar la connexió utilitzant les ordres següents:

```
lsdev  -Cc if  -s SL
lsattr -El sl0
```

Missatge:

la xarxa no està disponible actualment

el camí a l'amfitrió remot no està disponible

Causa possible: Aquests errors es produeixen molt sovint quan un usuari intenta fer ping a un amfitrió a través de l'enllaç **SLIP** i l'enllaç s'ha establert incorrectament. El problema més probable és que un o els dos ports tty associats amb la interfície sl# es troben en un estat habilitat. També és possible que existeixi un conflicte d'adreça o camí entre els sistemes amfitrions.

Accions:

- Elimineu la interfície sl# utilitzant el camí d'accés ràpid `smit rminet`. Això s'ha de fer tant a l'amfitrió SLIP local com al remot.
- Efectueu aquests passos per a cada amfitrió SLIP:
  1. Escriviu `pdisable | grep tty#`.
  2. Si el dispositiu tty NO està llistat a la sortida de l'ordre anterior, el tty no està inhabilitat. Inhabiliteu el tty mitjançant la SMIT o la línia d'ordres. Amb els ports tty inhabilitats, utilitzeu la SMIT per tornar a crear les interfícies **SLIP** en ambdós sistemes. Si el problema persisteix, verifiqueu els camins i les adreces de xarxa (si n'hi ha). Utilitzeu l'ordre **netstat -ir** per veure ràpidament informació sobre l'adreça, el camí i la interfície.

Problema: Quan l'indret remot fa un marcatge d'entrada a l'amfitrió local, el mòdem de l'amfitrió local es connecta però no completa el procés d'inici de sessió.

Causes possibles: Si els dos mòdems es connecten i comencen a donar la conformitat de connexió o a intercanviar informació de connexió però després es desconnecten, el problema pot ser a causa dels codis de resultats del mòdem. Aquest problema també pot produir-se per una sèrie de marcatge **slattach** incorrecta. Si els dos mòdems sonen però no comencen mai el procés de conformitat de connexió, la causa del problema pot ser que el mòdem no està configurat per a resposta automàtica.

Accions:

1. Primer proveu la connexió del mòdem amb l'ordre **cu**. El mòdem de l'amfitrió remot ha de permetre a l'usuari iniciar una sessió en el sistema. No ha d'haver caràcters inservibles a la pantalla durant l'intent d'inici de sessió; si n'hi ha, podria indicar una línia telefònica sorollosa que pot ser part del problema. Durant l'inici de sessió, *no* hi ha d'haver múltiples indicadors d'inici de sessió que es desplacin per la pantalla. Si hi són presents, podria indicar un cop més un problema amb la línia telefònica o valors incorrectes del mòdem.
2. Comproveu les configuracions del mòdem i intenteu desactivar els codis ARQ si actualment estan activats. A la majoria de mòdems compatibles amb Hayes, es tracta del valor &A0. El fet d'inhabilitar els codis de resultats ARQ no afecta les connexions controlades per errors ni tampoc impedeix que el mòdem torni missatges CONNECT estàndard (si els codis de resultats estan habilitats) segons calgui per a la sèrie de marcatge **slattach**.

Problema: L'usuari no pot fer **ping** en una connexió **SLIP** del mòdem. L'ordre **ping** es pot bloquejar o pot tornar missatges d'error.

Causes possibles:

1. Els mòdems i/o els ports tty poden estar configurats per utilitzar el control de flux XON/XOFF.
2. És possible que el procés **slattach** hagi finalitzat a l'amfitrió remot o que s'hagi eliminat la connexió del mòdem.
3. Les adreces assignades als amfitrions **SLIP** poden ser incorrectes.

Accions:

1. Examineu les configuracions dels mòdems local i remot. S'han d'establir per què utilitzin el control de flux RTS/CTS (maquinari) o bé per què no utilitzin cap control de flux. L'usuari ha d'intentar fer ping des de cada sistema. Feu ping del sistemaA al sistemaB.
2. Verifiqueu que el procés **slattach** encara s'executa tant al sistema local com al sistema remot. Utilitzeu l'ordre: `ps -ef |grep slat`. Verifiqueu que la interfície sl# es troba en un estat d'execució. Utilitzeu l'ordre: `ifconfig sl#`.
3. Verifiqueu que no existeixi cap conflicte entre les adreces **SLIP** i les que estan associades amb altres interfícies de xarxa (si n'hi ha). Utilitzeu l'ordre: **netstat -ir**. Si l'adreça o la classe d'adreça està en qüestió, torneu a configurar **SLIP** utilitzant un esquema d'adreces més senzill, com ara 1.1.1.1 per a l'amfitrió local i 1.1.1.2 per a l'amfitrió remot.

Qüestionari SLIP

Utilitzeu aquest qüestionari per enregistrar dades sobre les configuracions d'**SLIP**.

La informació recollida en aquests fulls es pot enviar per fax a un representant de servei quan faci falta assistència addicional amb la configuració d'**SLIP**.

1. Funcionava anteriorment aquesta configuració d'**SLIP**? (S/N) ____
2. Quins són els tipus de màquina? (per exemple: UNIX/PC, DOS/PC, etc.)

   Sistema local: _____ Sistema remot: _____

   Si l'amfitrió no és un sistema IBM UNIX, indiqueu el tipus de progr amari que s'utilitza per establir la connexió **SLIP**.

_____

3. Quines versions del sistema operatiu IBM UNIX hi ha a cadascuna de les unitats del sistema? Executeu l'ordre `/bin/oslevel`. Si aquesta ordre no es reconeix, utilitzeu el mètode següent:
   ```
   lslpp -h bos.rte
   ```
   cerqueu el nivell de release de línia *confirmació activa*.
   Sistema local: _____ Sistema remot: _____
4. Indiqueu totes les interfícies que estan disponibles en ambdós sistemes (per exemple, sl0, sl1). Per fer-ho, utilitzeu l'ordre: `lsdev -Cc if`
   Sistema local: _____ Sistema remot: _____

   _____ _____

   _____ _____

   _____ _____

   El número d'interfície **SLIP** ha de coincidir amb el número de dispositiu tty. Per exemple, `/dev/tty53` s'ha d'utilitzar amb sl53.
5. **SLIP** es configura mitjançant la SMIT o amb ordres? Les configuracions d'SLIP que utilitzen ordres no són permanents i no estan presents després de reengegar el sistema.

   _____
6. **SLIP** es configura a través de mòdems o d'una línia sèrie directa?

   _____
7. Si s'utilitzen mòdems, indiqueu el fabricant i el tipus de mòdem tant per al sistema local com per al sistema remot.

   ```
          TIPUS      VELOCITAT BAUDS  CABLATGE IBM Si no és cable IBM,
                               (Sí/No)    quin tipus?
   Local:  _________ __________    ___      _________________________
   Remot: _________ __________    ___      _________________________
   ```
8. Si s'utilitzen mòdems, quin és el tipus de portadora telefònica? (línia llogada o commutada normal)

   _____
9. Sobre quin maquinari s'utilitza la línia **SLIP**?
   Adaptador de 128 ports (amb RAN de 16 ports): ___
   Adaptador de 2 ports: ___
   Adaptador de 8 ports: ___
   Ports sèrie nadius, S1 o S2: ___
10. És possible fer ping des del sistema local al sistema remot?
    `(S/N) _____  (al sistema local, escriviu: ping <adreça remota> )`
11. És possible fer ping des del sistema remot al sistema local?
    `(S/N) _____  (al sistema remot, escriviu: ping <adreça local> )`
12. Els ports tty estan inhabilitats tant al sistema local com al sistema remot?
    `(S/N) _____`

    Utilitzeu l'ordre: `pdisable | grep tty#`. Només els números de tty inhabilitats es visualitzen com a sortida d'aquesta ordre.
13. Es visualitzen missatges d'error? En cas afirmatiu, indiqueu-los a continuació:

    _____

    _____

    _____

    _____

    _____

Emulació de terminal asíncron

El programa ATE (Emulació de terminal asíncron) permet als terminals del sistema operatiu emular un terminal, amb la qual cosa els usuaris disposen d'un mitjà per connectar-se a la majoria dels altres sistemes que donen suport als terminals asíncrons.

L'ATE ho aconsegueix fent que el sistema remot consideri un terminal com una pantalla del sistema o com un terminal DEC VT100. L'opció VT100 permet a l'usuari iniciar una sessió a sistemes que no donen suport al seu terminal però sí que en donen a terminals VT100.

L'ATE utilitza tant connexions directes (amb cable) com connexions via mòdem perquè el sistema de l'usuari i un sistema remot es comuniquin, tal com es mostra a la següent il•lustració.

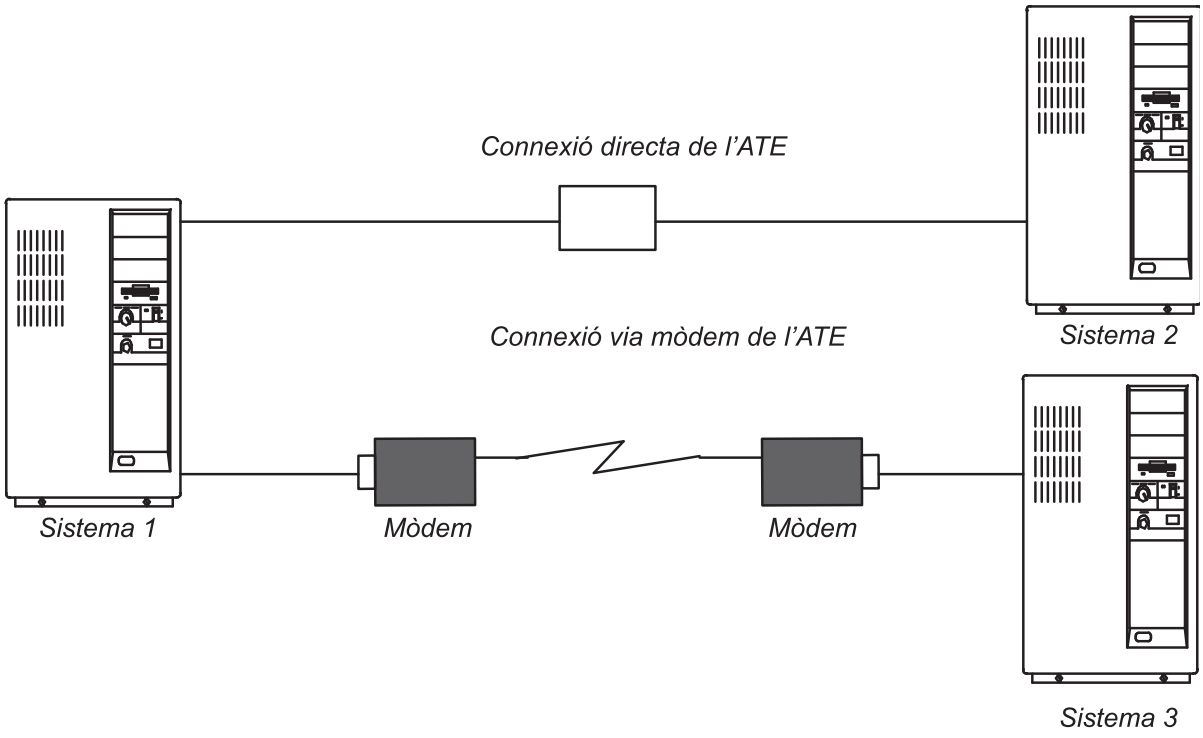


Figura 41. Tipus de connexions ATE

Depenent del tipus de connexió utilitzat, l'usuari pot configurar l'ATE per connectar-se a un sistema que sigui a la sala del costat com a un sistema que sigui a l'altra banda del país. Per establir una connexió directa, l'usuari ha de saber quin port ha d'utilitzar al seu sistema. Per una connexió via mòdem, els usuaris han de saber quin port s'ha utilitzar al seu sistema i el número de telèfon del sistema remot A més, els usuaris han de disposar d'un ID d'inici de sessió i una paraula clau per al sistema remot.

L'ATE permet que un usuari executi ordres al sistema remot, enviï i rebi fitxers, i utilitzi el protocol **xmodem** per comprovar la integritat de les dades dels fitxers transferits entre sistemes. L'usuari també pot capturar i arxivar dades que entren procedents del sistema remot.

Nota: Cal ser membre del grup UUCP (Programa de còpia UNIX a UNIX) a fi d'utilitzar l'ATE. Un usuari amb autorització root utilitza la SMIT (System Management Interface Tool) per instal•lar usuaris individuals en grups.

Configuració de l'ATE

Abans d'executar l'ATE, l'administrador del sistema ha d'instal•lar el programari adequat (si és necessari) i configurar el ports i connexions tty.

- L'ATE és un producte programa opcional. Tots els fitxers necessaris pel funcionament de l'ATE es troben dins del producte programa **bos.net.ate** que està disponible al suport d'emmagatzematge d'instal•lació. Utilitzeu les ordres següents per verificar que l'ATE està disponible en el sistema:

  ```
  lslpp -h | more   <return>
  /bos.net.ate      <return>
  ```

  Si l'ATE no està disponible en el sistema, instal•leu la imatge **bos.net.ate** des del suport d'emmagatzematge d'instal•lació (cinta, disquet o servidor de xarxa).
- Si l'ATE està instal•lat al sistema, es pot visualitzar una llista de fitxers associats amb aquest programa utilitzant les ordres següents:

  ```
  lslpp -f | more   <return>
  /bos.net.ate      <return>
  ```
- L'usuari ha de tenir autorització d'usuari root per configurar el port per al dispositiu de comunicacions.

L'ATE utilitza tant connexions directes (amb cable) com connexions via mòdem. Les connexions RS-232C locals permeten una distància màxima de 15 metres (50 peus) entre les màquines, i les connexions RS-422A permeten fins a 1200 metres (4000 peus) entre les màquines.

Abans d'utilitzar l'ATE per cridar un sistema remot, verifiqueu que el dispositiu tty del sistema remot està preparat per acceptar una crida.

Per tal de preparar l'ATE per què s'executi en el sistema , efectueu els passos següents:

1. Instal•leu una targeta adaptadora asíncrona en una ranura apropiada de la unitat del sistema, a menys que el sistema tingui un port en sèrie incorporat.
2. Endolleu el cable RS-232C o RS-422A a la targeta adaptadora o al port en sèrie incorporat.
3. Afegiu un dispositiu tty per al port de comunicacions utilitzant el camí d'accés ràpid `smit mkdev`.
4. Seleccioneu el tipus de terminal que s'ha d'emular amb l'ATE i feu els ajustaments necessaris per a l'entorn. Els canvis més comuns són la velocitat de línia, els valors de paritat, el nombre de bits per caràcter i si la línia s'ha de controlar com una línia remota o com una línia local. Utilitzeu bpc 8 i sense paritat si es requereix el Suport d'idioma nacional (NLS).
5. Configureu el port per al dispositiu. Per configurar un port per fer una crida de sortida amb l'ATE, utilitzeu l'ordre **pdisable**. Per exemple, per configurar el port tty1, escriviu:

   ```
   pdisable tty1
   ```

   Per configurar un port per tal que altres sistemes puguin fer una crida d'entrada, utilitzeu l'ordre **penable**. Per exemple, per permetre que altres sistemes facin una crida d'entrada al port tty2, escriviu:

   ```
   penable tty2
   ```
6. Assegureu-vos que el dispositiu s'hagi definit prèviament en el sistema remot. Un cop definit el dispositiu, cal personalitzar el programa ATE per tal que els valors del dispositiu es reflecteixin en el sistema remot. Personalitzeu els valors per defecte amb les subordres alter i modify o bé editant el fitxer per defecte `ate.def`. Per canviar els valors per defecte d'una connexió telefònica, utilitzeu una entrada del fitxer del directori de marcatge.

Menús principals de l'ATE

L'ATE visualitza menús segons les subordres utilitzades.

Si l'ATE s'inicia amb l'ordre **ate**, apareix l'Unconnected Main Menu, que permet:

- Canviar temporalment les característiques de l'ATE (**modify**, **alter**)
- Connectar-se a un altre sistema (**directory**, **connect**)
- Obtenir ajuda (**help**)
- Executar ordres del sistema operatiu de l'estació de treball al sistema (**perform**)
- Sortir de l'ATE (**quit**)

En funció de la subordre executada des de l'Unconnected Main Menu, l'ATE mostra diversos submenús:

Taula 107. Submenús ATE

Quan s'utilitza	**l'ATE mostra**
subordre **modify**	Modify Menu (per obtenir informació, vegeu l'ordre **ate** a *Commands Reference, Volume 1*)
subordre **alter**	Alter Menu (per obtenir informació, vegeu l'ordre **ate** a *Commands Reference, Volume 1*)
subordre **connect** o **directory** per connectar a un sistema remot	Connected Main Menu
subordre **directory**	directori de marcatge (una llista de números de telèfon)

Des del Connected Main Menu, es poden executar subordres per:
- Enviar fitxers al sistema remot i rebre'n (**send**, **receive**)
- Enviar un senyal de trencament al sistema remot (**break**)
- Finalitzar la connexió amb el sistema remot (**terminate**)

A més a més, les subordres **modify**, **alter**, **help**, **perform** i **quit** duen a terme les mateixes funcions que les que es proporcionen a l'Unconnected Main Menu.

És possible controlar algunes accions de l'ATE amb seqüències de tecles de control. Aquestes seqüències de tecles es coneixen com CAPTURE_KEY, MAINMENU_KEY i PREVIOUS_KEY. Les seqüències de tecles es comenten a l'apartat "Seqüències de tecles de control de l'ATE" a la pàgina 632. L'ATE està instal•lada amb les combinacions per defecte d'aquestes tecles, però es poden canviar les combinacions modificant el fitxer per defecte de l'ATE, `ate.def`.

ATE Unconnected Main Menu:

S'utilitza l'ordre **ate** per visualitzar l'ATE Unconnected Main Menu.

Un cop s'ha establert la connexió, s'utilitza la subordre de l'ATE **connect** per mostrar l'Unconnected Main Menu.

Les següents subordres es poden executar des de l'ATE Unconnected Main Menu. Per executar la subordre, escriviu la primera lletra de la subordre a l'indicador d'ordres del menú. Per exemple, escriviu **d** per executar la subordre **directory**.

Element	**Descripció**
alter	Canvia temporalment les característiques de la transmissió de dades, com ara la velocitat de transmissió.
connect	Estableix una connexió.
directory	Mostra una guia de telèfons.
help	Mostra la informació d'ajuda.
modify	Modifica temporalment els valors locals, com ara el fitxer de captura per a les dades entrants.
perform	Permet dur a terme ordres del sistema operatiu de l'estació de treball dins l'ATE.
quit	Surt del programa ATE.

Nota: De les seqüències de tecles de control CAPTURE_KEY, MAINMENU_KEY i PREVIOUS_KEY, només PREVIOUS_KEY es pot utilitzar des de l'ATE Unconnected Main Menu.

ATE Connected Main Menu:

Utilitzeu la subordre **connect** des del Unconnected Main Menu de l'ATE per veure el Connected Main Menu.

Com a alternativa, feu clic MAINMENU_KEY durant una connexió a un sistema remot.

Les següents subordres es poden executar des de l'ATE Connected Main Menu. Per veure les definicions d'aquestes subordres, consulteu l'ordre **ate** a *Commands Reference, Volume 1*. Per executar la subordre, escriviu la primera lletra de la subordre a l'indicador d'ordres del menú. Per exemple, escriviu `a` per executar la subordre **alter**.

Element	Descripció
alter	Canvia temporalment les característiques de la transmissió de dades, com ara la velocitat de transmissió.
break	Envia un senyal de trencament al sistema remot.
help	Mostra la informació d'ajuda.
modify	Modifica temporalment els valors locals utilitzats per l'emulador, com ara el fitxer de captura per a les dades entrants.
perform	Permet dur a terme ordres del sistema operatiu de l'estació de treball dins l'ATE.
quit	Surt del programa ATE.
receive	Rep fitxers des d'un sistema remot.
send	Envia fitxers a un sistema remot.
terminate	Interromp la connexió de l'ATE.

Les tres seqüències de tecles de control de l'ATE es poden utilitzar des de l'ATE Connected Main Menu.

Seqüències de tecles de control de l'ATE

Utilitzeu les següents tecles de control amb l'ATE. Canvieu la seqüència de tecles de cada funció editant el fitxer `ate.def`.

Element	Descripció
CAPTURE_KEY	Inicia o atura el desament de les dades que apareixen en pantalla durant una connexió. La seqüència de tecles per defecte de la CAPTURE_KEY és Control-B. La CAPTURE_KEY té un efecte de commutació. Si es fa clic a aquesta tecla de control s'inicia el desament de dades. Si es fa clic a aquesta tecla de control una segona vegada s'atura el desament de dades. Les dades es desen al fitxer de captura definit al fitxer `ate.def`. El nom del fitxer de captura per defecte és el fitxer `$HOME/kapture`. Utilitzeu la subordre **modify** per canviar temporalment el nom del fitxer de captura. Editeu el fitxer per defecte de l'ATE per canviar permanentment el nom del fitxer de captura. Consulteu l'apartat "Edició del fitxer per defecte de l'ATE" a la pàgina 641. La seqüència de tecles CAPTURE_KEY no funciona mentre el terminal està duent a terme una operació de transferència de fitxers, i és vàlida només quan s'estableix una connexió. Si feu clic la seqüència de tecles CAPTURE_KEY abans que s'estableixi una connexió, la següent ordre especificada no s'executa satisfactòriament i apareix un missatge d'error.
PREVIOUS_KEY	Torna a la pantalla anterior. La PREVIOUS_KEY també s'utilitza per aturar una operació de transferència de fitxers. La seqüència de tecles per defecte de la PREVIOUS_KEY és Control-R. La PREVIOUS_KEY també es pot utilitzar des de qualsevol ATE Main Menu.

Element	Descripció
MAINMENU_KEY	Mostra el Connected Main Menu per poder executar una subordre de l'ATE. La seqüència de tecles per defecte de la MAINMENU_KEY és Control-V. Utilitzeu aquesta tecla de control per visualitzar el Connected Main Menu després que s'hagi establert una connexió a un sistema remot. Si feu clic la seqüència de tecles MAINMENU_KEY abans que s'estableixi una connexió, la següent ordre especificada no s'executa satisfactòriament i apareix un missatge d'error. Si l'usuari personalitza el fitxer per defecte de l'ATE, es poden canviar permanentment els valors de tecles de control i el nom del fitxer de captura. Consulteu l'apartat "Edició del fitxer per defecte de l'ATE" a la pàgina 641.

Personalització de l'ATE

L'ATE crea el fitxer `ate.def` per defecte al directori actual la primera vegada que l'usuari executa l'ATE. Editeu el fitxer `ate.def` per personalitzar diversos aspectes de l'ATE.

Per exemple, l'usuari pot canviar el nom del fitxer de directori de marcatge, el tipus de protocols de transferència utilitzats per enviar i rebre fitxers des del sistema remot i la velocitat en bauds que l'ATE preveu que el mòdem utilitzi. Consulteu l'apartat "Edició del fitxer per defecte de l'ATE" a la pàgina 641 per obtenir més informació sobre el fitxer `ate.def`.

Els usuaris també poden fer canvis temporals a alguns aspectes de l'ATE amb les subordres **modify** i **alter**. Aquestes subordres poden modificar tots els valors per defecte de l'ATE excepte les seqüències de tecles de control (que només es poden canviar editant el fitxer per defecte) i el nom del directori de marcatge (que es pot canviar amb la subordre **directory** o editant el fitxer per defecte). Tots els canvis efectuats amb les subordres **modify**, **alter** o **directory** només són efectius per a aquella sessió de l'ATE. La propera vegada que l'usuari executa l'ATE, els valors utilitzats són els que es defineixen al fitxer per defecte.

Quan s'utilitza un mòdem amb l'ATE, l'usuari pot crear un directori de marcatge de fins a 20 números de telèfon. La subordre **directory** mostra els números de telèfon en forma de menú i permet a l'usuari seleccionar el sistema que desitja cridar. Consulteu l'apartat "Configuració d'un directori de marcatge de l'ATE" a la pàgina 637 per obtenir més informació.

Amb la utilització d'un directori de marcatge, l'usuari s'evita haver de buscar el número de telèfon quan vol cridar un sistema en concret. L'usuari també pot especificar algunes característiques de transmissió de dades al fitxer del directori de marcatge. Això és útil si algunes connexions utilitzen característiques que difereixen dels valors per defecte de l'ATE.

