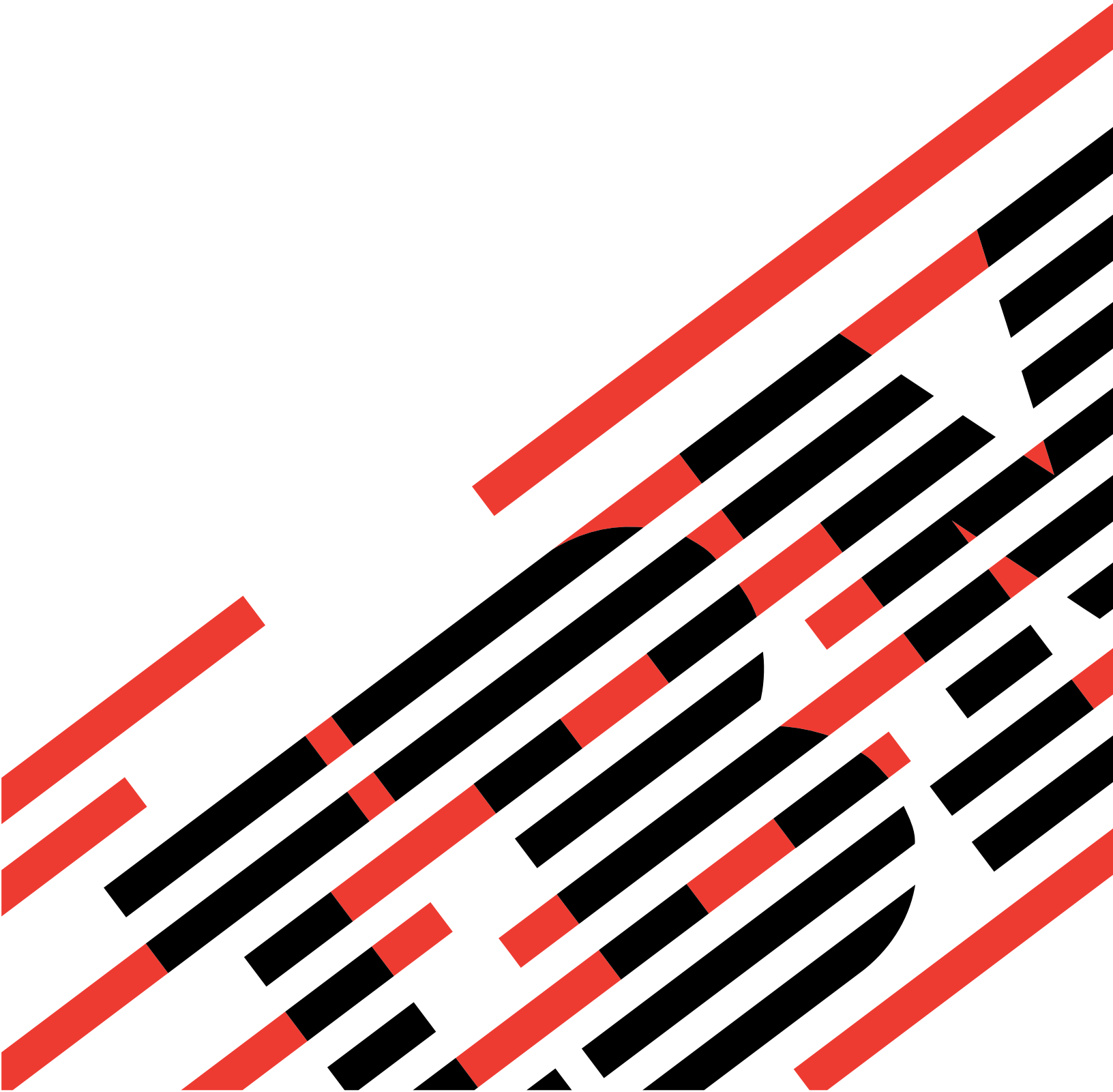
IBM

eserver

iSeries

Setarea reţelei TCP/IP

Versiunea 5 Ediţia 3



IBM

@server

iSeries

Setarea reţelei TCP/IP

Versiunea 5 Ediţia 3

Notă

Înainte de a utiliza aceste informaţii şi produsul la care se referă, aveţi grijă să citiţi “Observaţii”, la pagina 57.

Ediţia a şaptea (august 2005)

Această ediţie este valabilă pentru Operating System/400 (5722–SS1) Versiunea 5, Ediţia 3, Modificarea 0 şi pentru toate ediţiile şi modificările următoare, până când se specifică altceva în noile ediţii. Această versiune nu rulează pe toate modelele RISC (reduced instruction set computer - calculator cu set de instrucţiuni redus) şi nici pe modelele CICS.

Cuprins

Partea 1. Setarea TCP/IP

Serverul dumneavoastră a sosit şi sunteţi pregătit să îl puneţi în funcţiune. Acest subiect vă prezintă uneltele şi procedurile pentru configurarea TCP/IP în OS/400. De exemplu, puteţi folosi aceste informaţii pentru a crea o descriere de linie, o interfaţă TCP/IP şi o rută. Aflaţi cum să vă personalizaţi configuraţia TCP/IP folosind Navigator iSeries şi învăţaţi despre diverse tehnici TCP/IP care vă permit să direcţionaţi datele care circulă în şi în afara reţelei dumneavoastră.

Înainte de a folosi aceste informaţii pentru a configura TCP/IP, vedeţi Instalarea şi utilizarea hardware-ului pentru a vă asigura că aţi instalat toate componentele hardware necesare. După ce executaţi task-urile iniţiale pentru configurarea TCP/IP, sunteţi pregătit să vă extindeţi capabilităţile serverului cu aplicaţii, protocoale şi servicii TCP/IP, pentru a îndeplini necesităţile dumneavoastră unice.

Ce este nou în V5R3
Aflaţi ce este nou şi modificat în funcţia TCP/IP.

Tipăriţi acest subiect
Folosiţi acest subiect pentru a tipări sau pentru a descărca o versiune PDF (Portable Document Format) a documentaţiei de setare a TCP/IP.

Internet Protocol versiunea 6 (IPv6)
Noul Internet Protocol, IPv6, joacă un rol cheie în viitorul Internetului şi puteţi folosi IPv6 pe serverul iSeries. Acest subiect ofreră informaţii generale despre IPv6 şi modul cum este implementat pe serverul iSeries.

Planificarea setării TCP/IP
Acest subiect vă ajută să vă pregătiţi pentru instalarea şi configurarea TCP/IP pe serverul iSeries. Sunt furnizate cerinţele de bază pentru instalare şi configurare, astfel încât să aveţi toate informaţiile necesare la îndemână când începeţi configurarea TCP/IP. Sunt oferite trimiteri la termeni şi concepte înrudite.

Instalarea TCP/IP
Acest subiect vă conduce prin instalarea produselor care vă pregătesc serverul iSeries pentru operare.

Configurarea TCP/IP
Acest subiect vă arată cum să vă conectaţi serverul iSeries şi cum să configuraţi TCP/IP. În plus, vedeţi instrucţiunile pentru configurarea IPv6.

Pesonalizarea TCP/IP cu Navigator iSeries
Acest subiect prezintă opţiuni de personalizare cu Navigator iSeries.

Tehnici TCP/IP peste Ethernet virtual
Aflaţi cum să folosiţi Ethernet virtual în OS/400.

Depanarea TCP/IP
Dacă vă confruntaţi cu probleme privind conexiunile sau traficul TCP/IP, folosiţi Depanarea TCP/IP ca ajutor la găsirea soluţiilor. Acest ghid de depanare vă ajută să rezolvaţi problemele atât pentru versiunea IPv4, cât şi pentru IPv6.

Informaţii înrudite pentru setarea TCP/IP
Acest subiect răspunde întrebării: ″Ce pot face în plus?″ Găsiţi trimiteri la servicii şi aplicaţii care vă îmbunătăţesc performanţele serverului.

Capitolul 1. Ce este nou în V5R3

Îmbunătăţiri ale setării TCP/IP

Dacă folosiţi o reţea Ethernet virtual pentru a permite partiţiilor dumneavoastră să comunice una cu alta, ar putea fi necesar să extindeţi comunicaţia către o reţea LAN fizică externă. Vedeţi Tehnici TCP/IP de conectare a reţelei Ethernet virtual la o reţea LAN externă pentru a afla cum să vă conectaţi reţeaua Ethernet virtual la o reţea LAN externă. Folosiţi aceste informaţii pentru a trece în revistă exemple ce ilustrează trei metode diferite de legare a traficului din reţeaua Ethernet virtual la o reţea LAN externă.

Pentru a obţine alte informaţii despre ce este nou sau modificat în această ediţie, vedeţi Memo către utilizatori.

Cum să vedeţi ce este nou sau modificat

Pentru a vă ajuta să vedeţi unde au fost făcute modificările tehnice, aceste informaţii folosesc:

- Imaginea » pentru a marca locul unde încep informaţiile noi sau modificate.
- Imaginea « pentru a marca locul unde se termină informaţiile noi sau modificate.

Capitolul 2. Tipăriţi acest subiect

Pentru a vizualiza sau descărca versiunea PDF a acestui document, selectaţi Setarea TCP/IP (aproximativ 362 KO).

Alte informaţii

Puteţi de asemenea vizualiza sau tipări oricare dintre următoarele PDF-uri:

- Manuale:
  - **Configurarea TCP/IP şi referinţe** (592 KO)
    Această carte furnizează informaţii despre configurarea TCP/IP şi operarea şi utilizarea reţelei.
  - **Indicii şi unelte pentru a vă securiza sistemul iSeries** (1 MO)
    Această carte oferă recomandări de bază privind utilizarea opţiunilor de securitate ale iSeries, pentru a vă proteja serverul şi operaţiile sale asociate.
- Redbooks:
  - **Îndrumar TCP/IP şi privire generală tehnică** (7 MO)
    Această carte oferă informaţii de bază despre TCP/IP.
  - **TCP/IP for AS/400 : More Cool Things Than Ever** (9 MB)
    Această carte include o listă extinsă de aplicaţii şi servicii TCP/IP obişnuite.

Salvarea fişierelor PDF

Pentru a salva un PDF pe staţia de lucru proprie pentru vizualizare sau tipărire:

1. Faceţi clic dreapta pe PDF în browser-ul dumneavoastră (clic dreapta pe legătura de mai sus).
2. Faceţi clic pe **Save Target As...** dacă folosiţi Internet Explorer. Faceţi clic pe **Save Link As...** dacă folosiţi Netscape Communicator.
3. Navigaţi în directorul în care doriţi să salvaţi fişierul PDF.
4. Faceţi clic pe **Save**.

Descărcarea programului Adobe Acrobat Reader

Aveţi nevoie de Adobe Acrobat Reader pentru a vizualiza sau tipări aceste PDF-uri. Puteţi descărca o copie de pe situl Web Adobe (www.adobe.com/products/acrobat/readstep.html) .

Capitolul 3. Internet Protocol versiunea 6 (IPv6)

Internet Protocol versiunea 6 (IPv6) este versiunea actualizată a protocolului Internet Protocol versiunea 4 (IPv4) şi înlocuieşte treptat IPv4 ca standard Internet.

Vă puteţi întreba cum să folosiţi IPv6 pentru dezvoltarea afacerilor electronice ale companiei dumneavoastră sau puteţi fi un programator care doreşte să creeze aplicaţii IPv6 pentru ca firma să poată beneficia de pe urma acestui protocol îmbunătăţit. Citiţi aceste subiecte pentru a afla informaţii de bază despre IPv6 şi cum se foloseşte IPv6 pe serverul iSeries:

Ce este IPv6?
Aflaţi de ce IPv6 înlocuieşte IPv4 ca standard Internet şi cum îl puteţi folosi avantajele pe care le oferă.

Ce funcţii ale IPv6 sunt disponibile?
Învăţaţi cum este implementat în prezent IPv6 pe serverul iSeries.

Scenarii IPv6
Vedeţi exemple care vă ajută să înţelegeţi situaţiile în care aţi putea să folosiţi IPv6 pentru activitatea companiei dumneavoastră.

Concepte IPv6
Învăţaţi conceptele de bază IPv6. Dacă nu sunteţi sigur de diferenţele care există între IPv4 şi IPv6, vedeţi comparaţii detaliate, cum ar fi compararea adreselor IPv4 şi IPv6, sau prin ce se deosebesc anteturile pachetului IPv4 de anteturile pachetului IPv6.

Configurarea IPv6
Aflaţi care sunt cerinţele de hardware şi software şi găsiţi instrucţiuni pentru configurarea IPv6 pe server.

Depanarea IPv6
Găsiţi soluţii la problemele IPv6.

Informaţii înrudite pentru IPv6
Găsiţi legături la resurse care vă ajută să înţelegeţi IPv6.

Ce este IPv6?

Internet Protocol versiunea 6 (IPv6) este nivelul următor de evoluţie a protocolului Internet Protocol. În prezent, pe Internet se foloseşte în cea mai mare parte IPv4, un protocol care de peste 20 de ani se dovedeşte fiabil şi eficient. Însă IPv4 are limitări importante, care, pe măsură ce Internetul se extinde, produc tot mai multe probleme.

De exemplu, se resimte din ce în ce mai mult lipsa adreselor IPv4, de care este nevoie pentru toate dispozitivele noi adăugate la Internet. Cheia pentru îmbunătăţirea IPv6 este expansiunea spaţiului de adrese IP de la 32 de biţi la 128 de biţi, ceea ce permite, practic, un număr nelimitat de adrese IP unice. Noul format al textului de adresă IPv6 este:

```
xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
```

unde fiecare x este o cifră hexazecimală care reprezintă 4 biţi.

Capacitatea de adresare extinsă a protocolului IPv6 oferă o soluţie la problema epuizării adreselor. Acest lucru este cu atât mai important cu cât tot mai mulţi oameni folosesc calculatoare mobile, cum ar fi telefoanele mobile şi calculatoarele de mână. Cererile crescânde ale celor care utilizează comunicaţiile fără fir contribuie la epuizarea adreselor IPv4. Capacitatea de extindere a adresei IP a protocolului IPv6 rezolvă această problemă prin furnizarea de adrese IP suficiente pentru numărul în creştere al dispozitivelor fără fir.

Pe lângă această capacitate de adresare, IPv6 furnizează funcţii noi, care simplifică sarcinile de configurare şi de administrare a adreselor pe reţea. Configurarea şi întreţinerea reţelelor este o activitate foarte laborioasă. IPv6 reduce volumul de muncă prin automatizarea mai multor sarcini ale administratorului de reţea.

Dacă folosiţi IPv6, nu trebuie să renumerotaţi adresele de dispozitiv când schimbaţi furnizorul de servicii Internet (ISP). Puteţi păstra aceleaşi adrese, deoarece sunt adrese unice global.

Opţiunea de autoconfigurare a protocolului IPv6 configurează automat adresele de ruter şi de interfaţă, în locul dumneavoastră. În autoconfigurarea stateless, IPv6 ia adresa MAC a maşinii şi un prefix de reţea furnizat de un nod local şi combină aceste două adrese pentru a crea o adresă IPv6 nouă, unică. Această opţiune elimină necesitatea unui server DHCP şi economiseşte timpul administratorului şi banii companiei dumneavoastră.

Pentru mai multe surse de informaţie despre IPv6, vedeţi Informaţii înrudite pentru IPv6

Vedeţi Ce funcţii ale IPv6 sunt disponibile? pentru informaţii IPv6 referitoare strict la serverul iSeries.

Ce funcţii ale IPv6 sunt disponibile?

IBM implementează IPv6 pentru serverul iSeries în mai multe ediţii de software. În prezent IPv6 este implementat într-o platformă de dezvoltare de aplicaţii, cu scopul dezvoltării şi testării aplicaţiilor IPv6. Funcţiile IPv6 sunt transparente pentru aplicaţiilor TCP/IP existente şi coexistă cu funcţiile IPv4.

Principalele funcţii ale serverului iSeries care sunt afectate de IPv6 sunt următoarele:

- **Configurarea**
  Trebuie să ştiţi că procesul de configurare pentru IPv6 se deosebeşte de cel pentru IPv4. Pentru a folosi funcţia IPv6, trebuie să modificaţi configurarea TCP/IP a serverului prin configurarea unei linii pentru IPv6. Trebuie să configuraţi IPv6 pe o linie Ethernet sau pe o linie tunel.

  În cazul în care configuraţi o linie Ethernet pentru traficul IPv6, trimiteţi pachetele IPv6 printr-o reţea IPv6. Vedeţi în Crearea unei reţele locale (LAN) IPv6 un scenariu ce descrie o situaţie în care puteţi configura o linie Ethernet pentru IPv6.

  În cazul în care configuraţi linii tunel, trimiteţi pachete IPv6 printr-o reţea IPv4 existentă. Vedeţi în Trimiterea pachetelor IPv6 printr-o reţea locală (LAN) IPv4 şi Trimiterea pachetelor IPv6 printr-o reţea de mare suprafaţă (WAN) IPv4 scenarii ce descriu două situaţii în care puteţi crea o linie tunel configurată pentru IPv6.

  Vedeţi Configurarea IPv6 pentru a vă configura reţeaua pentru IPv6.
- **Socket-urile**
  Dezvoltaţi şi testaţi aplicaţii cu socket-uri folosind API-urile şi uneltele IPv6. IPv6 îmbunătăţeşte socket-urile, astfel că aplicaţiile pot folosi IPV6 cu o familie nouă de adrese: AF_INET6. Aceste îmbunătăţiri nu afectează aplicaţiile IPv4 existente. Puteţi crea aplicaţii care suportă concurent traficul IPv6 şi IPv4 sau numai trafic IPv6. Vedeţi Folosirea familiei de adrese AF_INET6 pentru informaţii suplimentare despre IPv6 pentru socket-uri.
- **DNS**
  DNS (Domain Name System) suportă adresele AAAA şi un domeniu nou pentru căutările inverse: IP6.ARPA. În timp ce DNS extrage informaţiile IPv6, serverul trebuie să folosească IPv4 pentru a comunica cu DNS.
- **Depanarea TCP/IP**
  Folosiţi unelte de depanare standard, cum ar fi PING, netstat, trace route şi urmărirea comunicaţiilor, pentru reţele şi tuneluri IPv6. Aceste unelte suportă acum formatul de adresă IPv6. Vedeţi Depanarea TCP/IP pentru a rezolva probleme pentru ambele reţele, IPv4 şi IPv6.

Vedeţi Informaţii înrudite pentru IPv6 pentru resurse despre IPv6.

Scenarii: IPv6

Revedeţi următoarele scenarii pentru a înţelege de ce ar trebui să implementaţi IPv6 şi cum să vă configuraţi reţeaua în fiecare din aceste situaţii:

- Crearea unei reţele locale (LAN) IPv6
- Trimiterea pachetelor IPv6 printr-o reţea locală (LAN) IPv4
- Trimiterea pachetelor IPv6 printr-o reţea de mare suprafaţă (WAN) IPv4

Notă: În acest scenariu, adresele IP 10.x.x.x reprezintă adrese IP publice. Toate adresele folosite în aceste scenarii au numai rolul de exemplu.

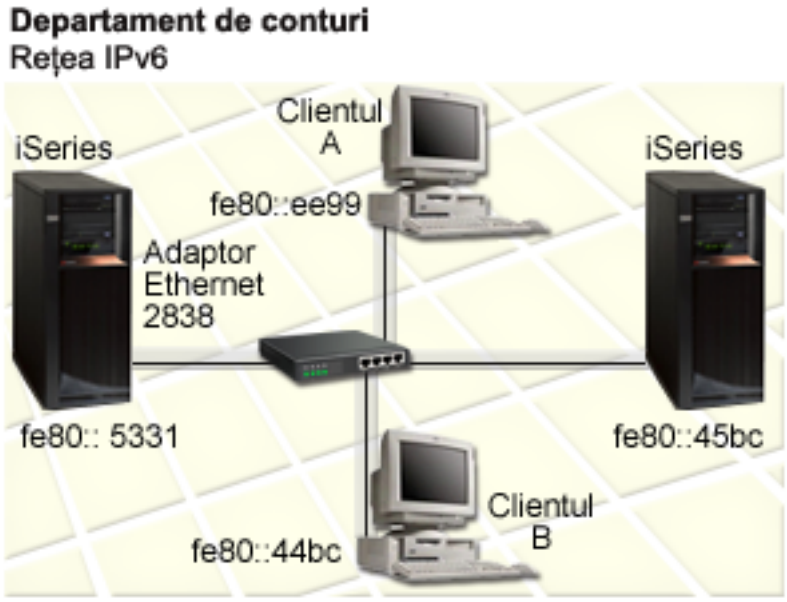
Vedeţi Configurarea IPv6 pentru a vă configura serverul pentru IPv6.

Vedeţi Concepte IPv6 pentru definiţiile conceptelor de bază IPv6.

Crearea unei reţele locale (LAN) IPv6

Situaţie

IPv6 va înlocui în cele din urmă IPv4 ca standard Internet. În consecinţă, compania dumneavoastră decide să implementeze IPv6 pentru operaţiile sale financiare şi cumpără o nouă aplicaţie de contabilitate, care foloseşte IPv6 pentru conectivitate. Aplicaţia trebuie să se conecteze la altă instanţă a aplicaţiei, care se află pe alt server, conectat la reţeaua locală (LAN) Ethernet a sediului. Sarcina dumneavoastră este să vă configuraţi serverul pentru IPv6 astfel încât firma dumneavoastră să poată începe să folosească aplicaţia de contabilitate. Ilustraţia următoare prezintă setarea reţelei în acest scenariu.



Soluţie

Pentru a crea o reţea locală (LAN) IPv6, trebuie să configuraţi o descriere de linie Ethernet pentru IPv6. Pentru ca angajaţii să folosească aplicaţia de contabilitate, între serverele iSeries şi clienţii din reţea circulă pachete IPv6.

Cerinţele de setare includ:

- OS/400 versiunea 5 ediţia 2 sau ulterioară
- Adaptoare Ethernet 2838 sau 2849, deoarece sunt singurele tipuri de resurse hardware suportate în prezent pentru IPv6.
- iSeries Access pentru Windows şi Navigator iSeries (componenta Reţea din Navigator iSeries)
- Serverul trebuie să aibă configurată o interfaţă fizică IPv4 separată înainte de a configura linia Ethernet pentru IPv6, deoarece pe server trebuie să ruleze TCP/IP. Dacă nu aţi configurat serverul pentru IPv4, vedeţi Configurarea TCP/IP pentru prima dată înainte de configurarea liniei pentru IPv6.

Configurare

Pentru a configura o descriere de linie Ethernet pentru IPv6, trebuie să folosiţi vrăjitorul **Configurare IPv6** din Navigator iSeries. IPv6 poate fi configurat numai din Navigator iSeries, nu şi din interfaţa bazată pe caractere.

Vrăjitorul cere numele resursei hardware de comunicaţii de pe serverul pe care veţi configura IPv6; de exemplu, CMN01. Aceasta trebuie să fie un adaptor Ethernet 2838 sau 2849 care nu este configurat în cael moment pentru IPv4.