Podeu crear un directori de marcatge personalitzat i l'administrador del sistema pot crear un directori de marcatge que abasti tot el sistema. Especifiqueu quin directori de marcatge cal utilitzar al fitxer per defecte de l'ATE. Vegeu l'apartat "Configuració d'un directori de marcatge de l'ATE" a la pàgina 637 per obtenir més informació.

Fitxer de configuració ate.def:

El fitxer `ate.def` estableix els valors per defecte que s'utilitzaran en les connexions asíncrones i en les transferències de fitxers.

Aquest fitxer es crea en el directori actual durant la primera execució de l'ATE. El fitxer `ate.def` conté els valors per defecte del programa ATE utilitzats per:

- Característiques de la transmissió de dades
- Característiques del sistema local
- Fitxer del directori de marcatge
- Tecles de control.

La primera vegada que el programa ATE s'executa des d'un determinat directori, crea un fitxer `ate.def` en aquest directori.

```
LENGTH          8
STOP            1
PARITY          0
RATE            1200
DEVICE          tty0
INITIAL         ATDT
FINAL
WAIT            0
ATTEMPTS        0
TRANSFER        p
CHARACTER       0
NAME            kapture
LINEFEEDS       0
ECHO            0
VT100           0
WRITE           0
XON/XOFF        1
DIRECTORY       /usr/lib/dir
CAPTURE_KEY     002
MAINMENU_KEY    026
PREVIOUS_KEY    022
```

Editeu el fitxer `ate.def` amb qualsevol editor de textos ASCII per canviar de manera permanent els valors d'aquestes característiques. Canvieu temporalment els valors d'aquestes característiques amb les subordres **alter** i **modify** de l'ATE, accessibles des de l'ATE Main Menu.

Escriviu noms de paràmetres en lletres majúscules en el fitxer `ate.def`. Escriviu els paràmetres exactament tal com apareixen al fitxer per defecte original. Definiu només un paràmetre per línia. Un valor definit incorrectament per a un paràmetre fa que l'ATE torni un missatge del sistema. No obstant això, el programa segueix executant-se utilitzant el valor per defecte. Són els paràmetres del fitxer `ate.def`:

LENGTH
Especifica el nombre de bits en un caràcter de dades. Aquesta longitud ha de coincidir amb la longitud que espera el sistema remot.

```
Opcions:  7 ó 8
Valor per defecte:  8
```

STOP Especifica el nombre de bits d'aturada afegits a un caràcter per senyalar el final d'aquest caràcter durant la transmissió de dades. Aquest nombre ha de coincidir amb el nombre de bits d'aturada que utilitza el sistema remot.

```
Opcions:  1 ó 2
Valor per defecte:  1
```

PARITY
Comprova si un caràcter s'ha transmès satisfactòriament a o des d'un sistema remot. Ha de coincidir amb la paritat del sistema remot.

Per exemple, si l'usuari selecciona la paritat parell, quan el nombre de bits 1 del caràcter es senar, s'activa el bit de paritat per fer un nombre parell de bits 1.

```
Opcions: 0 (cap), 1 (senar) o 2 (parell)
Valor per defecte: 0.
```

RATE Determina la velocitat en bauds, o el nombre de bits transmesos per segon (bps). La velocitat ha de coincidir amb la velocitat del mòdem i amb la del sistema remot.

```
Opcions: 50,75,110,134,150,300,600,1200,1800,2400,4800,9600,19200
Valor per defecte: 1200
```

DEVICE
Especifica el nom del port asíncron utilitzat per establir una connexió amb un sistema remot.

```
Opcions: Noms de port creats localment.
Valor per defecte: tty0.
```

INITIAL
Defineix el prefix de marcatge, una sèrie que ha de precedir al número de telèfon quan l'usuari realitza un marcatge automàtic amb un mòdem. Per veure les ordres de marcatge correctes, consulteu la documentació del mòdem.

```
Opcions: ATDT, ATDP o altres, en funció del tipus de mòdem.
Valor per defecte: ATDT.
```

FINAL
Defineix el sufix de marcatge, una sèrie que ha de seguir al número de telèfon quan l'usuari realitza un marcatge automàtic amb un mòdem. Per veure les ordres de marcatge correctes, consulteu la documentació del mòdem.

```
Opcions: Espai en blanc (cap) o un sufix de mòdem vàlid.
Valor per defecte: Cap.
```

WAIT Especifica el temps que s'ha d'esperar entre els intents de tornar a marcar. El període d'espera no comença fins que l'intent de connexió esgota el temps d'espera o fins que s'interromp. Si el paràmetre ATTEMPTS està establert en 0, no es produeix cap intent de tornar a marcar.

```
Opcions: 0 (cap) o un enter positiu que designa el nombre de segons que cal esperar.
Valor per defecte: 0
```

ATTEMPTS
Especifica el nombre màxim de vegades que el programa ATE intenta tornar a marcar per establir una connexió. Si el paràmetre ATTEMPTS està establert en 0, no es produeix cap intent de tornar a marcar.

```
Opcions: 0 (cap) o un enter positiu que designa el nombre d'intents.
Valor per defecte: 0
```

TRANSFER
Defineix el tipus de protocol asíncron que transfereix fitxers durant una connexió.

p (pacing)
El protocol de transferència de fitxers controla la velocitat de transmissió de dades esperant un caràcter especificat o un determinat nombre de segons entre transmissions de línies. D'aquesta manera s'evita la pèrdua de dades quan els blocs de transmissió són massa grans o s'envien massa de pressa per què el sistema els pugui processar.

x (xmodem)
Un protocol de transferència de fitxers de 8 bits per detectar errors de transmissió de dades i retransmetre les dades.

```
Opcions: p (pacing), x (xmodem)
Valor per defecte: p.
```

CHARACTER
Especifica el tipus de protocol pacing que s'ha d'utilitzar. Senyal per transmetre una línia. Seleccioneu un caràcter.

Quan la subordre **send** troba un caràcter de salt de línia mentre es transmeten dades, la subordre s'espera per rebre el caràcter pacing abans d'enviar la línia següent.

Quan la subordre **receive** està preparada per rebre dades, envia el caràcter pacing i després espera 30 segons per rebre les dades. La subordre **receive** torna a enviar un caràcter pacing sempre que troba un caràcter de retorn de carro a les dades. La subordre **receive** finalitza quan no rep cap dada durant 30 segons.

```
Opcions: Qualsevol caràcter
Valor per defecte: 0
```

Interval
Nombre de segons que el sistema espera entre cada línia que transmet. El valor de la variable Interval ha de ser un enter. El valor per defecte és 0, que indica un retard de pacing de 0 segons.

```
Valor per defecte: 0.
```

NAME
Nom de fitxer per a les dades d'entrada (fitxer de captura).

```
Opcions: Un nom de fitxer vàlid amb menys de 40 caràcters.
Valor per defecte: kapture
```

LINEFEEDS
Afegeix un caràcter de salt de línia després de cada caràcter de retorn de carro del corrent de dades d'entrada.

```
Opcions: 1 (activat) o 0 (desactivat).
Valor per defecte: 0.
```

ECHO Mostra l'entrada que ha escrit l'usuari. Per a un ordinador remot que dóna suport a l'eco, cada caràcter enviat es retorna i es visualitza a la pantalla. Quan el paràmetre ECHO està activat, cada caràcter es visualitza dues vegades; primer quan s'escriu i després quan es retorna a través d'un connexió. Quan el paràmetre ECHO està desactivat, cada caràcter només es visualitza quan es retorna a través de la connexió.

```
Opcions: 1 (activat) o 0 (desactivat).
Valor per defecte: 0.
```

VT100 La consola local emula un terminal DEC VT100 de manera que el codi DEC VT100 pot utilitzar-se amb el sistema remot. Amb el paràmetre VT100 desactivat, la consola local funciona com una estació de treball.

```
Opcions: 1 (activat) o 0 (desactivat).
Valor per defecte: 0.
```

WRITE
Captura les dades d'entrada i les encamina al fitxer especificat en el paràmetre NAME així com a la pantalla. Les combinacions de retorn de carro o salt de línia es converteixen en caràcters de salt de línia abans que s'escriguin al fitxer de captura. En un fitxer existent, les dades s'afegeixen al final del fitxer.

Es pot utilitzar el paràmetre CAPTURE_KEY (normalment la seqüència de tecles Control-B) per commutar el mode de captura entre activat i desactivat durant una connexió.

```
Opcions: 1 (activat) o 0 (desactivat).
Valor per defecte: 0.
```

XON/XOFF
Controla la transmissió de dades en un port, tal com s'indica a continuació:

- Quan es rep un senyal XOFF, la transmissió s'atura.
- Quan es rep un senyal XON, la transmissió es reprèn.
- S'envia un senyal XOFF quan el buffer de recepció es gairebé ple.
- S'envia un senyal XON quan el buffer ja no està ple.

```
Opcions: 1 (activat) o 0 (desactivat).
Valor per defecte: 1.
```

DIRECTORY
Especifica el fitxer que conté el directori de marcatge de l'usuari.

```
Valor per defecte: El fitxer /usr/lib/dir.
```

CAPTURE_KEY
Defineix la seqüència de tecles de control que commuta el mode de captura. Quan es fa clic, el paràmetre CAPTURE_KEY (normalment la seqüència de tecles Control-B) inicia o atura la captura (desament) de les dades que es visualitzen a la pantalla durant una connexió activa.

Opcions: Qualsevol caràcter de control ASCII.
Valor per defecte: 002 octal ASCII (STX).

MAINMENU_KEY
Defineix la seqüència de tecles de control que torna el Connected Main Menu per tal que l'usuari pugui executar una ordre durant una connexió activa. El paràmetre MAINMENU_KEY (normalment la seqüència de tecles Control-V) només funciona des de l'estat connectat.

Opcions: Qualsevol caràcter de control ASCII.
Valor per defecte: 026 octal ASCII (SYN).

PREVIOUS_KEY
Defineix la seqüència de tecles de control que mostra la pantalla anterior en qualsevol moment durant l'execució del programa. La pantalla que es visualitzada varia en funció de la pantalla que està ús quan l'usuari fa clic a PREVIOUS_KEY (normalment la seqüència de tecles Control-R).

Opcions: Qualsevol caràcter de control ASCII.
Valor per defecte: 022 octal ASCII (DC2).
El caràcter de control ASCII es mapeja amb el senyal d'interrupció.

Configuració d'un directori de marcatge de l'ATE

El fitxer del directori de marcatge de l'ATE conté una llista de números de telèfon que el programa ATE utilitza per establir connexions remotes via mòdem.

Per configurar un directori de marcatge de l'ATE, s'han de complir els següents requisits:

- Cal configurar el programa ATE (Emulació de terminal asíncron) al sistema
- Per configurar un directori de marcatge que abasti tot el sistema, l'usuari ha de tenir accés d'escriptura al fitxer /usr/lib/dir

El usuaris assignen un nom de fitxer vàlid al fitxer del directori de marcatge i el col•loquen en un directori que tingui accés de lectura i escriptura. Editeu el fitxer del directori de marcatge amb qualsevol editor de textos ASCII. La informació del directori de marcatge per defecte es troba al fitxer /usr/lib/dir, com es mostra a continuació:

Nota: En el contingut següent, algunes entrades de l'ATE s'han descomposat en diferents línies per facilitar la seva lectura. No obstant això, en un fitxer del directori de marcatge, tots els elements d'una entrada s'han de declarar en una sola línia contínua.

```
#   NOM_COMPONENT: BOS dir
#
#   FUNCIONS:
#
#   ORIGENS: 27
#
#
#   (C) COPYRIGHT International Business Machines Corp. 1985, 1989
#   Materials sota llicència - Propietat d'IBM
#
#  Drets restringits als usuaris del governs dels EUA - L'ús, la duplicació o
#  la divulgació estan subjectes a les restriccions publicades al GSA ADP Schedule Contract amb IBM Corp.
#
#   dir - directori de marcatge d'exemple
#
#
# Micom   9,555-9400 1200 7 1 2 0 0
# R20     9,555-9491 1200 7 1 2 0 0
# QT      9,555-8455 1200 7 1 2 0 0
# Dallas1 9,555-7051 1200 8 1 0 0 0
```

Els usuaris poden accedir a la informació del directori de marcatge des de dins de l'ATE utilitzant la subordre **directory** que està disponible a l'**UNCONNECTED MAIN MENU**. La pantalla mostrarà la informació del directori tal com apareixeria des de dins del programa ATE.

Els usuaris poden tenir més d'un directori de marcatge. Per canviar el fitxer del directori de marcatge que utilitza el programa ATE, l'usuari ha de modificar el fitxer `ate.def` del directori actual.

> **Nota:** El fitxer del directori de marcatge pot contenir fins a 20 línies (una entrada per línia). L'ATE ignora les línies subsegüents.

El fitxer del directori de marcatge és semblant a una pàgina d'una llibreta de telèfons que conté entrades per als sistemes remots cridats amb el programa ATE. Una entrada del directori de marcatge té el següent format:

```
Nom Telèfon Velocitat Longitud BitAturada Paritat Eco Saltlínia
```

Els camps han estar separats almenys per un espai. Es poden utilitzar més espai fer facilitar la lectura de cada entrada. Els camps són els següents:

Nom Identifica un número de telèfon. El nom pot ser qualsevol combinació de 20 o menys caràcters. Utilitzeu el caràcter de subratllat (_) en comptes d'un espai en blanc entre les paraules d'un nom; per exemple, banc_dades.

Telèfon
El número de telèfon que s'ha de marcar. El número pot tenir fins a 40 caràcters. Consulteu la documentació del mòdem per veure una llista de dígits i caràcters acceptables. Per exemple, si s'ha de marcar un 9 per accedir a una línia externa, inclogueu un 9, (el numeral 9 i una coma) abans del número de telèfon, com a l'exemple següent: 9,1112222.

Malgrat que el número de telèfon pot tenir fins a 40 caràcters, la subordre directory només mostra els primers 26 caràcters.

Velocitat
Velocitat de transmissió o en bauds expressada en bits per segon (bps). Determina el nombre de caràcters que es transmeten per segon. Seleccioneu una velocitat en bauds que sigui compatible amb la línia de comunicacions que s'està utilitzant. Les següents velocitats són acceptables:

50, 75, 110, 134, 150, 300, 600, 1200, 1800, 2400, 4800, 9600 o 19200.

En els cas de les velocitats en bauds no POSIX, el fet d'establir la velocitat en 50 fa que l'ATE utilitzi la velocitat en bauds configurada que s'ha establert mitjançant la SMIT per al dispositiu en qüestió.

Longitud
Nombre de bits que composen un caràcter. L'entrada per al camp Longitud pot ser 7 o 8.

BitAturada
Els bits d'aturada indiquen el final d'un caràcter. L'entrada per al camp BitAturada pot ser 1 o 2.

Paritat
Comprova si un caràcter s'ha transmès satisfactòriament a o des d'un sistema remot. L'entrada per al camp Paritat pot ser 0 (cap), 1 (senar) o 2 (parell).

Eco Determina si els caràcters escrits es visualitzen localment. L'entrada per al camp Eco pot ser 0 (desactivat) o 1 (activat).

Saltlínia
Afegeix un caràcter de salt de línia al final de cada línia de dades que entra des d'un sistema remot. La funció del caràcter de salt de línia és semblant a la dels caràcters de retorn de carro i línia nova. L'entrada per al camp Saltlínia pot ser 0 (desactivat) o 1 (activat).

Nota: Si les tecles de control entren en conflicte entre aplicacions, és possible que calgui canviar-les o remapejar-les. Per exemple, si les tecles de control mapejades per al programa ATE entren en conflicte amb les d'un editor de textos, remapegeu les tecles de control de l'ATE.

Nota: El caràcter de control ASCII seleccionat pot estar en format octal, decimal o hexadecimal, com s'indica a continuació:

octal 000 a 037. El zero inicial és obligatori.

decimal
0 a 31.

hexadecimal
0x00 a 0x1F. El 0x inicial és obligatori. La x pot estar en majúscula o en minúscula.

Creeu un fitxer `ate.def` que defineixi aquestes característiques per canviar les característiques d'una emulació ATE. Per exemple, per canviar la velocitat (RATE) a 300 bps, el dispositiu (DEVICE) a tty3, el mode de transferència (TRANSFER) a x (protocol xmodem) i el directori (DIRECTORY) a my.dir, creeu un fitxer `ate.def` amb les següents entrades, al directori que executa el programa ATE:

```
RATE          300
DEVICE        tty3
TRANSFER      x
DIRECTORY     my.dir
```

El programa utilitza els valors definits des del moment en què el programa ATE s'inicia des d'aquest directori.

1. Creeu el fitxer del directori de marcatge:
   a. Canvieu al directori en el qual residirà el fitxer del directori de marcatge.
   b. Copieu el fitxer `/usr/lib/dir` per utilitzar-lo com a plantilla. Canvieu el nom del fitxer per un nom de fitxer vàlid.
   c. Creeu entrades de números de telèfon mitjançant el format que es determina al format de fitxer del directori de marcatge.
   d. Deseu el fitxer.

   Nota: Si el nou fitxer del directori de marcatge ha de ser el fitxer per defecte en tot el sistema, deseu el fitxer amb el nom `/usr/lib/dir`.
2. Si el nom del fitxer del directori de marcatge no està establert per defecte (`/usr/lib/dir`), editeu el fitxer `ate.def` al directori des del qual s'executa el programa ATE. Canvieu el paràmetre *DIRECTORI* del fitxer `ate.def` pel nou fitxer del directori de marcatge. Consulteu l'apartat "Edició del fitxer per defecte de l'ATE" a la pàgina 641
3. Inicieu l'ATE i visualitzeu el directori de marcatge amb la subordre **directory**.

Marcatge de sortida amb l'ATE

Utilitzeu aquest procediment per fer un marcatge de sortida d'un sistema utilitzant l'ATE i un fitxer del directori de marcatge `/usr/lib/dir` personalitzat.

Verifiqueu que es compleixen tots els prerequisits i condicions següents abans d'intentar fer un marcatge de sortida.

- L'ATE està instal•lat al sistema.
- Un mòdem està connectat, configurat i preparat per a l'ús.
- L'usuari és membre del grup UUCP (vegeu l'apartat "Configuració de l'ATE" a la pàgina 630 per obtenir més informació).
- El fitxer del directori de marcatge `/usr/lib/dir` ja està personalitzat amb la informació correcta.
- El directori de treball actual de l'usuari (`pwd`) conté un fitxer `ate.def` que està correctament actualitzat.
- El port `/dev/tty` ha de tenir el seu camp Habilitar INICI DE SESSIÓ de la SMIT establert en disable, share o delay.

1. Especifiqueu:
   ```
   ate
   ```

2. En el menú principal, escriviu `d` i feu clic a Intro.
3. Escriviu el nom de fitxer del directori que voleu visualitzat i feu clic a Intro. Per utilitzar el directori actual, simplement feu clic a Intro.
4. Especifiqueu el número d'entrada del directori apropiat sota la columna **#** per marcar el corresponent número de telèfon.

Transferència d'un fitxer utilitzant l'ATE

Utilitzeu aquest procediment per transferir un fitxer des d'un amfitrió local al sistema remot.

Verifiqueu que es compleixen tots els prerequisits i condicions següents abans d'intentar transferir un fitxer mitjançant ATE.

- Cal que ja s'hagi establert una connexió utilitzant el programa **ATE**.
- Cal que ja existeixi el protocol de transferència de fitxers Xmodem tant al sistema local com al sistema remot. Al sistema operatiu, Xmodem es troba en el directori `/usr/bin`.

1. Executeu la següent ordre **xmodem** en el sistema remot després d'iniciar una sessió:

   ```
   xmodem -r fitxer_nou
   ```

   on **r** és el senyalador Xmodem per rebre i *fitxer_nou* és el nom de fitxer que s'ha de rebre. No cal que aquest nom sigui el mateix que el fitxer que s'està transferint.
2. Premeu Intro.
3. Apareix el següent missatge:

   ```
   ate: 0828-005 El sistema està preparat per rebre el fitxer fitxer_nou.
   Utilitzeu Control-X per aturar el mòdem.
   ```

   Si el missatge no es visualitza, és possible que el sistema no tingui el programa **xmodem** instal•lat o ubicat al seu CAMÍ D'ACCÉS d'ordres.
4. Premeu Control-V per tornar a l'ATE CONNECTED MAIN MENU.
5. Premeu la tecla S per enviar un fitxer.
6. Apareix el següent missatge:

   ```
   Escriviu el nom del fitxer que voleu enviar i feu clic a Intro. Per utilitzar el darrer
   nom de fitxer (), simplement feu clic a Intro.
   ```
7. Escriviu el nom i el camí d'accés complet del fitxer que s'ha de transferir.
8. Premeu Intro.
9. L'ATE mostrarà el següent missatge i començarà a transferir el fitxer:

   ```
   ate: 0828-024 El programa està preparat per enviar el fitxer fitxer_nou. Rebreu un altre
   missatge quan hagi finalitzat la transferència.
   ate: 0828-025 El sistema està enviant el bloc 1.
   ate: 0828-025 El sistema està enviant el bloc 2.
   ate: 0828-015 La transferència del fitxer ha finalitzat.
   ate: 0828-040 Premeu Intro
   ```
10. Premeu Intro quan la transferència hagi finalitzat.

Recepció d'un fitxer utilitzant l'ATE

Utilitzeu aquest procediment per rebre un fitxer transferit des d'un amfitrió remot.

Verifiqueu que es compleixen tots els prerequisits i condicions següents abans d'intentar rebre un fitxer mitjançant ATE.

- Cal que ja s'hagi establert una connexió utilitzant el programa ATE.
- Cal que ja existeixi el protocol de transferència de fitxers Xmodem tant al sistema local com al sistema remot. Al sistema operatiu, Xmodem es troba en el directori `/usr/bin`.

1. Executeu la següent ordre **xmodem** en el sistema remot després d'iniciar una sessió:

   ```
   xmodem -s fitxer_nou
   ```

on **s** és l'ordre **xmodem** que s'ha d'enviar i *fitxer_nou* és el nom i el camí d'accés complet del fitxer que s'ha de transferir.

2. Premeu Intro.
3. Apareix el següent missatge:

   ```
   ate: 0828-005 El sistema està preparat per enviar el fitxer fitxer_nou.
   Utilitzeu Control-X per aturar el mòdem.
   ```

   Si el missatge no es visualitza, és possible que el sistema no tingui el programa **xmodem** instal•lat o ubicat al seu CAMÍ D'ACCÉS d'ordres.
4. Premeu Control-V per tornar a l'ATE CONNECTED MAIN MENU.
5. Premeu la tecla R per rebre el fitxer.
6. Apareix el següent missatge:

   ```
   Escriviu el nom del fitxer en el que voleu emmagatzemar les dades rebudes i feu clic
   Intro.  Per utilitzar el darrer nom de fitxer (), simplement feu clic a Intro.
   ```
7. Escriviu el nom i el camí d'accés complet del fitxer que s'ha de transferir.
8. Premeu Intro.
9. L'ATE mostrarà el següent missatge i començarà a transferir el fitxer:

   ```
   ate: 0828-020 El programa està preparat per rebre el fitxer fitxer_nou. Rebreu
   un altre missatge quan hagi finalitzat la transferència.
   ate: 0828-028 El sistema està rebent el bloc 1.
   ate: 0828-028 El sistema està rebent el bloc 2.
   ate: 0828-040 Premeu Intro.
   ```
10. Premeu Intro quan la transferència hagi finalitzat.

Edició del fitxer per defecte de l'ATE

Per editar el fitxer per defecte de l'ATE, cal configurar el programa ATE al sistema.

Per canviar els valors del fitxer `ate.def`:

1. Obriu el fitxer `ate.def` amb un editor de text ASCII.
2. Escriviu nous valors per als paràmetres que han de canviar. Els altres valors es poden suprimir o deixar. El sistema utilitza els seus valors per defecte per a tots els paràmetres que se suprimeixen.
3. Deseu el fitxer modificat `ate.def`.

Els canvis efectuats al fitxer `ate.def` comencen a tenir efecte la següent vegada que l'ATE s'executa des del directori que conté el fitxer `ate.def` personalitzat.

És possible conservar una còpia del fitxer `ate.def` en qualsevol directori per al qual tingueu permís de lectura i d'escriptura. Per exemple, si necessiteu executar el programa ATE amb valors per defecte diferents en moments diferents, conserva diverses còpies del fitxer `ate.def`, amb els valors adequats, en subdirectoris diferents del directori `$HOME`. De tota manera, les diverses còpies del fitxer `ate.def` utilitzen l'emmagatzematge del sistema. Com a alternativa, canvieu temporalment la majoria de valors amb les subordres **alter** i **modify** de l'ATE. Utilitzeu l'entrada del directori de marcatge per canviar els valors d'una connexió individual via mòdem. Consulteu l'apartat "Configuració d'un directori de marcatge de l'ATE" a la pàgina 637.

Resolució de problemes de l'ATE

Si teniu els següents problemes comuns de l'ATE, considereu aquestes solucions.

Problema:

En transferir o rebre fitxers, l'ordre **xmodem** sembla bloquejar-se. Control-X corregeix el problema.

Solució:

Examineu el menú Alter per verificar que s'està utilitzant el protocol xmodem (o el mètode Transfer).

Problema:

En transferir o rebre fitxers, el fitxer es desplaça per la pantalla i es visualitza un missatge que indica que la transferència o la recepció ha finalitzat quan, de fet, no és així.

Solució:

Examineu el menú Alter per verificar que s'està utilitzant el protocol **xmodem** (o el mètode Transfer).

Problema:

En iniciar l'ATE, l'usuari rep el següent error:

```
ate: 0828-008 El sistema ha intentat obrir el port /dev/tty0 però no ho ha aconseguit.
Si el nom del port no és correcte, canvieu-lo utilitzant el menú Alter.
O bé, realitzeu l'acció que indica el missatge del sistema següent.

Connect: Els permisos d'accés al fitxer no permeten l'acció especificada.
ate: 0828-040 Premeu Intro.
```

Solució:

La línia Connect: del missatge d'error redueix el problema. Verifiqueu si l'usuari que intenta executar l'ATE és membre del grup UUCP. Per comprovar-ho, l'usuari pot escriure *id* a la línia d'ordres; `uucp` hauria d'aparèixer al llistat de sortida.

Problema:

En intentar establir una connexió amb l'ATE, es rep el següent error:

```
ate: 0828-008 El sistema ha intentat obrir el port /dev/tty0 però no ho ha aconseguit.
Si el nom del port no és correcte, canvieu-lo utilitzant el menú Alter.
O bé, realitzeu l'acció que indica el missatge del sistema
següent.

Connect: Un fitxer o directori que hi ha al nom de camí d'accés no existeix.
ate: 0828-040 Premeu Intro.
```

Solució:

L'ATE ha seleccionat utilitzar un tty que és incorrecte o que no està disponible. Examineu la pantalla Alter de l'ATE.

Problema:

El fitxer es transfereix correctament, però la grandària del fitxer és més gran que el fitxer original.

Solució:

El protocol xmodem omple el fitxer durant la transferència. Per evitar-ho, utilitzeu l'ordre **tar** per comprimir el fitxer i transferir-lo. També és una manera de vèncer una altra limitació d'xmodem en què només s'envia un fitxer a la vegada. L'usuari pot comprimir amb l'ordre **tar** diversos fitxers en una única imatge tar i transferir-la utilitzant xmodem.

Ordres ATE i les seves subordres

Es una llista de les ordres ATE i de les seves subordres amb una descripció breu del que fan.

Consulteu l'apartat “Formats de fitxer de l'ATE” a la pàgina 643 si voleu obtenir més informació de consulta.

Element	Descripció
ate	Inicia el programa ATE. Per veure les definicions de les seves subordres, que s'indiquen a continuació, consulteu l'ordre **ate**:
	break Entra l'activitat actual en un sistema remot.
	connect Estableix una connexió amb un sistema remot.
	directory Mostra el directori de marcatge de l'ATE i permet triar una entrada des del directori per connectar-se amb un sistema remot.
	help Proporciona ajuda per utilitzar les subordres de l'ATE.
	perform Permet executar ordres del sistema operatiu de l'estació de treball mentre s'utilitza l'ATE.
	quit Surt del programa ATE.
	receive Rep un fitxer des d'un sistema remot.
	send Envia un fitxer a un sistema de fitxers remot.
	terminate Interromp una connexió ATE amb un sistema remot.

A més, l'ordre **xmodem** és útil per transferir fitxers amb el protocol xmodem, que detecta errors de transmissió de dades durant la transmissió asíncrona.

Formats de fitxer de l'ATE

Els formats de fitxer d'emulació de terminal asíncron (ATE) inclouen els formats de directori `ate.def` i de marcatge.

Element	Descripció
`ate.def`	Estableix els valors per defecte per a les connexions.
Directori de marcatge	Defineix els números de telèfon i els valors per a les connexions específiques via mòdem.

Consulteu l'apartat “Ordres ATE i les seves subordres” a la pàgina 642 si voleu obtenir més informació de consulta.

Utilitat de pantalla dinàmica

La utilitat de pantalla dinàmica, o ordre **dscreen**, és una utilitat que permet a un únic terminal físic connectar-se simultàniament amb diverses sessions (pantalles) de terminal virtual.

Està prevista per ser utilitzada principalment amb terminals que tenen dues o més pàgines de memòria de pantalla (per exemple, la pantalla IBM 3151 Models 310 o 410 amb el cartutx d'expansió). Amb aquests terminals, la commutació entre pantalles virtuals també commuta entre pàgines de la pantalla del terminal físic permetent desar i restaurar la imatge de cada pantalla virtual. En els terminals sense múltiples pàgines de memòria de pantalla, l'ordre **dscreen** encara es pot utilitzar per commutar entre sessions de pantalla virtual malgrat que no es mantindrà l'aspecte de la pantalla.

Nota: Per obtenir suport total de la utilitat **dscreen**, el terminal ha de poder commutar pàgines de la pantalla interna de l'ordre i ha de recordar la posició del cursor per a cada pàgina. Mentre que la utilitat **dscreen** funciona tant en terminals intel•ligents com en terminals passius, les imatges de pantalla no es desen durant els canvis de pantalla en els terminals passius.

Fitxer d'informació de configuració de terminal de dscreen

El fitxer d'informació de configuració de terminal de la utilitat **dscreen** (o fitxer `dsinfo`) s'utilitza per definir un conjunt diferent de tecles que s'utilitzaran amb la utilitat **dscreen**.

Això es podria fer, per exemple, quan les tecles de la utilitat **dscreen** definides originalment entren en conflicte amb una aplicació de programari que s'utilitza al sistema.

El tipus de terminal del fitxer `dsinfo` pressuposa una única pàgina de memòria de pantalla. Per tant, si un terminal dóna suport a pàgines addicionals de memòria de pantalla, el fitxer `dsinfo` s'ha de personalitzar per què utilitzi la seqüència apropiada de control de memòria de pàgina. Consulteu la guia de referència de terminal apropiada per a la seqüència de control específica.

El fitxer `dsinfo` per defecte és `/usr/lbin/tty/dsinfo`. Utilitzeu el senyalador **-i** per especificar un fitxer `dsinfo` diferent. La resta d'aquesta secció fa referència al fitxer per defecte. No obstant això, la mateixa informació s'aplica a qualsevol fitxer `dsinfo` personalitzat que creeu.

Per obtenir més informació relacionada amb el fitxer `dsinfo`, consulteu l'apartat "Assignació dinàmica de pantalla" a la pàgina 645.

Assignacions d'accions de tecles de dscreen

Quan s'executa una ordre **dscreen**, s'inicia una pantalla virtual. Algunes de les tecles del teclat del terminal no passen a la pantalla virtual; en el seu lloc, la utilitat **dscreen** intercepta aquestes tecles i realitza determinades accions quan es premen.

Les accions són les següents:

Element	Descripció
Seleccionar (consulteu l'apartat "Tecles Seleccionar de dscreen")	Selecciona una pantalla especificada.
Bloquejar (consulteu l'apartat "Tecles Bloquejar de dscreen")	Bloqueja tota l'entrada i sortida.
Nova (consulteu l'apartat "Tecles Nova de dscreen" a la pàgina 645)	Inicia una sessió de pantalla nova.
Finalitzar (consulteu l'apartat "Tecles Finalitzar i Sortir de dscreen" a la pàgina 645)	Finalitza la utilitat **dscreen**.
Sortir (consulteu l'apartat "Tecles Finalitzar i Sortir de dscreen" a la pàgina 645)	Surt de la utilitat **dscreen**.
Anterior (consulteu l'apartat "Tecla Anterior de dscreen" a la pàgina 645)	Commuta a la pantalla anterior.
Llistar (consulteu l'apartat "Tecla Llistar de dscreen" a la pàgina 645)	Mostra un llista les tecles assignades per **dscreen** i les seves accions.

La funció de cada tecla depèn del terminal i de la descripció del terminal al fitxer `/usr/lbin/tty/dsinfo`.

Tecles Seleccionar de dscreen:

Quan es crea una nova pantalla virtual, se li assigna una tecla Seleccionar.

En prémer la tecla Seleccionar es produeixen les següents accions:

- Una commutació des del terminal físic a la pàgina de vídeo associada amb la pantalla virtual concreta.
- L'entrada i la sortida es dirigeixen de forma apropiada entre el terminal físic i la pantalla virtual.

Un cop s'han assignat pantalles virtuals a totes les tecles Seleccionar definides al fitxer `dsinfo`, no es crearan més pantalles. Les sessions de les pantalles individuals finalitzen quan el procés de l'intèrpret d'ordres original realitza l'acció de sortir. Aquesta acció allibera a la tecla Seleccionar associada per ser utilitzada amb una altra pantalla virtual. La utilitat **dscreen** finalitza quan no hi ha més pantalles actives.

Tecles Bloquejar de dscreen:

Les tecles Bloquejar s'utilitzen per aturar la sortida de manera semblant a la tecla Control-S quan s'utilitza el control de flux IXON.

La finalitat d'aquestes tecles es permetre la configuració transparent de sessions de terminal en dos ordinadors utilitzant un terminal que té dos ports en sèrie.

Tecles Nova de dscreen:

En prémer una tecla de pantalla nova es crea una nova pantalla lògica i s'assigna a una de les tecles seleccionades.

Cada pantalla nova requereix el següent:
- Una tecla de selecció tal com es defineix al fitxer dsinfo
- Un dispositiu de pseudoterminal **dscreen**
- Memòria suficient per a les diverses estructures utilitzades per fer el seguiment de la pantalla
- Un procés des del qual executar l'intèrpret d'ordres.

Si algun d'aquests elements no està disponible, l'operació de la pantalla nova no és satisfactòria i s'emet un missatge que indica el motiu de l'anomalia.

Tecles Finalitzar i Sortir de dscreen:

Quan es premen les tecles Finalitzar i Sortir, es produeix una seqüència d'accions.

En prémer la tecla Finalitzar es produeix el següent:
- S'envia un senyal **SIGHUP** a totes les sessions de pantalla
- S'esborra tot
- Se surt amb un estat de 0.

En prémer una tecla Sortir es realitzen les mateixes accions però se surt amb un estat d'1.

Tecla Anterior de dscreen:

En prémer una tecla Anterior, el terminal commuta a l'última pantalla que s'ha visualitzat.

Nota:
1. No commuteu entre pantalles quan s'està escrivint a la pantalla actual; es podria truncar una seqüència d'escapament i deixar el terminal en un estat desconegut.
2. Algunes pantalles de terminal poden desar la posició del cursor de pantalles individuals però podrien no desar altres estats, com ara el mode d'inserció, el vídeo invers, etcètera. Si aquest és el cas, els usuaris han d'evitar aquests modes mentre commuten entre pantalles.

Tecla Llistar de dscreen:

En prémer una tecla Llistar es visualitza una llista de tecles i les seves accions a la pantalla del terminal.

Només es mostraran les tecles que reconeix la utilitat **dscreen**. Quan es crea una nova pantalla utilitzant la utilitat **dscreen**, al terminal es visualitza el missatge `Premeu TECLA per obtenir ajuda`, on `TECLA` és el nom de la tecla Llistar. Tingueu en compte que el missatge *només* es visualitza si s'ha definit una tecla Llistar.

Assignació dinàmica de pantalla

L'entrada de descripció de terminal del fitxer `/usr/lbin/tty/dsinfo` té el mateix nombre de tecles de selecció de pantalla que el nombre pàgines de pantalla física del terminal. Si s'han definit més tecles de selecció de pantalla que el nombre de pàgines de pantalla física, la utilitat **dscreen** assignarà dinàmicament pàgines de pantalla física a les pantalles virtuals.

Quan se selecciona una pantalla virtual que no té associada una pàgina de memòria de pantalla, la utilitat **dscreen** assigna la pantalla física utilitzada menys recentment a la pantalla virtual. Depenent de

les especificacions establertes en el fitxer de descripció /usr/lbin/tty/dsinfo, es podria observar una indicació de que la pantalla física està connectada a una pantalla virtual diferent; per exemple, la pantalla s'ha esborrat.

Fitxer dsinfo

El fitxer dsinfo és una base de dades de descripcions de terminal que utilitza la utilitat de pantalla múltiple **dscreen**.

El fitxer conté la següent informació:

- Les tecles de la utilitat **dscreen** i les funcions que realitzen
- Nombre de pàgines de memòria de pantalla del terminal
- Seqüències de codis enviades o rebudes per utilitzar les característiques anteriors.

Les entrades de tipus de terminal del fitxer dsinfo per defecte s'assemblen als següents valors de terminal ASCII 3151:

```
# El cartutx d'expansió (pn: 64F9314) necessari per a aquesta entrada
ibm3151|3151|IBM 3151,
dsks=\E!a^M|Majús-F1|,            # Selecciona la primera pantalla
dsks=\E!b^M|Majús-F2|,            # Selecciona la segona pantalla
dsks=\E!c^M|Majús-F3|,            # Selecciona la tercera pantalla
dsks=\E!d^M|Majús-F4|,            # Selecciona la quarta pantalla
dskc=\E!e^M|Majús-F5|,            # Crea una nova pantalla
dske=\E!f^M|Majús-F6|\E pA\EH\EJ, # Anar a la pantalla 1 i finalitzar
dskl=\E!g^M|Majús-F7|,            # Llista tecles de funció (ajuda)
dskp=\E!h^M|Majús-F8|,            # Anar a la pantalla anterior
dskq=\E!i^M|Majús-F9|\E pA\EH\EJ, # Anar a la pantalla 1 i sortir
dsp=\E pA|\EH\EJ,                 # Seqüència de terminal per a la pantalla 1
dsp=\E pB|\EH\EJ,                 # Seqüència de terminal per a la pantalla 2
dsp=\E pC|\EH\EJ,                 # Seqüència de terminal per a la pantalla 3
dsp=\E pD|\EH\EJ,                 # Seqüència de terminal per a la pantalla 4
dst=10,                           # Permetre 1 segon de temps d'espera de buffer
```

Format de les entrades per a dsinfo:

Les entrades del fitxer dsinfo estan formades per camps separats per comes.

El primer camp és una llista de noms alternatius per al terminal, on cada nom està separat per un caràcter de barra vertical (|). El text precedit per un caràcter de número (#) es considera un comentari i **dscreen** l'ignora. La resta de camps són sèries que descriuen les possibilitats del terminal per a la utilitat **dscreen**. Dins d'aquestes sèries, es reconeixen els següents codis d'escapament:

Taula 108. Camps de fitxer dsinfo

Seqüència d'escapament	Descripció
\E,\e	caràcter d'escapament
\n,\l	caràcter de nova línia (o salt de línia)
\r	retorn de carro
\t	caràcter de tabulació
\b	caràcter de retrocés
\f	caràcter de salt de pàgina
\s	caràcter d'espai
nnn	caràcter amb el valor octal *nnn*
^*x*	Control-X per a qualsevol valor *x* apropiat

Qualsevol altre caràcter precedit per una barra inversa produirà el propi caràcter. Les sèries s'especifiquen com a *tipus=sèrie*, on *tipus* és el tipus de sèrie tal com s'indica a continuació, i *sèrie* és el valor de la sèrie.

És important que els camps d'entrada del fitxer `dsinfo` estiguin separats per comes. Si s'omet o es trunca una coma del final de l'entrada del fitxer `dsinfo`, el fitxer serà il•legible per a la utilitat **dscreen** i es tornarà un error a la pantalla.

Tipus de sèries de disinfo:

A continuació es descriuen els tipus de sèries de disinfo.

Els tipus de sèries són els següents:

Element **Descripció**

dskx Un tipus de sèrie que comença amb dsk descriu una tecla. El tipus ha de tenir una longitud de quatre lletres, i la quarta lletra *x* indica l'acció que es duu a terme quan es rep la tecla. Els tipus de tecles són:

Tipus	Acció
dsks	Commutar pantalles
dskb	Bloquejar l'entrada i la sortida
dske	Finalitzar **dscreen**
dskq	Sortir de **dscreen** (estat de sortida=1)
dskc	Crear nova pantalla
dskp	Commutar a la pantalla anterior
dskl	Llistar tecles i accions

Qualsevol altre tipus de tecla (és a dir, un tipus de sèrie dsk*x* que no acabi amb s, b, e, q, p ni l) no produirà cap acció interna de **dscreen**, però apareixerà al llistat de tecles i es reconeixerà i s'hi actuarà. Cal utilitzar un tipus de dskn (n significa Cap operació) quan no es desitja cap acció interna de **dscreen**.

La sèrie de valor per a cada tecla té tres subsèries, que estan separades per caràcters de barra vertical (|).
Nota: Utilitzeu \| per incloure el caràcter | en una de les subsèries.

La primera subsèrie és la seqüència de caràcters que el terminal envia quan es fa clic a la tecla. La segona subsèrie és una etiqueta per a la tecla que s'imprimeix quan es visualitza una llista de tecles. La tercera subsèrie és una seqüència de caràcters que **dscreen** envia al terminal quan es fa clic a aquesta tecla abans de realitzar l'acció que sol•licita aquesta tecla.

dsp Un tipus de sèrie de dsp descriu una pantalla física del terminal. Una sèrie dsp ha d'estar present en cada pantalla física del terminal. La sèrie de valor per a cada pantalla física té dues subsèries, que estan separades per un caràcter de barra vertical (|).

La primera subsèrie és la seqüència de caràcters que s'han d'enviar al terminal per visualitzar-se i enviar-se a la pàgina física del terminal.

La segona subsèrie s'envia al terminal quan la pàgina s'utilitza per a alguna cosa nova. Aquesta segona subsèrie sovint s'estableix en la seqüència d'esborrar pantalla. S'envia sota les dues condicions següents:

1. Quan es crea una nova sessió de terminal virtual.
2. Quan hi ha més terminals virtuals que pantalles físiques. Si se selecciona un terminal virtual que requereix que **dscreen** reutilitzi una de les pantalles físiques, enviarà aquesta seqüència a la pantalla per indicar que el contingut de la pantalla no coincideix amb la sortida del terminal virtual connectat.

Nota: L'execució amb més terminals virtuals que pantalles físiques pot ser confusa i no s'aconsella; pot evitar-se definint un nombre de tecles de selecció de pantalla (dsks=) que no sigui superior al de pantalles físiques (dsp=) a l'entrada de dsinfo.

Element	Descripció
dst A	La sèrie amb un tipus de dst ajusta el temps d'espera d'entrada de **dscreen**. El valor de la sèrie és un número decimal. El valor del temps d'espera és en dècimes de segon i té un valor màxim de 255 (valor per defecte=**1** [o bé 0,1 segons]). Quan **dscreen** reconeix un prefix d'una seqüència de tecles d'entrada però no té tots els caràcters de la seqüència, s'esperà a que s'enviïn més caràcters fins que es pugui reconèixer. Si s'esgota el temps d'espera abans que es rebin més caràcters, els caràcters s'envien cap a la pantalla virtual i **dscreen** no considerarà aquests caràcters com a part d'una seqüència de tecles d'entrada. És possible que s'hagi d'augmentar aquest valor si una o més de les tecles que **dscreen** ha de desencadenar és realment un nombre de pulsacions de tecles (que assigna Control-Z 1, Control-Z 2, Control-Z 3, etc., per a la selecció de pantalla i Control-Z N per a una nova pantalla i així successivament).

Exemples de dysinfo:

Els següents exemples de `dysinfo` són per a Wyse-60 amb tres sessions de pantalla.

```
wy60|wyse60|wyse model 60,
dsks=^A~^M|Majús-F1|,
dsks=^Aa^M|Majús-F2|,
dsks=^Ab^M|Majús-F3|,
dskc=\200|Control-F1|,
dske=\201|Control-F2|\Ew0\E+,
dskl=\202|Control-F3|,
dsp=\Ew0|\E+,
dsp=\Ew1|\E+,
dsp=\Ew2|\E+,
```

Amb aquesta entrada:

- Majús-F1 a Majús-F3 s'utilitzen per seleccionar les pantalles 1 a 3.
- Control-F1 crea una nova pantalla.
- Control-F2 envia: `Esc w 0 Esc +` a la pantalla (commutant a la pantalla 0 i esborrant la pantalla) i, a continuació, finalitza **dscreen**.
- Control-F3 mostra una llista de les tecles i les seves funcions.

Cada vegada que una pantalla física s'utilitza per a una nova pantalla, la seqüència `Esc +` s'enviarà al terminal, que esborrarà la pantalla.

El següent exemple és per a un Wyse-60 amb tres sessions de pantalla, però una de les pantalles es troba en un segon ordinador que es comunica a través del segon port en sèrie del terminal:

```
wy60-1|wyse60-1|wyse model 60 - primer port en sèrie
dsks=^A~^M|Majús-F1|,
dsks=^Aa^M|Majús-F2|,
dsks=^Ab^M|Majús-F3|\Ed#^Ab\r^T\Ee9,
dskc=\200|Control-F1|,
dske=\201|Control-F2|\Ed#\201^T\Ew0\E+,
dskl=\202|Control-F3|,
dsp=\Ew0|\E+,dsp=\Ew1|\E+,
wy60-2|wyse60-2|wyse model 60 - segon port en sèrie
dsks=^A~^M|Majús-F1|\Ed#^A~\r^T\Ee8,
dsks=^Aa^M|Majús-F2|\Ed#^Aa\r^T\Ee8,
dsks=^Ab^M|Majús-F3|,
dskc=\200|Control-F1|,
dske=\201|Control-F2|\Ed#\201^T\Ew0\E+,
dskl=\202|Control-F3|,
dsp=\Ew2|\E+,
```

dscreen s'ha d'executar en els dos ordinadors, amb el tipus de terminal wy60-1 en el primer ordinador i el tipus de terminal wy60-2 en el segon ordinador (utilitzant l'opció **-t** a **dscreen**). L'entrada wy60-1 s'examinarà en primer lloc.

Les dues primeres entrades de tecles no es modifiquen respecte a l'entrada wy60 original. La tercera tecla, però, té el tipus dskb, que significa que es bloqueja tant l'entrada com la sortida. Quan es fa clic a aquesta tecla, la seqüència:

```
Esc d # Control-A b CR Control-T Esc e 9
```

s'envia al terminal; a continuació, la sortida es bloqueja i **dscreen** segueix escanejant l'entrada per trobar seqüències de tecles però descarta totes les altres entrades.

La seqüència `Esc d #` col•loca el terminal en mode d'impressió transparent, que fa eco a tots els caràcters fins a un Control-T cap a fora a través de l'altre port en sèrie.

Els caràcters `Control-A b CR` s'envien fora de l'altre port en sèrie, informant al procés **dscreen** de l'altre ordinador que ha d'activar la finestra associada amb la tecla Majús-F3.

La seqüència de tecles Control-T surt del mode d'impressió transparent. La seqüència de tecles Esc 9 fa que el terminal commuti a l'altre port en sèrie AUX per a les comunicacions de dades.

En aquest punt, l'altre ordinador agafa el control, envia una seqüència `Esc w 2` per commutar a la tercera pantalla física i reprèn la comunicació normal.

L'entrada wy60-2 segueix el mateix patró general per les tecles Majús-F1 i Majús-F2:

- Commutar al mode d'impressió transparent
- Enviar la sèrie de tecles de funció a l'altre ordinador
- Desactivar la impressió transparent.
- Commutar a l'altre port en sèrie

La tecla de finalització, Control-F2, funciona de la mateixa manera en ambdós ordinadors: envia la seqüència de tecles de finalització a l'altre ordinador mitjançant un mecanisme d'impressió transparent, commuta el terminal a la finestra 0, esborra la pantalla i després surt.

Entorn de control d'enllaç de dades genèriques

El control d'enllaç de dades genèriques (GDLC) és una definició d'interfície genèrica que ofereix als usuaris del kernel i de l'aplicació un conjunt comú d'ordres per controlar els gestors de dispositius DLC (control d'enllaç de dades) del sistema operatiu.