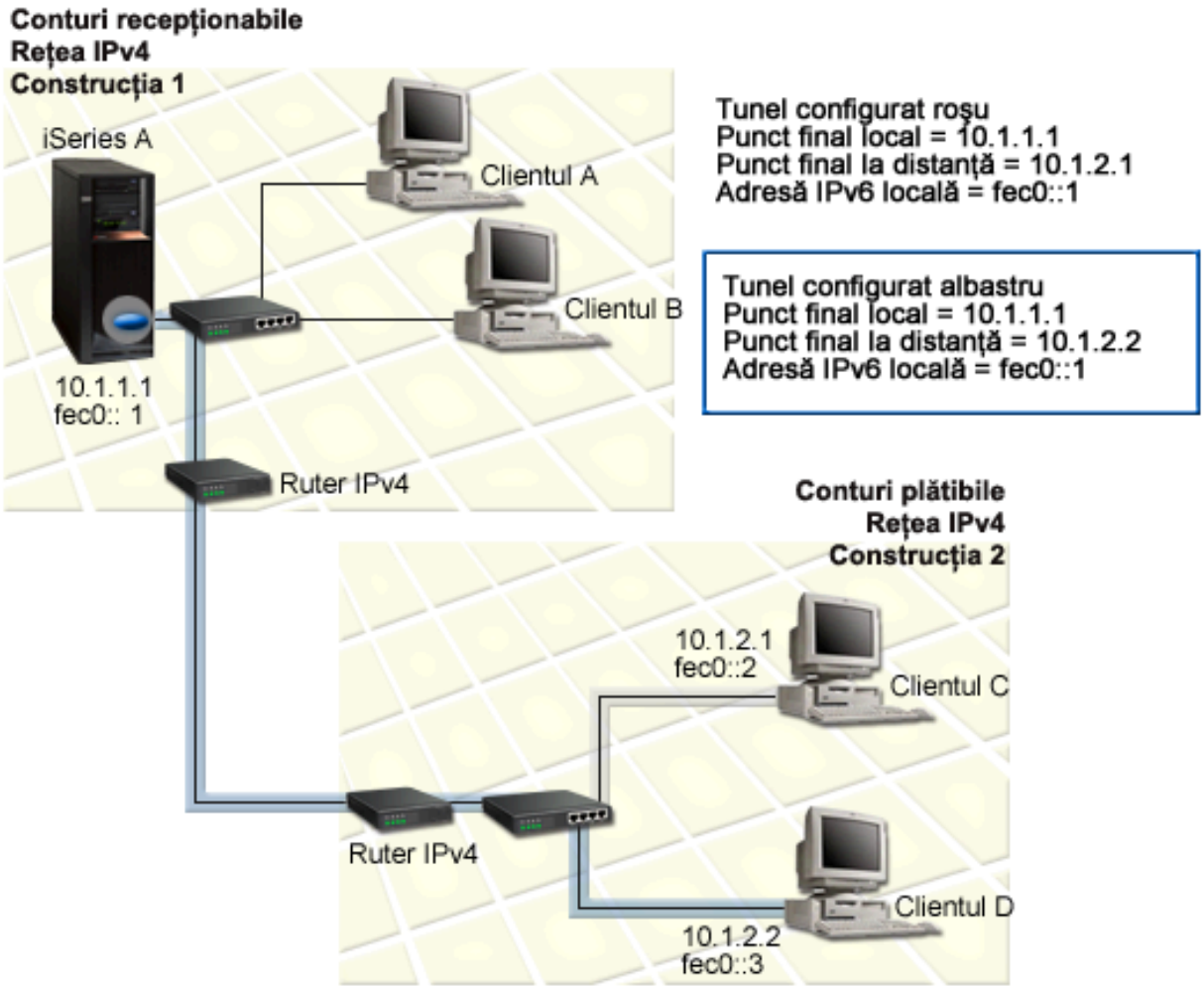
Pentru a folosi vrăjitorul **Configurare IPv6**, parcurgeţi paşii următori:

1. În Navigator iSeries, selectaţi **serverul —> Reţea —> Configurare TCP/IP**.
2. Faceţi clic dreapta pe **IPv6**, selectaţi **Configurare IPv6** şi urmaţi instrucţiunile vrăjitorului pentru a configura o linie Ethernet pentru IPv6.

Trimiterea pachetelor IPv6 printr-o reţea locală (LAN) IPv4

Situaţie

Firma dumneavoastră a scris o nouă aplicaţie de contabilitate IPv6. Aceasta este o aplicaţie server-la-client pe care o veţi folosi local. Aplicaţia comunică cu alte instanţe ale sale care se află în acelaşi sediu, dar în clădiri şi LAN-uri diferite. Deşi firma dumneavoastră doreşte să folosească IPv6 pentru această aplicaţie, nu este pregătită să-şi schimbe întreaga infrastructură de la IPv4 la IPv6. Sarcina dumneavoastră este să configuraţi linii tunel IPv6 care să permită pachetelor IPv6 să traverseze reţelele IPv4 locale. Ilustraţia următoare prezintă setarea reţelei în acest scenariu.



Soluţie

Pentru a folosi IPv6 peste aceste reţele locale IPv4, trebuie să creaţi două tuneluri configurate şi mai multe rute asociate. Pentru acest exemplu, un tunel este reprezentat cu roşu, iar celălalt este reprezentat cu albastru.

Mai întâi, să luăm în considerare tunelul roşu:

- Tunelul roşu începe la iSeries A (punct final local 10.1.1.1) în clădirea 1 şi se termină la clientul C (punct final la distanţă 10.1.2.1) în clădirea 2.
- iSeries A încapsulează un pachet IPv6 într-un pachet IPv4 şi trimite pachetul IPv4 prin tunel la clientul C, care decapsulează pachetul IPv6 pentru a se putea conecta la o altă instanţă a aplicaţiei IPv6.

În continuare, să luăm în considerare tunelul albastru:

- Tunelul albastru începe la iSeries A (punct final local 10.1.1.1) în clădirea 1, ca şi tunelul roşu; însă tunelul albastru se termină la clientul D (punct final 10.1.2.2) în clădirea 2.
- iSeries A încapsulează un pachet IPv6 într-un pachet IPv4 şi trimite pachetul IPv4 prin tunel la clientul D, care decapsulează pachetul IPv6 pentru a se putea conecta la o altă instanţă a aplicaţiei IPv6.

Fiecare conexiune prin tunel este punct-la-punct, deci trebuie să definiţi un punct final la distanţă pentru fiecare tunel. Aceasta se realizează prin crearea a două rute. Fiecare rută este asociată cu aceeaşi linie tunel, dar defineşte un punct final la distanţă diferit ca următorul hop. Cu alte cuvinte, definiţi punctele finale ale fiecărui tunel pe măsură ce creaţi rutele.

Pe lângă crearea rutelor iniţiale care definesc puncte finale ale tunelului şi permit pachetelor să ajungă la clienţii din clădirea 2, trebuie să mai creaţi încă două rute, pentru ca pachetele să se poată întoarce la serverul din clădirea 1.

Cerinţele de setare includ:

- OS/400 versiunea 5 ediţia 2 sau ulterioară
- iSeries Access pentru Windows şi Navigator iSeries (componenta Reţea din Navigator iSeries)
- Pe server trebuie să fie configurat TCP/IP (folosind IPv4) înainte de a crea linia tunel configurată. Dacă nu aţi configurat serverul pentru IPv4, vedeţi Configurarea TCP/IP pentru prima dată înainte de a configura linia tunel pentru IPv6.

Configurare

Pentru a crea o linie tunel configurată, trebuie să folosiţi vrăjitorul **Configurare IPv6** şi vrăjitorul **Rută IPv6 nouă** din Navigator iSeries. IPv6 poate fi configurat numai din Navigator iSeries, nu şi din interfaţa bazată pe caractere.

Pentru a folosi vrăjitorul **Configurare IPv6** pentru a crea linia tunel roşie, urmaţi aceşti paşi:

1. În Navigator iSeries, selectaţi **serverul —> Reţea —> Configurare TCP/IP**.
2. Faceţi clic dreapta pe **IPv6**, selectaţi vrăjitorul **Configurare IPv6** şi urmaţi instrucţiunile vrăjitorului pentru a configura o linie tunel pentru IPv6. După ce aţi completat vrăjitorul **Configurare IPv6**, acesta vă promptează pentru a crea o rută nouă pentru linia tunel configurată şi va apărea dialogul vrăjitorului **Rută IPv6 nouă**. Trebuie să creaţi o rută nouă pentru a permite pachetelor IPv6 să călătorească prin tunelul roşu.
3. Din vrăjitorul **Rută IPv6 nouă**, creaţi o rută pentru tunel roşu. Specificaţi punctul final la distanţă 10.1.2.1 ca următorul hop şi specificaţi fec0::2 ca adresa destinaţie.

Folosiţi vrăjitorul **Rută IPv6 nouă** din nou pentru a crea o rută pentru tunelul albastru. Reţineţi că nu este necesar să creaţi tunelul albastru folosind vrăjitorul **Configurare IPv6**. Tunelul albastru este creat când definiţi punctul lui final la distanţă folosind vrăjitorul **Rută IPv6 nouă**. Pentru a folosi vrăjitorul **Rută IPv6 nouă**, parcurgeţi paşii următori:

1. În Navigator iSeries, selectaţi **serverul —> Reţea —> Configurare TCP/IP —> IPv6**.
2. Faceţi clic dreapta pe **Rute**, selectaţi **Rută nouă** şi urmaţi instrucţiunile vrăjitorului pentru a configura o rută IPv6 pentru tunelul albastru. Specificaţi punctul final la distanţă 10.1.2.2 ca următorul hop şi specificaţi fec0::3 ca adresă destinaţie.

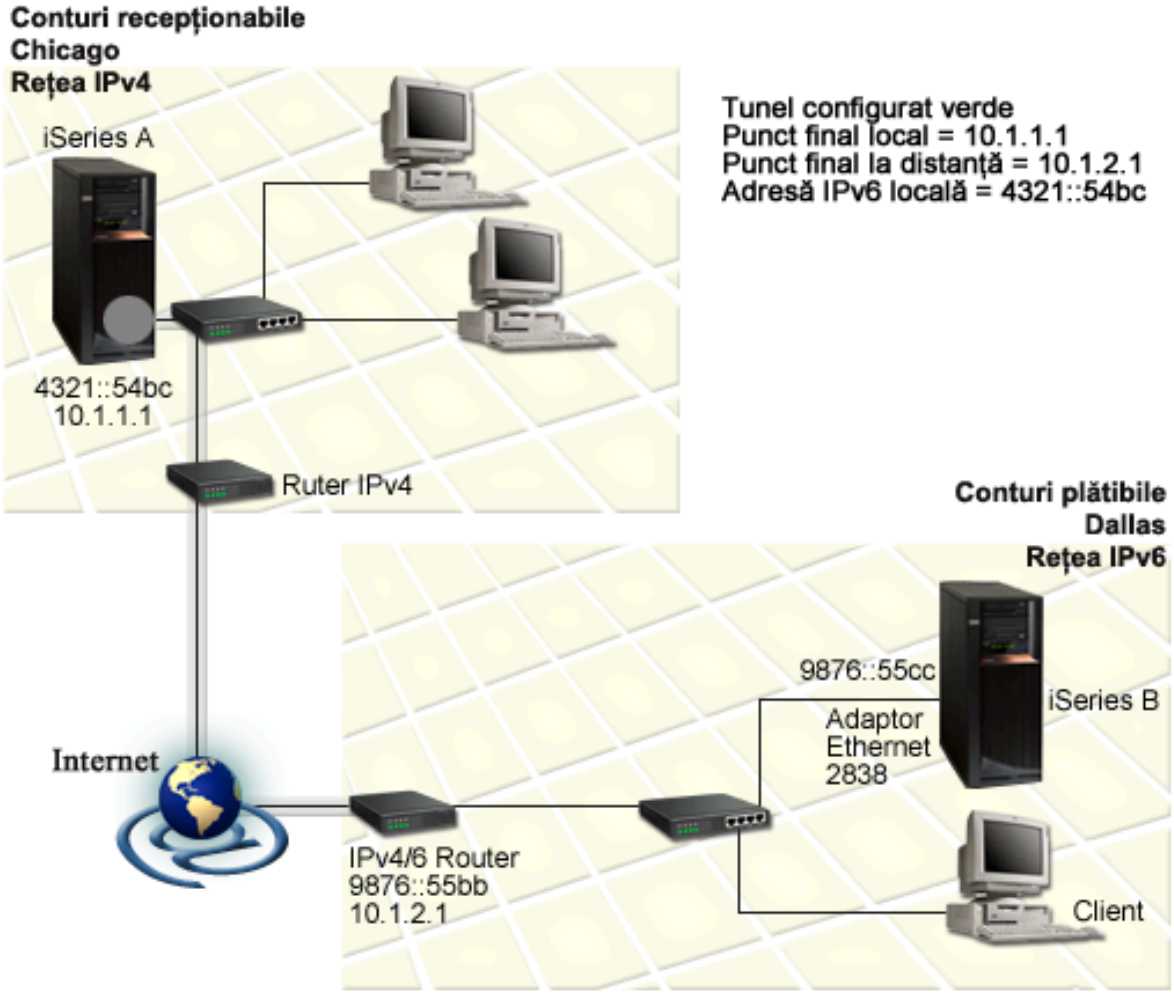
După ce aţi creat liniile tunel configurate şi rutele care definesc punctele finale ale tunelului, trebuie să creaţi o rută pe clientul C şi o rută pe clientul D care să permită pachetelor să călătorească înapoi la serverul din clădirea 1. Pentru fiecare dintre aceste rute, trebuie să specificaţi 10.1.1.1 ca următorul hop şi să specificaţi fec0::1 ca adresa destinaţie.

Trimiterea pachetelor IPv6 printr-o reţea de mare suparafaţă (WAN) IPv4

Situaţie

Firma dumneavoastră foloseşte o aplicaţie de contabilitate pentru conturile de încasări de pe serverul din biroul său din Chicago. Trebuie să conectaţi aplicaţia la un server din biroul din Dalas. Această aplicaţie foloseşte adresarea IPv6 pe serverele din ambele oraşe. Deoarece ISP-ul dumneavoastră nu poate furniza rute IPv6 între cele două locaţii, trebuie să configuraţi un tunel între cele două servere. Pachetele aplicaţiei circulă prin tunel, de-a lungul reţelei de mare suprafaţă IPv4, între cele două servere. Ilustraţia următoare prezintă setarea reţelei în acest scenariu.

Notă: În acest scenariu, adresele IP 10.x.x.x reprezintă adrese IP publice care pot fi rutate global. Toate adresele folosite sunt date numai ca exemplu.



Soluţie

Pentru a folosi IPv6 de-a lungul unei reţele de mare suprafaţă care are o infrastructură IPv4, trebuie să creaţi o linie tunel configurată şi mai multe rute asociate. Modul de funcţionare este următorul:

- Tunelul începe la iSeries A (punct final local 10.1.1.1) din Chicago şi se termină la ruterul IPv4/6 (punct final la distanţă 10.1.2.1) din Dallas.
- Aplicaţia care se află pe iSeries A trebuie să se conecteze la o aplicaţie care se află pe iSeries B. iSeries A încapsulează pachetul IPv6 într-un pachet IPv4 şi îl trimite prin tunel la ruterul IPv4/6, care decapsulează pachetul IPv6 şi expediază pachetul IPv6 la iSeries B.
- Pachetul se întoarce la Chicago urmând calea inversă.

Conexiunea prin tunel este punct-la-punct, deci trebuie să definiţi punctul final la distanţă al tunelului. Aceasta se realizează prin crearea unei rute care este asociată cu această linie tunel. Ruta defineşte punctul final (10.1.2.1) ca următorul hop. Cu alte cuvinte, definiţi punctul final la distanţă în momentul în care creaţi ruta. În plus, ruta defineşte adresa destinaţie ca 9876::55cc (adresa IPv6 asociată cu iSeries B).

Pe lângă crearea rutei iniţiale care defineşte punctul final al tunelului şi permite pachetului să călătorească la iSeries B din Dallas, trebuie să creaţi încă două rute pentru ca pachetul să se poată întoarce la iSeries A din Chicago.

Cerinţele de setare includ:

- OS/400 versiunea 5 ediţia 2 sau ulterioară
- iSeries Access pentru Windows şi Navigator iSeries (componenta Reţea din Navigator iSeries)
- Pe server trebuie să fie configurat TCP/IP (folosind IPv4) înainte de a crea linia tunel configurată. Dacă nu aţi configurat serverul pentru IPv4, vedeţi Configurarea TCP/IP pentru prima dată înainte de a configura linia tunel pentru IPv6.

Configurare

Pentru a crea o linie tunel configurată, trebuie să folosiţi vrăjitorul **Configurare IPv6** şi vrăjitorul **Rută IPv6 nouă** din Navigator iSeries. Tunelurile configurate pot fi configurate doar din Navigator iSeries, nu şi din interfaţa bazată pe caractere.

Pentru a folosi vrăjitorul **Configurare IPv6** pentru a crea linia tunel, parcurgeţi paşii următori:

1. În Navigator iSeries, selectaţi **serverul —> Reţea —> Configurare TCP/IP**.
2. Faceţi clic dreapta pe **IPv6**, selectaţi vrăjitorul **Configurare IPv6** şi urmaţi instrucţiunile vrăjitorului pentru a configura o linie tunel pentru IPv6. După ce aţi completat vrăjitorul **Configurare IPv6**, acesta vă promptează pentru a crea o rută nouă pentru linia tunel configurată şi va apărea dialogul vrăjitorului **Rută IPv6 nouă**. Trebuie să creaţi o rută nouă pentru a permite pachetelor IPv6 să călătorească prin tunel.
3. Din vrăjitorul **Rută IPv6 nouă**, creaţi o rută gazdă pentru tunel. Specificaţi punctul final la distanţă 10.1.2.1 ca următorul hop şi specificaţi 9876::55cc ca adresa destinaţie.

După ce aţi creat linia tunel configurată şi ruta cere defineşte punctul final al tunelului, trebuie să creaţi rute pe iSeries B şi pe ruterul IPv4/6 care permit pachetelor să călătorească înapoi la Chicago. Pentru ruta pe iSeries B, ar trebui să specificaţi 9876::55bb ca următorul hop şi 4321::54bc ca adresă destinaţie. Pentru ruta pe ruterul IPv4/6, ar trebui să specificaţi 10.1.1.1 ca următorul hop şi 4321::54bc ca adresă destinaţie.

Notă: Ruterul IPv4/6 din Dallas trebuie să aibă o rută directă la 9876::55cc, dar nu este necesară nici o configurare manuală deoarece această rută este creată automat.

Concepte: IPv6

Citiţi descrierile acestor concepte IPv6 pentru a înţelege mai bine cum lucrează IPv6:

Comparaţie între IPv4 şi IPv6
Vedeţi o comparaţie între atributele IPv4 şi atributele IPv6. Această tabelă vă permite să căutaţi repede anumite funcţii şi să comparaţi utilizarea lor în fiecare protocol.

Formatele de adresă IPv6
Găsiţi informaţii despre dimensiunea şi formatul adresei IPv6.

Tipurile de adresă IPv6
Găsiţi informaţii despre noile tipuri de adrese din domeniul IPv6.

Tunelarea IPv6
Aflaţi cum permite tunelarea IPv6 pachetelor IPv6 să călătorească printr-o reţea IPv4.

Descoperirea vecinilor
Aflaţi cum pot gazdele şi ruterele să comunice unele cu celelalte prin descoperirea vecinilor.

Autoconfigurarea adresei stateless
Aflaţi cum automatizează autoconfigurarea adresei stateless mai multe sarcini ale administratorului de reţea.

Formatele de adresă IPv6

Dimensiunea adresei IPv6 este de 128 biţi. Reprezentarea preferată a adresei IPv6 este: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, unde fiecare x este o cifră hexazecimală reprezentând 4 biţi. IPv6 adresează un interval de la 0000:0000:0000:0000:0000:0000:0000:0000 la ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff.

Pe lângă acest format preferat, adresele IPv6 pot fi specificate în alte două formate mai scurte:

- **Omiterea zerourilor precedente**
  Specificaţi adresele IPv6 prin omiterea zerourilor precedente. De exemplu, adresa IPv6 1050:0000:0000:0000:0005:0600:300c:326b poate fi scrisă folosind forma 1050:0:0:0:5:600:300c:326b.
- **Două caractere două puncte**
  Specificaţi adresele IPv6 folosind două caractere două puncte (::) în locul unei serii de zerouri. De exemplu, adresa ff06:0:0:0:0:0:0:c3 poate fi scrisă ca ff06::c3. Într-o adresă IP se poate folosi o singură dată caracterul puncte de două ori.

Un format alternativ pentru adresele IPv6 combină caracterul două puncte şi notaţia cu punct, astfel că adresa IPv4 poate fi inclusă în adresa IPv6. Valorile hexazecimale sunt specificate pentru cei mai din stânga 96 de biţi, iar valorile zecimale sunt specificate pentru cei mai din dreapta 32 biţi, indicând adresa IPv4 înglobată. Acest format asigură compatibilitatea dintre nodurile IPv6 şi nodurile IPv4 când lucraţi într-un mediu de reţea mixt.

Următoarele două tipuri de adresă IPv6 folosesc acest format alternativ:

- **Adresă IPv6 mapată la IPv4**
  Acest tip de adresă este folosit pentru reprezentarea nodurilor IPv4 ca adrese IPv6. Permite aplicaţiilor IPv6 să comunice direct cu aplicaţiile IPv4. De exemplu, 0:0:0:0:0:ffff:192.1.56.10 şi ::ffff:192.1.56.10/96 (format prescurtat).
- **Adresă IPv6 compatibilă cu IPv4**
  Acest tip de adresă este folosit pentru tunelare. Permite nodurilor IPv6 să comunice de-a lungul unei infrastructuri IPv4. De exemplu, 0:0:0:0:0:0:192.1.56.10 şi ::192.1.56.10/96 (format prescurtat).

Toate aceste formate sunt formate valide de adresă IPv6. Specificaţi oricare dintre aceste formate de adresă în Navigator iSeries.

Tipurile de adresă IPv6

Adresele IPv6 sunt împărţite în 3 tipuri de bază:

Adresă unicast
Adresa unicast specifică o singură interfaţă. Un pachet trimis la o adresă unicast circulă de la o gazdă la gazda destinaţie.

Trei tipuri de adrese unicast includ:

Adresă legătură-locală
Adresele legătură-locală sunt concepute pentru a fi utilizate pentru o singură legătură locală (reţea locală). Adresele legătură-locală sunt configurate automat pe toate interfeţele. Prefixul folosit pentru o adresă legătură-locală este fe80::/10. Ruterele nu expediază pachete cu o adresă sursă sau destinaţie conţinând o adresă legătură-locală.

Adresă locaţie-locală
Adresele locaţie-locală sunt concepute pentru folosirea într-o anumită locaţie. Prefixul folosit pentru o adresă locaţie-locală este fec0::/10. Ruterele nu expediază pachete cu o adresă sursă conţinând o adresă locaţie-locală în afara unei locaţii specifice.

Adresă globală
Adresele globale sunt concepute pentru folosirea în orice reţea. Prefixul folosit pentru o adresă globală începe cu cifrele binare 001.

Două tipuri specifice ale adreselor unicast includ:

Adresă nespecificată
Adresa nespecificată este 0:0:0:0:0:0:0:0 sau poate fi prescurtată cu două caractere două puncte (::). Adresa nespecificată indică absenţa unei adrese şi nu poate fi niciodată alocată unei gazde. Poate fi folosită de o gazdă IPv6 care nu are încă asignată o adresă. De exemplu, când gazda trimite un pachet pentru a descoperi o adresă de la un alt nod, gazda foloseşte adresa nespecificată ca adresă sursă.

Adresă loopback
Adresa loopback este 0:0:0:0:0:0:0:1 sau poate fi prescurtată ca ::1. Adresa loopback este folosită de un nod pentru a-şi trimite lui un pachet.