Per a la determinació de problemes, consulteu l'apartat GDLC Problem Determination de la publicació *Communications Programming Concepts*.

El control d'enllaç de dades genèriques (GDLC) és una definició d'interfície genèrica que proporciona als usuaris del kernel i de l'aplicació un conjunt comú d'ordres per controlar els gestors de dispositius DLC del sistema operatiu.

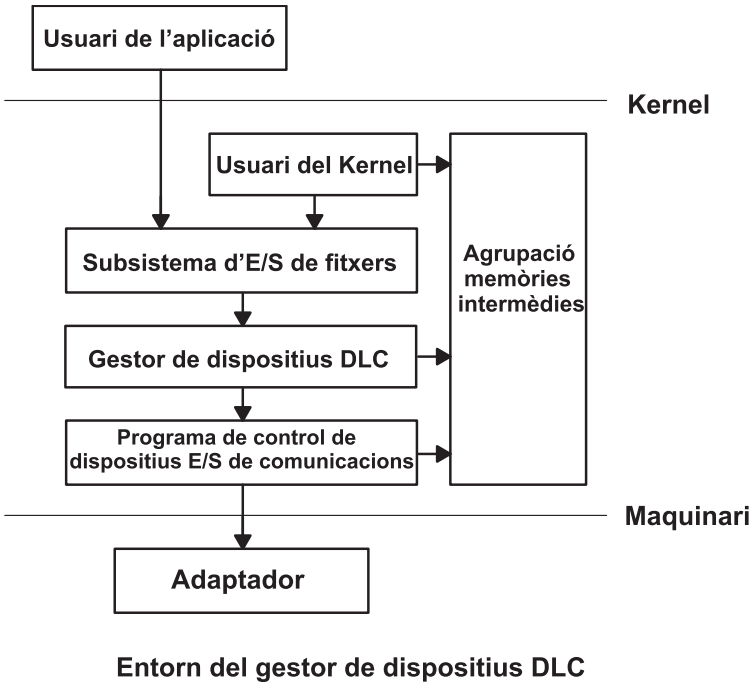
La interfície GDLC especifica requisits per a les definicions de punt d'entrada, les funcions proporcionades i les estructures de dades per a tots els gestors de dispositius DLC. Els DLC que s'ajusten a la interfície GDLC són:

- 8023 (IEEE 802.3 per a Ethernet)
- ETHER (Ethernet estàndard)
- SDLC (Control síncron d'enllaç de dades)
- TOKEN (Token-Ring)
- FDDI (Interfície de dades distribuïdes per fibra)

Els gestors de dispositius DLC realitzen protocols i funcions de capes superiors que van més enllà de l'àmbit d'un programa de control de dispositius del kernel. No obstant això, els gestors resideixen dins del kernel per tal d'oferir un rendiment màxim i utilitzen un programa de control de dispositius del kernel per a les seves sol•licituds d'E/S a l'adaptador. Un usuari DLC es troba per damunt o dins del kernel.

SDLC (control síncron d'enllaç de dades) i Control d'enllaç de dades IEEE 802.2 són exemples de gestors de dispositius DLC. Cada gestor de dispositius DLC funciona amb un programa de control de dispositius específic o amb un conjunt de programes de control de dispositius. Per exemple, SDLC funciona amb el programa de control de dispositius multiprotocol per al producte del sistema i el seu adaptador associat.

L'estructura bàsica d'un entorn DLC es mostra a la figura "Entorn del gestor de dispositius DLC". Els usuaris que es troben dins del kernel tenen accés als buffers de memòria de comunicacions (mbufs) i criden els punts d'entrada add mitjançant els serveis de kernel **fp**. El usuaris que es troben per damunt del kernel accedeixen al programes de control de dispositius d'interfície a kernel estàndard, i el sistema de fitxers crida els punts d'entrada **dd**. Les transferències de dades requereixen un moviment de dades entre l'usuari i l'espai del kernel.



Entorn del gestor de dispositius DLC

Figura 42. Entorn del gestor de dispositius DLC

Aquesta il•lustració mostra l'enllaç entre l'usuari de l'aplicació i l'adaptador (nivell de maquinari). Les àrees que hi ha entremig són l'usuari del kernel, el subsistema d'E/S de fitxers, el gestor de dispositius DLC, el programa de control de dispositius d'E/S de comunicacions i l'agrupació de buffers. Aquestes entitats "intermèdies" estan a nivell de kernel.

Els components de l'entorn del gestor de dispositius DLC són:

Element	Descripció
Usuari de l'aplicació	Resideix per damunt del kernel com a aplicació o mètode d'accés.
Usuari del kernel	Resideix dins del kernel com a procés de kernel o gestor de dispositius.
Subsistema d'E/S de fitxers	Converteix les subrutines de descriptor de fitxer i de punter de fitxer en accessos de punter de fitxer de la taula de commutació.
Agrupació de buffers	Proporciona serveis de buffer de dades per al subsistema de comunicacions.
Programa de control de dispositius d'E/S de comunicacions	Controla els enregistraments DMA (accés directe a memòria) i d'E/S d'adaptador de maquinari, i encamina els paquets de recepció a múltiples DLC.
Adaptador	S'adjunta al suport de comunicacions.

Un gestor de dispositius escrit d'acord amb les especificacions GDLC s'executa en totes les configuracions de maquinari del sistema operatiu que contenen un programa de control de dispositius de comunicacions i el seu adaptador de destinació. Cada gestor de dispositius dóna suport a múltiples usuaris que es troben per damunt així com a múltiples programes de control de dispositius i adaptadors que es troben per sota. En general, els usuaris operen simultàniament a través d'un sol adaptador, o bé cada usuari opera a través de múltiples adaptadors. Els gestors de dispositius DLC varien en funció de les seves restriccions de protocol.

La Figura 43 il•lustra una configuració de múltiples usuaris:

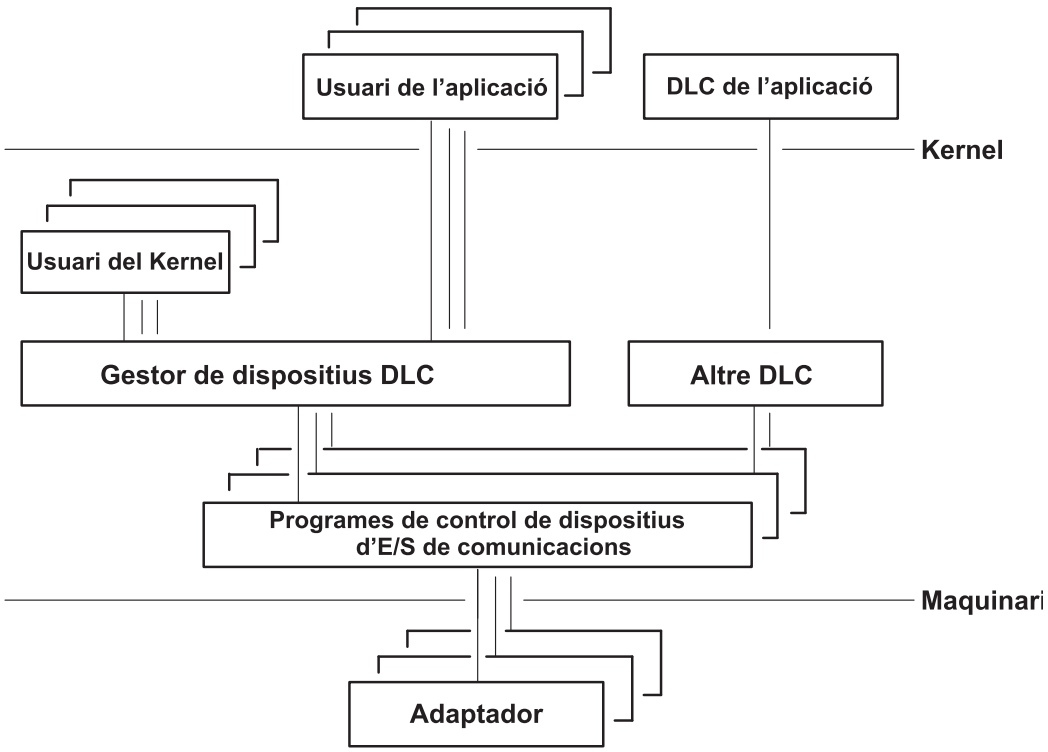


Figura 43. Configuració de múltiples usuaris i múltiples adaptadors

Aquesta il•lustració és una altra vista del nivell de kernel entre l'usuari de l'aplicació i l'adaptador. Mostra múltiples entitats que representen múltiples usuaris.

Criteris de GDLC

Una interfície GDLC ha de complir els següents criteris.

- Ser flexible i accessible per als usuaris del kernel i de l'aplicació.

- Tenir capacitat per a múltiples usuaris i múltiples adaptadors, la qual cosa permet al protocols utilitzar múltiples sessions i ports.
- Donar suport tant a serveis sense connexions com a serveis orientats a connexions quan sigui possible.
- Permetre una transferència de dades transparent per a requisits especials més enllà de l'àmbit del gestor de dispositius DLC en ús.

Interfície GDLC

Cada gestor de dispositius DLC és una entrada `/dev` estàndard que funciona en el kernel com a gestor de dispositius multiplexats per a un protocol especificat.

En el cas d'un adaptador que no està sent utilitzat pel DLC, cada subrutina **open** per un gestor de dispositius DLC crea un procés de kernel. També s'executa una subrutina **open** per al manejador de dispositius de l'adaptador de destinació. Si és necessari, executeu subrutines **open** addicionals per a múltiples ports de l'adaptador de DLC. Qualsevol subrutina **open** executada per al mateix port no crea processos de kernel addicionals, sinó que enllaça la subrutina **open** amb el procés existent. Sempre hi ha un procés de kernel per a cada port que s'està utilitzant.

L'estructura interna d'un gestor de dispositius DLC té la mateixa estructura bàsica que un manejador de dispositius del kernel, excepte que un procés de kernel substitueix el manejador d'interrupcions en les incidències asíncrones. La figura "Gestor de dispositius de kernel estàndard" mostra com funcionen els blocs de lectura, escriptura, control d'E/S i selecció.

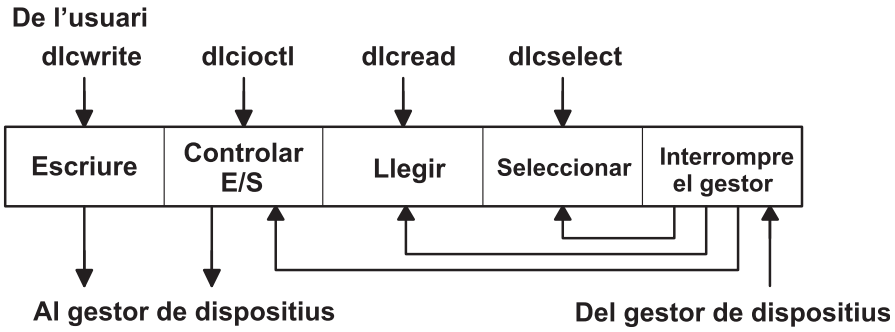


Figura 44. Gestor de dispositius de kernel estàndard

Aquesta il•lustració mostra l'estructura interna d'un gestor de dispositius DLC. Aquesta estructura està formada pels blocs d'escriptura, control d'E/S, lectura, selecció i manejador d'interrupcions. El gestor de dispositius rep informació de l'usuari i la passa a les diferents àrees abans de passar-la al manejador de dispositius.

Controls d'enllaç de dades GDLC

Podeu instal•lar els DLC per separat o en un grup. Un gestor de dispositius DLC s'afegeix automàticament al kernel i s'estableix en l'estat "Disponible" per a cada tipus de DLC instal•lat.

La instal•lació es pot verificar executant l'ordre **lslpp**, com s'indica a continuació:

```
lslpp -h tipus_dlc
```

on *tipus_dlc* és un dels següents:

Element	Descripció
bos.dlc.8023	Control d'enllaç de dades Ethernet IEEE (802.3)
bos.dlc.ether	Control d'enllaç de dades Ethernet estàndard
bos.dlc.fddi	Control d'enllaç de dades FDDI
bos.dlc.sdlc	Control d'enllaç de dades SDLC
bos.dlc.token	Control d'enllaç de dades Token-Ring

La informació sobre un DLC instal•lat es pot visualitzar mitjançant la SMIT (System Management Interface Tool) o la línia d'ordres. En els ports de comunicacions o sistemes que s'utilitzen intensament, podria ser necessari canviar els atributs de DLC per sintonitzar de manera més precisa el rendiment de DLC. Si el rendiment de recepció és lent, i l'enregistrament d'errors del sistema indica que s'està produint un sobreeiximent de la cua d'anell, augmenteu la profunditat de la cua DLC per a les dades d'entrada. Finalment, s'aconsella eliminar del kernel un DLC instal•lat quan no es necessiti durant un llarg període de temps. Aquesta operació no elimina el DLC del sistema, però permet alliberar recursos del kernel per a altres tasques fins que es torni a necessitar el DLC. Podeu trobar les instruccions per a totes aquestes tasques a l'apartat "Gestió del programa de control de dispositius DLC" a la pàgina 656.

Operacions de punt d'entrada ioctl de la interfície GDLC

La interfície GDLC (control d'enllaç de dades genèriques) dóna suport a les següents operacions de la subrutina **ioctl**.

Element	Descripció
DLC_ENABLE_SAP	Habilita un punt d'accés de servei (SAP).
DLC_DISABLE_SAP	Inhabilita un SAP.
DLC_START_LS	Inicia una estació d'enllaç en un determinat SAP com a emissor o receptor.
DLC_HALT_LS	Atura una estació d'enllaç.
DLC_TRACE	Traça l'activitat d'una estació d'enllaç per a les activitats curtes o llargues.
DLC_CONTACT	Contacta amb una estació remota per a una determinada estació d'enllaç local.
DLC_TEST	Prova l'enllaç amb una estació remota per a una determinada estació d'enllaç local.
DLC_ALTER	Modifica els paràmetres de configuració d'una estació d'enllaç.
DLC_QUERY_SAP	Consulta les estadístiques d'un determinat SAP.
DLC_QUERY_LS	Consulta les estadístiques d'una determinada estació d'enllaç.
DLC_ENTER_LBUSY	Entra en el mode d'ocupat local d'una determinada estació d'enllaç.
DLC_EXIT_LBUSY	Surt de mode d'ocupat local d'una determinada estació d'enllaç.
DLC_ENTER_SHOLD	Entra en el mode de retenció curta d'una determinada estació d'enllaç.
DLC_EXIT_SHOLD	Surt del mode de retenció curta d'una determinada estació d'enllaç.
DLC_GET_EXCEP	Torna notificacions d'excepcions asíncrones a l'usuari de l'aplicació. **Nota:** L'usuari del kernel no utilitza aquesta operació de la subrutina **ioctl** perquè totes les condicions d'excepció es passen a l'usuari del kernel a través del seu manejador d'excepcions.
DLC_ADD_GRP	Afegeix una adreça de recepció de grup o de difusió múltiple a un port.
DLC_DEL_GRP	Elimina una adreça de recepció de grup o de difusió múltiple d'un port.
DLC_ADD_FUNC_ADDR	Afegeix una adreça funcional de recepció de grup o de difusió múltiple a un port.
DLC_DEL_FUNC_ADDR	Elimina una adreça funcional de recepció de grup o de difusió múltiple d'un port.
IOCINFO	Torna una estructura que descriu el gestor de dispositius GDLC. Consulteu el format del fitxer `/usr/include/sys/devinfo.h` per obtenir més informació.

Punt d'accés de servei de GDLC

Un punt d'accés de servei (SAP) identifica un determinat servei d'usuari que envia i rep un classe específica de dades.

Això permet que diferents classes de dades s'encaminin per separat als seus corresponents manejadors de serveis. Els DLC que donen suport a múltiples SAP simultanis tenen adreces conegudes com a SAP de destinació i SAP d'origen incorporades en les seves capçaleres de paquet. Els DLC que només poden donar suport a un únic SAP no necessiten ni utilitzen l'adreçament SAP, però encara tenen el concepte d'habilitar l'únic SAP. En general, hi ha un SAP habilitat per a cada usuari DLC de cada port.

La majoria de valors d'adreces SAP es defineixen mitjançant entitats de gestió de xarxa estandarditzades de la IEEE o mitjançant valors definits per l'usuari tal com s'especifica a la publicació *Token-Ring Network Architecture Reference*. Algunes de les adreces SAP comunes són:

Element	Descripció
Null SAP (0x00)	Proporciona una certa capacitat de respondre a nodes remots fins i tot quan no s'ha habilitat cap SAP. Aquest SAP només dóna suport al serveix sense connexió i només respon a la identificació d'intercanvi (XID) i a les unitats de dades de protocol d'enllaç (LPDU) de PROVA.
SNA Path Control (0x04)	Indica l'adreça SAP individual per defecte que utilitzen els nodes SNA (Systems Network Architecture).
PC Network NETBIOS (0xF0)	S'utilitza per a totes les comunicacions DLC controlades per l'emulació NetBIOS (sistema bàsic d'entrada/sortida de xarxa).
Discovery SAP (0xFC)	L'utilitzen els serveis de descobriment de noms de la xarxa d'àrea local (LAN).
Global SAP (0xFF)	Identifica tots els SAP actius.

Estació d'enllaç GDLC

Una estació d'enllaç (LS) identifica una connexió entre dos nodes per a un determinada parella SAP.

Aquesta connexió pot funcionar com un servei sense connexions (datagrama) o com un servei orientat a connexions (transferència de dades completament seqüenciades amb recuperació d'errors). En general, s'inicia una LS per a cada connexió remota.

Mode d'ocupat local de GDLC

Quan una LS funciona en un mode orientat a connexions, ha d'aturar l'enviament de paquets d'informació de l'estació remota per motius com ara una interrupció de recursos. Aleshores, la notificació es pot enviar a l'estació remota per tal que l'estació local entri en mode d'ocupat local.

Un cop els recursos estan disponibles, l'estació local notifica a la remota que ja no està ocupada i que els paquets d'informació poden tornar a fluir. Només Només els paquets d'informació seqüenciada s'aturen amb el mode d'ocupat local. Tots els altres tipus de dades no es veuen afectats.

Mode de retenció curta de GDLC

Podeu utilitzar el mode de funcionament de retenció curta quan treballeu en determinades xarxes de dades.

El mode de retenció curta és útil amb xarxes de dades que tenen les següents característiques:

- Temps curt de configuració de crides
- Estructura tarifària que especifica una tarifa relativament petita per a la configuració de crides en comparació amb el preu de temps de connexió.

Durant el mode de retenció curta, només es manté una adjunció entre dues estacions mentre hi ha dades disponibles per transferir entre les dues estacions. Quan no hi ha dades per enviar, l'adjunció s'elimina després d'un període de temps d'espera especificat i només es restableix quan hi ha dades noves per transferir.

Prova i traça d'enllaços GDLC

Per provar una connexió entre dues estacions, doneu instruccions a una LS per què enviï un paquet de prova des de l'estació local. Aquest paquet fa eco de tornada des de l'estació remota si la connexió funciona correctament.

Alguns enllaços de dades estan limitats en el seu suport d'aquesta funció a causa de restriccions del protocol. SDLC, per exemple, només genera el paquet de prova des de l'estació d'amfitrió o l'estació primària. No obstant això, la majoria dels altres protocols permeten iniciar els paquets de prova des de qualsevol de les dues estacions.

Per traçar un enllaç, dades de línia i incidències especials (com ara l'activació, acabament i temps d'espera de l'estació), obtingueu un canal de traça genèrica i doneu instruccions a una LS per què escrigui els seus enregistraments de traça en el recurs de traça genèrica de cada LS. Aquesta funció ajuda a determinar la causa d'alguns problemes de connexió de comunicacions. Tenen suport tant les entrades de traça curta com les de traça llarga.

Estadístiques de GDLC

Un usuari de GDLC pot consultar tant les estadístiques de SAP com les estadístiques d'LS.

Les estadístiques d'un SAP estan formades per l'estat del SAP actual i la informació sobre el manejador de dispositiu. Les estadístiques de l'LS estan formades pels estats de l'estació actual i diversos comptadors de fiabilitat, disponibilitat i capacitat de donar servei que supervisen l'activitat de l'estació des del moment en què s'inicia.

Serveis de kernel especials GDLC

El control d'enllaç de dades genèriques (GDLC) proporciona serveis especials per a un usuari del kernel.

No obstant això, ha d'existir un entorn fiable dins del kernel. En comptes de que el gestor de dispositius DLC copiï dades d'incidències asíncrones a l'espai de l'usuari, l'usuari del kernel ha d'especificar punters de funció a rutines especials anomenades manejadors de funcions. DLC crida els manejadors de funcions durant l'execució. D'aquesta manera s'assoleix un rendiment màxim entre l'usuari del kernel i les capes DLC. Cada usuari del kernel ha de restringir el nombre de manejadors de funcions a una longitud mínima de camí d'accés i ha d'utilitzar l'esquema de buffer de memòria de comunicacions (mbuf).

Un manejador de funcions no ha de cridar mai directament una altra entrada DLC. El motiu és que les crides directes es realitzin sota bloqueig, la qual cosa produeix una suspensió molt greu. L´única excepció a aquesta regla és que un usuari del kernel podria cridar el punt d'entrada **dlcwritex** mentre realitza tasques de servei de qualsevol de les quatre funcions de recepció de dades. Cridar el punt d'entrada **dlcwritex** permet generar respostes immediates sense un commutador de tasques intermedi. Cal una lògica especial dins del gestor de dispositius DLC per comprovar la identificació de procés de l'usuari que crida una operació d'escriptura. Si es tracta d'un procés DLC i s'ha sobrepassat la capacitat de col•locació en cua interna, l'escriptura s'envia de tornada amb un codi de retorn codi erroni (valor de retorn **EAGAIN**) en comptes de col•locar en suspensió el procés de crida (DLC). Aleshores dependrà de la subrutina de l'usuari de crida que es torni una notificació especial al DLC des de la seva funció de recepció de dades per tal d'assegurar que més endavant es realitzarà un reintent del buffer de recepció.

Els manejadors de funcions proporcionats per l'usuari són:

Element	Descripció
Rutina de dades de datagrama rebudes	Es crida sempre que es rep un paquet de datagrames per a l'usuari del kernel.
Rutina de condició d'excepció	Es crida sempre que es produeix una incidència asíncrona que s'ha de notificar a l'usuari del kernel, com ara SAP tancat o Estació contactada.
Rutina de dades de trames I rebudes	Es crida sempre que es rep un paquet de dades seqüenciades normals per a l'usuari del kernel.
Rutina de dades de xarxa rebudes	Es crida sempre que es reben dades específiques de la xarxa per a l'usuari del kernel.
Rutina de dades XID rebudes	Es crida sempre que es rep un paquet d'identificació d'intercanvi (XID) per a l'usuari del kernel.

L'usuari del kernel no crida els punts d'entrada **dlcread** i **dlcselect** per a DLC perquè el gestor de dispositius DLC crida directament les entrades funcionals asíncrones. En general, la col•locació en cua d'aquestes incidències s'ha de dur a terme al manejador de funcions de l'usuari. Si, malgrat això, l'usuari del kernel no pot manejar un determinat paquet de recepció, el gestor de dispositius DLC pot retenir el darrer buffer de recepció i especificar un de dos modes especials d'ocupat d'usuari:

Mode d'ocupat finalitzat per l'usuari (només trames I)

Si l'usuari del kernel no pot manejar una trama I rebuda (a causa de problemes com ara un bloqueig de la cua), es torna un codi de retorn DLC_FUNC_BUSY, i DLC reté el punter del buffer i entra en mode d'ocupat local per aturar les transmissions de trames I de l'estació remota. L'usuari del kernel ha de cridar la funció Sortir d'ocupat local per restablir el mode d'ocupat local i tornar a iniciar la recepció de trames I. Només es poden aturar les trames I seqüenciades normals. Les dades de xarxa, datagrama i XID no es veuen afectades pel mode d'ocupat local.

Mode d'ocupat finalitzat per temporitzador (tots els tipus de trames)

Si l'usuari del kernel no pot manejar un determinat paquet de recepció i vol que DLC retingui el buffer de recepció durant un curt període de temps i després torni a cridar la funció de recepció d'usuari, es torna un codi de retorn DLC_FUNC_RETRY a DLC. Si el paquet de recepció és una trama I seqüenciada, l'estació entra en mode d'ocupat local durant aquest període de temps. En tots els casos, s'inicia un temporitzador; quan caduca el temporitzador, es torna a cridar l'entrada funcional de recepció de dades.