Adresă anycast
Adresa anycast specifică un set de interfeţe, posibil la locaţii diferite, care partajează o singură adresă. Un pachet trimis la o adresă anycast merge doar la cel mai apropiat membru al grupului. Serverul iSeries nu suportă în prezent adresarea anycast.

Adresă multicast
Adresa multicast specifică un set de interfeţe, posibil la mai multe locaţii. Prefixul folosit pentru o adresă multicast este ff. Dacă este trimis un pachet la o adresă multicast, este livrată o copie a pachetului fiecărui membru al grupului. Serverul iSeries furnizează în prezent suport de bază pentru adresarea multicast. Crearea de interfeţe multicast şi suportul pentru aplicaţii nu sunt suportate în prezent.

Tunelarea IPv6

Tunelarea IPv6 face posibilă conectarea serverului iSeries la noduri IPv6 (gazde şi rutere) de-a lungul unor domenii IPv4. Tunelarea permite nodurilor IPv6 izolate sau reţelelor să comunice fără modificarea infrastructurii IPv4 de bază. Tunelarea permite protocoalelor IPv4 şi IPv6 să coopereze, furnizând astfel o metodă de tranziţie, pentru a implementa IPv6 în timp ce se menţine conectivitatea IPv4.

Un tunel constă din două noduri stivă-dublă (IPv4 şi IPv6) printr-o reţea IPv4. Aceste noduri stivă-dublă sunt capabile să proceseze ambele comunicaţii, IPv4 şi IPv6. Unul dintre nodurile cu stivă-dublă de la marginea infrastructurii IPv6 inserează (încapsulează) un antet IPv4 în faţa fiecărui pachet IPv6 care soseşte şi îl trimite ca şi cum ar fi trafic IPv4 normal, prin legăturile existente. Ruterele IPv4 continuă să înainteze acest trafic. Pe de altă parte a tunelului, un alt nod stivă-dublă înlătură (decapsulează) antetul IP în plus de la pachetul IPv6 şi îl rutează la ultima destinaţie folosind standardul IPv6.

Tunelarea IPv6 pentru serverul iSeries rulează peste liniile tunel configurate, care sunt linii virtuale. Liniile tunel configurate furnizează comunicaţii IPv6 oricărui nod cu o adresă IPv4 rutabilă care suportă tuneluri IPv6. Aceste noduri pot exista oriunde, adică în domeniul local IPv4 sau într-un domeniu la distanţă.

Conexiunile tunel configurate sunt punct la punct. Pentru a configura acest tip de linie tunel, trebuie să specificaţi punctul tunel local (adresă IPv4), cum ar fi 124.10.10.150, şi adresa IPv6 locală, cum ar fi 1080:0:0:0:8:800:200c:417a. Trebuie de asemenea să creaţi o rută IPv6 pentru a permite traficului să călătorească prin tunel. Pe măsură ce creaţi ruta, veţi defini unul dintre punctele finale la distanţă ale tunelului (adresă IPv4) ca următorul hop al rutei. Puteţi configura un număr nelimitat de puncte finale pentru un număr nelimitat de tuneluri.

Vedeţi Trimiterea pachetelor IPv6 printr-o reţea locală (LAN) IPv4 şi Trimiterea pachetelor IPv6 printr-o reţea de mare suprafaţă (WAN) IPv4 pentru scenarii şi figuri care demonstrează tunelarea IPv6.

Descoperierea vecinilor

Funcţiile de descoperire a vecinilor sunt folosite de nodurile IPv6 (gazde şi rutere) pentru a descoperi prezenţa altor noduri IPv6, pentru a determina adresele la nivel legătură ale nodurilor, pentru a găsi rutere care sunt capabile să înainteze pachete IPv6 şi pentru a menţine un cache de vecini IPv6 activi. Nodurile IPv6 folosesc următoarele cinci mesaje ale protocolului Internet Control Message Protocol versiunea 6 (ICMPv6) pentru a comunica cu alte noduri:

Solicitare ruter
Gazdele trimit aceste mesaje pentru a cere ruterelor să genereze anunţuri de ruter. O gazdă trimite o solicitare de ruter iniţială când devine disponibilă pe reţea prima dată.

Anunţ ruter
Ruterele trimit aceste mesaje fie periodic, fie ca urmare a unei solicitări de ruter. Informaţiile furnizate de anunţurile de ruter sunt folosite de gazde pentru a crea automat interfeţe locaţie-locală, interfeţe globale şi rute asociate. Anunţurile de ruter conţin de asemenea alte informaţii de configurare folosite de o gazdă, de exemplu unitatea de transmisie maximă şi limita de hopuri.

Solicitare vecin
Nodurile trimit aceste mesaje pentru a determina adresa de nivel legătură a unui vecin sau pentru a verifica dacă un vecin este încă accesibil.

Anunţ vecin
Nodurile trimit aceste mesaje ca răspuns la o solicitare de vecin sau ca un mesaj nesolicitat pentru anunţarea schimbării unei adrese.

Redirectare
Ruterele folosesc aceste mesaje pentru a informa gazdele despre un prim hop mai bun pentru o destinaţie.

Vedeţi RFC 2461 pentru informaţii suplimentare despre descoperirea vecinilor şi descoperirea ruterelor. Pentru a vizualiza RFC 2461, vedeţi RFC Editor (http://www.rfc-editor.org/rfcsearch.html)  .

Autoconfigurarea adresei stateless

Autoconfigurarea de adrese stateless este procesul prin care nodurile IPv6 (gazde şi rutere) configurează automat adresele IPv6 pentru interfeţe. Nodul construieşte diverse adrese IPv6 combinând un prefix de adresă fie cu adresa MAC a nodului, fie cu identificatorul de interfaţă specificat de utilizator. Prefixele includ prefixul legătură-locală (fe80::/10) şi prefixele de lungime 64 anunţate de ruterele IPv6 locale (dacă există). Autoconfigurarea de adresă stateless creează de asemenea interfeţe multicast corespunzătoare când tipul de legătură are capacitate multicast.

Nodul realizează detectarea adreselor duplicat, pentru a verifica unicitatea unei adrese înainte de a o asocia unei interfeţe. Nodul trimite o interogare solicitare de vecin către noua adresă şi aşteaptă răspuns. Dacă nodul nu obţine nici un răspuns, atunci adresa este presupusă a fi unică. Dacă nodul primeşte un răspuns sub forma unui anunţ de vecin, adresa este deja folosită. Dacă nodul determină că adresa sa IPv6 temporară nu este unică, atunci configurarea automată se opreşte şi este necesară configurarea manuală a interfeţei.

Comparaţie între IPv4 şi IPv6

IBM implementează IPv6 pentru serverul iSeries în mai multe ediţii de software. În prezent IPv6 este implementat într-o platformă de dezvoltare de aplicaţii, cu scopul dezvoltării şi testării aplicaţiilor IPv6.

Poate vă întrebaţi prin ce se deosebeşte IPv6 de IPv4. Această tabelă vă permite să faceţi o comparaţie rapidă între atributele familiare din IPv4 şi atribute similare din IPv6. Selectaţi un atribut din lista următoare pentru a sări la comparaţia din tabelă.

- “adresă” la pagina 19
- “alocarea adreselor” la pagina 19
- “timpul de viaţă al adresei” la pagina 19
- “masca de adresă” la pagina 19
- “prefix adresă” la pagina 19
- “ARP (Address Resolution Protocol)” la pagina 19
- “domeniu de adresă” la pagina 19
- “tipuri de adrese” la pagina 19
- “urmărirea comunicaţiilor” la pagina 19
- “configuraţie” la pagina 19
- “DNS (Domain Name System)” la pagina 20
- “DHCP (Dynamic Host Configuration Protocol)” la pagina 20
- “FTP (File Transfer Protocol)” la pagina 20

	IPv4	IPv6
adresă	Are o lungime de 32 de biţi (4 octeţi). Adresa este compusă dintr-o porţiune de reţea şi una de gazdă, care depind de clasa de adrese. Sunt definite diverse clase de adrese: A, B, C, D, sau E, în funcţie de câţiva biţi iniţiali. Numărul total al adreselor IPv4 este 4 294 967 296. Forma textului adresei este nnn.nnn.nnn.nnn, unde 0<= nnn<=255, şi fiecare n este o cifră zecimală. Zerourile precedente pot fi omise. Numărul maxim de caractere de tipărire este 15, fără numărarea unei măşti.	Are o lungime de 128 de biţi (16 octeţi). Arhitectura de bază este de 64 biţi pentru numărul de reţea şi de 64 biţi pentru numărul gazdă. Deseori, porţiunea de gazdă a unei adrese IPv6 va fi o adresă MAC sau alt identificator de interfaţă. În funcţie de prefixul subreţelei, IPv6 are o arhitectură mai complicată decât IPv4. Numărul adreselor IPv6 este de 10^{28} (79 228 162 514 264 337 593 543 950 336) ori mai mare decât numărul adreselor IPv4. Formatul textului adresei IPv6 este xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, unde fiecare x este o cifră hexazecimală, ce reprezintă 4 biţi. Zerourile precedente pot fi omise. Se poate folosi o dată un caracter două puncte dublu (::) în forma text a unei adrese, pentru a desemna un număr de biţi 0. De exemplu, ::ffff:10.120.78.40 este o adresă IPv6 mapată la IPv4. (Vedeţi RFC 2373 pentru detalii. Pentru a vizualiza acest RFC, vedeţi RFC Editor (http://www.rfc-editor.org/rfcsearch.html).
alocarea adreselor	Iniţial, adresele erau alocate după clasa de reţea. Cum spaţiul de adrese s-a epuizat, se fac alocări mai mici, care folosesc CIDR (Classless Inter-Domain Routing - Rutarea între domenii fără clase). Alocarea nu a fost echilibrată între instituţii şi naţiuni.	Alocarea este într-o etapă de început. IETF (Internet Engineering Task Force) şi IAB (Internet Architecture Board) au recomandat ca, în esenţă, fiecare organizaţie, casă sau entitate să aibă alocată lungimea de prefix de subreţea /48. Aceasta ar lăsa 16 biţi pentru ca organizaţia să realizeze subreţele. Spaţiul de adrese este destul de mare pentru a da fiecărei persoane din lume propria lungime de prefix de subreţea /48.
timpul de viaţă al adresei	În general, nu este un concept aplicabil, cu excepţia adreselor asignate folosind DHCP.	Adresele IPv6 au doi timpi de viaţă: preferat şi valid, timpul de viaţă preferat fiind întotdeauna <= timpul de viaţă valid. După ce timpul de viaţă preferat expiră, adresa nu poate fi folosită ca o adresă IP sursă. După ce timpul de viaţă valid expiră, adresa nu este folosită (recunoscută) ca o adresă IP destinaţie validă pentru pachetele de intrare. Unele adrese IPv6 au, prin definiţie, timpi de viaţă preferaţi şi valizi infiniţi; de exemplu legătură-locală (vedeţi “domeniu de adresă”).
masca de adresă	Este folosită pentru a indica reţeaua din porţiunea gazdă.	Nefolosită (vedeţi “prefix adresă”).
prefix adresă	Câteodată folosit pentru a indica reţeaua din porţiunea gazdă. Câteodată este scris ca sufix /nn în forma de prezentare a adresei.	Folosit pentru a indica prefixul subreţelei unei adrese. Scris ca sufix /nnn (până la 3 cifre zecimale, 0 <= nnn <= 128) după forma tipăribilă. Un exemplu este fe80::982:2a5c/10, unde primii 10 biţi cuprind prefixul subreţelei.
ARP (Address Resolution Protocol)	Protocolul de rezolvare a adreselor este folosit de IPv4 pentru a găsi o adresă fizică, cum ar fi adresa MAC sau de legătură, asociată cu o adresă IPv4.	IPv6 înglobează aceste funcţii în IP, ca parte a algoritmilor pentru autoconfigurarea stateless şi descoperirea vecinilor folosind ICMPv6 (Internet Control Message Protocol versiunea 6). Ca urmare, nu există ARP6.
domeniu de adresă	Pentru adrese unicast, nu se aplică conceptul. Există intervale desemnate pentru adrese private şi loopback. În afara de aceasta, adresele sunt presupuse a fi globale.	În IPv6, domeniul de adresă face parte din arhitectură. Adresele unicast au definite 3 domenii, incluzând legătură-locală, locaţie-locală şi global; adresele multicast au 14 domenii. Selecţia de adresă implicită pentru sursă şi destinaţie ţine cont de domeniu. O zonă de domeniu este o instanţă a domeniului într-o anumită reţea. În consecinţă, uneori adresele IPv6 trebuie să fie introduse sau asociate cu un ID de zonă. Sintaxa este %idz, unde idz este un număr (de obicei mic) sau un nume. ID-ul de zonă este scris după adresă şi înainte de prefix. De exemplu, 2ba::1:2:14e:9a9b:c%3/48.
tipuri de adrese	Unicast, multicast şi broadcast.	Unicast, multicast şi anycast. Vedeţi Tipurile de adresă IPv6 pentru descriere.
urmărirea comunicaţiilor	O unealtă pentru a colecta o urmărire detaliată a pachetelor TCP/IP (şi altele) care intră şi părăsesc un server iSeries.	La fel şi pentru IPv6, IPv6 fiind suportat, inclusiv pachetele ICMPv6 şi IPv6 tunelate în IPv4.
configuraţie	Pentru ca un sistem nou instalat să poată comunica, trebuie să fie făcută configuraţia; aceasta înseamnă că trebuie să fie asignate adresele IP şi rutele.	Configuraţia este opţională, depinzând de funcţiile necesare. O interfaţă Ethernet sau tunel corespunzătoare, trebuie desemnată ca o interfaţă IPv6 utilizând Navigator iSeries. După ce se face aceasta, interfeţele IPv6 sunt autoconfigurabile. Deci, sistemul va fi capabil să comunice cu alte sisteme IPv6 care sunt locale sau la distanţă, în funcţie de tipul reţelei şi de existenţa unui ruter IPv6.

	IPv4	IPv6
DNS (Domain Name System)	Aplicaţiile acceptă nume de gazdă şi apoi folosesc DNS pentru a obţine o adresă IP, folosind API-ul pentru socket gethostbyname(). Aplicaţiile acceptă de asemenea adrese IP şi atunci folosesc DNS pentru a obţine numele de gazdă folosind gethostbyaddr(). Pentru IPv4, domeniul pentru căutări inverse este in-addr.arpa.	La fel pentru IPv6. Suportul pentru IPv6 foloseşte tipul de înregistrare AAAA (patru A) şi căutarea inversă (IP-la-nume). O aplicaţie poate decide să accepte adresele IPv6 pentru DNS (sau nu) şi atunci foloseşte IPv6 pentru a comunica (sau nu). API-ul pentru socket gethostbyname() este nemodificat pentru IPv6 şi API-ul getaddrinfo() poate fi folosit pentru a obţine (la alegerea aplicaţiei) numai adrese IPv6 sau IPv4 şi IPv6. Pentru IPv6, domeniul folosit pentru căutări nibble inverse este ip6.arpa şi, dacă nu este găsit, ip6.int (vedeţi API-ul getnameinfo()).
DHCP (Dynamic Host Configuration Protocol)	Este utilizat pentru a obţine dinamic o adresă IP şi alte informaţii de configurare.	În prezent, DHCP nu suportă IPv6.
FTP (File Transfer Protocol)	Protocolul FTP vă permite trimiterea şi primirea fişierelor între reţele.	În mod curent, FTP nu suportă IPv6.
fragmente	Când un pachet este prea mare pentru următoarea legătură prin care va trece, poate fi fragmentat de expeditor (gazdă sau ruter).	Pentru IPv6, fragmentarea poate avea loc numai la nodul sursă, iar reasamblarea este făcută doar la nodul destinaţie. În prezent, antetul extensiei de fragmentare nu este suportat.
tabelă gazde	În Navigator iSeries, o tabelă configurabilă care asociază o adresă Internet cu un nume de gazdă; de exemplu, 127.0.0.1, loopback. Această tabelă este folosită de rezolvatorul de nume de socket-uri, fie înaintea unei căutări DNS, fie după ce eşuează o căutare DNS (determinată de prioritatea căutării numelui gazdă).	În prezent, această tabelă nu suportă IPv6. Clienţii trebuie să configureze o înregistrare AAAA într-un DNS pentru rezolvarea de domeniu IPv6. Puteţi rula DNS local, pe acelaşi sistem cu rezolvatorul, sau îl puteţi rula pe un sistem diferit.
interfaţă	Entitatea conceptuală şi logică folosită de TCP/IP pentru a trimite şi primi pachete şi întotdeauna asociată strâns cu o adresă IPv4, dacă nu este numită cu o adresă IPv4. Câteodată se referă la o interfaţă logică. Interfeţele pot fi pornite şi oprite independent de celelalte şi independent de TCP/IP folosind comenzile STRTCPIFC şi ENDTCPIFC sau folosind Navigator iSeries.	Acelaşi concept ca la IPv4. Interfeţele pot fi pornite şi oprite independent de celelalte şi independent de TCP/IP folosind Navigator iSeries.
ICMP (Internet Control Message Protocol)	ICMP este folosit de IPv4 pentru a comunica informaţii de reţea.	Folosit similar pentru IPv6; însă ICMPv6 furnizează mai multe atribute noi. Tipurile de eroare de bază rămân, de exemplu destinaţie inaccesibilă, cerere ecou şi răspuns. Sunt adăugate tipuri şi coduri noi pentru a suporta descoperirea vecinilor şi funcţiile legate de aceasta.
IGMP (Internet Group Management Protocol)	IGMP este folosit de ruterele IPv4 pentru găsi gazde care doresc trafic pentru un anumit grup multicast şi este utilizat de gazdele IPv4 pentru a informa ruterele IPv4 despre ascultătorii grupului multicast existent (pe gazdă).	Înlocuit de protocolul MLD (multicast listener discovery - descoperire ascultător multicast) pentru IPv6. Face, în esenţă, ceea ce face IGMP pentru IPv4, dar foloseşte ICMPv6 prin adăuga câteva valori de tip ICMPv6 specifice MLD.
antet IP	Lungime variabilă de 20-60 octeţi, în funcţie de opţiunile IP prezente.	Lungime fixă de 40 octeţi. Nu există opţiuni ale antetului IP. În general, antetul IPv6 este mai simplu decât antetul IPv4.
opţiuni antet IP	Opţiuni diverse care pot însoţi un antet IP (înaintea oricărui antet de transport).	Antetul IPv6 nu are opţiuni. În schimb, IPv6 adaugă anteturi de extensie suplimentare (opţionale). Anteturile de extensie sunt AH şi ESP (nemodificat de la IPv4), hop-cu-hop, rutare, fragment şi destinaţie. În prezent, IPv6 nu suportă nici un antet de extensie.
octet protocol antet IP	Codul protocolului nivelului de transport sau a încărcăturii utile a pachetului; de exemplu, ICMP.	Tipul antetului urmează imediat după antetul IPv6. Foloseşte aceleaşi valori ca şi câmpul protocolului IPv4. Dar efectul arhitectural este acela de a permite un interval definit curent al următoarelor anteturi şi este uşor de extins. Următorul antet va fi un antet de transport, un antet de extensie sau ICMPv6.
octet TOS (Type of Service) antet IP	Folosit de QoS şi serviciile diferenţiate pentru a desemna o clasă de trafic.	Desemnează clasa de trafic IPv6, similară cu IPv4. Foloseşte coduri diferite. În prezent, IPv6 nu suportă TOS.
suport Navigator iSeries	Navigator iSeries furnizează o funcţie de configurare totală pentru TCP/IP.	Configurarea opţională pentru IPv6 este asigurată complet de Navigator iSeries, inclusiv vrăjitorul **Configurare IPv6**.
conexiune LAN	Folosită de o interfaţă IP pentru a ajunge în reţeaua fizică. Există multe tipuri; de exemplu token ring, Ethernet şi PPP. Câteodată se referă la interfaţa fizică, legătură sau linie.	IPv6 are acelaşi concept. În prezent, sunt suportate doar plăcile Ethernet 2838 şi 2849 şi liniile tunel.
L2TP (Layer 2 Tunnel Protocol)	L2TP poate fi considerat PPP virtual, funcţionând peste orice tip de linie suportat.	În prezent, L2TP nu suportă IPv6.

	IPv4	IPv6
adresă loopback	O interfaţă cu adresa 127.*.*.* (tipic 127.0.0.1) care poate fi folosită de un nod doar pentru a-şi trimite pachete lui însuşi. Interfaţa fizică (descriere de linie) este numită *LOOPBACK.	Conceptul este acelaşi ca în IPv4, singura adresă loopback fiind 0000:0000:0000:0000:0000:0000:0000:0001 sau ::1 (versiunea prescurtată). Interfaţa fizică virtuală este numită *LOOPBACK6.
MTU (Maximum Transmission Unit)	Numărul maxim de unităţi de transmisie al unei legături este numărul maxim de octeţi pe care îi suportă un anumit tip de legătură, cum ar fi modemul sau Ethernet. Pentru IPv4, 576 este valoarea minimă tipică.	Valoarea MTU minimă prevăzută de arhitectura IPv6 este de 1280 octeţi. De aceea, IPv6 nu va fragmenta pachetele mai jos de această limită. Pentru a trimite IPv6 peste o legătură cu mai puţin de 1280 MTU, nivelul legătură trebuie să fragmenteze şi să defragmenteze transparent pachetele IPv6.
netstat	O unealtă de urmărit starea conexiunilor TCP/IP, interfeţe sau rute. Este disponibilă utilizând Navigator iSeries şi 5250.	La fel pentru IPv6, IPv6 fiind suportat atât pentru 5250, cât şi pentru Navigator iSeries.
NAT (Network Address Translation)	Funcţii firewall de bază integrate în TCP/IP, configurate folosind Navigator iSeries.	În mod curent, NAT nu suportă IPv6. Mai general, IPv6 nu necesită NAT. Spaţiul de adrese extins al IPv6 elimină problema lipsei de adrese şi dă posibilitatea renumerotării uşoare.
tabelă de reţele	În Navigator iSeries, o tabelă configurabilă care asociază un nume de reţea cu o adresă IP fără mască. De exemplu, gazda Reţea14 şi adresa IP 1.2.3.4.	În prezent, nu s-au făcut modificări la această tabelă pentru IPv6.
interogare informaţii nod	Nu există.	O unealtă de reţea simplă şi comodă care lucrează ca ping, cu excepţia conţinutului: un nod IPv6 poate interoga alt nod IPv6 pentru numele DNS al destinaţiei, adresă unicast IPv6 sau adresă IPv4. În prezent nu este suportată.
filtrare pachete	Funcţii firewall de bază integrate în TCP/IP, configurate folosind Navigator iSeries.	În prezent, filtrarea de pachete nu suportă IPv6. Însă filtrarea IPv4 poate fi aplicată traficului IPv6 de tunel.
înaintare pachete	Serverul iSeries poate fi configurat să înainteze pachetele IP pe care le primeşte la adrese IP nelocale. Tipic, interfaţa de intrare şi interfaţa de ieşire sunt conectate la LAN-uri diferite.	În prezent, pachetele IPv6 nu sunt înaintate.
tunelare pachete	În IPv4, tunelarea are loc în VPN pentru conexiunile VPN mod-tunel (IPv4 tunelat în IPv4) şi în L2TP.	Pentru IPv6, tunelarea în pachete IPv4 este aşteptată să fie o parte importantă a evoluţiei. În prezent, IEFT a definit cel puţin 5 tipuri diferite de tunelare 6-în-4, fiecare cu atribute şi avantaje diferite. Este suportat un tip de bază şi flexibil al tunelării IPv6-în-IPv4 pentru a permite nodurilor IPv6A să comunice peste Internetul IPv4 existent. Numită **tunelare configurată**, furnizează o legătură punct la punct virtuală şi foloseşte un tip nou de linie tunel numită *TNLCFG64.
PING	Unealtă TCP/IP de bază pentru testarea accesibilităţii. Este disponibilă utilizând Navigator iSeries şi 5250.	La fel pentru IPv6, IPv6 fiind suportat atât pentru 5250, cât şi pentru Navigator iSeries.
PPP (Point-to-Point Protocol)	PPP suportă interfeţe dial-up pe diferite tipuri de linie şi modem.	În prezent, PPP nu suportă IPv6.
restricţii de port	Aceste panouri iSeries permit unui client să configureze numărul de port selectat sau intervale pentru numărul de port pentru TCP sau UDP astfel încât sunt disponibile doar pentru un anumit profil.	Nesuportat pentru IPv6. Se aplică restricţii de configurare doar la IPv4.
porturi	TCP şi UDP au spaţii de port separate, fiecare identificat de numere de port din intervalul 1-65535.	Pentru IPv6, porturile lucrează la fel ca la IPv4. Deoarece acestea sunt într-o nouă familie de adrese, există acum patru spaţii de porturi separate. De exemplu, există două spaţii de 80 de porturi TCP la care poate fi asociată o aplicaţie, una în AF_INET şi una în AF_INET6.
adrese publice şi private	Toate adresele IPv4 sunt publice, cu excepţia a trei intervale de adrese care sunt desemnate ca private de IETF RFC 1918: 10.*.*.* (10/8), 172.16.0.0 prin 172.31.255.255 (172.16/12) şi 192.168.*.* (192.168/16). Domeniile de adrese private sunt folosite de obicei în organizaţii. Adresele private nu pot fi rutate în Internet.	IPv6 are un concept analog, dar cu diferenţe importante. Adresele sunt publice sau temporare, anterior fiind numite anonime. Vedeţi RFC 3041. Spre deosebire de adresele private IPv4, adresele temporare pot fi rutate global. Motivaţia este de asemenea diferită; adresele temporare IPv6 sunt intenţionate să protejeze identitatea unui client când iniţializează comunicaţia (o legătură privată). Adresele temporare au un timp de viaţă limitat şi nu conţin un identificator de interfaţă care este o adresă de legătură (MAC). Sunt în general de nedistins de adresele publice. IPv6 are notaţia domeniului de adresă limitat folosind denumirile domeniului de arhitectură (vedeţi “domeniu de adresă” la pagina 19).

	IPv4	IPv6
tabelă de protocoale	În Navigator iSeries, o tabelă configurabilă care asociază un nume de protocol cu numărul de protocol asignat acestuia; de exemplu, UDP, 17. Sistemul este echipat cu un număr mic de intrări: IP, TCP, UDP, ICMP.	Tabela suportă IPv6 fără modificare.
QoS (Quality of Service)	QoS (Quality of Service - Calitatea serviciului vă permite să primiţi prioritatea pachetelor şi lăţimea de bandă pentru aplicaţii TCP/IP.	În prezent, QoS nu suportă IPv6. Însă când IPv6 este tunelat în IPv4, facilităţile QoS existente ale iSeries pot fi aplicate traficului IPv4, care apoi manevrează transparent încărcarea utilă IPv6.
renumerotare	Făcută prin reconfigurarea manuală, cu excepţia posibilă a DHCP. În general, pentru o locaţie sau organizaţie, un proces anevoios care trebuie evitat dacă este posibil.	Este un element de arhitectură important al IPv6 şi se presupune a fi în mare automatizat, în special în prefixul /48.
rută	Logic, o mapare a unui set de adrese IP (poate conţine numai 1) la o interfaţă fizică şi o singură adresă IP de hop următor. Pachetele IP a căror adresă destinaţie este definită ca parte a setului sunt expediate la următorul hop folosind linia. Rutele IPv4 sunt asociate cu o interfaţă IPv4, de aici, o adresă IPv4. Ruta implicită este *DFTROUTE.	Conceptual, la fel ca la IPv4. O diferenţă importantă: rutele IPv6 sunt asociate (legate) la o interfaţă fizică (o legătură, cum ar fi *TNLCFG64 or ETH03) mai degrabă decât o interfaţă. Există motive diverse pentru aceasta. Un motiv este că selecţia adresei sursă funcţionează diferit în IPv6 faţă de IPv4. Consultaţi “selectarea adresei sursă”. Sunt permise rute duplicat pentru a îmbunătăţii robusteţea, dar sunt ignorate în timpul căutării rutei.
RIP (Routing Information Protocol)	RIP este un protocol de rutare suportat de demonul rutat.	În prezent, RIP nu suportă IPv6. Rutarea IPv6 foloseşte rute statice.
tabelă de servicii	Pe serverul iSeries, o tabelă de configurare care asociază un nume de serviciu cu un port şi protocol; de exemplu, nume serviciu FTP-control, port 21, TCP şi UDP. Un mare număr de servicii bine cunoscute sunt menţionate în tabela de servicii. Multe aplicaţii folosesc această tabelă pentru a determina ce port să folosească.	Nu sunt făcute modificări la această tabelă pentru IPv6.
SNMP (Simple Network Management Protocol)	SNMP este un protocol pentru gestionarea sistemului.	În prezent, SNMP nu suportă IPv6. Rutarea IPv6 foloseşte rute statice.
API pentru socket-uri	Aceste API-uri sunt metoda prin care aplicaţiile folosesc TCP/IP. Aplicaţiile care nu au nevoie de IPv6 nu sunt afectate de modificările socket-urilor pentru suportul IPv6.	IPv6 îmbunătăţeşte socket-urile astfel încât aplicaţiile pot folosi acum IPv6, folosind o nouă familie de adrese: AF_INET6. Îmbunătăţirile au fost concepute astfel încât aplicaţiile IPv4 existente să fie complet neafectate de modificările IPv6 şi API. Aplicaţiile care doresc să suporte trafic IPv4 şi IPv6 concurent, se adaptează uşor folosind adresele IPv6 mapate la IPv4, de forma ::ffff:a.b.c.d, unde a.b.c.d este adresa IPv4 a clientului. Noile API-uri includ suport pentru convertirea adreselor IPv6 de la text la binar şi de la binar la text. Vedeţi Utilizarea familiei de adrese AF_INET6, pentru informaţii suplimentare despre îmbunătăţirile socket-urilor pentru IPv6.
selectarea adresei sursă	O aplicaţie poate desemna o adresă IP sursă (tipic, folosind socket-uri bind()). Dacă se asociază la INADDR_ANY, este aleasă o adresă IP sursă pe baza rutei.	Ca şi la IPv4, o aplicaţie poate desemna o adresă IPv6 sursă folosind bind(). La fel ca la IPv4, se poate folosi in6addr_any pentru a lăsa sistemul să alegă o adresă sursă IPv6. Dar, deoarece liniile IPv6 au multe adrese IPv6, metoda internă de alegere a adresei IP sursă este diferită.
pornire şi oprire	Folosiţi STRTCP şi ENDTCP pentru a porni sau a opri TCP/IP.	La fel ca la IPv4. IPv4 şi IPv6 nu sunt pornite sau oprite independent unul faţă de celălalt şi nici independent faţă de TCP/IP. Acesta înseamnă că porniţi sau opriţi în întregime TCP/IP, nu doar IPv4 sau IPv6. Oricare dintre interfeţele IPv6 sunt pornite automat dacă parametrul AUTOSTART = *YES (implicit). IPv6 nu poate fi folosit sau configurat fără IPv4, iar IPv6 trebuie să aibă loopback IPv6 configurat (::1).
Telnet	Telnet vă permite să vă logaţi şi să folosiţi un calculator la distanţă ca şi cum aţi fi conectat direct.	În prezent, Telnet nu suportă IPv6.
urmărire rută	Unealtă TCP/IP de bază pentru determinarea căii. Este disponibilă utilizând Navigator iSeries şi 5250.	La fel pentru IPv6, IPv6 fiind suportat atât pentru 5250, cât şi pentru Navigator iSeries.

	IPv4	IPv6
niveluri transport	TCP, UDP, RAW. Un transport nou, SCTP (Stream Control Transmission Protocol), intenţionează să ofere caracteristicile cele mai bune ale TCP şi UDP, adică o comunicaţie garantată fără conexiune. SCTP este într-o etapă iniţială de utilizare, nefiind suportat pe iSeries.	Aceleaşi trei transporturi există şi sunt modificate funcţional pentru IPv6.
adresă nespecificată	Aparent, nedefinită. Programarea cu socket-uri foloseşte 0.0.0.0 ca INADDR_ANY.	Definită ca ::/128 (128 de biţi 0). Este folosită ca sursă IP în câteva pachete de descoperire vecini şi diverse alte contexte, cum ar fi socket-uri. Programarea cu socket-uri foloseşte ::/128 ca in6addr_any.
reţea privată virtuală (VPN)	Reţeaua privată virtuală (folosind IP-uri) vă permite să extindeţi în siguranţă reţeaua privată peste o reţea publică existentă.	În prezent, VPN nu suportă IPv6. Însă când IPv6 este tunelat în IPv4, facilităţile VPN iSeries existente pot fi aplicate traficului IPv4, care apoi manevrează transparent încărcarea utilă IPv6.

Depanarea IPv6

Dacă aveţi IPv6 configurat pe server, trebuie să folosiţi mai multe dintre uneltele de depanare, aşa cum faceţi pentru IPv4. De exemplu, uneltele ca urmărirea rutei şi PING acceptă ambele formate de adresă, IPv4 şi IPv6, aşa că puteţi să le folosiţi pentru a testa conexiuni şi rute pentru ambele tipuri de reţele. În plus, puteţi folosi funcţia urmărire comunicaţii pentru a urmări datele pe ambele linii de comunicaţie, IPv4 şi IPv6.

Vedeţi Depanarea TCP/IP pentru un ghid de depanare general, care furnizează tehnici pentru rezolvarea problemelor raportate de IPv4 şi IPv6.

Informaţii înrudite pentru IPv6

Pentru informaţii suplimentare despre IPv6, vedeţi aceste surse de informaţii:

IETF (Internet Engineering Task Force) (http://www.ietf.cnri.reston.va.us/)
Învăţaţi despre grupul de persoane care dezvoltă protocolul Internet, inclusiv IPv6.

IP versiunea 6 (IPv6) (http://playground.sun.com/pub/ipng/html/ipng-main.html)
Găsiţi specificaţiile IPv6 curente şi trimiteri la mai multe surse despre IPv6.

Forum IPv6 (http://www.ipv6forum.com/)
Găsiţi articole noi şi evenimente care comunică ultimile dezvoltări ale IPv6.

Capitolul 4. Planificarea setării TCP/IP

Înainte de a începe să instalaţi şi să configuraţi serverul iSeries, acordaţi puţin timp planificării operaţiei. Vedeţi subiectul de mai jos pentru indicaţii de planificare. Aceste indicaţii de planificare se referă la setarea TCP/IP de bază folosind IPv4. Dacă intenţionaţi să configuraţi IPv6, vedeţi Configurarea IPv6 pentru cerinţele de setare şi instrucţiuni de configurare.

Cerinţele de setare TCP/IP
Adunaţi şi înregistraţi informaţiile de configurare de bază care sunt necesare pentru setarea TCP/IP.

Considerente privind securitatea TCP/IP
Luaţi în considerare nevoile dumneavoastră de securitate ca nou membru al reţelei.

Cerinţele de setare TCP/IP

Tipăriţi această pagină şi înregistraţi informaţiile de configurare despre serverul dumneavoastră şi reţeaua TCP/IP la care vă conectaţi. Va trebui să consultaţi aceste informaţii mai târziu, când configuraţi TCP/IP. Folosiţi instrucţiunile prezentate în continuarea acestei tabele pentru a vă ajuta să determinaţi valorile pentru primele două rânduri. Dacă nu sunteţi familiarizat cu unul dintre aceşti termeni, vedeţi cartea roşie de la IBM TCP/IP for AS/400: More Cool Things Than Ever şi citiţi Capitolul doi, ″TCP/IP: Basic Installation and Configuration.″

Informaţii necesare	Pentru sistemul dumneavoastră	Exemplu
Tipul adaptorului de comunicaţii instalat pe sistemul dumneavoastră (consultaţi instrucţiunile de mai jos)		Ethernet
Nume resursă		CMN01
Adresa IP pentru serverul dumneavoastră iSeries		199.5.83.158
Masca de subreţea pentru serverul dumneavoastră iSeries		255.255.255.0
Adresă gateway		199.5.83.129
Numele de gazdă şi numele de domeniu pentru sistemul dumneavoastră		sys400.xyz.company.com
Adresa IP pentru serverul de nume de domenii		199.4.191.76

Pentru a obţine informaţii despre adaptorul dumneavoastră de comunicaţii, parcurgeţi paşii următori:

1. În linia de comandă a serverului, tastaţi go hardware şi apăsaţi **Enter**.
2. Pentru a selecta Gestionare resurse de comunicare (Opţiunea 1), tastaţi 1 şi apăsaţi **Enter**.

   Resursele dumneavoastră de comunicaţii vor fi listate după numele resursei. Urmaţi instrucţiunile dacă doriţi să gestionaţi resursele sau să vedeţi mai multe detalii.

Ce este de făcut în continuare:
Instalarea TCP/IP

Considerente privind securitatea TCP/IP

Când planificaţi configurarea TCP/IP, ar trebui să vă gândiţi la nevoile de securitate. Aceste strategii vă pot ajuta să reduceţi expunerea TCP/IP:

- **Porniţi doar acele aplicaţii TCP/IP de care aveţi nevoie.**
  Fiecare aplicaţie TCP/IP îşi are propriile expuneri de securitate. Nu vă bazaţi pe un ruter pentru a respinge cereri pentru o anumită aplicaţie. Ca un al doilea mijloc de apărare, setaţi valorile autostart pentru aplicaţiile care nu sunt necesare la NO.
- **Limitaţi orele în care rulează aplicaţiile TCP/IP.**
  Limitaţi expunerea reducând orele în care rulează serverele. Dacă este posibil, opriţi servere TCP/IP, cum ar fi FTP şi Telnet în timpul orelor libere.
- **Controlaţi cine poate porni şi modifica aplicaţiile dumneavoastră TCP/IP.**
  Implicit, este necesară autorizarea *IOSYSCFG pentru a modifica setările de configurare TCP/IP. Un utilizator fără autorizarea *IOSYSCFG are nevoie de autorizarea *ALLOBJ sau autorizarea explicită pentru comenzile de pornire TCP/IP. Acordarea de autorizări speciale pentru utilizatori reprezintă o expunere de securitate. Evaluaţi necesitatea de a acorda autorizări speciale fiecărui utilizator şi menţineţi numărul de autorizări speciale la minim. Urmăriţi utilizatorii cu autorizări speciale şi revedeţi periodic necesitatea lor de a fi autorizaţi. Aceasta limitează şi posibilitatea de acces la server în timpul orelor din afara programului.
- **Controlaţi rutarea TCP/IP:**
  - Nu permiteţi înaintarea (forwarding) IP, pentru ca hacker-ii să nu poată folosi serverul dumneavoastră Web ca să atace alte sisteme de încredere.
  - Definiţi doar o rută la serverul public de Web: ruta implicită la ISP.
  - Nu configuraţi nume de gazde şi adrese IP ale sistemelor interne securizate în tabela de gazde TCP/IP a serverului dumneavoastră de Web. În această tabelă puneţi doar numele altor servere publice la care trebuie să ajungeţi.
- **Controlaţi serverele TCP/IP create pentru deschidere de sesiuni interactive la distanţă.**
  Aplicaţiile cum ar fi FTP şi Telnet sunt mai vulnerabile la atacuri din exterior. Pentru detalii privind modul în care vă puteţi controla expunerea, citiţi capitolul despre indicii pentru controlul interactiv al logării din Tips and Tools for Securing Your iSeries  .

Pentru informaţii suplimentare despre securitate şi despre opţiunile disponibile, citiţi Securitatea iSeries şi Internetul.

Capitolul 5. Instalarea TCP/IP

Suportul TCP/IP de bază este livrat o dată cu OS/400 şi vă permite să conectaţi un server iSeries la o reţea. Dacă însă vreţi să folosiţi orice aplicaţie TCP/IP, cum ar fi Telnet, FTP sau SMTP, trebuie să instalaţi TCP/IP Connectivity Utilities. Acesta este un program licenţiat care se instalează separat şi este inclus în sistemul de operare.

Pentru a instala TCP/IP Connectivity Utilities pe serverul iSeries, parcurgeţi paşii următori:

1. Introduceţi în server mediul de stocare pentru instalarea TCP/IP. Dacă mediul dumneavoastră de instalare este un CD-ROM, introduceţi-l în dispozitivul optic. Dacă mediul este o bandă, introduceţi-l în unitatea de bandă.
2. În linia de comandă, introduceţi GO LICPGM şi apăsaţi **Enter** pentru a accesa ecranul Gestionare programe licenţiate.
3. Selectaţi opţiunea **11** (Instalare programe licenţiate) din ecranul Gestionare programe licenţiate pentru a vedea lista cu programele licenţiate şi părţile opţionale ale acestora.
4. Tastaţi **1** (Instalare) în coloana de opţiune de lângă 57*xx*TC1 (TCP/IP Connectivity Utilities pentru iSeries). Apăsaţi **Enter**. Ecranul Confirmare instalare programe licenţiate vă arată programul licenţiat pe care l-aţi selectat pentru instalare. Apăsaţi **Enter** pentru confirmare.
5. Completaţi următoarele opţiuni din ecranul Opţiuni de instalare:

Dispozitiv de instalare	Tastaţi QOPT dacă instalaţi de pe unitatea de CD-ROM. Tastaţi TAP01 dacă instalaţi de pe o unitate de bandă.
Obiecte de instalat	Această opţiune permite instalarea programelor şi a obiectelor de limbă, doar a programelor sau doar a obiectelor de limbă.
Repornire automată	Această opţiune determină dacă sistemul porneşte automat când procesul de instalare s-a terminat cu succes.

   După ce TCP/IP Connectivity Utilities s-a instalat cu succes, apare meniul Gestionare programe licenţiate sau ecranul Semnare.
6. Selectaţi opţiunea **50** (Afişare istoric pentru mesaje) pentru a verifica dacă aţi instalat cu succes programul licenţiat.

   Dacă există erori, va apărea mesajul Funcţia de gestionare programe licenţiate nu s-a terminat în partea de jos a ecranului Gestionare programe licenţiate. Dacă apare o problemă, încercaţi să re-instalaţi TCP/IP Connectivity Utilities. Dacă problema nu se rezolvă, poate fi necesar să contactaţi suportul tehnic.

Notă:

Alte programe licenţiate pe care ar putea fi necesar să le instalaţi sunt:

- iSeries Access pentru Windows 95/NT (5769–XD1 V3R1M3 sau mai recent) - furnizează suport pentru Navigator iSeries, care este folosit pentru a configura unele dintre componentele TCP/IP.
- IBM HTTP Server pentru iSeries (57*xx*–DG1) - furnizează suport pentru server Web.
- Unele aplicaţii TCP/IP necesită instalarea de programe licenţiate suplimentare. Pentru a afla de ce programe este nevoie, revedeţi instrucţiunile de setare pentru aplicaţia specifică pe care o doriţi.

Capitolul 6. Configurarea TCP/IP

Puteţi configura TCP/IP pentru prima dată sau puteţi modifica o configurare existentă pentru a folosi funcţia IPv6. Acest subiect furnizează instrucţiuni pentru configurarea TCP/IP în fiecare dintre aceste situaţii. Vedeţi opţiunile de mai jos pentru instrucţiuni privind modul în care puteţi configura TCP/IP pe serverul dumneavoastră:

Configurarea TCP/IP pentru prima dată
Folosiţi aceste instrucţiuni atunci când configuraţi un server nou. Veţi stabili o conexiune şi veţi configura TCP/IP pentru prima dată.

Configurarea IPv6
Folosiţi aceste instrucţiuni pentru a vă configura serverul pentru funcţia IPv6. Veţi beneficia de capacitatea de adresare îmbunătăţită şi caracteristicile robuste ale acestui protocol Internet. Dacă nu sunteţi familiarizat cu IPv6, vedeţi Internet Protocol versiunea 6 (IPv6), pentru o privire generală. Pentru a configura IPv6, trebuie să aveţi TCP/IP configurat pe server.

Configurarea TCP/IP când sistemul de operare se află în stare restricţionată
Folosiţi această metodă dacă este nevoie să rulaţi TCP/IP în timp ce sistemul de operare se află în stare restricţionată.

Configurarea TCP/IP pentru prima dată

Selectaţi una dintre următoarele metode pentru a configura TCP/IP pe noul dumneavoastră server:

Configurarea TCP/IP folosind vrăjitorul EZ-Setup
Folosiţi această metodă preferată dacă PC-ul dumneavoastră este echipat pentru a folosi vrăjitorul EZ-Setup. Vrăjitorul EZ-Setup este împachetat cu serverul dumneavoastră iSeries.

Configurarea TCP/IP folosind intefaţa bazată pe caractere
Folosiţi această metodă dacă nu puteţi să folosiţi vrăjitorul EZ-Setup. De exemplu, dacă doriţi să folosiţi Navigator iSeries de pe un PC care necesită configurarea TCP/IP de bază pentru ca Navigator iSeries să ruleze, atunci nu veţi putea folosi această metodă.

Configurarea TCP/IP folosind vrăjitorul EZ-Setup

Navigator iSeries este o interfaţă de utilizator grafică care furnizează casete de dialog concise şi vrăjitori pentru a configura TCP/IP. Pentru setarea iniţială, folosiţi vrăjitorul EZ-Setup din Navigator iSeries pentru a stabili o conexiune şi pentru a configura TCP/IP pentru prima dată. Aceasta este metoda preferată pentru lucrul cu serverul dumneavoastră, deoarece interfaţa este uşor de folosit. CD-ROM-ul care conţine vrăjitorul EZ-Setup este trimis o dată cu serverul iSeries.

Pentru a vă configura serverul, parcurgeţi paşii următori:

1. Folosiţi vrăjitorul EZ-Setup. Accesaţi vrăjitorul de pe CD-ROM-ul livrat o dată cu serverul. Urmaţi instrucţiunile vrăjitorului pentru a configura TCP/IP.
2. Pornirea TCP/IP
   a. În Navigator iSeries, expandaţi-vă **serverul –> Reţea**.
   b. Faceţi clic dreapta pe **Configurare TCP/IP** şi selectaţi **Pornire**. Vor fi pornite toate interfeţele şi serverele care au fost setate să pornească automat la pornirea TCP/IP.

Aţi terminat de configurat TCP/IP pe server. Folosiţi Navigator iSeries pentru a modifica configuraţia, după cum necesită reţeaua dumneavoastră. Vedeţi Personalizarea TCP/IP cu Navigator iSeries pentru a adăuga rute şi interfeţe sau Configurarea IPv6 pentru a folosi Internet Protocol versiunea 6 pe reţeaua dumneavoastră.

Configurarea TCP/IP folosind interfaţa bazată pe caractere

Dacă nu puteţi să folosiţi vrăjitorul EZ-Setup din Navigator iSeries, folosiţi în loc interfaţa bazată pe caractere. De exemplu, dacă doriţi să folosiţi Navigator iSeries de pe un PC care necesită configurarea TCP/IP de bază pentru ca Navigator iSeries să ruleze, atunci trebuie să utilizaţi interfaţa bazată pe caractere pentru a efectua configurarea de bază.