Gestió del programa de control de dispositius DLC

Cal afegir un DLC al sistema abans d'utilitzar-lo.

Cada DLC instal•lat s'afegeix automàticament després de la instal•lació i en cada reinici del sistema (vegeu l'apartat "Controls d'enllaç de dades GDLC" a la pàgina 652). Si un DLC s'ha eliminat sense un reinici subsegüent, es pot tornar a afegir.

Taula 109. Tasques per gestionar els programes de control de dispositius DLC

Tasca	Camí d'accés ràpid de la SMIT	Ordre o fitxer
Afegir un DLC instal•lat	Escolliu-ne un (per nom de programa de control de dispositius): `smit cmddlc_sdlc` `smit cmddlc_token` `smit cmddlc_qllc` `smit cmddlc_ether`[1] `smit cmddlc_fddi` i, a continuació, seleccioneu **Afegir**	**mkdev**[2]
Canviar atributs de DLC[3,4]	Escolliu-ne un (per nom de programa de control de dispositius): `smit cmddlc_sdlc_ls` `smit cmddlc_token_ls` `smit cmddlc_qllc_ls` `smit cmddlc_ether_ls`[1] `smit cmddlc_fddi_ls`	**chdev**[2]
Iniciar traça del supervisor de xarxa d'àrea local de DLC[5]	`smit trace`	**trace -j** *nnn* on el valor *nnn* es l'ID d'enganxament que s'ha de traçar
Aturar traça del supervisor de xarxa d'àrea local de DLC	`smit trcstop`	**trcstop**[2]
Generar informe de traça del supervisor de xarxa d'àrea local de DLC	`smit trcrpt`	**trcrpt -d** *nnn* on el valor *nnn* és l'ID d'enganxament sobre el que s'ha d'informar
Llistarinformació de DLC actual[3]	Escolliu-ne un (per nom de programa de control de dispositius): `smit cmddlc_sdlc_ls` `smit cmddlc_token_ls` `smit cmddlc_qllc_ls` `smit cmddlc_ether_ls`[1] `smit cmddlc_fddi_ls`	**lsdev**[2] o **lsattr**[2]
Eliminar un DLC[3,6]	Escolliu-ne un (per nom de programa de control de dispositius): `smit cmddlc_sdlc_rm` `smit cmddlc_token_rm` `smit cmddlc_qllc_rm` `smit cmddlc_ether_rm`[1] `smit cmddlc_fddi_rm`	**rmdev**[2]

Nota:

1. El camí d'accés ràpid de la SMIT per a un gestor de dispositius d'Ethernet inclou tant el gestor de dispositius d'Ethernet estàndard com el gestor de dispositius d'Ethernet IEEE 802.3.

2. Els detalls sobre les opcions de la línia d'ordres es proporcionen a les descripcions de les ordres **mkdev**, **chdev**, **trace**, **trcstop**, **trcrpt**, **lsdev**, **lsattr**, o **rmdev** a *Commands Reference, Volume 4*.
3. Un DLC s'ha d'instal•lar i afegir abans de que pugueu llistar, mostrar, canviar o eliminar els seus atributs (vegeu l'apartat "Controls d'enllaç de dades GDLC" a la pàgina 652). Un canvi d'atribut només és satisfactori si no hi ha subrutines open actives respecte al DLC de destinació. Abans d'executar l'acció de canvi, és possible que l'usuari hagi d'impedir que els serveis com ara SNA, OSI o NetBIOS utilitzin el DLC.
4. Canviar la grandària de la cua de recepció afecta directament els recursos del sistema. Només heu de realitzar aquest canvi si el DLC té problemes amb la cua de recepció, com ara un rendiment lent o sobreeiximents entre el DLC i el seu manejador de dispositiu.
5. Aneu amb compte a l'hora d'habilitar la traça del supervisor ja que afecta directament el rendiment dels DLC i de les seus associacions.
6. L'eliminació d'un DLC només és satisfactòria si no hi ha subrutines open actives respecte al DLC de destinació. Abans d'executar l'acció d'eliminació, és possible que l'usuari hagi d'impedir que els serveis com ara SNA, OSI o NetBIOS utilitzin el DLC.

Consulta d'adaptadors de xarxes i comunicacions

Aquest tema descriu diferents casos pràctics de configuració tant per a adaptador PCI com per a adaptadors asíncrons.

Adaptadors PCI

L'informació sobre l'instal•lació i la configuració dels adaptadors PCI s'introdueix aquí.

Els temes que es tracten són el suport i la configuració dels adaptadors de xarxa d'àrea ampla (WAN) ("Controlador de dispositiu de xarxa HDLC de multiprotocol de 2 ports" i "Adaptador PCI ARTIC960Hx" a la pàgina 658).

Controlador de dispositiu de xarxa HDLC de multiprotocol de 2 ports

El programa de control de dispositiu de control d'enllaç de dades d'alt nivell (HDLC) de l'adaptador multiprotocol de 2 ports és un component del subsistema d'E/S de comunicació. Aquest programa de control de dispositiu proporciona suport per l'operació HDLC a través de l'adaptador de multiprotocol de 2 ports a velocitats de fins a 1.544Mbps.

Les opcions següents proporcionen accés al programa de control de dispositiu de xarxa HDLC de multiprotocol de 2 ports:

- Arquitectura de xarxa de sistemes (SNA)
- La versió de control síncron d'enllaç de dades (SDLC) de l'interfície de programació GDLC
- Aplicacions escrites per usuari compatibles amb SDLC MPQP-API (Multiprotocol Quad Port-Application Programming Interface)

Nota: Les opcions anteriors requereixen l'us del fitxer especial `mpc`*n*, el qual permet accedir al programa de control de dispositiu HDLC de l'adaptador de multiprotocol de 2 ports a través del subsistema d'emulació del programa de control de dispositiu SDLC COMIO. Aquest subsistema s'ha d'instal•lar i configurar per a cada dispositiu de xarxa HDLC.

- Aplicacions escrites per l'usuari compatibles amb l'API CDLI (Common Data Link Interface)

El programa de control de dispositiu d'adaptador multiprotocol de 2 ports permet la connectivitat amb sistemes d'amfitrió remots mitjançant l'adaptador multiprotocol de 2 ports, ja sigui directament per una línia llogada o per circuits commutats. El programa de control de dispositiu pot proporcionar una passarel•la entre entorns de grup de treball i recursos de processament de dades remotes.

Configuració de l'adaptador de multiprotocol de 2 ports

Utilitzeu aquestes explicacions per configurar l'adaptador de multiprotocol de 2 ports.

Taula 110. Tasques per configurar l'adaptador de multiprotocol de 2 ports

Tasca	Camí d'accés ràpid de SMIT
Afegir un programa de control de dispositiu a l'adaptador	`smit mkhdlcdpmpdd`
Reconfigurar el programa de control de dispositiu a l'adaptador	`smit chhdlcdpmpdd`
Eliminar un programa de control de dispositiu de l'adaptador	`smit rmhdlcdpmpdd`
Fer que un programa de control de dispositiu definit estigui disponible	`smit cfghdlcdpmpdd`
Afegir un emulador SDLC COMIO a l'adaptador	`smit mksdlcsciedd`
Reconfigurar l'emulador SDLC COMIO a l'adaptador	`smit chsdlcsciedd`
Eliminar un emulador SDLC COMIO de l'adaptador	`smit rmsdlcsciedd`
Fer que un emulador SDLC COMIO estigui disponible	`smit cfgsdlcsciedd`

Adaptador PCI ARTIC960Hx

L'emulador de programa de control del dispositiu MPQP COMIO de l'adaptador PCI ARTIC960Hx és un component del subsistema d'E/S de comunicació. Aquest programa de control de dispositiu proporciona suport per l'adaptador PCI ARTIC960Hx a la velocitat màxima de 2M bps.

Els mòdems utilitzats han de proporcionar la sincronització, donat que només se suporta la sincronització externa.

Les opcions següents proporcionen accés al programa de control de dispositiu MPQP COMIO de l'adaptador PCI ARTIC960Hx:

- Arquitectura de xarxa de sistemes (SNA)
- L'interfície de programació de control d'enllaços de dades genèriques (GDLC)
- Les aplicacions escrites per usuari compatibles amb MPQP-API (Multiprotocol Quad Port-Application Programming Interface) com, per exemple, les aplicacions SDLC i BiSync.

Aquestes opcions requereixen la utilització del fitxer especial `mpqx`, el qual permet accedir a l'adaptador PCI ARTIC960Hx a través del programa de control de dispositiu d'emulació MPQP COMIO. Aquest programa de control de dispositiu s'ha d'instal•lar i configurar per a cada port de l'adaptador PCI ARTIC960Hx. El fitxer especial `mpqx` es troba al directori `/dev`.

Nota: La variant *x* de `mpqx` especifica la instància del programa de control de dispositiu; per exemple, `mpq0`.

El programa de control de dispositiu d'emulació MPQP COMIO permet la connectivitat a sistemes d'amfitrió remots mitjançant l'adaptador PCI ARTIC960Hx, ja sigui directament o per una línia llogada. El programa de control de dispositiu pot proporcionar una passarel•la entre entorns de grup de treball i recursos de processament de dades remotes.

Configuració del programa de control d'emulació MPQP COMIO mitjançant l'adaptador ARTIC960Hx PCI

Utilitzeu aquestes explicacions per configurar el programa de control d'emulació MPQP COMIO mitjançant l'adaptador ARTIC960Hx PCI.

Taula 111. Tasques per configurar el programa de control d'emulació MPQP COMIO

Tasca	Camí d'accés ràpid de SMIT
Afegir un programa de control de dispositiu	`smit mktsdd`
Reconfigurar el programa de control d'emulació MPQP COMIO	`smit chtsdd`
Eliminar un programa de control de dispositiu	`smit rmtsdd`
Configurar un programa de control de dispositiu definit	`smit cfgtsdd`
Afegir un port	`smit mktsdports`
Reconfigurar un port d'emulació MPQP COMIO	`smit chtsdports`
Eliminar un port	`smit rmtsdports`
Configurar un port definit	`smit cfgtsdports`
Rastrejar el programa de control d'emulació MPQP COMIO	`smit trace_link`

Adaptadors asíncrons

Els adaptadors asíncrons de 8 i 16 ports estàndards estan llistats en aquesta taula.

A la taula següent trobareu un resum d'aquests productes:

Taula 112. Adaptadors asíncrons

Connexió asíncrona	Tipus de bus	Codi de dispositiu o tipus de màquina (model)	Velocitat màxima de dades per port (KBits/seg)	Característiques destacades
EIA 232 de 8 ports	Micro Channel	2930	76,8	Estàndard generalitzat
EIA 422A de 8 ports	Micro Channel	2940	76,8	Més distància
MIL-STD 188 de 8 ports	Micro Channel	2950	Seleccionable en funció de la velocitat del rellotge generador de velocitat en bauds de l'UART.	MIL-STD 188-114 per a interfície digital de voltatge no equilibrada
EIA 232 de 8 ports	ISA	2931	115,2	Major eficiència
EIA 232 de 8 ports	ISA	2932	115,2	Major eficiència
EIA 422 de 8 ports	PCI	2943	230	Major eficiència
EIA 232 de 16 ports	Micro Channel	2955	76,8	Focus en la connexió local
EIA 422A de 16 ports	Micro Channel	2957	76,8	Més distància
-	ISA	2933	-	-
-	PCI	2944	-	-

A la taula següent es mostren les característiques detallades dels productes.

Taula 113. Característiques dels productes de connexió asíncrona

	Ports en sèrie nadius	8 ports		16 ports	128 ports amb RAN	
		MC	ISA		MC	ISA
Nombre de ports asíncrons per adaptador	n/d	8	8	16	128	128
Nombre màxim d'adaptadors	n/d	8	7	8	7	7
Nombre màxim de ports asíncrons	2 ó 3	64	56	128	896	896
Nombre de ports asíncrons per RAN	n/d	n/d	n/d	n/d	16	16

Taula 113. Característiques dels productes de connexió asíncrona (continuació)

	Ports en sèrie nadius	**8 ports**		**16 ports**	**128 ports amb RAN**	
Nombre màxim de RAN	n/d	n/d	n/d	n/d	56	56
Velocitat màxima (KBits/seg)	Seleccionable en funció de la velocitat del rellotge generador de velocitat en bauds de l'UART.	76,8	115,2	76,8	230	230
Mètode d'adjunció	estàndard	directa	directa	directa	node	node
Interfícies elèctriques asíncrones suportades	EIA 232	EIA 232 EIA 422A[4]MIL-STD[4]188-114[4]	EIA 232 EIA 422A	EIA 232 EIA 422A	EIA 232 EIA 422	EIA 232 EIA 422
Connector estàndard	DB25M/ MODU	DB25M	DB25M	DB25M	RJ-45[2]	RJ-45[2]
Opcions de cable DB25	n/d	n/d	n/d	n/d	RJ-45-DB25	RJ-45-DB25
Opció muntada sobre bastidor	n/d	n/d	n/d	n/d	sí	sí
Font d'alimentació	n/d	n/d	n/d	n/d	externa	externa
Senyals suportats (EIA 232)	TxD RxD RTS CTS DTR DSR DCD RI	TxD RxD RTS RTS CTS DTR DSR DCD RI	TxD RxD RTS CTS DTR DSR DCD RI	TxD RxD RTS[3]-DTR -DCD -	TxD RxD RTS CTS DTR DSR DCD RI	TxD RxD RTS CTS DTR DSR DCD RI

Nota:

1. El sòcol accepta endolls RJ-45 8p, RJ-11 6p o RJ-11 4p amb una reducció en els senyals suportats.
2. El senyal RTS està activat (+12V) a la caixa del connector del ventall de sortida del cable de la interfície de 16 ports EIA 232 (codi de dispositiu 2996).
3. Només Micro Channel.

Cada oferta de productes està caracteritzada per un cas pràctic representatiu dels seus punts forts. A continuació es mostren les recomanacions per a cadascun d'ells.

Conceptes relacionats:

"Dispositiu de terminal TTY" a la pàgina 581
Un dispositiu de terminal tty és un dispositiu de caràcter que realitza l'entrada i sortida caràcter a caràcter.

Informació relacionada:

2-Port Asynchronous EIA-232 PCI Adapter Installation and Using Guide

Micro Channel de 8 ports

Les característiques de l'adaptador Micro Channel de 8 ports inclouen una ranura de bus Micro Channel disponible per a E/S asíncrona.

Altres característiques són les següents:

- Menys de vuit ports amb poca expansió o sense expansió.
- Tots els terminals locals estan situats a menys de 61 metres (200 peus) del sistema.
- Es necessiten terminals remots (suport a través de multiplexor/mòdem OEM).
- Demanda baixa a moderada d'amplada de banda de dispositiu (fins a 76,8 Kbps).

EIA 232 o EIA 232/EIA 422 de bus ISA de 8 ports

Les característiques de l'adaptador EIA 232 o EIA 232/EIA 422 de bus ISA de 8 ports inclouen una ranura ISA.

Altres característiques són les següents:

- Es necessiten menys de vuit ports amb poca expansió o sense expansió.
- Necessita tots els ports EIA 232, tots els ports EIA 422 o una combinació de ports EIA 232 i EIA 422.
- Descàrrega del processament d'E/S de terminal i interrupció de caràcters de la UCP principal.
- Velocitats asíncrones de fins a 115,2 Kbps.
- Rendiment màxim per a mòdems d'alta velocitat (28,8 Kbps) amb compressió de dades.

Micro Channel de 16 ports

Les característiques de l'adaptador Micro Channel de 16 ports inclouen una ranura de bus Micro Channel disponible per a E/S asíncrona.

Altres característiques són les següents:

- Vuit ports actualment, menys de 16 ports amb poca expansió o sense expansió.
- Tots els terminals locals estan situats a 61 metres (200 peus) com a màxim del sistema.
- Es necessiten terminals remots (suport a través de multiplexor/mòdem OEM).
- Els dispositius no necessiten tots els senyals EIA 232.
- Demanda baixa a moderada d'amplada de banda de dispositiu (fins a 38,4 Kbps per a dispositius asíncrons).

Adaptador de 128 ports (Micro Channel, ISA)

Les característiques de l'adaptador ISA o Micro Channel de 128 ports inclouen setze ports amb possibilitat d'expansió fins a 128 ports sense ranures addicionals.

Altres característiques són les següents:

- Una ranura de bus Micro Channel, ISA, o PCI disponible per E/S asíncrona. (Per obtenir més informació sobre PCI, consulteu “Consideracions sobre la selecció del producte” a la pàgina 571.)
- Terminal més distant situat a uns 300 metres (1000 peus) del sistema a velocitat màxima de dades per a adaptadors Micro Channel i ISA.
- Terminals planificats: pròxims o al mateix local, distants al mateix local, i remots.
- Necessiten alta productivitat asíncrona amb baixa demanda de processador.
- Necessiten capacitat d'impressora adjuntada a terminal.
- Necessiten connexió amb locals remots a través de fibra òptica o mòdems síncrons.

Llistat d'adaptadors asíncrons de 128 ports Micro Channel definits utilitzant la SMIT

Utilitzeu aquest procediment per fer un llistat de tots els adaptadors asíncrons de 128 ports definits, tant si estan disponibles com si no.

1. Utilitzeu el camí d'accés ràpid `smit lsd128psync`. El sistema escaneja la informació i la visualitza.
2. Sortiu de la interfície SMIT.

Adaptador ISA/PCI asíncron de 8 ports

L'adaptador ISA asíncron de 8 ports és una característica de comunicacions en sèrie, intel•ligent i multicanal que està disponible per a ordinadors Basat en el processador POWER.

Els adaptadors ISA contenen 128K de RAM (memòria d'accés aleatori) d'alta velocitat i doble port que s'utilitzen per la col•locació de codi de programa i dades al buffer. Els ports asíncrons s'executen mitjançant un processador 3041 IDT de 16 MHz i 32 bits que admet velocitats de transferència de dades de 115 Kbps.

El processador 3041 i la RAM de doble port ajuden a descarregar una part considerable del processament de caràcters del sistema. Els blocs grans de dades es transfereixen directament a l'adaptador i, a continuació, els caràcters s'envien d'un en un als ports en sèrie.

Tant l'adaptador com l'ordinador poden accedir a la RAM de doble port per realitzar operacions de lectura i escriptura. L'ordinador considera la RAM de doble port com a memòria pròpia i hi accedeix utilitzant les mateixes ordres de referència de memòria d'alta velocitat que utilitza per a la memòria interna.

L'adaptador ISA EIA 232 de 8 ports només dóna suport a dispositius EIA 232. Aquest adaptador necessita que el paquet de dispositiu `devices.isa.cxia` estigui instal•lat al sistema.

L'adaptador ISA EIA 232/422 de 8 ports dóna suport als dispositius EIA 232 i EIA 422. Ambdós tipus de dispositius poden estar configurats en qualsevol combinació segons el port en qüestió. Aquest adaptador necessita que el paquet de dispositiu `devices.isa.pc8s` estigui instal•lat al sistema.

Els paquets anteriors necessiten el paquet `devices.common.IBM.cx`.

Instal•lació d'adaptadors de 8 ports:

Els adaptadors ISA no es poden detectar automàticament pel sistema operatiu i s'han d'instal•lar manualment.

1. Per configurar els adaptadors ISA EIA 232/EIA 422 asíncrons de 8 ports d'IBM, utilitzeu el camí d'accés ràpid `smit mkdev_isa` per accedir a la pantalla **Afegir un adaptador ISA**.
2. Seleccioneu **pcxr** (per a l'adaptador EIA 232 de 8 ports) o **pc8s** (per a l'adaptador EIA 232/EIA 422 de 8 ports) i feu clic a Intro.
3. Seleccioneu el bus apropiat i feu clic a Intro.
4. Al camp Adreça d'E/S de bus, estabiu l'adreça en l'adreça del adaptador (definida pels commutadors DIP de l'adaptador). Per obtenir més informació sobre els commutadors DIP, consulteu la publicació *8 Port Asynchronous ISA Adapter Installation Guide*. La resta de la configuració de l'adaptador es realitza automàticament quan el sistema mostra `saX disponible`.
5. Quan hagueu acabat, seleccioneu **Realitzar**.

stty-cxma és un programa d'utilitats que estableix i mostra les opcions de terminal per als adaptadors Micro Channel de 128 ports i ISA de 8 i 128 ports, i es troba al directori `/usr/lbin/tty`. El format és:

```
stty-cxma [-a] [opció(ns)] [ttyname]
```

Sense cap opció, **stty-cxma** mostra tots els valors especials del programa de control, el senyals del mòdem i tots els paràmetres estàndard que visualitza **stty(1)** per al dispositiu tty al que fa referència l'entrada estàndard. S'inclouen opcions d'ordres per canviar els valors de control de flux, establir opcions d'impressió transparent, forçar línies de control de mòdem i visualitzar tots els valors tty. Les opcions no reconegudes es passen a **stty(1)** per ser interpretades. Les opcions són les mateixes que les utilitzades per als adaptadors PCI. Per obtenir més informació, consulteu l'apartat “Opcions de terminal d'stty-cxma” a la pàgina 610.

Ports d'E/S estàndard

La majoria de models de la unitat del sistema tenen dos ports en sèrie asíncrons EIA 232 (estàndard) integrats.

El model M20/M2A té un únic port en sèrie asíncron integrat que es pot convertir per donar suport a dos dispositius sèrie utilitzant un cable de ventall de sortida opcional. Els dispositius sèrie asíncrons EIA 232 poden adjuntar-se directament als ports en sèrie estàndard utilitzant cables sèrie estàndard amb connectors d'intèrpret d'ordres D de 9 o 25 potes.

Nota: Per a la plataforma basada en Itanium, els dispositius sèrie asíncrons EIA 232 poden adjuntar-se directament als ports en sèrie estàndard utilitzant cables sèrie estàndard amb connectors d'intèrpret d'ordres D de 9 potes.

Les màquines amb capacitat de multiprocessament tenen tres ports en sèrie.

Configuració d'un dispositiu de terminal asíncron EIA 232:

Aquest procediment permet definir i configurar un dispositiu tty connectat a un port en sèrie estàndard o a un adaptador asíncron de 8 o 16 ports.

1. Utilitzeu el camí d'accés ràpid `smit mktty` per accedir al menú **Afegir un TTY**.
2. Seleccioneu **Afegir un TTY**.
3. Seleccioneu **Terminal asíncron tty rs232**.
4. Realitzeu una selecció a partir dels adaptadors de 8 ports, 16 ports o E/S estàndard disponibles que es visualitzen a la pantalla. Si no es visualitza cap adaptador o si els adaptadors estan en un estat definit, torneu a comprovar la configuració, el cablatge i la instal•lació.
5. En els camps de diàleg visualitzats, podeu afegir o canviar els atributs tty.
6. Quan hagueu acabat, seleccioneu **Realitzar**.

Configuració d'un dispositiu d'impressora/traçador asíncron EIA 232:

Aquest procediment permet definir i configurar un dispositiu d'impressora/traçador connectat a un port en sèrie estàndard o a un adaptador asíncron de 8 o 16 ports.

1. Per crear un dispositiu d'impressora/traçador en un adaptador asíncron, utilitzeu el camí d'accés ràpid `smit pdp` per accedir al menú **Dispositius d'impressora/traçador**.
2. Seleccioneu **Afegir una impressora/traçador**.
3. Efectueu una selecció a partir de la llista de tipus d'impressora i traçador que apareix a la pantalla i, a continuació, feu clic a Intro. Per a aquest exemple, s'ha realitzat la següent selecció:

   ```
   osp Other serial printer
   ```

4. Seleccioneu l'opció **rs232**.
5. Realitzeu una selecció a partir dels controladors de 8 ports disponibles que apareixen a la pantalla. Si no es visualitza cap controlador o si els controladors es mostren en un estat definit, torneu a comprovar la configuració, el cablatge i la instal•lació.
6. En els camps de diàleg visualitzats, podeu afegir o canviar els atributs dels dispositius d'impressora/traçador.
7. Quan hagueu acabat, seleccioneu **Realitzar**.

Adaptadors asíncrons Micro Channel de 8 ports

La família d'adaptadors asíncrons es basa en un disseny funcional comú. No obstant això, les característiques dels adaptadors individuals estan determinades per les interfícies de dispositiu suportades.

Nota: La secció següent no és aplicable a la plataforma basada en Itanium.

La família consta de 3 adaptadors:

- Adaptador asíncron de 8 ports - EIA 232
- Adaptador asíncron de 8 ports - MIL-STD-188
- Adaptador asíncron de 8 ports - EIA 422A

La família d'adaptadors de 8 ports es basa en el xip DUART (dual universal asynchronous receiver and transmitter), que proporciona dos canals de comunicacions en sèrie.

Les seccions següents contenen informació detallada sobre els adaptadors de 8 ports.

Adaptador asíncron de 8 ports - EIA 232:

L'EIA 232 és un adaptador asíncron de 8 ports que proporciona suport per adjuntar un màxim de vuit dispositius sèrie asíncrons EIA 232D (com ara mòdems, terminals, traçadors i impressores) a una unitat del sistema.

El sistema s'ha de basar en un bus Micro Channel o un bus ISA i ha de donar suport fins a un total de vuit adaptadors de 8 ports.

Aquest adaptador és completament programable i només dóna suport a comunicacions asíncrones. També pot afegir i eliminar bits d'inici i aturada i dóna suport a la paritat parell, senar o cap de les dades en sèrie. Un generador de velocitat en bauds programable permet una operació de 50 a 38.400 bps per al bus Micro Channel i de 50 a 115.200 bps per al bus ISA. Els adaptadors admeten caràcters de 5, 6, 7 ó 8 bits amb 1, 1,5 o 2 bits d'aturada. Un sistema d'interrupció de prioritat controla les interrupcions de transmissió, recepció, error, estat de línia i conjunt de dades.

Instal•lació de l'adaptador asíncron de 8 ports:

L'adaptador asíncron de 8 ports es col•loca en una única ranura Micro Channel del sistema. Seguiu aquests passos per instal•lar l'adaptador.

1. Verifiqueu que tots els usuaris estan desconnectats del sistema i executeu la següent ordre:
   ```
   shutdown -F
   ```
2. Quan hagi finalitzat l'ordre **shutdown**, desconnecteu l'alimentació del sistema.
3. Obriu la caixa del sistema i inseriu l'adaptador asíncron de 8 ports a una ranura Micro Channel lliure.
4. Adjunteu el connector d'intèrpret d'ordres D de 78 potes des del cable de la interfície de 8 ports a l'adaptador de 8 ports.
5. Torneu a posar els panells de la coberta a la unitat del sistema.
6. Enceneu l'alimentació del sistema. El sistema reconeixerà i configurarà l'adaptador de 8 ports durant el procés d'engegada.
7. Un cop hagi finalitzat l'engegada, inicieu una sessió utilitzant el procés d'engegada amb l'ID d'usuari root.
   ```
   lsdev -Cc adapter | pg
   ```

Només els adaptadors que es troben en un estat disponible estan preparats per ser utilitzats pel sistema.

Si l'adaptador que s'ha acabat d'instal•lar *no* està disponible, verifiqueu el següent:

- L'adaptador està instal•lat correctament a la ranura Micro Channel.
- Tot el cablatge necessari s'adjunta i es fixa bé en el seu lloc.
- Executeu l'ordre: **errpt -a | pg** i examineu l'informe d'errors del sistema per veure el problemes relacionats amb els adaptadors.
- Executeu l'ordre: **cfgmgr -v | pg**. Aquesta ordre intentarà tornar a configurar l'adaptador sense reengegar. Observeu si hi ha errors a la sortida paginada.

Si l'execució de l'ordre **cfgmgr** no és satisfactòria, caldrà reengegar.

Informació de maquinari d'adaptador asíncron de 8 ports:

La interfície del sistema presenta una adreça de 3 bits i dades de 8 bits, així com línies de control en el xip DUART. Les dades de la interfície del sistema se serialitzen per ser transmeses a un dispositiu extern. Les dades en sèrie poden incloure un bit de paritat al límit d'octets. A la inversa, les dades d'un

dispositiu extern es deserialitzen per ser transmeses a la interfície del sistema. Aquestes dades poden incloure un bit de paritat, que pot ser comprovat opcionalment. Com a opció, el canal pot funcionar en mode FIFO (first-in-first-out).

En mode FIFO, es poden col•locar al buffer fins a 16 octets tant al transmissor com al receptor. La interfície sèrie utilitza el protocol d'inici-aturada tant per a la transmissió com per a la recepció de dades. És a dir, cada octet (més el bit de paritat) està emmarcat per un o més bits d'inici i bits d'aturada, la qual cosa permet la sincronització per caràcters (octets) individuals.

El xip DUART utilitza un oscil•lador de 12,288 MHz que genera la seva temporització interna per controlar la lògica del transmissor i receptor. El canal dóna suport a l'operació dúplex. En cada adaptador de 8 ports s'implementen quatre xips DUART.

Tretze enregistraments accessibles pel sistema estan disponibles. Les característiques programables de cada canal inclouen:

- Longitud de caràcter: 5, 6, 7 ó 8 bits
- Generació/detecció de paritat: Parell, senar o cap
- Nombre de bits d'aturada: 1, 1,5 ó 2
- Habilitar/inhabilitar interrupcions. Dades rebudes disponibles
- Registre de retenció de transmissor buit
- Estat de línia
- Error de sobrepassar el límit
- Error de paritat
- Error de trama
- Salt.

A la taula següent trobareu les característiques de port (interfície de dispositiu) dels adaptadors.

Taula 114. Característiques de port d'adaptador asíncron de 8 ports

Paràmetre	**EIA 232**	**MIL-STD 188**	**EIA 422A**
Topologia	Punt a punt	Punt a punt	Punt a punt
Velocitat màxima de dades	138,4 Kbps (MC)/115,2 (ISA)	138,4 Kbps	138,4 Kbps
Mitjà de transmissió	Multiconductor	Multiconductor	Multiconductor
Nombre de fils de cable	9 inclòs el senyal de terra	9 inclòs el senyal de terra	5 inclòs el senyal de terra
Longitud màxima de cable	61 metres (200 peus)	130 metres a 38,4 Kbps	1200 metres < 90 Kbps
Connector de dispositiu	D de 25 potes	D de 25 potes	D de 25 potes
Interfície elèctrica	No equilibrada	No equilibrada	Equilibrada
Codificació de bits	Digital de dos nivells	Digital de dos nivells	Digital de dos nivells

La lògica d'arbitratge d'interrupcions estableix la prioritat dels adaptadors d'acord amb el següent esquema:

```
Adaptador   Prioritat
    1     Més alta
    2        |
    3        |
    4        |
    5        |
    6        |
    7        |
    8     Més baixa
```

Prioritat dels canals de comunicacions:

Els canals DUART amb interrupcions pendents es reparen seguint un esquema de prioritat fixa.

La prioritat més alta s'assigna al port 0. A continuació, la prioritat s'assigna al port 1 i així successivament. La prioritat més baixa la té el port 7.

Descripció de la lògica d'interrupcions dels adaptadors asíncrons de 8 ports:

La lògica d'interrupcions es divideix en la lògica de generació d'interrupcions i en la lògica d'arbitratge d'interrupcions.

Les dues seccions lògiques s'implementen en cada adaptador de 8 ports. La lògica de generació d'interrupcions proporciona la interfície al sistema. Aquesta lògica genera les sol•licituds d'interrupció del sistema i conté el circuit de compartiment d'interrupcions.

La funció de la lògica d'arbitratge d'interrupcions s'utilitza per identificar l'adaptador de 8 ports amb la interrupció que té la prioritat més alta pendent. Aleshores la lògica col•loca la informació d'interrupció del port amb la prioritat més alta a l'enregistrament d'arbitratge d'interrupcions. Això s'aconsegueix en una sola operació de lectura.

La lògica d'arbitratge d'interrupcions és exclusiva de l'adaptador de 8 ports i no s'ha de confondre amb la lògica d'arbitratge de Micro Channel.

Lògica de generació d'interrupcions de 8 ports:

L'adaptador asíncron implementa vuit línies de sol•licitud d'interrupció del sistema.

L'adaptador implementa les següents vuit línies de sol•licitud d'interrupció del sistema:
- IRQ 3
- IRQ 5
- IRQ 9
- IRQ 10
- IRQ 11
- IRQ 12
- IRQ 14
- IRQ 15

Només una línia de sol•licitud està activa durant el funcionament normal. Tots els adaptadors de 8 ports d'un sistema han d'utilitzar el mateix nivell d'interrupció per tal d'assolir un rendiment òptim del sistema. La línia activa se selecciona escrivint en l'enregistrament POS apropiat durant el cicle de configuració. L'adaptador permet compartir interrupcions i implementa una configuració de recollidor oberta. En aquesta disposició, una resistència d'actuació del sistema puja la línia d'interrupció. L'adaptador baixa la línia per indicar una sol•licitud d'interrupció activa.

Lògica d'arbitratge d'interrupcions de 8 ports:

La lògica d'arbitratge d'interrupcions determina la prioritat de la reparació de programari quan dos o més adaptadors de 8 ports o 16 ports generen interrupcions.

Fins a vuit adaptadors de 8 ports poden co-residir i funcionar simultàniament en un sistema. Aquest lògica proporciona al sistema la identificació d'adaptador i port així com el tipus d'interrupció en una sola operació de lectura. Un cop detectada la sol•licitud d'interrupció, el sistema llegeix l'enregistrament d'arbitratge d'interrupcions de 16 bits, que es troba a l'adreça d'E/S 0130.

Senyals d'interfície MIL-STD 188 d'adaptadors asíncrons de 8 ports:

Aquests senyals d'interfície s'implementen en cada port de l'adaptador.

Senyal	Definició
Tx Data	Dades de transmissió
RTS	Sol•licitud per enviar
CTS	Preparat per emetre
DSR	Conjunt de dades preparat
Rx Data	Dades de recepció
DCD	Detecció de portadora de dades
DTR	Terminal de dades preparat
RI	Indicador de timbre
Sig Gnd	Senyal de terra

Nivells de voltatge dels senyals MIL-STD 188 de 8 ports:

Els nivells de voltatge per a l'adaptador MIL-STD 188 es poden explicar per la polaritat de marca i espai normal o per la inversió de polaritat de marca i espai.

Els nivells de voltatge per a l'adaptador MIL-STD 188 s'expliquen a les seccions següents:

- Polaritat de marca i espai normal
- Inversió de polaritat de marca i espai.

El senyal es troba en l'estat de marca quan el voltatge del circuit d'intercanvi, mesurat al punt d'interfície, és inferior a -4 V cc respecte al senyal de terra. El senyal es troba en l'estat d'espai quan el voltatge és superior a +4 V cc respecte al senyal de terra. La regió entre +4 V cc i -4 V cc es defineix com a regió de transició i no és un nivell vàlid. El voltatge que és inferior a -6 V cc o superior a +6 V cc tampoc és un nivell vàlid.

Durant la transmissió de dades, l'estat de marca indica binari 1 i l'estat d'espai indica binari 0.

Per als circuits de control d'interfície, la funció està "activada" quan el voltatge és superior a +4 V cc respecte al senyal de terra i està "desactivada" quan el voltatge és inferior a -4 V cc respecte al senyal de terra. Els nivells de senyal d'MIL-STD 188 es mostren a la taula següent:

Taula 115. Nivells de senyal MIL-STD 188

Voltatge d'intercanvi	Estat binari	Condició del senyal	Funció de control d'interfície
+ Voltatge	0	Espai	Activada
- Voltatge	1	Marca	Desactivada

L'estàndard militar MIL-STD 188 requereix que els adaptadors proporcionin la capacitat d'invertir opcionalment les polaritats dels estats de marca i espai de les línies de transmissió i recepció. Aquesta capacitat es proporciona de manera independent a cada port.

Per a aquesta finalitat, s'utilitza el bit d'enregistrament de control 3 de mòdem DUART (Out 2). Quan el bit 3 s'estableix en un valor d'1, les polaritats per als estats de marca i espai s'estableixen en l'estat normal. Quan el bit 3 s'estableix en un valor de 0, les polaritats per als estats de marca i espai s'inverteixen.

El senyal es troba en l'*estat d'espai* quan el voltatge és inferior a -4 V cc respecte al senyal de terra. El senyal es troba en l'estat de marca quan el voltatge és superior a +4 V cc respecte al senyal de terra.

La regió entre +4 V cc i -4 V cc es defineix com a *regió de transició* i no és un nivell vàlid. El voltatge que és inferior a -6 V cc o superior a +6 V cc tampoc és un nivell vàlid.

Les característiques elèctriques dels ports de l'adaptador MIL-STD 188 asíncron de 8 ports compleixen les seccions de l'MIL-STD 188-114 per a una interfície de voltatge no equilibrada. L'estàndard és del 24 de març de 1976.

Els ports de l'adaptador compleixen els requisits funcionals per a l'operació asíncrona (protocol d'inici-aturada), tal com es descriu a l'estàndard EIA 232C d'octubre de 1969 i a l'estàndard EIA 232D de gener de 1987.

Senyals d'interfície EIA 422A d'adaptadors asíncrons de 8 ports:

El següents senyals d'interfície EIA 422A s'implementen en cada port de l'adaptador.

Senyal	Definició
TxA	Dades de transmissió
TxB	Dades de transmissió
RxA	Dades de recepció
RxB	Dades de recepció
Sig Gnd	Senyal de terra

Nivells de voltatge dels senyals EIA 422A de 8 ports:

El programa de control de línia genera un voltatge diferencial dins l'interval de 2 a 6 volts (mesurats al punt d'interfície de generador). La magnitud del voltatge diferencial al receptor ha d'estar dins l'interval de 200 mil•livolts a 6 volts (mesurats al punt d'interfície de càrrega).

Els mesuraments es prenen al terminal A (conductor positiu) respecte al terminal B (conductor negatiu). La taula següent descriu els estats dels senyals respecte als nivells de voltatge:

Taula 116. Estats de senyals EIA 422A de 8 ports

Voltatge d'intercanvi	Estat binari	Condició del senyal
+ Voltatge	0	Espai
- Voltatge	1	Marca

L'adaptador EIA 422A asíncron de 8 ports admet una longitud de cablatge interior de fins a 1200 metres (4000 peus). Els cables d'aquestes longituds són susceptibles a sobrecàrregues sobtades de voltatge a causa de voltatges induïts com poden ser els impactes indirectes de llamps. Un circuit secundari de protecció contra sobrecàrregues s'implementa a l'adaptador EIA 422A per protegir-lo d'aquestes sobrecàrregues de voltatge. El circuit de protecció contra sobrecàrregues s'implementa a les línies de dades de la interfície de l'adaptador.

S'ha afegit un circuit a prova d'errors als conductors d'entrada de cada receptor EIA 422A per tal d'evitar condicions d'error quan el receptor no està connectat a un programa de control (cable obert). El circuit a prova d'errors estableix el receptor en l'estat de marca (1 binari) sempre que el receptor no estigui connectat a un programa de control.

Les característiques elèctriques de l'adaptador EIA 422A asíncron de 8 ports compleixen l'estàndard EIA 422A de desembre de 1978.

Senyals d'interfície EIA 232 d'adaptadors asíncrons de 8 ports:

Aquests senyals d'interfície s'implementen en cada port de l'adaptador asíncron de 8 ports.

Els següents senyals d'interfície s'implementen en cada port de l'adaptador:

Senyal	Definició
TxD	Dades de transmissió
RTS	Sol•licitud per enviar
CTS	Preparat per emetre
DSR	Conjunt de dades preparat
RxD	Dades de recepció
DCD	Detecció de portadora de dades
DTR	Terminal de dades preparat
RI	Indicador de timbre
Sig Gnd	Senyal de terra

Nivells de voltatge dels senyals EIA 232 de 8 ports:

El senyal es troba en l'estat de marca quan el voltatge del circuit d'intercanvi, mesurat al punt d'interfície, és inferior a -3 V cc respecte al senyal de terra. El senyal es troba en l'estat d'espai quan el voltatge és superior a +3 V cc respecte al senyal de terra. La regió entre +3 V cc i -3 V cc es defineix com a *regió de transició* i no és un nivell vàlid. El voltatge inferior a -15 V cc o superior a +15 V cc tampoc és un nivell vàlid.

Durant la transmissió de dades, l'estat de marca indica l'estat binari 1 i l'estat d'espai indica l'estat binari 0.

Per als circuits de control d'interfície, la funció està activada quan el voltatge és superior a +3 V cc respecte al senyal de terra i està desactivada quan el voltatge és inferior a -3 V cc respecte al senyal de terra. Consulteu la taula següent per veure el nivells dels senyals EIA 232:

Taula 117. Nivells de senyal EIA 232

Voltatge d'intercanvi	Estat binari	Condició del senyal	Funció de control d'interfície
+ Voltatge	0	Espai	Activada
- Voltatge	1	Marca	Desactivada

Les característiques elèctriques dels ports de l'adaptador EIA 232 asíncron de 8 ports compleixen l'estàndard EIA 232C d'octubre de 1969 i l'estàndard EIA 232D de gener de 1987.

Els ports de l'adaptador compleixen els requisits funcionals per a l'operació asíncrona (protocol d'inici-aturada), tal com es descriu a l'estàndard EIA 232C d'octubre de 1969 i a l'estàndard EIA 232D de gener de 1987.

Lògica de control dels adaptadors asíncrons de 8 ports:

La secció de lògica de control basada en PAL coordina les activitat de totes les funcions més importants de l'adaptador.

Està sincronitzada amb un generador d'ona quadrada de 40 MHz. Opera interactivament amb el Micro Channel i les seves funcions inclouen descodificar adreces, comprovar la paritat d'adreces, respondre amb els senyals de control d'E/S correctes i controlar la línia de sol•licitud d'interrupció (IRQ) seleccionada (una de vuit línies IRQ).

La lògica de control opera interactivament amb els altres blocs de lògica de l'adaptador i gràcies a aquesta capacitat proporciona les línies de control als canals de comunicacions (DUART) i a la lògica d'arbitratge d'interrupcions. La lògica de control també opera interactivament amb la lògica del programa de control del bus de dades i proporciona control per a la direcció del flux de dades i per a la selecció d'octets de dades, que es col•loquen al bus local. Controla el generador de paritat de dades, el comprovador de paritat i les baldes.

Adaptadors asíncrons de 16 ports

La família d'adaptadors es basa en un disseny funcional comú. No obstant això, les característiques dels adaptadors individuals estan determinades per les interfícies de dispositiu suportades. La família consta de dos adaptadors: l'adaptador asíncron EIA 422A de 16 ports i l'adaptador asíncron EIA 232 de 16 ports.

Nota: La secció següent no és aplicable a la plataforma basada en Itanium.

La família d'adaptadors de 16 ports es basa en el xip DUART (dual universal asynchronous receiver and transmitter), que proporciona dos canals de comunicacions en sèrie. Per obtenir més informació sobre el xip DUART i el seu funcionament, consulteu l'apartat Informació de maquinari d'adaptador asíncron de 16 ports.

Adaptador asíncron de 16 ports - EIA 422A:

L'adaptador asíncron de 16 ports - EIA 232 proporciona suport per adjuntar un màxim de 16 dispositius sèrie asíncrons EIA 232 (impressores i terminals) a una unitat del sistema.

Es poden utilitzar fins a un total de vuit adaptadors (qualsevol combinació de la família) en una sola unitat del sistema.

Aquest adaptador es completament programable i només dóna suport a comunicacions asíncrones. Afegeix i elimina bits d'inici i bits d'aturada. Els adaptadors donen suport a la paritat parell, senar o cap de les dades en sèrie. Un generador de velocitat en bauds programable permet una operació de 50 a 38400 bps. Els adaptadors admeten caràcters de 5, 6, 7 o 8 bits amb 1, 1,5 o 2 bits d'aturada. Un sistema d'interrupció de prioritat controla les interrupcions de transmissió, recepció, error, estat de línia i conjunt de dades. Els 16 connectors per a l'adjunció de dispositius es proporcionen a l'acoblament de cables de 16 ports de l'EIA 422A.

L'adaptador de 16 ports EIA 422A té les següents característiques:

- Targeta de factor de format Micro Channel estàndard.
- Velocitats de dades fins a 38,4 Kbps per port.
- Col•locació al buffer de 16 octets per la transmissió i recepció.
- Connector de sortida de 78 potes senzill (el cable de la interfície multiport s'adjunta a aquest connector).
- Circuit de protecció contra sobrecàrregues.
- Admet una longitud de cablatge de fins a 1200 metres (4000 peus).
- Dóna suport als senyals d'interfície TxD i RxD.
- Interfície esclava Micro Channel de 8 bits/16 bits.

Instal•lació de l'adaptador asíncron de 16 ports:

L'adaptador asíncron de 16 ports es col•loca en una única ranura Micro Channel del servidor. Per instal•lar l'adaptador, seguiu aquests passos.

1. Verifiqueu que tots els usuaris estan desconnectats del sistema i executeu la següent ordre:
   ```
   shutdown -F
   ```
2. Quan hagi finalitzat l'ordre **shutdown**, desconnecteu l'alimentació del sistema.
3. Obriu la caixa del servidor i inseriu l'adaptador asíncron de 16 ports en una ranura Micro Channel lliure.
4. Adjunteu el connector d'intèrpret d'ordres D de 78 potes des del cable de la interfície de 16 ports a l'adaptador de 16 ports.
5. Torneu a posar els panells de la coberta a la unitat del sistema.

6. Enceneu l'alimentació del sistema. El sistema reconeixerà i configurarà l'adaptador de 16 ports durant el procés d'engegada.

Un cop hagi finalitzat l'engegada, inicieu una sessió utilitzant l'ID d'usuari root i executeu la següent ordre per comprovar la disponibilitat de l'adaptador:

```
lsdev -Cc adapter | pg
```

Només els adaptadors en estat disponible estan preparats per ser utilitzats pel sistema.

Si l'adaptador que s'ha acabat d'instal•lar NO està disponible, verifiqueu el següent:

1. L'adaptador està instal•lat correctament a la ranura Micro Channel.
2. Tot el cablatge necessari s'adjunta i es fixa bé en el seu lloc.
3. Executeu l'ordre: **errpt -a | pg** i examineu l'informe d'errors del sistema per veure el problemes relacionats amb els adaptadors.
4. Executeu l'ordre: **cfgmgr -v | pg**. Aquesta ordre intentarà tornar a configurar l'adaptador sense reengegar. Examineu si hi ha errors a la sortida paginada.
5. Si l'execució de l'ordre **cfgmgr** no és satisfactòria, caldrà reengegar.

Informació de maquinari d'adaptador asíncron de 16 ports:

La interfície del sistema presenta una adreça de 3 bits i dades de 8 bits, així com línies de control en el xip. Les dades de la interfície del sistema se serialitzen per ser transmeses a un dispositiu extern. Les dades en sèrie poden incloure un bit de paritat al límit d'octets. A la inversa, les dades d'un dispositiu extern es deserialitzen per ser transmeses a la interfície del sistema. Aquestes dades poden incloure un bit de paritat, que pot ser comprovat opcionalment. Com a opció, el canal pot funcionar en mode FIFO (first-in-first-out).

En mode FIFO, es poden col•locar al buffer fins a 16 octets tant al transmissor com al receptor. La interfície sèrie utilitza el protocol d'inici-aturada tant per a la transmissió com per a la recepció de dades. És a dir, cada octet (més el bit de paritat) està emmarcat per un bit d'inici i un bit d'aturada, la qual cosa permet la sincronització per caràcters (octets) individuals.

El xip DUART utilitza un oscil•lador de 12,288 MHz que genera la seva temporització interna per controlar la lògica del transmissor i receptor. El canal dóna suport a l'operació dúplex. En cada adaptador de 16 ports s'implementen vuit xips DUART.

Tretze enregistraments accessibles pel sistema estan disponibles. Les característiques programables de cada canal inclouen:

- Longitud de caràcter: 5,6, 7 ó 8 bits
- Generació/detecció de paritat: parell, senar o cap
- Nombre de bits d'aturada: 1, 1,5 ó 2
- Habilitar/inhabilitar interrupcions. Dades rebudes disponibles
- Registre de retenció de transmissor buit
- Estat de línia
- Error de sobrepassar el límit
- Error de paritat
- Error de trama
- Salt.

A la taula següent trobareu les característiques de port (interfície de dispositiu) dels adaptadors.