Pentru a executa paşii de configurare discutaţi în această secţiune, aveţi nevoie de autorizarea specială *IOSYSCFG în profilul dumneavoastră de utilizator. Pentru informaţii suplimentare despre acest tip de autorizare, vedeţi capitolul despre profilurile de utilizator din Referinţe pentru securitatea iSeries  .

Pentru a configura TCP/IP folosind interfaţa bazată pe caractere, urmaţi aceşti paşi:

1. În lina de comandă, tastaţi GO TCPADM pentru a afişa meniul Administrare TCP/IP şi apăsaţi Enter.
2. Specificaţi opţiunea 1 (Configurare TCP/IP) pentru a afişa meniul de configurare TCP/IP (CFGTCP) şi apăsaţi Enter.Folosiţi acest meniu pentru a selecta operaţiile de configurare.Rezervaţi-vă câteva momente pentru a trece în revistă meniul înainte de a începe configurarea serverului.

Executaţi următorii paşi pentru a configura TCP/IP pe serverul dumneavoastră.

1. Configuraţi o descriere de linie
2. Activaţi înaintarea (forwarding) datagramelor IP
3. Configuraţi o interfaţă
4. Configuraţi o rută
5. Definiţi domeniul local şi numele de gazdă
6. Definire tabela de gazde
7. Porniţi TCP/IP

Configurarerea unei descriere de linie (Ethernet)

Aceste instrucţiuni se referă la configurarea TCP/IP pe un adaptor de comunicaţii Ethernet. Dacă folosiţi un tip diferit de adaptor, cum ar fi un token-ring, vedeţi Configurarea TCP/IP şi referinţe, *Anexa A*, pentru o comandă specifică adaptorului dumneavoastră.

Pentru a configura o descriere de linie, urmaţi aceşti paşi:

1. În linia de comandă, tastaţi CRTLINETH pentru a accesa meniul Creare descriere linie (Ethernet) (CRTLINETH) şi apăsaţi Enter.
2. Specificaţi numele de linie şi apăsaţi Enter. (Folosiţi orice nume.)
3. Specificaţi numele resursei dumneavoastră şi apăsaţi Enter.

Ce este de făcut în continuare:
Activarea înaintării datagramelor IP

Activarea înaintării datagramelor IP

Activaţi înaintarea (forwarding) datagramelor IP, astfel încât pachetele să poată fi expediate de-a lungul diferitelor subreţele.

Pentru a activa înaintarea datagramelor IP, urmaţi aceşti paşi:

1. În linia de comandă, tastaţi CHGTCPA şi apăsaţi F4.
2. Pentru promptul *Înaintare datagramă IP*, tastaţi *YES.

Ce este de făcut în continuare:
Configurarea unei interfeţe

Configurarea unei interfeţe

Pentru a configura o interfaţă, urmaţi aceşti paşi:

1. În linia de comandă, tastaţi CFGTCP pentru a accesa meniul Configurare TCP/IP şi apăsaţi Enter.
2. Selectaţi opţiunea 1 (Gestionare interfeţele TCP/IP) din meniul Configurare TCP/IP şi apăsaţi Enter.
3. Specificaţi opţiunea 1 (Adăugare) pentru a afişa ecranul Adăugare interfaţă TCP/IP şi apăsaţi Enter.
4. Specificaţi valoarea adresei care doriţi să reprezinte serverul dumneavoastră iSeries, adresa mască de subreţea şi numele descrierii de linie pe care aţi definit-o anterior şi apoi apăsaţi Enter.

Pentru a porni interfaţa, specificaţi opţiunea 9 (Pornire) pentru interfaţa pe care aţi configurat-o şi apăsaţi Enter.

Ce este de făcut în continuare:
Configurarea unei rute

Configurarea unei rute

Pentru a ajunge în reţelele la distanţă, este necesară cel puţin o intrare de rutare. Dacă nici o intrare de rutare nu este adăugată manual, serverul dumneavoastră nu poate ajunge la sistemele care nu sunt în reţeaua la care a fost ataşat serverul. Trebuie să adăugaţi de asemenea intrări de rutare pentru a permite clienţilor TCP/IP care încearcă să ajungă la serverul dumneavoastră dintr-o reţea la distanţă să funcţioneze corect.

Ar trebui să planificaţi să aveţi tabela de rutare definită astfel încât să existe întotdeauna o intrare pentru cel puţin o rută implicită (*DFTROUTE). Dacă nu există nici o potrivire cu intrările din tabela de rutare, datele sunt trimise la ruterul IP specificat de prima intrare de rută implicită disponibilă.

Pentru a configura o rută implicită, urmaţi aceşti paşi:

1. Selectaţi opţiunea 2 (Gestionare rute TCP/IP) din meniul Configurare TCP/IP şi apăsaţi Enter.
2. Specificaţi opţiunea 1 (Adăugare) pentru a merge în ecranul Adăugare rută TCP/IP (ADDTCPRTE) şi apăsaţi Enter.
3. Specificaţi *DFTROUTE pentru destinaţia rutei, specificaţi *NONE pentru masca de subreţea, specificaţi adresa IP pentru următorul hop şi apăsaţi Enter.

Ce este de făcut în continuare:
Definirea domeniului local şi a numelui de gazdă

Definirea domeniului local şi a numelui de gazdă

Pentru a defini domeniul local şi numele de gazdă, parcurgeţi paşii următori:

1. Selectaţi opţiunea 12 (Modificare domeniu TCP/IP) din meniul Configurare TCP/IP şi apăsaţi Enter.
2. Specificaţi numele selectate pentru a fi numele dumneavoastră de gazdă locală şi nume de domeniu local, lăsaţi ceilalţi parametri la valorile implicite şi apăsaţi Enter.

Ce este de făcut în continuare:
Definirea unei tabele de gazde

Definirea unei tabele de gazde

Pentru a defini o tabelă de gazde, urmaţi aceşti paşi:

1. Selectaţi opţiunea 10 (Gestionare intrări din tabela de gazde TCP/IP) din meniul Configurare TCP/IP şi apăsaţi Enter.
2. Specificaţi opţiunea 1 (Adăugare) pentru a merge în ecranul Adăugare rută TCP/IP şi apăsaţi Enter.
3. Specificaţi adresa IP, numele de gazdă local asociat şi numele de gazdă complet calificat şi apoi apăsaţi Enter.
4. Specificaţi un semn plus (+) pentru a face spaţiu disponibil pentru mai multe nume de gazdă, dacă e necesar.
5. Repetaţi aceşti paşi pentru fiecare gazdă din reţeaua cu care doriţi să comunicaţi folosind numele şi adăugaţi o intrare pentru fiecare.

Ce este de făcut în continuare:
Pornirea TCP/IP

Pornirea TCP/IP
Serviciile TCP/IP nu sunt disponibile decât după ce porneşte TCP/IP.

Pentru a porni TCP/IP, tastaţi STRTCP în linia de comandă.

Comanda Start TCP/IP (STRTCP) iniţializează şi activează procesarea TCP/IP, porneşte interfeţele TCP/IP şi porneşte joburile serverului. Doar interfeţele TCP/IP şi severele cu AUTOSTART *YES pornesc cu comanda STRTCP.

Aţi terminat de configurat TCP/IP pe serverul dumneavoastră. Folosiţi Navigator iSeries pentru a modifica configuraţia, după cum necesită reţeaua dumneavoastră. Vedeţi Personalizarea TCP/IP cu Navigator iSeries pentru a adăuga rute şi interfeţe sau Configurarea IPv6 pentru a folosi Internet Protocol versiunea 6 pe reţeaua dumneavoastră.

Configurarea IPv6

Dacă folosiţi IPv6 în reţeaua dumneavoastră, puteţi beneficia de avantajele următoarei generaţii de Internet. Pentru a folosi funcţia IPv6, trebuie să modificaţi configuraţia TCP/IP pe server, configurând o linie dedicată pentru IPv6. Trebuie să configuraţi fie o line pentru un adaptor Ethernet 2838 sau 2849, fie o linie tunel configurată (linie virtuală). Citiţi aceste subiecte pentru instrucţiuni de configurare a IPv6:

Cerinţele de setare
Acest subiect prezintă cerinţele de hardware şi de software pentru configurarea serverului pentru IPv6.

Configurarea IPv6 folosind vrăjitorul Configurare IPv6
Vedeţi instrucţiunile pentru folosirea vrăjitorului **Configurare IPv6**, cu care puteţi să configuraţi IPv6 pe serverul dumneavoastră.

Cerinţele de setare
Determinaţi care dintre aceste două tipuri de configuraţii IPv6 este corespunzătoare pentru situaţia dumneavoastră. Dacă nu sunteţi sigur ce tip să alegeţi, vedeţi Scenarii IPv6 pentru exemple.

Trebuie să îndepliniţi aceste cerinţe pentru ca IPv6 să funcţioneze pe serverul dumneavoastră:

Pentru configurarea unei linii Ethernet pentru IPv6:
- OS/400 Versiunea 5 Ediţia 2 sau ulterioară
- iSeries Access pentru Windows şi Navigator iSeries
  - Componenta Reţea din Navigator iSeries
- Adaptor Ethernet 2838 sau 2849 care să fie dedicat pentru IPv6.
- Este necesar un ruter capabil de IPv6 doar dacă doriţi să trimiteţi traficul IPv6 mai departe de LAN-ul imediat.
- TCP/IP (folosind IPv4) trebuie să fie configurat pe un adaptor fizic separat, deoarece TCP/IP trebuie să ruleze pe server. Dacă nu aţi configurat serverul pentru IPv4, vedeţi Configurarea TCP/IP pentru prima dată înainte de configurarea liniei pentru IPv4.

Pentru crearea unei linii tunel configurate (TNLCFG64):
- OS/400 Versiunea 5 Ediţia 2 sau ulterioară
- iSeries Access pentru Windows şi Navigator iSeries
  - Componenta Reţea din Navigator iSeries
- TCP/IP (folosind IPv4) trebuie să fie configurat pe server înainte de a configura linia tunel pentru IPv6. Dacă nu aţi configurat serverul pentru IPv4, vedeţi Configurarea TCP/IP pentru prima dată.

Pentru indicaţii privind accesarea vrăjitorului, mergeţi la Configurarea IPv6 folosind vrăjitorul Configurare IPv6.

Configurarea IPv6 folosind vrăjitorul Configurare IPv6

Pentru a configura IPv6 pe server, trebuie să modificaţi configuraţia serverului folosind vrăjitorul **Configurare IPv6** din Navigator iSeries. IPv6 poate fi configurat numai din Navigator iSeries, nu şi din interfaţa bazată pe caractere.

Notă: Puteţi configura descrierea de linie ethernet IPv6 prin folosind comanda CRTLINETH (Create Line Desc Ethernet - Creare descriere de linie Ethernet) în interfaţa bazată pe caractere; însă trebuie să specificaţi adresa de grup multicast hexazecimală 333300000001. Apoi trebuie să folosiţi vrăjitorul **Configurare IPv6** pentru a termina configurarea IPv6.

Vrăjitorul va cere următoarea intrare:

Pentru configurarea unei linii Ethernet pentru IPv6:
Această configurare vă permite să trimiteţi pachete IPv6 printr-o reţea locală (LAN) IPv6. Vrăjitorul cere numele resursei hardware pe serverul pe care veţi configura IPv6; de exemplu, CMN01. Aceasta trebuie să fie un adaptor Ethernet 2838 sau 2849 care nu este configurat curent pentru IPv4. Vedeţi Crearea unei reţele locale (LAN) IPv6 pentru un scenariu care descrie o situaţie în care puteţi configura o linie Ethernet pentru IPv6.

Pentru crearea unei linii tunel configurate (TNLCFG64):
Această configurare vă permite să trimiteţi pachete prin reţelele IPv4. Vrăjitorul cere adresa IPv4 pentru punctul final local şi adresa IPv6 pentru interfaţa locală asociată cu tunelul. Vedeţi Trimiterea pachetelor IPv6 printr-o reţea locală (LAN) IPv4 şi Trimiterea pachetelor IPv6 printr-o reţea de mare suprafaţă (WAN) IPv4 pentru scenarii care descriu două situaţii în care puteţi crea linii tunel configurate pentru IPv6.

Pentru a folosi vrăjitorul **Configurare IPv6**, parcurgeţi paşii următori:

1. În Navigator iSeries, expandaţi-vă **serverul —>Reţea —> Configurare TCP/IP**.
2. Faceţi clic dreapta pe **IPv6** şi selectaţi **Configurare IPv6**.
3. Urmaţi instrucţiunile vrăjitorului pentru a configura IPv6 pe server.

Configurarea TCP/IP când sistemul de operare se află în stare restricţionată

Situaţie

Ca administrator de reţea, aveţi nevoie să obţineţi rapoarte cu starea copiilor de rezervă ale serverului dumneavoastră. Când rulaţi procedurile de salvare de rezervă, sistemul de operare trebuie să se afle în stare restricţionată pentru a împiedica utilizatorii să modifice vreo configurare. Deoarece vă aflaţi la distanţă, accesaţi rapoartele de stare folosind un dispozitiv PDA (sau orice dispozitiv de reţea TCP/IP). PDA-ul foloseşte o aplicaţie activată pentru socket-uri, care necesită o interfaţă TCP/IP activă şi disponibilă pentru a comunica cu serverul. Pentru a permite această comunicaţie, trebuie să porniţi mai întâi TCP/IP folosind parametri speciali. După ce porniţi TCP/IP, trebuie să porniţi o anumită interfaţă TCP/IP pentru a permite accesul la sistem. Informaţiile de mai jos furnizează detalii suplimentare.

Cerinţe preliminare

Pe serverul dumneavoastră iSeries rulează OS/400(R) V5R2 sau o versiune mai recentă.

Restricţii

Următoarele restricţii se aplică atunci când sistemul de operare rulează în stare restricţionată:

- Nu se pot porni serverele TCP/IP (comanda CL STRTCPSRV), din moment ce ele necesită subsisteme active.
- Se poate porni doar o interfaţă pentru un anumit tip de linie (Ethernet, token-ring, sau DDI) care nu este ataşată la o descriere de server de reţea (NWSD) sau la o descriere de interfaţă de reţea (NWID).

Paşi de configurare

1. Porniţi TCP/IP folosind parametri speciali

Când sistemul iSeries se află în stare restricţionată, executaţi următoarea comandă din interfaţa de linie de comandă: STRTCP STRSVR(*NO) STRIFC(*NO). Aceştia sunt singurii parametri acceptaţi când sistemul de operare se află în stare restricţionată. Comanda de mai sus va porni TCP/IP; însă ea nu va porni şi nici nu poate porni servere de aplicaţii TCP/IP sau interfeţe IP.

2. Porniţi o anumită interfaţă TCP/IP

   După ce porniţi TCP/IP în starea restricţionată, puteţi porni interfaţa necesară pentru aplicaţia dumneavoastră activată pentru socket-uri.

   a. Verificaţi dacă interfaţa pe care doriţi să o porniţi foloseşte descrierea de linie *ELAN, *TRLAN sau *DDI.

      Pentru a vizualiza tipul liniei pentru interfaţa dumneavoastră, într-o interfaţă de linie de comandă introduceţi CFGTCP şi selectaţi opţiunea 1 - Gestionare interfeţe TCP/IP.

   b. Verificaţi că interfaţa nu este ataşată la o descriere NWID sau NWSD. Orice alte încercări vor afişa un mesaj de eroare.

      Pentru a verifica faptul că interfaţa nu este ataşată la o descriere NWID sau NWSD, dintr-o interfaţă de linie de comandă introduceţi DSPLIND abc (unde abc este numele descrierii dumneavoastră de linie). Verificaţi că numele de resursă nu este *NWID sau *NWSD.

      Notă: Dacă interfaţa este ataşată la o descriere NWID sau NWSD, se recomandă să selectaţi o altă interfaţă.

   c. În sfârşit, porniţi interfaţa. Într-o interfaţă de linie de comandă, introduceţi următoarele: STRTCPIFC INTNETADR('a.b.c.d'). Înlocuiţi a.b.c.d cu adresa dumneavoastră IP de interfaţă.

      Notă: Verificaţi că nu este specificat STRTCPIFC INTNETADR(*AUTOSTART).

3. Verificaţi că interfaţa este activă.

   Faceţi ping la interfaţa corespunzătoare aplicaţiei dumneavoastră. Există foarte puţine utilitare referitoare la TCP/IP care vor funcţiona în stare restricţionată. Totuşi, Ping şi Netstat pot fi folosite. Pentru informaţii suplimentare despre utilizarea comenzilor ping şi netstat, vă rugăm citiţi Uneltele pentru verificarea structurii reţelei, din Depanarea TCP/IP.

Capitolul 7. Pesonalizarea TCP/IP cu Navigator iSeries

După ce aţi configurat TCP/IP, puteţi decide să vă personalizaţi configurarea. Pe măsură ce reţeaua dumneavoastră creşte, poate fi necesar să modificaţi proprietăţile, să adăugaţi interfeţe sau să adăugaţi rute pe server. Puteţi avea nevoie să configuraţi serverul pentru IPv6 pentru a folosi aplicaţii IPv6. Folosiţi vrăjitorii din Navigator iSeriespentru a realiza rapid multe dintre aceste operaţii.

Alegeţi oricare dintre subiectele de mai jos pentru a vă personaliza configurarea folosind Navigator iSeries. Aceste subiecte vă oferă un punct de pornire pentru gestionarea configuraţiei TCP/IP cu Navigator iSeries.

Modificarea setărilor TCP/IP

Configurarea IPv6

Adăugarea interfeţelor IPv4

Adăugarea interfeţelor IPv6

Adăugarea rutelor IPv4

Adăugarea rutelor IPv6

Modificarea setărilor TCP/IP

Puteţi vizualiza şi modifica setările dumneavoastră TCP/IP folosind Navigator iSeries. De exemplu, puteţi modifica proprietăţile pentru numele de gazdă sau de domeniu, numele de server, intrări tabelă de gazde, atribute sistem, restricţii de porturi, conexiuni server sau client. Puteţi modifica proprietăţi generale sau proprietăţi care sunt specifice pentru IPv4 sau pentru IPv6, cum ar fi transporturile.

Pentru a accesa paginile de proprietăţi TCP/IP generale, parcurgeţi paşii următori:

1. În Navigator iSeries, selectaţi-vă **serverul —> Reţea**.
2. Faceţi clic dreapta pe **Configurare TCP/IP** şi selectaţi **Proprietăţi** pentru a deschide dialogul **Proprietăţi TCP/IP**.
3. Selectaţi fişele din partea de sus a dialogului pentru a vedea şi edita informaţiile TCP/IP.

Pentru a adăuga şi modifica intrări în tabela de gazde, urmaţi parcurgeţi paşii următori:

1. În Navigator iSeries, selectaţi-vă **serverul —> Reţea**.
2. Faceţi clic dreapta pe **Configurare TCP/IP** şi selectaţi **Tabelă de gazde** pentru a deschide dialogul **Tabelă de gazde**.
3. Folosiţi dialogul **Tabelă de gazde** pentru a adăuga, edita sau înlătura intrări din tabela de gazde.

Pentru a accesa pagini de proprietăţi care sunt specifice pentru IPv4, parcurgeţi paşii următori:

1. În Navigator iSeries, selectaţi-vă **serverul —> Reţea**.
2. Faceţi clic dreapta pe **IPv4** şi selectaţi **Proprietăţi** pentru a deschide dialogul **Proprietăţi IPv4**.
3. Selectaţi fişele din partea de sus a dialogului pentru a vedea şi edita setările de proprietăţi IPv4.

Pentru a accesa pagini de proprietăţi care sunt specifice pentru IPv6, parcurgeţi paşii următori:

1. În Navigator iSeries, selectaţi-vă **serverul —> Reţea**.
2. Faceţi clic dreapta pe **IPv6** şi selectaţi **Proprietăţi** pentru a deschide dialogul **Proprietăţi IPv6**.
3. Selectaţi fişele din partea de sus a dialogului pentru a vedea şi edita setările de proprietăţi IPv6.

Configurarea IPv6

Dacă nu sunteţi familiarizat cu IPv6, vedeţi Internet Protocol versiunea 6 (IPv6), pentru o privire generală.

Pentru a configura IPv6 pe server, trebuie să modificaţi configurarea serverului folosind vrăjitorul **Configurare IPv6**. Înainte de a folosi vrăjitorul, vedeţi Configurarea IPv6, pentru instrucţiuni şi cerinţe speciale.

Adăugarea interfeţelor IPv4

Pentru a crea o interfaţă nouă IPv4, parcurgeţi paşii următori:

1. În Navigator iSeries, selectaţi-vă **serverul —> Reţea —> Configurare TCP/IP —>IPv4.**
2. Faceţi clic dreapta pe **Interfeţe**, selectaţi **Interfaţă nouă** şi selectaţi **Reţea locală** , **Reţea de mare suprafaţă** sau **IP virtual** pentru a crea tipul corespunzător de interfaţă IPv4.
3. Urmaţi instrucţiunile vrăjitorului pentru a crea o nouă interfaţă IPv4.

Adăugarea interfeţelor IPv6

Pentru a crea o nouă interfaţă IPv6, parcurgeţi paşii următori:

1. În Navigator iSeries, selectaţi-vă **serverul —> Reţea —> Configurare TCP/IP —>IPv6**.
2. Faceţi clic dreapta pe **Interfeţe** şi selectaţi **Interfaţă nouă**.
3. Urmaţi instrucţiunile vrăjitorului pentru a crea o nouă interfaţă IPv6.

Adăugarea rutelor IPv4

Orice schimbare făcută în informaţiile de rutare are efect imediat.

Pentru a configura o rută nouă IPv4, parcurgeţi paşii următori:

1. În Navigator iSeries, selectaţi-vă **serverul —> Reţea —> Configurare TCP/IP —>IPv4.**
2. Faceţi clic dreapta pe **Rute** şi selectaţi **Rută nouă**.
3. Urmaţi instrucţiunile vrăjitorului pentru a configura o rută nouă IPv4.

Adăugarea rutelor IPv6

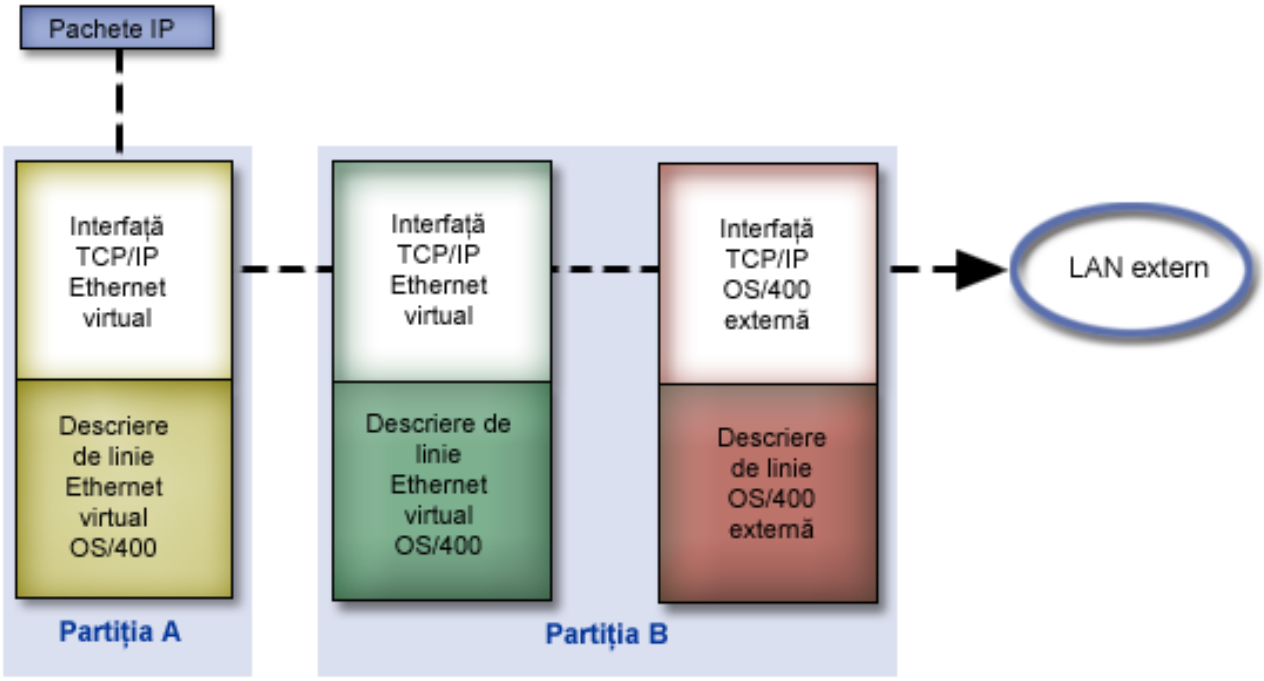
Orice schimbare făcută în informaţiile de rutare are efect imediat.