Taula 118. Característiques de port d'adaptador asíncron de 16 ports

Paràmetre	EIA 232	EIA 422A
Topologia	Punt a punt	Punt a punt
Velocitat màxima de dades (estàndard)	20 Kbps	2 Mbps
Velocitat màxima de dades (placa)	38,4 Kbps	38,4 Kbps
Mitjà de transmissió	Multiconductor	Multiconductor
Nombre de fils de cable	5 inclòs el senyal de terra	5 inclòs el senyal de terra
Longitud màxima de cable	61 metres (200 peus)	1200 metres < 90 Kbps
Connector de dispositiu	D de 25 potes	D de 25 potes
Interfície elèctrica	No equilibrada	Equilibrada
Codificació de bits	Digital de dos nivells	Digital de dos nivells

Prioritat de placa d'adaptador per als adaptadors asíncrons de 16 ports:

La lògica d'arbitratge d'interrupcions estableix la prioritat dels adaptadors segons un esquema específic.

```
Adaptador   Prioritat
    0     Més alta
    1       |
    2       |
    3       |
    4       |
    5       |
    6       |
    7       |
    8       |
    9       |
    10      |
    11      |
    12      |
    13      |
    14      |
    15    Més baixa
```

Els canals DUART amb interrupcions pendents es reparen seguint un esquema de prioritat fixa. La prioritat més alta s'assigna al port 0. A continuació, la prioritat s'assigna al port 1 i així successivament. La prioritat més baixa la té el port 15.

Lògica d'interrupcions dels adaptadors asíncrons de 16 ports:

Per als adaptadors asíncrons de 16 ports, la lògica d'interrupcions es divideix en la lògica de generació d'interrupcions i en la lògica d'arbitratge d'interrupcions.

Les dues seccions lògiques s'implementen en cada adaptador de 16 ports. La lògica de generació d'interrupcions proporciona la interfície al sistema. Aquesta lògica genera les sol•licituds d'interrupció del sistema i conté el circuit de compartiment d'interrupcions.

La funció de la lògica d'arbitratge d'interrupcions s'utilitza per identificar l'adaptador de 16 ports amb la interrupció que té la prioritat més alta pendent. Aleshores la lògica col•loca la informació d'interrupció del port amb la prioritat més alta a l'enregistrament d'arbitratge d'interrupcions. Això s'aconsegueix en una sola operació de lectura.

La lògica d'arbitratge d'interrupcions és exclusiva dels adaptadors de 16 ports i no s'ha de confondre amb la lògica d'arbitratge de Micro Channel.

Lògica de generació d'interrupcions de 16 ports:

L'adaptador asíncron de 16 ports implementa vuit línies de sol•licitud d'interrupció del sistema.

L'adaptador implementa les següents vuit línies de sol•licitud d'interrupció del sistema (IRQ):
- IRQ 3
- IRQ 5
- IRQ 9
- IRQ 10
- IRQ 11
- IRQ 12
- IRQ 14
- IRQ 15

Només una línia de sol•licitud està activa durant l'operació normal. Tots els adaptadors de 16 ports d'un sistema han d'utilitzar el mateix nivell d'interrupció per tal d'assolir un rendiment òptim del sistema. La línia activa se selecciona escrivint en l'enregistrament POS apropiat durant el cicle de configuració. L'adaptador permet compartir interrupcions i implementa una configuració de recollidor oberta, tal com es defineix a l'arquitectura de Micro Channel. En aquesta disposició, una resistència d'actuació del sistema puja la línia d'interrupció. L'adaptador baixa la línia per indicar una sol•licitud d'interrupció activa.

Lògica d'arbitratge d'interrupcions de 16 ports:

La lògica d'arbitratge d'interrupcions determina la prioritat de la reparació de programari quan dos o més adaptadors de 8 ports o 16 ports generen interrupcions.

Fins a vuit adaptadors de 8 ports o 16 ports poden co-residir i funcionar simultàniament en un sistema. Aquest lògica proporciona al sistema la identificació d'adaptador i port així com el tipus d'interrupció en una sola operació de lectura. Un cop es detecta una sol•licitud d'interrupció, el sistema llegeix l'enregistrament d'arbitratge d'interrupcions de 16 bits, que es troba a l'adreça d'E/S 0130.

Senyals d'interfície EIA 232 d'adaptadors asíncrons de 16 ports:

Els següents senyals d'interfície s'implementen en cada port de l'adaptador asíncron de 16 ports.

Senyal	Definició
TxD	Dades de transmissió
DCD	Detecció de portadora de dades
DTR	Terminal de dades preparat
RxD	Dades de recepció
Sig Gnd	Senyal de terra

Nivells de voltatge dels senyals EIA 232 de 16 ports:

El senyal es troba en l'estat de marca quan el voltatge del circuit d'intercanvi, mesurat al punt d'interfície, és inferior a -3 V cc respecte al senyal de terra. El senyal es troba en l'estat d'espai quan el voltatge és superior a +3 V cc respecte al senyal de terra. La regió entre +3 V cc i -3 V cc es defineix com a regió de transició i no és un nivell vàlid. El voltatge inferior a -15 V cc o superior a +15 V cc tampoc és un nivell vàlid.

Durant la transmissió de dades, l'estat de marca indica l'estat binari 1 i l'estat d'espai indica l'estat binari 0.

Per als circuits de control d'interfície, la funció està activada quan el voltatge és superior a +3 V cc respecte al senyal de terra i està desactivada quan el voltatge és inferior a -3 V cc respecte al senyal de terra. Consulteu la taula següent per veure el nivells dels senyals EIA 232.

Taula 119. Nivells de senyal EIA 232

Voltatge d'intercanvi	Estat binari	Condició del senyal	Funció de control d'interfície
+ Voltatge	0	Espai	Activada
- Voltatge	1	Marca	Desactivada

Les característiques elèctriques dels ports de l'adaptador EIA 232 asíncron de 16 ports compleixen l'estàndard EIA 232C d'octubre de 1969 i l'estàndard EIA 232D de gener de 1987.

Els ports de l'adaptador compleixen els requisits funcionals per a l'operació asíncrona (protocol d'inici-aturada), tal com es descriu a l'estàndard EIA 232C d'octubre de 1969 i a l'estàndard EIA 232D de gener de 1987.

Senyals d'interfície EIA 422A d'adaptadors asíncrons de 16 ports:

Aquests senyals d'interfície EIA 422A s'implementen en cada port de l'adaptador asíncron de 16 ports.

Senyal	Definició
TxA	Dades de transmissió
TxB	Dades de transmissió
RxA	Dades de recepció
RxB	Dades de recepció
Sig Gnd	Senyal de terra

Nivells de voltatge dels senyals EIA 422A de 16 ports:

El programa de control de línia genera un voltatge diferencial dins l'interval de 2 a 6 volts (mesurats al punt d'interfície de generador). La magnitud del voltatge diferencial al receptor ha d'estar dins l'interval de 200 mil•livolts a 6 volts (mesurats al punt d'interfície de càrrega).

Els mesuraments es prenen al terminal A (conductor positiu) respecte al terminal B (conductor negatiu). La taula següent descriu els estats dels senyals respecte als nivells de voltatge:

Taula 120. Estats de senyals EIA 422A de 16 ports

Voltatge d'intercanvi	Estat binari	Condició del senyal
+ Voltatge	0	Espai
- Voltatge	1	Marca

L'adaptador EIA 422A asíncron de 16 ports admet una longitud de cablatge interior de fins a 1200 metres (4000 peus). Els cables d'aquestes longituds són susceptibles a sobrecàrregues sobtades de voltatge a causa de voltatges induïts com poden ser els impactes indirectes de llamps. Un circuit secundari de protecció contra sobrecàrregues s'implementa a l'adaptador EIA 422A per protegir-lo d'aquestes sobrecàrregues de voltatge. El circuit de protecció contra sobrecàrregues s'implementa a les línies de dades de la interfície de l'adaptador.

S'ha afegit un circuit a prova d'errors als conductors d'entrada de cada receptor EIA 422A per tal d'evitar condicions d'error quan el receptor no està connectat a un programa de control (cable obert). El circuit a prova d'errors estableix el receptor en l'estat de marca (1 binari) sempre que el receptor no estigui connectat a un programa de control.

Les característiques elèctriques de l'adaptador EIA 422A asíncron de 16 ports compleixen l'estàndard EIA 422A de desembre de 1978.

Taula de conversió a ASCII, decimal, hexadecimal, octal i binari

En aquesta taula hi trobareu informació útil per convertir valors a ASCII, decimal, hexadecimal, octal i binari.

Taula 121. Conversions entre valors ASCII, decimal, hexadecimal, octal i binari

ASCII	Decimal	Hexadecimal	Octal	Binari
nul	0	0	0	0
inici de capçalera	1	1	1	1
inici de text	2	2	2	10
final de text	3	3	3	11
final de transmissió	4	4	4	100
interrogació	5	5	5	101
justificant de recepció	6	6	6	110
avisador acústic	7	7	7	111
caràcter de retrocés	8	8	10	1000
tabulador horitzontal	9	9	11	1001
salt de línia	10	A	12	1010
tabulador vertical	11	B	13	1011
salt de pàgina	12	C	14	1100
retorn de carro	13	D	15	1101
treure majúscules	14	E	16	1110
posar majúscules	15	F	17	1111
escapament d'enllaç de dades	16	10	20	10000
control 1/Xon de dispositius	17	11	21	10001
control 2 de dispositius	18	12	22	10010
control 3/Xoff de dispositius	19	13	23	10011
control 4 de dispositius	20	14	24	10100
justificant de recepció negatiu	21	15	25	10101
inactivitat síncrona	22	16	26	10110
final del bloc de transmissió	23	17	27	10111
cancel•lar	24	18	30	11000
final del suport	25	19	31	11001
final de fitxer/substitut	26	1A	32	11010
escapament	27	1B	33	11011
separador de fitxers	28	1C	34	11100
separador de grups	29	1D	35	11101
separador d'enregistraments	30	1E	36	11110
separador d'unitat	31	1F	37	11111
espai	32	20	40	100000
!	33	21	41	100001
"	34	22	42	100010

Taula 121. Conversions entre valors ASCII, decimal, hexadecimal, octal i binari (continuació)

ASCII	Decimal	Hexadecimal	Octal	Binari
#	35	23	43	100011
$	36	24	44	100100
%	37	25	45	100101
&	38	26	46	100110
'	39	27	47	100111
(	40	28	50	101000
)	41	29	51	101001
*	42	2A	52	101010
+	43	2B	53	101011
,	44	2C	54	101100
-	45	2D	55	101101
.	46	2E	56	101110
/	47	2F	57	101111
0	48	30	60	110000
1	49	31	61	110001
2	50	32	62	110010
3	51	33	63	110011
4	52	34	64	110100
5	53	35	65	110101
6	54	36	66	110110
7	55	37	67	110111
8	56	38	70	111000
9	57	39	71	111001
:	58	3A	72	111010
;	59	3B	73	111011
<	60	3C	74	111100
=	61	3D	75	111101
>	62	3E	76	111110
?	63	3F	77	111111
@	64	40	100	1000000
A	65	41	101	1000001
B	66	42	102	1000010
C	67	43	103	1000011
D	68	44	104	1000100
E	69	45	105	1000101
F	70	46	106	1000110
G	71	47	107	1000111
H	72	48	110	1001000
I	73	49	111	1001001
J	74	4A	112	1001010
K	75	4B	113	1001011
L	76	4C	114	1001100
M	77	4D	115	1001101
N	78	4E	116	1001110
O	79	4F	117	1001111

Taula 121. Conversions entre valors ASCII, decimal, hexadecimal, octal i binari (continuació)

ASCII	Decimal	Hexadecimal	Octal	Binari
P	80	50	120	1010000
Q	81	51	121	1010001
R	82	52	122	1010010
S	83	53	123	1010011
T	84	54	124	1010100
U	85	55	125	1010101
V	86	56	126	1010110
W	87	57	127	1010111
X	88	58	130	1011000
Y	89	59	131	1011001
Z	90	5A	132	1011010
[	91	5B	133	1011011
\	92	5C	134	1011100
]	93	5D	135	1011101
^	94	5E	136	1011110
_	95	5F	137	1011111
`	96	60	140	1100000
a	97	61	141	1100001
b	98	62	142	1100010
c	99	63	143	1100011
d	100	64	144	1100100
e	101	65	145	1100101
f	102	66	146	1100110
g	103	67	147	1100111
h	104	68	150	1101000
i	105	69	151	1101001
j	106	6A	152	1101010
k	107	6B	153	1101011
l	108	6C	154	1101100
m	109	6D	155	1101101
n	110	6E	156	1101110
o	111	6F	157	1101111
p	112	70	160	1110000
q	113	71	161	1110001
r	114	72	162	1110010
s	115	73	163	1110011
t	116	74	164	1110100
u	117	75	165	1110101
v	118	76	166	1110110
w	119	77	167	1110111
x	120	78	170	1111000
y	121	79	171	1111001
z	122	7A	172	1111010
{	123	7B	173	1111011
|	124	7C	174	1111100

Taula 121. Conversions entre valors ASCII, decimal, hexadecimal, octal i binari (continuació)

ASCII	Decimal	Hexadecimal	Octal	Binari
}	125	7D	175	1111101
~	126	7E	176	1111110
DEL	127	7F	177	1111111
	128	80	200	10000000
	129	81	201	10000001
	130	82	202	10000010
	131	83	203	10000011
	132	84	204	10000100
	133	85	205	10000101
	134	86	206	10000110
	135	87	207	10000111
	136	88	210	10001000
	137	89	211	10001001
	138	8A	212	10001010
	139	8B	213	10001011
	140	8C	214	10001100
	141	8D	215	10001101
	142	8E	216	10001110
	143	8F	217	10001111
	144	90	220	10010000
	145	91	221	10010001
	146	92	222	10010010
	147	93	223	10010011
	148	94	224	10010100
	149	95	225	10010101
	150	96	226	10010110
	151	97	227	10010111
	152	98	230	10011000
	153	99	231	10011001
	154	9A	232	10011010
	155	9B	233	10011011
	156	9C	234	10011100
	157	9D	235	10011101
	158	9E	236	10011110
	159	9F	237	10011111
	160	A0	240	10100000
	161	A1	241	10100001
	162	A2	242	10100010
	163	A3	243	10100011
	164	A4	244	10100100
	165	A5	245	10100101
	166	A6	246	10100110
	167	A7	247	10100111
	168	A8	250	10101000
	169	A9	251	10101001

Taula 121. Conversions entre valors ASCII, decimal, hexadecimal, octal i binari (continuació)

ASCII	Decimal	Hexadecimal	Octal	Binari
	170	AA	252	10101010
	171	AB	253	10101011
	172	AC	254	10101100
	173	AD	255	10101101
	174	AE	256	10101110
	175	AF	257	10101111
	176	B0	260	10110000
	177	B1	261	10110001
	178	B2	262	10110010
	179	B3	263	10110011
	180	B4	264	10110100
	181	B5	265	10110101
	182	B6	266	10110110
	183	B7	267	10110111
	184	B8	270	10111000
	185	B9	271	10111001
	186	BA	272	10111010
	187	BB	273	10111011
	188	BC	274	10111100
	189	BD	275	10111101
	190	BE	276	10111110
	191	BF	277	10111111
	192	C0	300	11000000
	193	C1	301	11000001
	194	C2	302	11000010
	195	C3	303	11000011
	196	C4	304	11000100
	197	C5	305	11000101
	198	C6	306	11000110
	199	C7	307	11000111
	200	C8	310	11001000
	201	C9	311	11001001
	202	CA	312	11001010
	203	CB	313	11001011
	204	CC	314	11001100
	205	CD	315	11001101
	206	CE	316	11001110
	207	CF	317	11001111
	208	D0	320	11010000
	209	D1	321	11010001
	210	D2	322	11010010
	211	D3	323	11010011
	212	D4	324	11010100
	213	D5	325	11010101
	214	D6	326	11010110

Taula 121. Conversions entre valors ASCII, decimal, hexadecimal, octal i binari (continuació)

ASCII	Decimal	Hexadecimal	Octal	Binari
	215	D7	327	11010111
	216	D8	330	11011000
	217	D9	331	11011001
	218	DA	332	11011010
	219	DB	333	11011011
	220	DC	334	11011100
	221	DD	335	11011101
	222	DE	336	11011110
	223	DF	337	11011111
	224	E0	340	11100000
	225	E1	341	11100001
	226	E2	342	11100010
	227	E3	343	11100011
	228	E4	344	11100100
	229	E5	345	11100101
	230	E6	346	11100110
	231	E7	347	11100111
	232	E8	350	11101000
	233	E9	351	11101001
	234	EA	352	11101010
	235	EB	353	11101011
	236	EC	354	11101100
	237	ED	355	11101101
	238	EE	356	11101110
	239	EF	357	11101111
	240	F0	360	11110000
	241	F1	361	11110001
	242	F2	362	11110010
	243	F3	363	11110011
	244	F4	364	11110100
	245	F5	365	11110101
	246	F6	366	11110110
	247	F7	367	11110111
	248	F8	370	11111000
	249	F9	371	11111001
	250	FA	372	11111010
	251	FB	373	11111011
	252	FC	374	11111100
	253	FD	375	11111101
	254	FE	376	11111110
	255	FF	377	11111111

uDAPL (user-level Direct Access Programming Library)

uDAPL (user Direct Access Programming Library) és una infraestructura d'accés directe perquè s'executi en transports compatibles amb l'accés directe a dades com InfiniBand , RNIC etc.

DAT Collaborative especifica el **uDAPL** API http://www.datcollaborative.org .

El codi base d'uDAPL es transfereix des d'Open Fabrics a AIX i actualment s'admet en adaptadors GX++HCA i en la targeta d'expansió 4X DDR (CFFh) InfiniBand.

La versió 1.2 d'**uDAPL** s'admet a AIX 6.1 amb 6100-06 i en versions posteriors. La imatge d'instal•lació **uDAPL** s'envia al paquet d'ampliació com a *udapl.rte*. Aquesta imatge inclou els fitxers de capçalera DAT, que hi ha a **/usr/include/dat**. La imatge d'instal•lació també inclou dues biblioteques, *libdat.a* i *libdapl.a*.

Les aplicaciones inclouen els fitxers de capçalera DAT i l'enllaç a la biblioteca DAT (*libdat.a* a **/usr/include/dat**). La capa DAT determina les biblioteques apropiades subjacents específiques de transport.

Un proveïdor AIX **uDAPL** es registra amb el registre DAT utilitzant les entrades *dat.conf*. El fitxer */etc/dat.conf* s'inclou a les entrades predeterminades i conté detalls sobre el format de l'entrada.

Per motius de depuració, les biblioteques **uDAPL** admeten el rastreig de sistema AIX . Els ID d'enganxament de rastreig de sistema**uDAPL** inclouen 5C3 (per a incidències DAPL), 5C4 (per a incidències d'error DAPL), 5C7 (per a incidències DAT), i 5C8 (per a incidències d'error DAT). El nivell de rastreig inicial es pot modificar a través de les variables d'entorn *DAT_TRACE_LEVEL* i *DAPL_TRACE_LEVEL* que poden tenir valors numèrics de 0 a 10. El nombre d'incidències i la quantitat de dades rastrejades augmenta amb el nivell i amb els nivells de rastreig clau existents

```
TRC_LVL_ERROR  = 1,
TRC_LVL_NORMAL = 3,
TRC_LVL_DETAIL = 7
```

Altres característiques de capacitat de servei estàndard AIX com ara el registre d'errors AIX, poden ser útils per determinar un problema. I les característiques de capacitat de servei de la capa de transport subjacent, com l'ordre ibstat i el component de rastreig InfiniBand, també ajuden a diagnosticar problemes.

Les API DAT tornen els codis de retorn estàndards que es poden descodificar amb el fitxer */usr/include/dat/dat_error.h*. L'explicació detallada dels codis de retorn es troba en l'especificació **uDAPL** de DAT Collaborative.

"Protocol d'Internet a través d'InfiniBand (IPoIB)" a la pàgina 394

API d'uDAPL compatibles amb AIX

De les moltes API **uDAPL** especificades per DAT Collaborative, n'hi ha unes quantes que no són compatibles amb AIX.

Aquestes són les API que no són compatibles amb les implementacions d'**uDAPL** comuns del sector i tampoc seran compatibles amb AIX.

Element	Descripció
dat_cr_handoff	// In DAT 1.2
dat_ep_create_with_srq	// In DAT 1.2
dat_ep_recv_query	// In DAT 1.2
dat_ep_set_watermark	// In DAT 1.2
dat_srq_create	// In DAT 1.2
dat_srq_post_recv	// In DAT 1.2
dat_srq_resize	// In DAT 1.2
dat_srq_set_lw	// In DAT 1.2
dat_srq_free	// In DAT 1.2
dat_srq_query	// In DAT 1.2

Les API addicionals que no són compatibles amb AIX,

- dat_lmr_sync_rdma_read
- dat_lmr_sync_rdma_write
- dat_registry_add_provider
- dat_registry_add_provider

Per a totes les API no compatibles, AIX segueix els mecanisme específics descrits en l'especificació DAT per identificar la falta de compatibilitat. Aquests inclouen valors d'atribut (com ara max_srq equaling zero) i codis de retorn específics (com ara DAT_MODEL_NOT_SUPPORTED). Com que és coherent amb la implementació del sector i l'especificació DAT, DAT_NOT_IMPLEMENTED es pot retornar per a una funció que no és compatible.

La compatibilitat d'API relacionades amb RMR com ara *dat_rmr_create* ,*dat_rmr_bind* ,*dat_rmr_free* i *dat_rmr_query* depèn de la capacitat HCA subjacent, i el bon funcionament o els errors del sistema els determina la infraestructura subjacent IB. Actualment, els adaptadors GX++ HCA i 4X DDR Expansion card (CFFh) InfiniBand no són compatibles amb aquestes operacions RMR.

"uDAPL (user-level Direct Access Programming Library)" a la pàgina 681

"Atributs específics del proveïdor per a uDAPL"

"Protocol d'Internet a través d'InfiniBand (IPoIB)" a la pàgina 394

Atributs específics del proveïdor per a uDAPL

Hi ha uns quants atributs específics de proveïdor compatibles amb AIX. Els noms dels atributs són **delayed_ack_supported** , **vendor_extension**, **vendor_ext_version**, **debug_query** i **debug_modify**.

delayed_ack_supported

El proveïdor de AIX per al transport d'InfiniBand (IB) inclou un atribut d'adaptador d'interfície (IA) anomenat **delayed_ack_supported**. El valor d'aquest atribut pot ser **true** o **false**. Si és **true**, els punts finals associats amb aquest IA tenen un atribut específic del proveïdor modificable anomenat named **delayed_ack**. Quan l'atribut **delayed_ack_supported** és **false**, un atribut **delayed_ack** de punt final específic del proveïdor no es pot modificar. El valor per defecte d'un atribut **delayed_ack** de punt final és **false**. En establir-lo com a **true** (mitjançant dat_ep_modify) s'habilita la característica ack retardat de l'adaptador de canal de sistema principal (HCA) d'IB subjacent per el parell de cues específic d'IB associat amb el punt final. Tots els HCA no implementen aquesta característica de maquinari, per tant, no està disponible per a tots els IA. Habilitar la característica fa que l'HCA retardi l'acusació de rebut fins que una operació de transferència de dades sigui visible a la memòria del sistema d'un servidor. Aquesta és una mica més semàntica que la que es proporciona en l'especificació d'IB, al cost potencial d'un petit augment de latència.

vendor_extension, vendor_ext_version, debug_query and debug_modify

Per motius de depuració, les biblioteques **uDAPL** admeten el rastreig de sistema AIX. El nivell de rastreig inicial es pot modificar utilitzant les variables d'entorn *DAT_TRACE_LEVEL* i *DAPL_TRACE_LEVEL*. Per canviar aquests nivells de rastreig dinàmicament mitjançant l'API, oferim suport de nivell de seguiment dinàmic en AIX. Per verificar si la biblioteca té un suport de nivell de seguiment dinàmic, les aplicacions poden consultar l'atribut d'IA específic del proveïdor, **vendor_extension**. Un cop feta la consulta, la presència de l'atribut **vendor_extension** indica suport de nivell de seguiment dinàmic. El valor de l'atribut està establert com a **true**; però independentment d'això, la presència de l'atribut indica el suport. Quan l'atribut **vendor_extension** és present, les aplicacions poden obtenir els punters de la funció a **dat_trclvl_query()** i **dat_trclvl_modify()**, consultant els atributs d'IA específics del proveïdor **debug_query** and **debug_modify**. El valor d'aquests atributs tindrà el punter per a les funcions corresponents. Perquè aquesta interfície **vendor_extension** sigui extensible per a un futur ús, tenim un altre atribut IA específic del proveïdor, **vendor_ext_version**. Com que ara només admetem una versió, el valor d'aquest atribut s'establirà com a **1.0**. Si l'atribut **vendor_extension** no existeix, les aplicacions no poden modificar el nivell de seguiment dinàmicament.

S'inclou un exemple de com manipular aquests atributs al codi de mostra **uDAPL** instal•lat amb la implementació AIX.

"uDAPL (user-level Direct Access Programming Library)" a la pàgina 681

"Protocol d'Internet a través d'InfiniBand (IPoIB)" a la pàgina 394

Suport per a l'adaptador RoCE PCIe2 10 GbE

L'adaptador PCIe2 10GbE RDMA Over Converged Ethernet (RoCE) s'admetia, en primera instància, a sistemes operatius AIX només com a dispositiu habilitat per a l'RDMA (Remote Direct Memory Access). El software que donava suport era un programari de propietat de l'IBM basat en la pila de l'AIX InfiniBand. Aquest suport va anomenar-se AIX RoCE. AIX 7 amb 7100-02 o posterior suporta l'adaptador en dos modes, els quals són el suport de l'AIX RoCE i el de l'Ethernet de 10G també anomenada Targeta d'interfície de xarxa (AIX NIC). El nou AIX 7 amb 7100-03 ara suporta RDMA conjuntament amb el mode NIC mode i l'OpenFabrics Enterprise Distribution (OFED). L'adaptador de bus amfitrió (HBA), que no estava disponible en versions anteriors de l'AIX, gestiona el mode habilitat.

La taula següent mostra l'evolució del programari de l'Adaptador PCIe2 10GbE:

Nivell de l'AIX	MODE 1	MODE 2
Abans AIX 7 amb 7100-02	AIX RoCE	ND
AIX 7 amb 7100-02	AIX RoCE	AIX NIC
AIX 7 amb 7100-03	AIX RoCE	AIX NIC + OFED RoCE

Per baixar l'últim controlador de dispositiu per aquest adaptador, completeu els passos següents:

1. Aneu al lloc web d'IBM (www.ibm.com)
2. Feu clic a **Suport i descàrregues**.
3. Baixeu-vos l'últim microprogramari d'AIX a l'ubicació de l'amfitrió (`/etc/microcode`)
4. Executeu l'eina **diag** per actualitzar el microprogramari mitjançant la tria d'un dels procediments següents:
   - Procediment curt:
     a. Escriviu l'ordre següent:
        ```
        *diag -d entX -T download
        ```
        Nota: Substituïu **entX** per **roceX** si esteu utilitzant la pila RoCE d'una versió anterior.
     b. Seleccioneu el microcodi que s'ha desat al directori `/etc/microcode`.

- Procediment llarg
  a. Escriviu l'ordre següent:
     ```
     *diag
     ```
  b. Feu clic a:**Selecció de tasques** > **Tasques de microcodi** > **Baixar microcodi**.
  c. Seleccioneu **entX** o **roceX**.
  d. Seleccioneu el microcodi que s'ha desat al directori `/etc/microcode`.

L'adaptador està configurat perquè admeti el mode RoCE de l'AIX per defecte. Completeu els passos de la secció "AIX NIC + OFED RDMA" per canviar-ho a un altre mode.

AIX NIC + OFED RDMA

Com a AIX 7 amb 7100-02, l'adaptador PCIe2 10 GbE RoCE pot configurar-se per ser executaten la configuració NIC de l'AIX. Com a AIX 7 amb 7100-03, la funcionalitat OFED RDMA també es va afegir a la configuració NIC de l'AIX. Si no teniu les aplicacions d'ús intensiu de xarxa que es beneficien de la configuració RDMA, podeu utilitzar l'adaptador només com a targeta de xarxa (NIC).

Per utilitzar l'adaptador PCIe2 10 GbE RoCE en la configuració AIX NIC + OFED RoCE o en la configuració AIX RoCE, els catàlegs de fitxers descrits a continuació són necessaris i estan disponibles al CD del sistema operatiu base de AIX 7 amb 7100-03.

devices.ethernet.mlx
: Controlador de dispositiu principal de l'adaptador d'Ethernet convergit (mlxentdd) per donar suport a la configuració NIC + OFED RoCE de l'AIX.

devices.pciex.b315506b3157265
: Paquet de suport per a l'adaptador d'Ethernet convergit Packaging NGP ITE ASIC2.

devices.pciex.b3155067b3157365
: Paquet de suport per a l'adaptador d'Ethernet convergit Packaging NGP ITE ASIC1.

devices.pciex.b315506714101604
: Paquet per a l'adaptador d'Ethernet convergit de 2 ports Mellanox 10 GbE amb transceptors compactes connectables (SFP+).

devices.pciex.b315506714106104
: Paquet per a l'adaptador d'Ethernet convergit de 2 ports Mellanox 10 GbE, que admet qualsevol transceptor SFP+.

devices.common.IBM.ib
: El programa de control de dispositiu ICM és necessari per utilitzar la configuració RoCE de l'AIX.

devices.pciex.b3154a63
: Programa de control de dispositiu del Mellanox 10 GbE Converge Ethernet Adapter que és necessari per utilitzar la configuració RoCE de l'AIX.

ofed.core
: Catàleg de fitxers de l'OFED Core Runtime Environment que és necessari només si es necessita l'OFED RDMA is required.

Després d'actualitzar els catàlegs de fitxers RoCE de l'AIX amb els nous càtalegs, els dispositius roce i ent poden aparèixer configurats. Si ambdós dispositius apareixen configurats quan executeu l'ordre **lsdev** en els adaptadors, completeu els passos següents:

1. Esborreu les instàncies *roceX* que estan relacionades amb l'adaptador RoCE PCIe2 10 GbE i introduïu l'ordre següent:
   ```
   # rmdev -dl roce0[, roce1][, roce2,...]
   ```
2. Esborreu les instàncies *entX* que estan relacionades amb l'adaptador RoCE PCIe2 10 GbE i introduïu l'ordre següent:

```
# rmdev -dl ent1[,ent2][, ent3...]
```

3. Si hi ha un o més adaptadors de bus amfitrió convergits que estan relacionats amb l'adaptador RoCe, elimineu-los mitjançant l'ordre següent:
   ```
   # rmdev -dl hba0[, hba1][,hba2...]
   ```
4. Executeu el gestor de configuració per incorporar els canvis i introduïu l'ordre següent:
   ```
   # cfgmgr
   ```

Completeu els passos següents per canviar a la configuració NIC + OFED RoCE de l'AIX des de la configuració RoCE de l'AIX:

1. Atureu totes les aplicacions RDMA que s'executen a l'adaptador RoCE PCIe2 10 GbE.
2. Suprimiu o redefiniu les instàncies de *roceX* mitjançant una de les ordres següents:
   - `# rmdev -d -l roce0`
   - `# rmdev -l roce0`

   L'ordre `rmdev -l roce0` reté la definició de la configuració `roce0`, de manera que ho podeu utilitzar la propera vegada que creeu instàncies.
3. Canvieu l'atribut del paràmetre hba stack_type de `aix_ib` (RoCE de l'AIX) a `ofed` (NIC + OFED RoCE de l'AIX) mitjançant l'ordre següent:
   ```
   # chdev -l hba0 -a stack_type=ofed
   ```
4. Executeu l'eina de gestió de configuració de manera que l'adaptador de bus amfitrió pugui configurar l'adaptador RoCE PCIe2 10 GbE RoCE Adapter com a un adaptador NIC mitjançant l'ordre següent:
   ```
   # cfgmgr
   ```
5. Verifiqueu que l'adaptador s'executa enn la configuració NIC mitjançant l'ordre següent:
   ```
   # lsdev -C -c adapter
   ```

   L'exemple següent mostra els resultats quan executeu l'ordre **lsdev** a l'adaptador configurat en el mode AIX NIC + OFED RoCE:

```
ent1 Available 00-00-01 PCIe2 10GbE RoCE Converged Network Adapter
ent2 Avaliable 00-00-02 PCIe2 10GbE RoCE Converged Network Adapter
hba0 Available 00-00 PCIe2 10GbE RoCE Converged Host Bus Adapter (b315506714101604)
```

Figura 45. Exemple de sortida per a l'ordre **lsdev** *a un adaptador amb la configuració AIX NIC + OFED RoCE*

Degut a això, AIX 7 amb 7100-03, AIX també dóna suport a OFED RDMA en el mode AIX NIC, si es necessita habilitar OFED RDMA, és necessari completar els següents passos addicionals:

1. Instal•leu el paquet ofed.core.
2. Definiu el mode RDMA en els dispositius ent1 i ent2 mitjançant l'ordre següent:
   ```
   # chdev –l ent1 –a rdma=desired
   # chdev –l ent2 -a rdma=desired
   ```

   El mode RDMA s'establirà abans que les interfícies en1 o en 2 s'hagin configurat.
3. Podeu inhabilitar el mode RDMA mitjançant l'ordre següent:
   ```
   # chdev –l ent1 –a rdma=disabled
   # chdev –l ent2 –a rdma=disabled
   ```

AIX RoCE

L'adaptador RoCE PCIe2 10 GbE s'ha preconfigurat per operar en el mode de configuració RDMA de l'AIX . Una xarxa que utilitza RDMA ofereix un rendiment millor que la configuració NIC per a aplicacions d'ús intensiu de xarxa. Aquest mode sovint és d'útilitat per a l'emmagatzematge de xarxa o per computació d'alt rendiment.

La configuració RoCE de l'AIX requereix l'utilització de biblioteques o interfícies, com ara:

- El Direct Access Programming Library (uDAPL), que s'utilitza pel sistema de base de dades DB2
- El Message Passing Interface (MPI), que s'utilitza per la computació d'alt rendiment (HPC)

Figura 46 a la pàgina 687 mostra la sortida quan l'adaptador s'executa en el mode RoCE de l'AIX.

L'adaptador RoCE PCIe2 10 GbE RoCE mostra només una instancia de l'adaptador quan està en el mode RoCE de l'AIX, però pot tenir fins a dos ports. Utilitzi l'ordre **ibstat** per determinar quants ports s'han configurat efectuant els passos següents:

1. Determinar si l'extensió del kernel `icm` està configurada introduint l'ordre següent:
   ```
   # lsdev -C | grep icm
   ```
2. Si el kernel icm no està configurat, entri l'ordre següent per configurar-lo:
   ```
   # mkdev -c management -s infiniband -t icm
   ```
3. Executar l'ordre **ibstat** introduint l'ordre següent:
   ```
   # ibstat roce0
   ```

Mentre l'adaptador PCIe2 10 GbE RoCE s'ha configurat inicialment pel mode RoCE de l'AIX, és possible que necessiteu tornar a la configuració NIC + OFED RoCE de l'AIX. Per caviar la configuració NIC + OFED RoCE de l'AIX a la configuració RoCE de l'AIX, completeu els passos següents:

1. Verifiqueu que l'adaptador està en el mode NIC + OFED RoCE de l'AIX mitjançant l'ordre següent:
   ```
   # lsdev -C -c adapter
   ```

   La sortida de l'ordre **lsdev** és semblant a l'exemple de Figura 45 a la pàgina 685.
2. Aturar el trànsit TCP/IP i desconnectar les interfícies IP introduint les ordres següents:
   ```
   # ifconfig en1 down detach; ifconfig en2 down detach
   ```
3. Suprimir o posar les instàncies de NIC en un estat definit mitjançant una de les ordres següents:
   - `# rmdev -d -l ent1; rmdev -d -l ent2`
   - `# rmdev -l ent1; rmdev -l ent2`

   L'ordre `rmdev -l ent1; rmdev -l ent2` reté la definició dels dispositius Ethernet, de manera que ho podeu utilitzar la propera vegada que creeu instàncies.
4. Canvieu l'atribut de l' hba stack_type des de `ofed` (NIC + OFED RoCE de l'AIX) a `aix_ib` (RoCE de l'AIX) mitjançant una de les ordres següents:
   ```
   # chdev -l hba0 -a stack_type=aix_ib
   ```
5. Executeu l'eina de gestió de configuració, de manera que l'adaptador de bus amfitrió pugui configurar l'adaptador RoCE PCIe2 10 GbE com a un adaptador RoCE de l'AIX mitjançant l'ordre següent:
   ```
   # cfgmgr
   ```
6. Verifiqueu que l'adaptador s'està executant en la configuració RoCE de l'AIX mitjançant l'ordre següent:
   ```
   # lsdev -C -c adapter
   ```

   L'exemple següent mostra els resultats quan executeu l'ordre **lsdev** per adaptadors i estan configurats en el mode RDMA de l'AIX .

```
roce0 Avaliable 00-00-00 PCIe2 10GbE RoCE Converged Network Adapter
hba0 Available  00-00-00 PCIe2 10GbE RoCE Converged Host Bus Adapter (b315506714101604)
```

Figura 46. Exemple de sortida per a l'ordre **lsdev** *per adaptadors que utilitzen la configuració RoCE de l'AIX*

Suport per a l'adaptador RoCE PCIe3 40 GbE

L'adaptador PCIe3 40 GbE RDMA Over Converged Ethernet (RoCE) admet accés de memòria directa remota (RDMA) amb l'OpenFabrics Enterprise Distribution (OFED) en el mode NIC normal. L'RDMA s'activa i té suport per defecte si el programari de l'OpenFabrics està instal•lat.

Per baixar l'últim controlador de dispositiu per aquest adaptador, completeu els passos següents:

1. Aneu al lloc web d'IBM (www.ibm.com).
2. Feu clic a **Suport i descàrregues**.
3. Baixeu-vos l'últim microprogramari d'AIX a l'ubicació de l'amfitrió (`/etc/microcode`).
4. Executeu l'eina **diag** per actualitzar el microprogramari mitjançant la tria d'un dels procediments següents:
   - Procediment curt:
     a. Escriviu l'ordre següent:
        ```
        *diag -d entX -T download
        ```
        Nota: Si el dispositiu Ethernet pertany al mateix adaptador bus d'amfitrió (per exemple, hba0, hba1 i així successivament), baixeu-vos el microprogramari a un dels dispositius **ent**.
     b. Seleccioneu el microcodi que s'ha desat al directori `/etc/microcode`.
   - Procediment llarg
     a. Escriviu l'ordre següent:
        ```
        *diag
        ```
     b. Feu clic a **Selecció de tasques** > **Tasques de microcodi** > **Baixar microcodi**.
     c. Seleccioneu **entX**.
     d. Seleccioneu el microcodi que s'ha desat al directori `/etc/microcode`.

Per utilitzar l'adaptador RoCE PCIe3 40 GbE i el AIX NIC + OFED RoCE, es necessiten els següents catàlegs de fitxers. Aquests catàlegs estàn disponibles These filesets are available en el CD base del sistema operatiu AIX 7 amb 7100-03.

devices.ethernet.mlx	Controlador de dispositiu principal de l'adaptador d'Ethernet convergit (mlxentdd).
devices.pciex.b31503101410b504	Paquet per al Mellanox 2 Ports 40 Gb Converged Ethernet Adapter que utilitza el ports de coure passius Quad Small Form-factor Pluggable (QSFP).
ofed.core	Catàleg de fitxers de l'OFED Core Runtime Environment que només es necessita si la funcionalitat OFED RDMA és necessària.

Per inhabilitar la funció RDMA, introduïu l'ordre següent

```
chdev  –l  <Ethernet_device> rdma=disabled
```

Exemple:

```
# chdev –l ent1 –a rdma=disabled
# chdev –l ent2 –a rdma=disabled
```

Per habilitar la funció RDMA, introduïu l'ordre següent

```
chdev –l <Ethernet_device> rdma=desired
```

Avisos

Aquesta informació s'ha desenvolupat per a productes i serveis que es comercialitzen als EUA.

És possible que IBM no ofereixi els productes, serveis o funcions descrites en aquest document a d'altres països. Consulteu el vostre representant d'IBM local per obtenir més informació sobre els productes i serveis que estan disponibles actualment a la vostra regió. Les referències a un producte, programa o servei d'IBM no signifiquen ni impliquen que només es pugui utilitzar aquest producte, programa o servei d'IBM. Es pot utilitzar qualsevol producte, programa o servei equivalent en funcions que no infringeixi cap dret de propietat intel•lectual d'IBM.Sigui com sigui, l'usuari es responsabilitza d'avaluar i verificar el funcionament dels productes, programes o serveis que no siguin d'IBM.

IBM pot tenir aplicacions amb patent o pendents de patent que cobreixin el tema descrit en aquest document. La possessió d'aquest document no atorga cap llicència per a aquestes patents. Podeu enviar per escrit les consultes referents a les llicències a:

IBM Director of Licensing
IBM
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
EUA

Per efectuar consultes en relació a informació sobre el joc de caràcters de doble byte (DBCS), poseu-vos en contacte amb el Departament de propietat intel•lectual d'IBM del vostre país o envieu les consultes, per escrit, a:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA AQUESTA PUBLICACIÓ "TAL QUAL" SENSE CAP GARANTIA, NI EXPLÍCITA NI IMPLÍCITA, INCLOENT-HI, PERÒ SENSE LIMITAR-SE A, LES GARANTIES IMPLÍCITES DE NO INFRACCIÓ, COMERCIALITZACIÓ O IDONEÏTAT PER A UNA FINALITAT CONCRETA. Algunes jurisdiccions no admeten la renúncia de responsabilitats de les garanties explícites o implícites en determinades transaccions, per la qual cosa és possible que aquesta informació no us afecti.

Pot ser que la publicació inclogui incorreccions tècniques o errors tipogràfics. La informació tècnica d'aquest document se sotmet periòdicament a revisions. Els canvis pertinents s'afegiran a les noves edicions que es publiquin. IBM pot efectuar millores i/o canvis en els productes i/o programes descrits en aquesta publicació en qualsevol moment sense cap avís previ.

Les referències contingudes a indrets web que no siguin d'IBM es faciliten en aquest document per a la comoditat de l'usuari i no suposen en cap cas una recomanació d'aquests indrets. La informació d'aquests llocs web no forma part de la informació d'aquest producte d'IBM i l'usuari és responsable de l'ús d'aquests llocs web.

IBM pot utilitzar o distribuir qualsevol informació que se li subministri de la manera que consideri adequada sense incórrer en cap obligació amb la part que l'ha subministrada.

Els propietaris d'una llicència d'aquest programa que vulguin obtenir-ne informació per tal de fer possible: (i) l'intercanvi d'informació entre programes creats de manera independent i altres programes (incloent-hi aquest) i (ii) l'ús mutu de la informació intercanviada, s'han de posar en contacte amb:

IBM Director of Licensing
IBM
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
EUA

Aquesta informació pot estar disponible de forma gratuïta depenent dels termes i condicions aplicables i, segons els casos, podria ser necessari fer efectiu el pagament d'una quota.

El programa sota llicència descrit en aquesta documentació, i tot el material sota llicència relacionat amb el programa, està proporcionat per IBM d'acord amb els termes de l'IBM Customer Agreement, IBM International Program License Agreement o qualsevol altre acord equivalent entre les parts.

Les dades de rendiment i exemples de client citats es presenten només amb finalitats il•lustratives. Els resultats de rendiment reals poden variar segons les configuracions específiques i les condicions de funcionament.

La informació referent als productes que no són d'IBM s'ha obtingut dels mateixos proveïdors dels productes, dels anuncis que han publicat o a partir de qualsevol font d'informació públicament disponible. IBM no ha comprovat aquests productes i no pot confirmar la precisió de les afirmacions sobre rendiment, compatibilitat o d'altra mena relacionades amb aquests productes. Els dubtes relacionats sobre els productes no IBM s'han d'adreçar als proveïdors d'aquests productes.

Les afirmacions relatives a les direccions o propòsits futurs d'IBM poden canviar-se o retirar-se sense avís previ, i representen només metes i objectius.

Tots els preus que es mostren són preus de venda al detall suggerits per IBM, són actualitzats i poden canviar sense avís previ. Els preus dels distribuïdors poden variar.

Aquesta informació només té finalitats de planificació. La informació d'aquest document pot canviar abans que els productes descrits estiguin disponibles.

Aquesta informació conté exemples de dades i informes utilitzats en operacions empresarials. Per fer-los creïbles, els exemples poden incloure noms de persones, empreses, marques i productes. Tots aquests noms són ficticis i qualsevol semblança amb persones o empreses comercials reals és pura coincidència.

LLICÈNCIA DE COPYRIGHT:

Aquesta informació conté programes d'aplicació d'exemple en llenguatge font, que il•lustren tècniques de programació en diverses plataformes operatives. Podeu copiar, modificar i distribuir aquests programes de mostra en qualsevol format sense haver d'efectuar cap pagament a IBM, amb l'objectiu de desenvolupar, utilitzar, comercialitzar o distribuir programes d'aplicació segons la interfície de programació d'aplicacions per a la plataforma operativa per a la qual estan escrits els programes de mostra. Aquests exemples no s'han provat a fons sota totes les condicions. Per aquesta raó, IBM no pot garantir o implicar la fiabilitat, operativitat o el funcionament d'aquests programes. Els programes d'exemple es proporcionen "TAL QUAL", sense cap garantia de cap tipus. IBM no serà responsable dels danys derivats de l'ús dels programes d'exemple.

Totes les còpies o parts d'aquests programes de mostra o treballs derivats han d'incloure un avís de copyright com el següent:

© (nom de la vostra empresa) (any).

Parts d'aquest codi provenen d'IBM Corp. Sample Programs.

Consideracions sobre la política de privacitat

Els productes de programari d'IBM, com ara el programari com a solucions del servei, (“Ofertes de programari”) poden utilitzar galetes o altres tecnologies per recopilar informació de l'ús del producte i millorar l'experiència de l'usuari final per adaptar les interacciones amb l'usuari final o per a altres finalitats. Les Ofertes de programari no tenen el costum de recopilar informació d'identificació personal. En alguns casos, aquestes Ofertes us ajuden a recopilar informació d'identificació personal. En el cas que utilitzin galetes per recopilar aquest tipus d'informació, tot seguit s'indica informació específica sobre l'ús de les galetes que fan aquestes ofertes.

Aquesta Oferta de programari no utilitza galetes ni altres tecnologies per recopilar informació d'identificació personal.

Si les configuracions desplegades per a aquesta Oferta de programari us proporcionen com a client, la capacitat de recopilar informació d'identificació personal d'usuaris finals mitjançant galetes i altres tecnologies, hauríeu de cercar assessorament judicial sobre les lleis aplicables referents a la recopilació de dades i ésser conscient dels requisits de notificació i consentiment.

Si voleu obtenir més informació sobre l'ús de diverses tecnologies i galetes per a la recopilació de dades, consulteu la Política de privadesa d'IBM a http://www.ibm.com/privacy i la Declaració de privadesa en línia d''IBM a http://www.ibm.com/privacy/details; la secció anomenada “Cookies, Web Beacons and Other Technologies” (Galetes, senyals webs i altres tecnologies” i “IBM Software Products and Software-as-a-Service Privacy Statement” (Declaració de privadesa dels productes de programari d'IBM i ofertes de Software-as-a-Service) a http://www.ibm.com/software/info/product-privacy.

Marques registrades

IBM, el logotip d'IBM i ibm.com són marques registrades o marques comercials d'International Business Machines Corp., registrades en moltes jurisdiccions de tot el món. És possible que d'altres productes o noms de servei siguin marques registrades d'IBM o d'altres empreses. Hi ha disponible una llista de les marques registrades d'IBM al lloc web a l'apartat Copyright and trademark information a www.ibm.com/legal/copytrade.shtml.

INFINIBAND, InfiniBand Trade Association i les marques de disseny d'INFINIBAND són marques registrades o marques de servei d'INFINIBAND Trade Association.

Intel, el logotip d'Intel, Intel Inside, el logotip d'Intel Inside, Intel Centrino, el logotip d'Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium i Pentium són marques registrades d'Intel Corporation o de les seves filials als Estats Units i /o a d'altres països.

Linux és una marca registrada de Linus Torvalds als EUA i a d'altres països.

Microsoft, Windows, Windows NT i el logotip de Windows són marques registrades de Microsoft Corporation als Estats Units i/o a d'altres països.

Java i totes les marques registrades i logotips basats en Java són marques registrades de Oracle i/o els seus afiliats.

UNIX és una marca registrada de The Open Group als EUA i a d'altres països.

Índex

Caràcters Especials

Números

A

B

C

D

E

F

G

H

N

O

P

Q

R

S

T

U

V

W

X

Imprès a Espanya