Pentru a configura o rută nouă IPv6, parcurgeţi paşii următori:

1. În Navigator iSeries, selectaţi-vă **serverul —> Reţea —> Configurare TCP/IP —>IPv6**.
2. Faceţi clic dreapta pe **Rute** şi selectaţi **Rută nouă**.
3. Urmaţi instrucţiunile vrăjitorului pentru a configura o rută nouă IPv6.

Capitolul 8. Tehnici TCP/IP de conectare a reţelei Ethernet virtual la reţele LAN externe

Dacă folosiţi o reţea Ethernet virtual pentru comunicaţia între partiţii, poate fi necesar să activaţi aceste partiţii să comunice cu o reţea LAN fizică externă. Există mai multe moduri de a conecta reţeaua Ethernet virtual la o reţea LAN externă, folosind diferite tehnici TCP/IP. Este nevoie să activaţi traficul TCP/IP să funcţioneze între reţeaua Ethernet virtual şi reţeaua LAN externă. Această ilustraţie prezintă un flux logic de pachete IP.



Traficul IP iniţiat de Partiţia A merge dinspre interfaţa sa Ethernet virtual spre interfaţa Ethernet virtual din Partiţia B. Implementând oricare dintre cele trei tehnici TCP/IP descrise mai jos, puteţi activa pachetele IP să meargă mai departe spre interfaţa externă şi către destinaţia lor.

Există trei metode de conectare a reţelelor Ethernet virtual şi LAN externă. În cazul fiecărei metode există anumite detalii pentru care sunt necesare cunoştinţe despre TCP/IP şi mediul de lucru. Alegeţi una dintre următoarele metode:

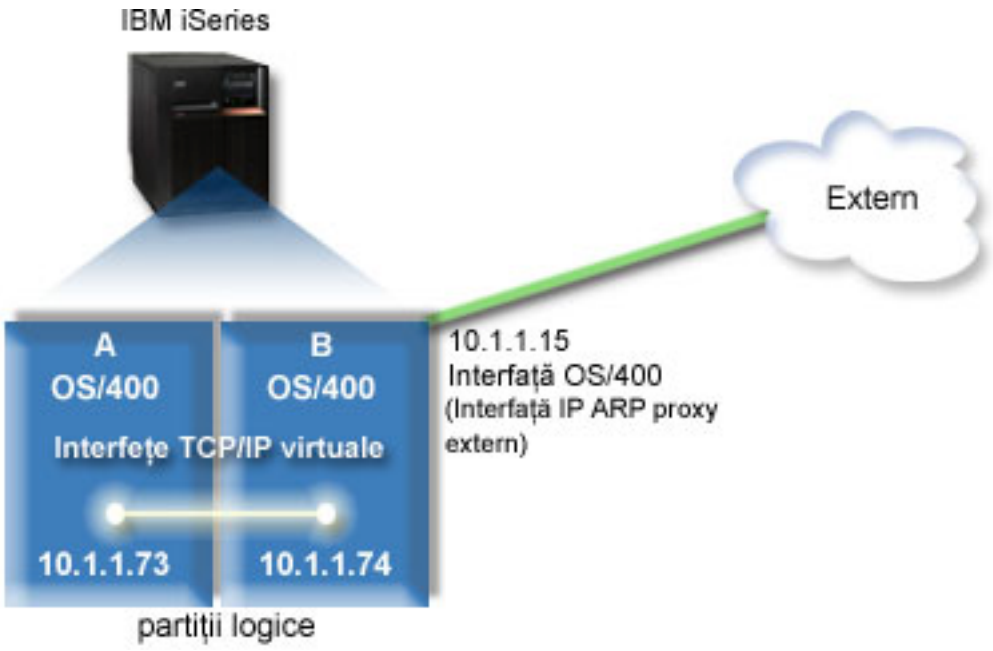
- **ARP proxy**
  Această metodă foloseşte legarea transparentă la subreţea pentru a asocia interfaţa virtuală a unei partiţii cu o interfaţă externă. Funcţia ARP proxy este încorporată în stiva TCP/IP. Dacă aveţi adresa IP necesară, este recomandată această abordare.
- **Translatare adresă de reţea**
  Poate fi folosită filtrarea de pachete OS/400 pentru a ruta traficul dintre o partiţie şi reţeaua externă.
- **Rutare TCP/IP**
  Rutarea TCP/IP standard este folosită pentru a ruta traficul către reţeaua Ethernet virtual în acelaşi mod în care aţi defini rutarea în orice altă reţea LAN.Pentru aceasta este necesar să vă actualizaţi informaţiile de rutare prin reţea.

Metoda ARP proxy

Metoda ARP proxy foloseşte o tehnică denumită *legare transparentă la subreţea*. Dacă doriţi să aflaţi informaţii suplimentare despre legarea transparentă la subreţea:

- V4 TCP/IP for AS/400: More Cool Things Than Ever
  Această carte roşie furnizează scenarii care demonstrează aplicarea soluţiilor obişnuite pentru exemple de configuraţii. Vă ajută de asemenea să planificaţi, să instalaţi, să organizaţi, să configuraţi şi să depanaţi TCP/IP pe serverul dumneavoastră iSeries.
- Rutarea TCP/IP şi echilibrarea operaţiilor
  Acest subiect furnizează tehnici şi instrucţiuni pentru rutare şi pentru echilibrarea operaţiilor.

Dacă alegeţi să utilizaţi metoda ARP proxy, trebuie să aveţi cunoştinţe temeinice de legare în subreţea şi de TCP/IP. Trebuie să obţineţi un bloc contiguu de adrese IP care să poată fi rutate de către reţeaua dumneavoastră. Veţi folosi în subreţea acest bloc de adrese IP. În acest exemplu este folosit un bloc contiguu de patru adrese IP (de la 10.1.1.72 la 10.1.1.75). Din moment ce este un bloc de patru adrese IP, masca de subreţea pentru aceste adrese este 255.255.255.252. Alocaţi o adresă pentru fiecare dintre interfeţele TCP/IP virtuale din partiţiile dumneavoastră, aşa cum este arătat în această ilustraţie.



În acest exemplu, traficul TCP/IP de la partiţia A trece prin reţeaua Ethernet virtual către interfaţa 10.1.1.74 din partiţia B. Din moment ce 10.1.1.74 este asociată cu interfaţa ARP proxy externă 10.1.1.15, pachetele merg în continuare în afara reţelei Ethernet virtual folosind interfaţa ARP proxy.

Pentru a configura o reţea Ethernet virtual să folosească metoda de conexiune ARP proxy, executaţi aceste operaţii de configurare.

1. Activaţi partiţiile logice să participe într-o reţea Ethernet virtual
2. Creaţi descrierile de linie Ethernet
3. Activaţi înaintarea (forwarding) datagramelor IP
4. Creaţi interfaţa care să activeze ARP proxy
5. Creaţi interfaţa TCP/IP virtuală în partiţia A
6. Creaţi interfaţa TCP/IP virtuală în partiţia B
7. Creaţi ruta
8. Verificaţi comunicaţiile din reţea

Pasul 1: Activarea partiţiilor logice pentru a participa într-o reţea Ethernet virtual

Notă: Dacă folosiţi alte modele de servere în afară de modelele 270 şi 8*xx*, trebuie să efectuaţi acest pas folosind consola Hardware Management Console pentru eServer (HMC) în locul partiţiei primare. Vedeţi Ethernet virtual pentru detalii.

Pentru a activa Ethernet virtual, parcurgeţi paşii următori:

1. În linia de comandă din partiţia primară (partiţia A), tastaţi STRSST şi apăsaţi Enter.
2. Tastaţi ID-ul dumneavoastră de utilizator de unelte de service şi parola.
3. În ecranul SST (System Service Tools - Unelte de service sistem), selectaţi opţiunea 5 (Gestionare partiţii sistem).
4. În ecranul Gestionare partiţii sistem, selectaţi opţiunea 3 (Gestionare configuraţie partiţie).
5. Apăsaţi F10 (Gestionare Ethernet virtual).
6. Tastaţi 1 în coloana corespunzătoare partiţiei A şi partiţiei B, pentru a permite partiţiilor să comunice una cu cealaltă prin Ethernet virtual.
7. Ieşiţi din SST (System Service Tools - Unelte de service sistem), pentru a vă întoarce la linia de comandă.

Ce este de făcut în continuare

Creaţi descrierile de linie Ethernet

Pasul 2: Crearea descrierilor de linie Ethernet

Trebuie să efectuaţi acest pas în unul dintre cele două moduri, în funcţie de modelul de server pe care îl folosiţi. Alegeţi una dintre aceste metode de creare a descrierilor de linie în funcţie de modelul dumneavoastră de server.

- Crearea descrierilor de linie Ethernet pe serverele model 270 şi 8*xx*
- Crearea descrierilor de linie Ethernet pe orice servere în afară de modelele 270 şi 8xx

Crearea descrierilor de linie Ethernet pe serverele model 270 şi 8*xx*

Pentru a configura noile descrieri de linie Ethernet să suporte Ethernet virtual, urmaţi aceşti paşi:

1. În linia de comandă din partiţia A, tastaţi WRKHDWRSC *CMN şi apăsaţi Enter.
2. Din ecranul Gestionare resurse de comunicaţie selectaţi opţiunea 7 (Afişare detalii resursă) de lângă portul Ethernet virtual corespunzător.

   Portul Ethernet identificat drept 268C este resursa Ethernet virtual. Va exista câte unul pentru fiecare Ethernet virtual care este conectat la partiţia logică.
3. În ecranul Afişare detalii resursă, derulaţi în jos pentru a găsi adresa de port. Adresa de port corespunde cu reţeaua Ethernet virtual pe care aţi selectat-o în timpul configurării partiţiei logice.
4. În ecranul Gestionare resurse de comunicaţie selectaţi opţiunea 5 (Gestionare descrieri de configurare) de lângă portul Ethernet virtual corespunzător şi apăsaţi Enter.
5. În ecranul Gestionare descrieri de configurare selectaţi opţiunea 1 (Creare) şi apăsaţi Enter pentru a vedea ecranul CRTLINETH (Create Line Description Ethernet - Creare descriere de linie Ethernet).
   a. Pentru promptul *Descriere de linie* tastaţi VETH0 . Numele VETH0, deşi arbitrar, corespunde coloanei cu numere din pagina Ethernet virtual în care aţi activat partiţia logică să comunice. Dacă folosiţi aceleaşi nume pentru descrierile de linie şi pentru reţelele lor Ethernet virtual asociate, puteţi ţine uşor evidenţa configuraţiilor dumneavoastră Ethernet virtual.
   b. Pentru promptul *Viteză linie* tastaţi 1G.
   c. Pentru promptul *Duplex* tastaţi *FULL şi apăsaţi Enter.
   d. Pentru promptul *Dimensiune maximă cadru* tastaţi 8996 şi apăsaţi Enter. Modificând dimensiunea cadru în 8996, transferul de date prin Ethernet virtual este îmbunătăţit.

   Veţi vedea un mesaj care spune că descrierea de linie a fost creată.
6. Activaţi descrierea de linie. Tastaţi WRKCFGSTS *LIN şi selectaţi opţiunea 1 (Activare) pentru VETH0.

7. Repetaţi paşii de la 1 la 6, dar efectuaţi paşii din linia de comandă din partiţia B pentru a crea o descriere de linie pentru partiţia B.

   Deşi numele descrierilor de linie sunt arbitrare, ajută să folosiţi aceleaşi nume pentru toate descrierile de linie asociate cu Ethernet virtual. În acest scenariu, toate descrierile de linie sunt numite VETH0.

Ce este de făcut în continuare

Activaţi înaintarea (forwarding) datagramelor IP

Crearea descrierilor de linie Ethernet pe orice servere în afară de modelele 270 şi 8xx

Pentru a configura noile descrieri de linie Ethernet să suporte Ethernet virtual, urmaţi aceşti paşi:

1. În linia de comandă din partiţia A, tastaţi WRKHDWRSC *CMN şi apăsaţi Enter.
2. În ecranul Gestionare resurse de comunicaţie selectaţi opţiunea 7 (Afişare detalii resursă) de lângă portul Ethernet virtual corespunzător.

   Porturile Ethernet identificate drept 268C sunt resurse Ethernet virtual. Va exista câte unul pentru fiecare adaptor Ethernet virtual. Fiecare port identificat drept 268C are un cod de locaţie asociat care este creat când creaţi adaptorul Ethernet virtual folosind HMC (Pasul 1).
3. În ecranul Afişare detalii resursă derulaţi în jos pentru a găsi resursa 268C care este asociată cu codul de locaţie anume creat pentru acest Ethernet virtual.
4. În ecranul Gestionare resurse de comunicaţie selectaţi opţiunea 5 (Gestionare descrieri de configurare) de lângă resursa Ethernet virtual corespunzătoare şi apăsaţi Enter.
5. În ecranul Gestionare descrieri de configurare selectaţi opţiunea 1 (Creare) şi apăsaţi Enter pentru a vedea ecranul CRTLINETH (Create Line Description Ethernet - Creare descriere de linie Ethernet).
   a. Pentru promptul *Descriere de linie* tastaţi VETH0 . Dacă folosiţi aceleaşi nume pentru descrierile de linie şi pentru reţelele lor Ethernet virtual asociate, cum ar fi VETHO, puteţi ţine uşor evidenţa configuraţiilor dumneavoastră Ethernet virtual.
   b. Pentru promptul *Viteză linie* tastaţi 1G.
   c. Pentru promptul *Duplex* tastaţi *FULL şi apăsaţi Enter.
   d. Pentru promptul *Dimensiune maximă cadru* tastaţi 8996 şi apăsaţi Enter. Modificând dimensiunea cadru în 8996, transferul de date prin Ethernet virtual este îmbunătăţit.

   Veţi vedea un mesaj care spune că descrierea de linie a fost creată.
6. Activaţi descrierea de linie. Tastaţi WRKCFGSTS *LIN şi selectaţi opţiunea 1 (Activare) pentru VETH0.
7. Repetaţi paşii de la 1 la 6, dar efectuaţi paşii din linia de comandă din partiţia B pentru a crea o descriere de linie pentru partiţia B.

   Deşi numele descrierilor de linie sunt arbitrare, ajută să folosiţi aceleaşi nume pentru toate descrierile de linie asociate cu Ethernet virtual. În acest scenariu, toate descrierile de linie sunt numite VETH0.

Ce este de făcut în continuare

Activaţi înaintarea (forwarding) datagramelor IP

Pasul 3: Activarea înaintării datagramelor IP

Activaţi înaintarea (forwarding) datagramelor IP, astfel încât pachetele să poată fi expediate de-a lungul diferitelor subreţele.

Pentru a activa înaintarea datagramelor IP, urmaţi aceşti paşi:

1. În linia de comandă din partiţia A, tastaţi CHGTCPA şi apăsaţi F4.
2. Pentru promptul *Înaintare datagramă IP*, tastaţi *YES.

Ce este de făcut în continuare

Creaţi interfaţa care să activeze ARP proxy

Pasul 4: Crearea interfeţei care să activeze ARP proxy

Pentru a crea interfaţa TCP/IP care să activeze ARP proxy, efectuaţi aceşti paşi:

1. Obţineţi un bloc contiguu de adrese IP care sunt rutabile de către reţeaua dumneavoastră.

   Din moment ce aveţi două partiţii în acest Ethernet virtual, aveţi nevoie de un bloc de patru adrese. Al patrulea segment al primei adrese IP din bloc trebuie să fie divizibil cu patru. Prima şi ultima adresă IP ale acestui bloc sunt adresele IP de subreţea şi de difuzare şi nu pot fi utilizate. A doua şi a treia adresă IP pot fi folosite pentru interfeţele TCP/IP pentru Ethernet virtual din partiţiile A şi B. Pentru această procedură, blocul de adrese IP este de la 10.1.1.72 la 10.1.1.75 cu masca de subreţea 255.255.255.252.

   Aveţi de asemenea nevoie de o singură adresă IP pentru adresa dumneavoastră TCP/IP externă. Această adresă IP nu trebuie să aparţină blocului de adrese contigue, dar trebuie să fie în aceeaşi mască de subreţea originală 255.255.255.0. În acesată procedură, adresa IP externă este 10.1.1.15.
2. Creaţi o interfaţă TCP/IP OS/400 pentru partiţia B. Această interfaţă este cunoscută drept interfaţa IP ARP proxy externă. Pentru a crea interfaţa, urmaţi aceşti paşi:
   a. În linia de comandă din partiţia B, tastaţi CFGTCP şi apăsaţi Enter pentru a vedea ecranul Configurare TCP/IP.
   b. Selectaţi opţiunea 1 (Gestionare interfeţe TCP/IP) şi apăsaţi Enter.
   c. Selectaţi opţiunea 1 (Adăugare) şi apăsaţi Enter pentru a vedea ecranul ADDTCPIFC (Add TCP/IP Interface - Adăugare interfaţă TCP/IP).
   d. Pentru promptul *Adresă internet*, tastaţi '10.1.1.15'.
   e. Pentru promptul *Descriere de linie* tastaţi numele descrierii dumneavoastră de linie, cum ar fi ETHLINE.
   f. Pentru promptul *Mască subreţea* tastaţi '255.255.255.0'.
3. Porniţi interfaţa. În ecranul Gestionare interfeţe TCP/IP selectaţi opţiunea 9 (Pornire) de lângă interfaţă.

Ce este de făcut în continuare

Crearea interfeţei TCP/IP virtuale în partiţia A

Pasul 5: Crearea interfeţei TCP/IP virtuale în partiţia A

Pentru a crea interfaţa virtuală, urmaţi aceşti paşi:

1. În linia de comandă din partiţia A, tastaţi CFGTCP şi apăsaţi Enter pentru a vedea ecranul Configurare TCP/IP.
2. Selectaţi opţiunea 1 (Gestionare interfeţe TCP/IP) şi apăsaţi Enter.
3. Selectaţi opţiunea 1 (Adăugare) şi apăsaţi Enter pentru a vedea ecranul ADDTCPIFC (Add TCP/IP Interface - Adăugare interfaţă TCP/IP).
4. Pentru promptul *Adresă internet*, tastaţi '10.1.1.73'.
5. Pentru promptul *Descriere de linie* tastaţi numele descrierii dumneavoastră de linie, cum ar fi ETHLINE.
6. Pentru promptul *Mască subreţea* tastaţi '255.255.255.252'.
7. Porniţi interfaţa. În ecranul Gestionare interfeţe TCP/IP selectaţi opţiunea 9 (Pornire) de lângă interfaţă.

Ce este de făcut în continuare

Creaţi interfaţa TCP/IP virtuală în partiţia B

Pasul 6: Crearea interfeţei TCP/IP virtuale în partiţia B

Pentru a crea interfaţa virtuală, urmaţi aceşti paşi:

1. În linia de comandă din partiţia B, tastaţi CFGTCP şi apăsaţi Enter pentru a vedea ecranul Configurare TCP/IP.
2. Selectaţi opţiunea 1 (Gestionare interfeţe TCP/IP) şi apăsaţi Enter.
3. Selectaţi opţiunea 1 (Adăugare) şi apăsaţi Enter pentru a vedea ecranul ADDTCPIFC (Add TCP/IP Interface - Adăugare interfaţă TCP/IP).

4. Pentru promptul *Adresă internet*, tastaţi '10.1.1.74'.
5. Pentru promptul *Descriere de linie* tastaţi numele descrierii dumneavoastră de linie, cum ar fi ETHLINE.
6. Pentru promptul *Mască subreţea* tastaţi '255.255.255.252'.
7. Pentru promptul *Interfaţă locală asociată*, tastaţi '10.1.1.15'. Aceasta asociază interfaţa virtuală cu interfaţa externă şi activează ARP proxy pentru a înainta pachete între interfaţa virtuală 10.1.1.74 şi o interfaţă externă 10.1.1.15.
8. Porniţi interfaţa. În ecranul Gestionare interfeţe TCP/IP selectaţi opţiunea 9 (Pornire) de lângă interfaţă.

Ce este de făcut în continuare

Creaţi ruta

Pasul 7: Crearea rutei

Pentru a crea ruta implicită care să permită pachetelor să iasă din reţeaua Ethernet virtual, urmaţi aceşti paşi:

1. În linia de comandă din partiţia A, tastaţi CFGTCP şi apăsaţi Enter.
2. Selectaţi opţiunea 2 (Gestionare rute TCP/IP) şi apăsaţi Enter.
3. Selectaţi opţiunea 1 (Adăugare) şi apăsaţi Enter.
4. Pentru promptul *Destinaţie rută* tastaţi *DFTROUTE.
5. Pentru promptul *Mască subreţea* tastaţi *NONE.
6. Pentru promptul *Hop următor*, tastaţi '10.1.1.74'.

   Pachetele din partiţia A merg prin Ethernet virtual către interfaţa 10.1.1.74 folosind această rută implicită. Din moment ce 10.1.1.74 este asociată cu interfaţa ARP proxy externă 10.1.1.15, pachetele merg în continuare în afara reţelei Ethernet virtual folosind interfaţa ARP proxy.

Ce este de făcut în continuare

Verificaţi comunicaţiile în reţea

Pasul 8: Verificarea comunicaţiilor în reţea

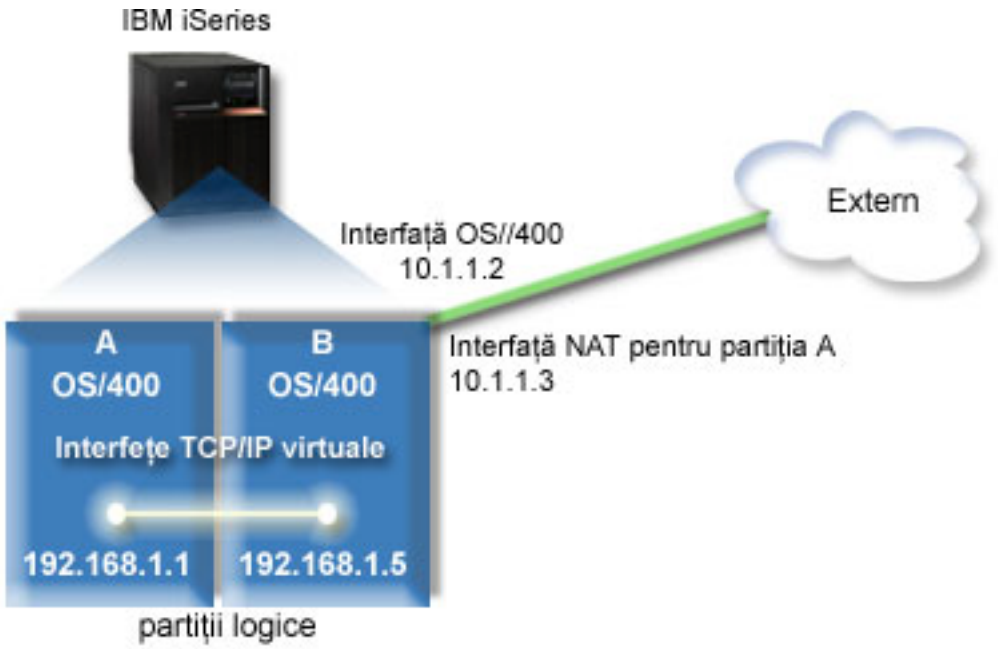
Verificaţi comunicaţiile reţelei dumneavoastră folosind comanda ping:

- Din partiţia A, executaţi ping pentru interfaţa Ethernet virtual 10.1.1.74 şi pentru o gazdă externă.
- Dintr-o gazdă externă OS/400, executaţi ping pentru interfeţele Ethernet virtual 10.1.1.73 şi 10.1.1.74.

Metoda translatării adresei de reţea

NAT (Network address translation - Translatarea adresei de reţea) poate ruta traficul între reţeaua dumneavoastră Ethernet virtual şi reţeaua externă. Această formă particulară de NAT este denumită NAT static şi va permite atât trafic IP de intrare cât şi trafic IP de ieşire către şi dinspre reţeaua Ethernet virtual. Vor funcţiona de asemenea şi alte forme de NAT, cum ar fi NAT cu travestire, dacă reţeaua dumneavoastră de Ethernet virtual nu trebuie să primească trafic iniţiat de clienţi externi. La fel ca la metodele de rutare TCP/IP şi ARP proxy, puteţi profita de conexiunile dumneavoastră de reţea OS/400. Din moment ce veţi folosi reguli de pachet IP, trebuie să folosiţi Navigator iSeries pentru a vă crea şi aplica propriile reguli.

Următoarea ilustraţie este un exemplu de utilizare a NAT pentru a vă conecta reţeaua Ethernet virtual la o reţea externă. Reţeaua 10.1.1.*x* reprezintă o reţea externă, în timp ce reţeaua 192.168.1.*x* reprezintă reţeaua Ethernet virtual.



În acest exemplu, orice trafic TCP/IP existent pentru server trece prin interfaţa 10.1.1.2. Din moment ce acesta este un scenariu de mapare statică, traficul de intrare este translatat din interfaţa 10.1.1.3 în interfaţa 192.168.1.5. Traficul de ieşire este translatat din interfaţa 192.168.1.5 către interfaţa externă 10.1.1.3. Partiţiile A şi B folosesc interfeţele lor virtuale 192.168.1.1 şi respectiv 192.168.1.5 pentru a comunica una cu alta.

Pentru a face ca NAT static să funcţioneze, trebuie să setaţi mai întâi comunicaţiile dumneavoastră OS/400 şi TCP/IP. Apoi veţi crea şi aplica câteva reguli de pachet IP. Pentru a configura Ethernet virtual să folosească metoda NAT, efectuaţi aceste operaţii de configurare:

1. Activaţi partiţiile logice să participe într-o reţea Ethernet virtual
2. Creaţi descrierile de linie Ethernet
3. Activaţi înaintarea (forwarding) datagramelor IP
4. Creaţi interfeţele
5. Verificaţi comunicaţiile de reţea
6. Creaţi reguli de pachet
7. Verificaţi comunicaţiile de reţea

Pasul 1: Activarea partiţiilor logice pentru a participa într-o reţea Ethernet virtual

Notă: Dacă folosiţi alte modele de servere în afară de modelele 270 şi 8*xx*, trebuie să efectuaţi acest pas folosind consola Hardware Management Console pentru eServer (HMC) în locul partiţiei primare. Vedeţi Ethernet virtual pentru detalii.

Pentru a activa Ethernet virtual, parcurgeţi paşii următori:

1. În linia de comandă din partiţia primară (partiţia A), tastaţi STRSST şi apăsaţi Enter.
2. Tastaţi ID-ul dumneavoastră de utilizator de unelte de service şi parola.
3. În ecranul SST (System Service Tools - Unelte de service sistem), selectaţi opţiunea 5 (Gestionare partiţii sistem).
4. În ecranul Gestionare partiţii sistem, selectaţi opţiunea 3 (Gestionare configuraţie partiţie).
5. Apăsaţi F10 (Gestionare Ethernet virtual).
6. Tastaţi 1 în coloana corespunzătoare partiţiei A şi partiţiei B, pentru a permite partiţiilor să comunice una cu cealaltă prin Ethernet virtual.

7. Ieşiţi din SST (System Service Tools - Unelte de service sistem), pentru a vă întoarce la linia de comandă.

Ce este de făcut în continuare

Creaţi descrierile de linie Ethernet

Pasul 2: Crearea descrierilor de linie Ethernet

Trebuie să efectuaţi acest pas într-unul dintre cele două moduri, în funcţie de modelul de server pe care îl folosiţi. Alegeţi una dintre aceste metode de creare a descrierilor de linie în funcţie de modelul dumneavoastră de server.

- Crearea descrierilor de linie Ethernet pe modelele de servere 270 şi 8*xx*
- Crearea descrierilor de linie Ethernet pe orice servere în afară de modelele 270 şi 8xx

Crearea descrierilor de linie Ethernet pe serverele model 270 şi 8*xx*

Pentru a configura noile descrieri de linie Ethernet să suporte Ethernet virtual, urmaţi aceşti paşi:

1. În linia de comandă din partiţia A, tastaţi WRKHDWRSC *CMN şi apăsaţi Enter.
2. În ecranul Gestionare resurse de comunicaţie selectaţi opţiunea 7 (Afişare detalii resursă) de lângă portul Ethernet virtual corespunzător.

   Portul Ethernet identificat drept 268C este resursa Ethernet virtual. Va exista câte unul pentru fiecare Ethernet virtual care este conectat la partiţia logică.
3. În ecranul Afişare detalii resursă, derulaţi în jos pentru a găsi adresa de port. Adresa de port corespunde cu reţeaua Ethernet virtual pe care aţi selectat-o în timpul configurării partiţiei logice.
4. În ecranul Gestionare resurse de comunicaţie selectaţi opţiunea 5 (Gestionare descrieri de configurare) de lângă portul Ethernet virtual corespunzător şi apăsaţi Enter.
5. În ecranul Gestionare descrieri de configurare selectaţi opţiunea 1 (Creare) şi apăsaţi Enter pentru a vedea ecranul CRTLINETH (Create Line Description Ethernet - Creare descriere de linie Ethernet).
   a. Pentru promptul *Descriere de linie* tastaţi VETH0 . Numele VETH0, deşi arbitrar, corespunde coloanei cu numere din pagina Ethernet virtual în care aţi activat partiţia logică să comunice. Dacă folosiţi aceleaşi nume pentru descrierile de linie şi pentru reţelele lor Ethernet virtual asociate, puteţi ţine uşor evidenţa configuraţiilor dumneavoastră Ethernet virtual.
   b. Pentru promptul *Viteză linie* tastaţi 1G.
   c. Pentru promptul *Duplex* tastaţi *FULL şi apăsaţi Enter.
   d. Pentru promptul *Dimensiune maximă cadru* tastaţi 8996 şi apăsaţi Enter. Modificând dimensiunea cadru în 8996, transferul de date prin Ethernet virtual este îmbunătăţit.

      Veţi vedea un mesaj care spune că descrierea de linie a fost creată.
6. Activaţi descrierea de linie. Tastaţi WRKCFGSTS *LIN şi selectaţi opţiunea 1 (Activare) pentru VETH0.
7. Repetaţi paşii de la 1 la 6, dar efectuaţi paşii din linia de comandă din partiţia B pentru a crea o descriere de linie pentru partiţia B.

   Deşi numele descrierilor de linie sunt arbitrare, ajută să folosiţi aceleaşi nume pentru toate descrierile de linie asociate cu Ethernet virtual. În acest scenariu, toate descrierile de linie sunt numite VETH0.

Ce este de făcut în continuare

Activaţi înaintarea (forwarding) datagramelor IP

Crearea descrierilor de linie Ethernet pe orice servere în afară de modelele 270 şi 8xx

Pentru a configura noile descrieri de linie Ethernet să suporte Ethernet virtual, urmaţi aceşti paşi:

1. În linia de comandă din partiţia A, tastaţi WRKHDWRSC *CMN şi apăsaţi Enter.
2. În ecranul Gestionare resurse de comunicaţie selectaţi opţiunea 7 (Afişare detalii resursă) de lângă portul Ethernet virtual corespunzător.

Porturile Ethernet identificate drept 268C sunt resurse Ethernet virtual. Va exista câte unul pentru fiecare adaptor Ethernet virtual. Fiecare port identificat drept 268C are un cod de locaţie asociat care este creat când creaţi adaptorul Ethernet virtual folosind HMC (Pasul 1).

3. În ecranul Afişare detalii resursă derulaţi în jos pentru a găsi resursa 268C care este asociată cu codul de locaţie anume creat pentru acest Ethernet virtual.
4. În ecranul Gestionare resurse de comunicaţie selectaţi opţiunea 5 (Gestionare descrieri de configurare) de lângă resursa Ethernet virtual corespunzătoare şi apăsaţi Enter.
5. În ecranul Gestionare descrieri de configurare selectaţi opţiunea 1 (Creare) şi apăsaţi Enter pentru a vedea ecranul CRTLINETH (Create Line Description Ethernet - Creare descriere de linie Ethernet).
   a. Pentru promptul *Descriere de linie* tastaţi VETH0 . Dacă folosiţi aceleaşi nume pentru descrierile de linie şi pentru reţelele lor Ethernet virtual asociate, cum ar fi VETHO, puteţi ţine uşor evidenţa configuraţiilor dumneavoastră Ethernet virtual.
   b. Pentru promptul *Viteză linie*, tastaţi 1G.
   c. Pentru promptul *Duplex*, tastaţi *FULL şi apăsaţi Enter.
   d. Pentru promptul *Dimensiune maximă cadru*, tastaţi 8996 şi apăsaţi Enter. Modificând dimensiunea cadru în 8996, transferul de date prin Ethernet virtual este îmbunătăţit.

   Veţi vedea un mesaj care spune că descrierea de linie a fost creată.
6. Activaţi descrierea de linie. Tastaţi WRKCFGSTS *LIN şi selectaţi opţiunea 1 (Activare) pentru VETH0.
7. Repetaţi paşii de la 1 la 6, dar efectuaţi paşii din linia de comandă din partiţia B pentru a crea o descriere de linie pentru partiţia B.

   Deşi numele descrierilor de linie sunt arbitrare, ajută să folosiţi aceleaşi nume pentru toate descrierile de linie asociate cu Ethernet virtual. În acest scenariu, toate descrierile de linie sunt numite VETH0.

Ce este de făcut în continuare

Activaţi înaintarea (forwarding) datagramelor IP

Pasul 3: Activarea înaintării datagramelor IP

Activaţi înaintarea (forwarding) datagramelor IP, astfel încât pachetele să poată fi expediate de-a lungul diferitelor subreţele.

Pentru a activa înaintarea datagramelor IP, urmaţi aceşti paşi:

1. În linia de comandă din partiţia A, tastaţi CHGTCPA şi apăsaţi F4.
2. Pentru promptul *Înaintare datagramă IP*, tastaţi *YES.

Ce este de făcut în continuare

Creaţi interfeţele

Pasul 4: Crearea interfeţelor

Pentru a crea interfeţele TCP/IP, efectuaţi aceşti paşi:

1. Creaţi şi porniţi o interfaţă TCP/IP OS/400 în partiţia B pentru comunicaţia generală către şi de la server. Pentru a crea interfaţa, urmaţi aceşti paşi:
   a. În linia de comandă din partiţia B, tastaţi CFGTCP şi apăsaţi Enter pentru a vedea ecranul Configurare TCP/IP.
   b. Selectaţi opţiunea 1 (Gestionare interfeţe TCP/IP) şi apăsaţi Enter.
   c. Selectaţi opţiunea 1 (Adăugare) şi apăsaţi Enter pentru a vedea ecranul ADDTCPIFC (Add TCP/IP Interface - Adăugare interfaţă TCP/IP).
   d. Pentru promptul *Adresă internet*, tastaţi '10.1.1.2' .
   e. Pentru promptul *Descriere de linie*, tastaţi ETHLINE .
   f. Pentru promptul *Mască subreţea*, tastaţi '255.255.255.0'.

g. Porniţi interfaţa. În ecranul Gestionare interfeţe TCP/IP selectaţi opţiunea 9 (Pornire) de lângă interfaţă.

2. Creaţi şi porniţi altă interfaţă TCP/IP care se conectează la reţeaua externă. Ea ar trebui să folosească aceeaşi descriere de linie ca şi interfaţa dumneavoastră TCP/IP existentă. Această interfaţă va realiza în cele din urmă translatarea de adresă pentru partiţia dumneavoastră. Pentru a crea interfaţa, urmaţi aceşti paşi:
   a. În linia de comandă din partiţia B, tastaţi CFGTCP şi apăsaţi Enter pentru a vedea ecranul Configurare TCP/IP.
   b. Selectaţi opţiunea 1 (Gestionare interfeţe TCP/IP) şi apăsaţi Enter.
   c. Selectaţi opţiunea 1 (Adăugare) şi apăsaţi Enter pentru a vedea ecranul ADDTCPIFC (Add TCP/IP Interface - Adăugare interfaţă TCP/IP).
   d. Pentru promptul *Adresă internet*, tastaţi '10.1.1.3'.
   e. Pentru promptul *Descriere de linie*, tastaţi ETHLINE .
   f. Pentru promptul *Mască subreţea*, tastaţi '255.255.255.0'.
   g. Porniţi interfaţa. În ecranul Gestionare interfeţe TCP/IP selectaţi opţiunea 9 (Pornire) de lângă interfaţă.
3. Creaţi şi porniţi interfaţa TCP/IP OS/400 în partiţia A pentru Ethernet virtual. Pentru a crea interfaţa, urmaţi aceşti paşi:
   a. În linia de comandă din partiţia A, tastaţi CFGTCP şi apăsaţi Enter pentru a vedea ecranul Configurare TCP/IP.
   b. Selectaţi opţiunea 1 (Gestionare interfeţe TCP/IP) şi apăsaţi Enter.
   c. Selectaţi opţiunea 1 (Adăugare) şi apăsaţi Enter pentru a vedea ecranul ADDTCPIFC (Add TCP/IP Interface - Adăugare interfaţă TCP/IP).
   d. Pentru promptul *Adresă internet*, tastaţi '192.168.1.1' .
   e. Pentru promptul *Descriere de linie*, tastaţi VETH0 .
   f. Pentru promptul *Mască subreţea*, tastaţi '255.255.255.0'.
   g. Porniţi interfaţa. În ecranul Gestionare interfeţe TCP/IP selectaţi opţiunea 9 (Pornire) de lângă interfaţă.
4. Creaţi şi porniţi interfaţa TCP/IP OS/400 în partiţia B pentru Ethernet virtual. Pentru a crea interfaţa, urmaţi aceşti paşi:
   a. În linia de comandă din partiţia B, tastaţi CFGTCP şi apăsaţi Enter pentru a vedea ecranul Configurare TCP/IP.
   b. Selectaţi opţiunea 1 (Gestionare interfeţe TCP/IP) şi apăsaţi Enter.
   c. Selectaţi opţiunea 1 (Adăugare) şi apăsaţi Enter pentru a vedea ecranul ADDTCPIFC (Add TCP/IP Interface - Adăugare interfaţă TCP/IP).
   d. Pentru promptul *Adresă internet*, tastaţi '192.168.1.5' .
   e. Pentru promptul *Descriere de linie*, tastaţi VETH0 .
   f. Pentru promptul *Mască subreţea*, tastaţi '255.255.255.0'.
   g. Porniţi interfaţa. În ecranul Gestionare interfeţe TCP/IP selectaţi opţiunea 9 (Pornire) de lângă interfaţă.

Ce este de făcut în continuare

Verificarea comunicaţiilor în reţea

Pasul 5: Verificarea comunicaţiilor în reţea

Verificaţi comunicaţiile reţelei dumneavoastră folosind comanda ping:

- Din partiţia A, executaţi ping pentru interfaţa Ethernet virtual 192.168.1.5 şi pentru o gazdă externă.
- Dintr-o gazdă externă OS/400, executaţi ping pentru fiecare din interfeţele Ethernet virtual 192.168.1.1 şi 192.168.1.5.

Ce este de făcut în continuare

Creaţi reguli de pachet

Pasul 6: Crearea regulilor de pachet

Folosiţi vrăjitorul Translatare adresă din Navigator iSeries pentru a crea regulile de pachet care mapează adresa privată din partiţia A în adresă publică în partiţia B.

Pentru a crea regulile de pachet, urmaţi aceşti paşi:

1. În Navigator iSeries, expandaţi-vă serverul **iSeries –> Politici IP–> de reţea**.
2. Faceţi clic dreapta pe **Reguli de pachet** şi selectaţi **Editor reguli**.
3. Selectaţi **Translatare adresă** din meniul **vrăjitorului**.
4. Urmaţi instrucţiunile vrăjitorului pentru a crea regulile de pachet. Această procedură foloseşte următoarele selecţii:
   - Selectaţi **Translatare adresă prin mapare**
   - Introduceţi adresa IP privată 192.168.1.1
   - Introduceţi adresa IP publică 10.1.1.3
   - Selectaţi linia în care sunt configurate interfeţele, cum ar fi ETHLINE
5. Selectaţi **Activare reguli** din meniul **Fişier**.

Ce este de făcut în continuare

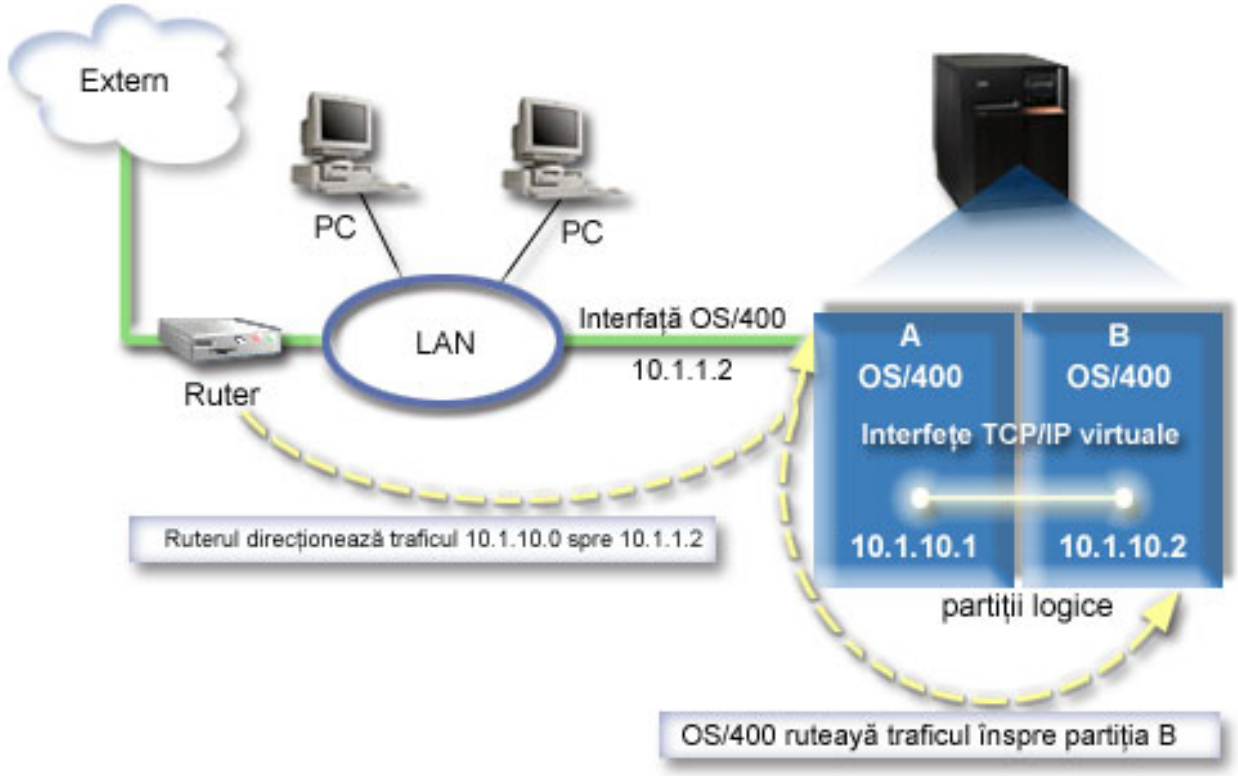
Verificaţi comunicaţiile în reţea

Pasul 7: Verificarea comunicaţiilor în reţea

După ce aţi creat regulile de pachet, trebuie să verificaţi comunicaţia reţelei. Pentru a testa comunicaţiile de ieşire, executaţi ping pentru o gazdă externă din partiţia A. Apoi, din acea gazdă externă, executaţi ping pentru partiţia A pentru a testa comunicaţiile de intrare.

Metoda de rutare TCP/IP

Puteţi de asemenea ruta traficul către partiţiile dumneavoastră prin serverul iSeries cu diverse tehnici de rutare. Această soluţie nu este dificil de configurat pe server dar, în funcţie de topologia reţelei dumneavoastră, este posibil să nu fie practică. Consultaţi următoarea ilustraţie.



Interfaţa TCP/IP existentă (10.1.1.2) se conectează la reţeaua LAN. Reţeaua LAN este conectată la reţele la distanţă printr-un ruter. Interfaţa TCP/IP virtuală din partiţia B este adresată drept 10.1.10.2, iar interfaţa TCP/IP virtuală din partiţia A drept 10.1.10.1. În OS/400, dacă activaţi înainatarea datagramelor IP, OS/400 va ruta pachetele IP către şi dinspre partiţia B. Când vă definiţi conexiunea TCP/IP pentru partiţia B, adresa ruterului trebuie să fie 10.1.10.1.

Dificultatea acestui tip de rutare este trimiterea pachetelor IP către iSeries. În acest scenariu, aţi putea defini o rută în ruter care să transmită pachetele destinate reţelei 10.1.10.0 către interfaţa 10.1.1.2. Aceasta funcţionează pentru clienţii de reţea la distanţă. Ar funcţiona de asemenea şi pentru clienţii reţelei LAN locale (clienţii conectaţi la aceeaşi reţea LAN ca şi iSeries) dacă ei ar recunoaşte acel ruter drept următorul lor hop. Dacă nu fac acest lucru, atunci fiecare client trebuie să aibă o rută care direcţionează traficul 10.1.10.0 către interfaţa 10.1.1.2 OS/400; de aici porneşte aspectul nepractic al acestei metode. Dacă aveţi mulţi clienţi LAN, atunci trebuie să definiţi multe rute.

Pentru a configura Ethernet virtual pentru a folosi metoda de rutare TCP/IP, folosiţi următoarele instrucţiuni:

1. Activaţi partiţiile logice să participe într-o reţea Ethernet virtual
2. Creaţi descrierile de linie Ethernet
3. Activaţi înaintarea (forwarding) datagramelor IP
4. Creaţi interfeţele

Pasul 1: Activarea partiţiilor logice pentru a participa într-o reţea Ethernet virtual

Notă: Dacă folosiţi alte modele de servere în afară de modelele 270 şi 8*xx*, trebuie să efectuaţi acest pas folosind consola Hardware Management Console pentru eServer (HMC) în locul partiţiei primare. Vedeţi Ethernet virtual pentru detalii.

Pentru a activa Ethernet virtual, parcurgeţi paşii următori:

1. În linia de comandă din partiţia primară (partiţia A), tastaţi STRSST şi apăsaţi Enter.
2. Tastaţi ID-ul dumneavoastră de utilizator de unelte de service şi parola.
3. În ecranul SST (System Service Tools - Unelte de service sistem), selectaţi opţiunea 5 (Gestionare partiţii sistem).
4. În ecranul Gestionare partiţii sistem, selectaţi opţiunea 3 (Gestionare configuraţie partiţie).
5. Apăsaţi F10 (Gestionare Ethernet virtual).
6. Tastaţi 1 în coloana corespunzătoare partiţiei A şi partiţiei B, pentru a permite partiţiilor să comunice una cu cealaltă prin Ethernet virtual.
7. Ieşiţi din SST (System Service Tools - Unelte de service sistem), pentru a vă întoarce la linia de comandă.

Ce este de făcut în continuare

Crearea descrierilor de linie Ethernet

Pasul 2: Crearea descrierilor de linie Ethernet

Trebuie să efectuaţi acest pas într-unul dintre cele două moduri, în funcţie de modelul de server pe care îl folosiţi. Alegeţi una dintre aceste metode de creare a descrierilor de linie în funcţie de modelul dumneavoastră de server.

- Crearea descrierilor de linie Ethernet pe modelele de servere 270 şi 8*xx*
- Crearea descrierilor de linie Ethernet pe orice servere în afară de modelele 270 şi 8xx

Crearea descrierilor de linie Ethernet pe serverele model 270 şi 8*xx*

Pentru a configura noile descrieri de linie Ethernet să suporte Ethernet virtual, urmaţi aceşti paşi:

1. În linia de comandă din partiţia A, tastaţi WRKHDWRSC *CMN şi apăsaţi Enter.
2. În ecranul Gestionare resurse de comunicaţie selectaţi opţiunea 7 (Afişare detalii resursă) de lângă portul Ethernet virtual corespunzător.

   Portul Ethernet identificat drept 268C este resursa Ethernet virtual. Va exista câte unul pentru fiecare Ethernet virtual care este conectat la partiţia logică.
3. În ecranul Afişare detalii resursă, derulaţi în jos pentru a găsi adresa de port. Adresa de port corespunde cu reţeaua Ethernet virtual pe care aţi selectat-o în timpul configurării partiţiei logice.
4. În ecranul Gestionare resurse de comunicaţie selectaţi opţiunea 5 (Gestionare descrieri de configurare) de lângă portul Ethernet virtual corespunzător şi apăsaţi Enter.
5. În ecranul Gestionare descrieri de configurare selectaţi opţiunea 1 (Creare) şi apăsaţi Enter pentru a vedea ecranul CRTLINETH (Create Line Description Ethernet - Creare descriere de linie Ethernet).
   a. Pentru promptul *Descriere de linie* tastaţi VETH0 . Numele VETH0, deşi arbitrar, corespunde coloanei cu numere din pagina Ethernet virtual în care aţi activat partiţia logică să comunice. Dacă folosiţi aceleaşi nume pentru descrierile de linie şi pentru reţelele lor Ethernet virtual asociate, puteţi ţine uşor evidenţa configuraţiilor dumneavoastră Ethernet virtual.
   b. Pentru promptul *Viteză linie*, tastaţi 1G.
   c. Pentru promptul *Duplex*, tastaţi *FULL şi apăsaţi Enter.
   d. Pentru promptul *Dimensiune maximă cadru*, tastaţi 8996 şi apăsaţi Enter. Modificând dimensiunea cadru în 8996, transferul de date prin Ethernet virtual este îmbunătăţit.

   Veţi vedea un mesaj care spune că descrierea de linie a fost creată.
6. Activaţi descrierea de linie. Tastaţi WRKCFGSTS *LIN şi selectaţi opţiunea 1 (Activare) pentru VETH0.

7. Repetaţi paşii de la 1 la 6, dar efectuaţi paşii din linia de comandă din partiţia B pentru a crea o descriere de linie pentru partiţia B.

   Deşi numele descrierilor de linie sunt arbitrare, ajută să folosiţi aceleaşi nume pentru toate descrierile de linie asociate cu Ethernet virtual. În acest scenariu, toate descrierile de linie sunt numite VETH0.

Ce este de făcut în continuare

Activaţi înaintarea (forwarding) datagramelor IP

Crearea descrierilor de linie Ethernet pe orice servere în afară de modelele 270 şi 8xx

Pentru a configura noile descrieri de linie Ethernet să suporte Ethernet virtual, urmaţi aceşti paşi:

1. În linia de comandă din partiţia A, tastaţi WRKHDWRSC *CMN şi apăsaţi Enter.
2. În ecranul Gestionare resurse de comunicaţie selectaţi opţiunea 7 (Afişare detalii resursă) de lângă portul Ethernet virtual corespunzător.

   Porturile Ethernet identificate drept 268C sunt resurse Ethernet virtual. Va exista câte unul pentru fiecare adaptor Ethernet virtual. Fiecare port identificat drept 268C are un cod de locaţie asociat care este creat când creaţi adaptorul Ethernet virtual folosind HMC (Pasul 1).
3. În ecranul Afişare detalii resursă derulaţi în jos pentru a găsi resursa 268C care este asociată cu codul de locaţie anume creat pentru acest Ethernet virtual.
4. În ecranul Gestionare resurse de comunicaţie selectaţi opţiunea 5 (Gestionare descrieri de configurare) de lângă resursa Ethernet virtual corespunzătoare şi apăsaţi Enter.
5. În ecranul Gestionare descrieri de configurare selectaţi opţiunea 1 (Creare) şi apăsaţi Enter pentru a vedea ecranul CRTLINETH (Create Line Description Ethernet - Creare descriere de linie Ethernet).
   a. Pentru promptul *Descriere de linie* tastaţi VETH0 . Dacă folosiţi aceleaşi nume pentru descrierile de linie şi pentru reţelele lor Ethernet virtual asociate, cum ar fi VETHO, puteţi ţine uşor evidenţa configuraţiilor dumneavoastră Ethernet virtual.
   b. Pentru promptul *Viteză linie*, tastaţi 1G.
   c. Pentru promptul *Duplex*, tastaţi *FULL şi apăsaţi Enter.
   d. Pentru promptul *Dimensiune maximă cadru*, tastaţi 8996 şi apăsaţi Enter. Modificând dimensiunea cadru în 8996, transferul de date prin Ethernet virtual este îmbunătăţit.

   Veţi vedea un mesaj care spune că descrierea de linie a fost creată.
6. Activaţi descrierea de linie. Tastaţi WRKCFGSTS *LIN şi selectaţi opţiunea 1 (Activare) pentru VETH0.
7. Repetaţi paşii de la 1 la 6, dar efectuaţi paşii din linia de comandă din partiţia B pentru a crea o descriere de linie pentru partiţia B.

   Deşi numele descrierilor de linie sunt arbitrare, ajută să folosiţi aceleaşi nume pentru toate descrierile de linie asociate cu Ethernet virtual. În acest scenariu, toate descrierile de linie sunt numite VETH0.

Ce este de făcut în continuare

Activaţi înaintarea (forwarding) datagramelor IP

Pasul 3: Activarea înaintării datagramelor IP

Activaţi înaintarea (forwarding) datagramelor IP, astfel încât pachetele să poată fi expediate de-a lungul diferitelor subreţele.

Pentru a activa înaintarea datagramelor IP, urmaţi aceşti paşi:

1. În linia de comandă din partiţia A, tastaţi CHGTCPA şi apăsaţi F4.
2. Pentru promptul *Înaintare datagramă IP*, tastaţi *YES.

Ce este de făcut în continuare

Pasul 4: Crearea interfeţelor

Pentru a crea interfeţele TCP/IP, efectuaţi aceşti paşi:

1. Creaţi o interfaţă TCP/IP OS/400 în partiţia A. Pentru a crea interfaţa, urmaţi aceşti paşi:
   a. În linia de comandă din partiţia A, tastaţi CFGTCP şi apăsaţi Enter pentru a vedea ecranul Configurare TCP/IP.
   b. Selectaţi opţiunea 1 (Gestionare interfeţe TCP/IP) şi apăsaţi Enter.
   c. Selectaţi opţiunea 1 (Adăugare) şi apăsaţi Enter pentru a vedea ecranul ADDTCPIFC (Add TCP/IP Interface - Adăugare interfaţă TCP/IP).
   d. Pentru promptul *Adresă internet*, tastaţi '10.1.1.2' .
   e. Pentru promptul *Descriere de linie* tastaţi numele descrierii dumneavoastră de linie, cum ar fi ETHLINE.
   f. Pentru promptul *Mască subreţea*, tastaţi '255.255.255.0'.
2. Porniţi interfaţa. În ecranul Gestionare interfeţe TCP/IP selectaţi opţiunea 9 (Pornire) de lângă interfaţă.
3. Repetaţi paşii 2 şi 3 pentru a crea şi porni interfeţele TCP/IP în partiţiile A şi B.

   Aceste interfeţe sunt folosite pentru Ethernet virtual. Folosiţi adresele IP 10.1.10.1 şi 10.1.10.2 pentru aceste interfeţe şi masca de subreţea 255.255.255.0.

Considerente Ethernet virtual

Puteţi folosi Ethernet virtual ca o alternativă la folosirea unei plăci de reţea pentru comunicaţia între partiţii. El vă permite să stabiliţi comunicaţii de mare viteză între partiţiile logice fără a cumpăra hardware suplimentar. Pentru fiecare din cele 16 porturi activate, sistemul crează un port de comunicaţie Ethernet virtual, cum ar fi CMN*xx* cu tipul de resursă 268C. Partiţiile logice alocate aceleiaşi reţele LAN devin atunci disponibile pentru comunicarea prin acea legătură. Un sistem fizic vă permite să configuraţi până la 16 reţele LAN virtuale diferite. Ethernet virtual furnizează aceeaşi funcţie ca şi când aţi folosi un adaptor Ethernet de 1 Gb. Reţelele locale Token Ring şi Ethernet 10 Mbps şi 100 Mbps nu sunt suportate cu Ethernet virtual.

Ethernet virtual este o soluţie economică de reţea care furnizează avantaje substanţiale:

- Economic: Nu este necesar aproape nici un hardware de reţea suplimentar. Puteţi adăuga partiţii la server şi puteţi comunica şi cu o reţea LAN externă fără a instala plăci LAN fizice suplimentare. Dacă serverul curent are sloturi de plăci disponibile limitate în care să instalaţi plăci LAN suplimentare, atunci folosirea Ethernet virtual oferă capabilitatea de a utiliza partiţii ataşate la reţeaua LAN fără a fi necesar să modernizaţi serverul.
- Flexibil: Este posibil să configuraţi un număr maxim de 16 conexiuni distincte care să activeze configuraţia căilor de comunicaţie selectivă între partiţii. Pentru o mai mare flexibilitate, modelul de configurare permite partiţiilor logice să implementeze atât o conexiune Ethernet virtual, cât şi o conexiune LAN fizică. Aceasta este o caracteristică de dorit la utilizarea partiţiei Linux la găzduirea unei aplicaţii firewall.
- Rapid: Ethernet virtual emulează o conexiune Ethernet de 1 GO şi furnizează o metodă de comunicaţie rapidă şi convenabilă între partiţii. Aceasta îmbunătăţeşte oportunitatea de a integra aplicaţii separate care rulează pe partiţii logice diferite.
- Multilateral: Indiferent dacă partiţiile dumneavoastră funcţionează în OS/400 sau în Linux, ele pot fi toate conectate la acelaşi Ethernet virtual.
- Aglomerare redusă: Folosind Ethernet virtual pentru comunicaţia între partiţii, traficul de comunicaţie este redus în reţeaua LAN externă. În cazul Ethernet, care este un standard bazat pe coliziuni, aceasta va ajuta desigur la împiedicarea degradării service-ului pentru alţi utilizatori LAN.

Capitolul 9. Informaţii înrudite pentru setarea TCP/IP

Acum, că serverul dumneavoastră este pornit şi funcţional, vă puteţi întreba ″Ce altceva mai pot realiza cu serverul meu?″ Mai jos sunt prezentate manuale şi cărţi IBM Redbooks (în format PDF) şi subiectul din Centrul de informare care tratează setarea TCP/IP. Puteţi vizualiza sau tipări PDF-urile. Folosiţi referinţele următoare pentru a configura cel mai bine TCP/IP pe serverul dumneavoastră iSeries :

Manuale

- **Configurarea TCP/IP şi referinţe** (592 KO)
  Această carte furnizează informaţii despre configurarea TCP/IP şi operarea şi utilizarea reţelei dumneavoastră.
- **Indicii şi unelte pentru securizarea sistemului iSeries** (1 MO)
  Această carte oferă recomandări de bază pentru utilizarea opţiunilor de securitate ale iSeries pentru a vă proteja serverul şi operaţiile lui asociate.

Cărţi roşii

- **TCP/IP Tutorial and Technical Overview** (7 MB)
  Această carte oferă informaţii de bază despre TCP/IP.
- **TCP/IP for AS/400 : More Cool Things Than Ever** (9 MB)
  Această carte include o listă întinsă de aplicaţii obişnuite TCP/IP şi servicii.

IPv6

- **The Internet Engineering Task Force (IETF)** (http://www.ietf.cnri.reston.va.us/)
  Învăţaţi despre grupul de indivizi care dezvoltă protocolul Internet, inclusiv IPv6.
- **IP Versiunea 6 (IPv6)** (http://playground.sun.com/pub/ipng/html/ipng-main.html)
  Găsiţi specificaţiile IPv6 curente şi trimiteri la mai multe surse despre IPv6.
- **Forum IPv6**(http://www.ipv6forum.com/)
  Găsiţi articole noi şi evenimente privind ultimele modificări din IPv6.

Alte informaţii

- **TCP/IP**
  Acest subiect conţine informaţii despre aplicaţiile şi serviciile TCP/IP, diferite de cele privind configurarea.

Pentru a salva un PDF pe staţia de lucru proprie pentru vizualizare sau tipărire:

1. Faceţi clic dreapta pe PDF în browser-ul dumneavoastră (clic dreapta pe legătura de mai sus).
2. Faceţi clic pe **Salvare destinaţie ca...**.
3. Navigaţi în directorul în care doriţi să salvaţi fişierul PDF.
4. Selectaţi **Salvare**.

Dacă aveţi nevoie de Adobe Acrobat Reader pentru a vedea sau tipări aceste PDF-uri, puteţi descărca o copie de pe situl Web Adobe (www.adobe.com/prodindex/acrobat/readstep.html) .

Partea 2. Anexe

Anexa. Observaţii

Aceste informaţii au fost elaborate pentru produse şi servicii oferite în S.U.A.

Este posibil ca IBM să nu ofere în alte ţări produsele, serviciile sau caracteristicile discutate în acest document. Luaţi legătura cu reprezentantul IBM local pentru informaţii despre produsele şi serviciile disponibile în zona dumneavoastră. Referirea la un produs, program sau serviciu IBM nu înseamnă că se afirmă sau că se sugerează faptul că poate fi folosit numai acel produs, program sau serviciu IBM. Poate fi folosit în loc orice produs, program sau serviciu care este echivalent din punct de vedere funcţional şi care nu încalcă dreptul de proprietate intelectuală al IBM. Însă evaluarea şi verificarea modului în care funcţionează un produs, program sau serviciu non-IBM ţine de responsabilitatea utilizatorului.

IBM poate avea brevete sau aplicaţii în curs de brevetare care să acopere subiectele descrise în acest document. Faptul că vi se furnizează acest document nu înseamnă că vi se acordă licenţa pentru aceste brevete. Puteţi trimite întrebări cu privire la licenţe, în scris, la:

| IBM Director of Licensing
| IBM Corporation
| North Castle Drive
| Armonk, NY 10504-1785
| U.S.A.

Pentru întrebări privind licenţa pentru informaţiile DBCS (double-byte character set), contactaţi departamentul de Proprietate intelectuală al IBM-ului din ţara dumneavoastră sau trimiteţi întrebările în scris la:

| IBM World Trade Asia Corporation
| Licensing
| 2-31 Roppongi 3-chome, Minato-ku
| Tokyo 106-0032, Japan

Următorul paragraf nu se aplică în cazul Marii Britanii sau al altor ţări unde asemenea prevederi nu sunt în concordanţă cu legile locale: INTERNATIONAL BUSINESS MACHINES CORPORATION OFERĂ ACEASTĂ PUBLICAŢIE “CA ATARE”, FĂRĂ NICI UN FEL DE GARANŢIE, EXPRIMATĂ SAU PRESUPUSĂ, INCLUSIV, DAR NELIMITÂNDU-SE LA ELE, GARANŢIILE IMPLICITE DE NEÎNCĂLCARE A UNOR DREPTURI SAU NORME, DE VANDABILITATE SAU DE POTRIVIRE LA UN ANUMIT SCOP. Unele state nu permit declinarea responsabilităţii pentru garanţiile exprese sau implicite în anumite tranzacţii şi de aceea este posibil ca aceste clauze să nu fie valabile în cazul dumneavoastră.

Aceste informaţii pot include inexactităţi tehnice sau erori tipografice. Se efectuează modificări periodice la informaţiile incluse aici; aceste modificări vor fi încorporate în noi ediţii ale publicaţiei. IBM poate aduce îmbunătăţiri şi/sau modifcări produsului (produselor) şi/sau programului (programelor) descrise în această publicaţie în orice moment, fără notificare.

Referirile din aceste informaţii la adrese de situri Web non-IBM sunt făcute numai pentru a vă ajuta, fără ca prezenţa lor să însemne un gir acordat acestor situri Web. Materialele de pe siturile Web respective nu fac parte din materialele pentru acest produs IBM, iar utilizarea acestor situri Web se face pe propriul risc.

| IBM poate utiliza sau distribui oricare dintre informaţiile pe care le furnizaţi, în orice mod considerat adecvat, fără ca
| aceasta să implice vreo obligaţie pentru dumneavoastră.

Posesorii de licenţe pentru acest program care doresc să aibă informaţii despre el în scopul de a permite: (I) schimbul de informaţii între programe create independent şi alte programe (inclusiv acesta) şi (II) utilizarea mutuală a informaţiilor care au fost schimbate, vor contacta:

| IBM Corporation

Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Aceste informaţii pot fi disponibile cu condiţia repectării termenilor şi condiţiilor, iar în unele cazuri cu plata unor taxe.

Programul licenţiat descris în aceste informaţii şi toate materialele licenţiate disponibile pentru el sunt furnizate de către IBM conform termenilor din IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code sau orice acord echivalent încheiat între noi.

Toate datele de performanţă din acest document au fost determinate într-un mediu controlat. De aceea, rezultatele obţinute în alte medii de funcţionare pot fi diferite. Unele măsurători s-ar putea să fi fost făcute pe sisteme la nivel de dezvoltare şi nu există nici o garanţie că aceste măsurători vor fi identice pe sistemele disponibile pe piaţă. Mai mult de atât, unele măsurători s-ar putea să fi fost estimate prin extrapolare. Rezultatele reale pot fi diferite. Utilizatorii acestui document trebuie să verifice datele aplicabile pentru mediul lor specific.

Informaţiile privind produsele non-IBM au fost obţinute de la furnizorii acestor produse, din anunţurile lor publicate sau din alte surse disponibile publicului. IBM nu a testat aceste produse şi nu poate confirma acurateţea performanţelor, compatibilitatea sau oricare alte pretenţii legate de produsele non-IBM. Întrebările legate de capacităţile produselor non-IBM le veţi adresa furnizorilor acestor produse.

Toate declaraţiile privind direcţiile de viitor şi intenţiile IBM-ului pot fi schimbate sau se poate renunţa la ele, fără notificare prealabilă şi reprezintă doar scopuri şi obiective.

Aceste informaţii conţin exemple de date şi rapoarte folosite în operaţiile comerciale de zi cu zi. Pentru a fi cât mai complete, exemplele includ nume de persoane, de companii, de mărci şi de produse. Toate aceste nume sunt fictive şi orice asemănare cu nume sau adrese folosite de o întreprindere reală este pură coincidenţă.

Dacă vizualizaţi aceste informaţii folosind o copie electronică, fotografiile şi ilustraţiile color s-ar putea să nu apară.

Mărci comerciale

Următorii termeni sunt mărci comerciale deţinute de International Business Machines Corporation în Statele Unite, în alte ţări sau ambele:

AS/400
e(logo)server
eServer
IBM
iSeries
OS/400
Redbooks

Microsoft, Windows, Windows NT şi logo-ul Windows sunt mărci comerciale deţinute de Microsoft Corporation în Statele Unite, în alte ţări sau ambele.

Alte nume de companii, produse şi servicii ar putea fi mărci comerciale sau mărci de serviciu ale altora.

Termeni şi condiţii pentru descărcarea şi tipărirea publicaţiilor

Permisiunile pentru folosirea informaţiilor pe care le-aţi selectat pentru descărcare sunt acordate în următorii termeni şi condiţii şi cu indicarea acceptării lor de către dumneavoastră.

Uz personal: Puteţi reproduce aceste informaţii pentru uzul dumneavoastră personal şi necomercial cu condiţia ca toate anunţurile de proprietate să fie păstrate. Nu puteţi distribui, afişa sau face lucrări derivate din aceste informaţii sau orice porţiune a lor, fără acordul explicit al IBM.

Uz comercial: Puteţi reproduce, distribui şi afişa aceste informaţii doar în întreprinderea dumneavoastră cu condiţia ca toate anunţurile de proprietate să fie păstrate. Nu puteţi face lucrări derivate din aceste informaţii sau să reproduceţi, să distribuiţi sau să afişaţi aceste informaţii sau orice porţiune a lor în afara întreprinderii dumneavoastră, fără acordul explicit al IBM.

Cu excepţia acestei permisiuni explicite, nici o altă permisiune, licenţă sau drepturi nu sunt acordate, fie explicite sau implicite, pentru informaţii sau alte date, software sau alte proprietăţi intelectuale conţinute în acestea.

IBM îşi rezervă dreptul de a retrage permisiunile acordate aici oricând consideră că folosirea informaţiilor este în detrimentul intereselor sale sau când personalul IBM constată că instrucţiunile de mai sus nu sunt urmate corespunzător.

Nu puteţi descărca, exporta sau reexporta aceste informaţii decât în deplină conformitate cu legile şi regulamentele aplicabile, inclusiv toate legile şi regulamentele de export ale Statelor Unite. IBM NU ACORDĂ NICI O GARANŢIE PENTRU CONŢINUTUL ACESTOR INFORMAŢII. INFORMAŢIILE SUNT FURNIZATE ″CA ATARE″ ŞI FĂRĂ NICI UN FEL DE GARANŢIE, EXPLICITĂ SAU IMPLICITĂ, INCLUZÂND, DAR FĂRĂ A SE LIMITA LA ELE, GARANŢIILE SUBÎNŢELESE DE NEÎNCĂLCARE A UNUI DREPT, DE VANDABILITATE SAU DE POTRIVIRE PENTRU UN ANUMIT SCOP.

Toate materialele au copyright IBM Corporation.

Prin descărcarea sau tipărirea de informaţii de pe acest sit, v-aţi dat acordul pentru aceşi termeni şi aceste condiţii.

Tipărit în S.U.A.