eNetwork Communications Server
Versione 6.0
per Windows NT

Guida per il responsabile di rete

Versione 6.0

SC13-2794-00

eNetwork Communications Server
Versione 6.0
per Windows NT

Guida per il responsabile di rete

Versione 6.0

SC13-2794-00

Nota:

Prima di utilizzare questo prodotto e le relative informazioni, leggere le informazioni riportate nella sezione “Informazioni particolari” a pagina xiii.

Prima edizione (giugno 1998)

Questa edizione fa riferimento alla Versione 6.0 dell'IBM eNetwork Communications Server per Windows NT e a tutti i rilasci e le modifiche successive, se non diversamente specificato in nuove edizioni.

Richieste di ulteriori copie di questo prodotto vanno indirizzate ad un rivenditore autorizzato o ad un rappresentante commerciale IBM. Tali copie non sono disponibili all'indirizzo riportato di seguito.

Come ultima pagina del manuale è stato predisposto un foglio riservato ai commenti del lettore. Se il modulo è stato rimosso, indirizzare i commenti alla:

SELFIN S.p.A.
Translation Assurance
Via F. Giordani, 7
80122 NAPOLI

Tutti i commenti ed i suggerimenti inviati possono essere utilizzati dalla IBM e dalla Selfin e diventeranno esclusiva delle stesse.

Indice

Figure

Tabelle

Informazioni particolari

I riferimenti contenuti in questa pubblicazione relativi a prodotti, programmi o servizi IBM non implicano che l'IBM intenda renderli disponibili in tutti i paesi in cui opera. Qualsiasi riferimento a programmi su licenza d'uso o ad altri prodotti o servizi IBM contenuto in questa pubblicazione non significa che soltanto tali programmi e/o prodotti possano essere usati. In sostituzione a quelli forniti dall'IBM, possono essere usati prodotti, programmi o servizi funzionalmente equivalenti che non comportino violazione dei diritti di proprietà intellettuale o di altri diritti dell'IBM. E' responsabilità dell'utente valutare e verificare la possibilità di utilizzare altri programmi e/o prodotti, fatta eccezione per quelli espressamente indicati dall'IBM.

L'IBM può avere brevetti o domande di brevetto in corso relativi a quanto trattato nella presente pubblicazione. La fornitura di questa pubblicazione non implica la concessione di alcuna licenza su di essi. Chi desiderasse ricevere informazioni relative a licenze può rivolgersi per iscritto a:

Director of Commercial Relations IBM Europe
Schoenaicher Str. 220
D-7030 Boeblingen
Deutschland

Coloro che detengono la licenza su questo programma e desiderano avere informazioni su di esso allo scopo di consentire: (i) uno scambio di informazioni tra programmi indipendenti ed altri (compreso questo) e (ii) l'uso reciproco di tali informazioni, dovrebbe rivolgersi a:

Site Counsel
Schoenaicher Str. 220
P.O. Box 12195
3039 Cornwallis Road
Research Triangle Park, NC 27709-2195

Queste informazioni possono essere rese disponibili, secondo condizioni contrattuali appropriate, compreso, in alcuni casi, l'addebito di un canone.

Il programma su licenza descritto in questo manuale e tutto il materiale su licenza ad esso relativo sono forniti dall'IBM nel rispetto delle condizioni previste dalla licenza d'uso.

QUESTO DOCUMENTO E' FORNITO "AS IS", SENZA ALCUNA GARANZIA ESPLICITA O IMPLICITA, IVI INCLUSE EVENTUALI GARANZIE DI COMMERCIABILITA' ED IDONEITA' AD UNO SCOPO PARTICOLARE. Alcune nazioni non escludono le garanzie implicite; di conseguenza la suddetta esclusione potrebbe, in questo caso, non essere applicabile.

Informazioni sul manuale

IBM eNetwork Communications Server per Windows NT (a cui si fa riferimento in questo manuale come *Communications Server*) è una piattaforma per i servizi di comunicazione. Questa piattaforma fornisce una grande varietà di servizi per le stazioni di lavoro Windows NT che comunicano con i computer host e con altre stazioni di lavoro. Gli utenti di Communications Server possono scegliere tra diverse opzioni di collegamento remoto.

La *Guida per il responsabile di rete* viene fornita come riferimento per la pianificazione e la gestione per gli utenti che utilizzano o intendono utilizzare Communications Server. Questo manuale risulterà utile al personale che si occupa della gestione, al personale tecnico e di supporto, ai coordinatori dei servizi, al personale IBM ed anche ai responsabili dei sistemi informativi. Esso fornisce una panoramica delle funzioni di Communications Server ed i passi richiesti per la creazione delle configurazioni di Communications Server per le stazioni di lavoro supportate.

Si presuppone che l'utente utilizzi Windows NT 4.0 Server come sistema operativo di base.

Utilizzo del manuale

La *Guida per il responsabile di rete* consente di eseguire la pianificazione richiesta per l'installazione e la configurazione di una rete di stazioni di lavoro. Esso fornisce istruzioni per la:

- Pianificazione di una rete
- Selezione degli strumenti di configurazione ed installazione
- Creazione di un file maschera per la configurazione
- Implementazione della pianificazione della rete
- Gestione della rete

L'impostazione di una rete di stazioni di lavoro richiede una pianificazione attenta e completa. Per creare una rete, è necessario conoscere quanto segue:

- I nomi delle stazioni di lavoro, i nomi di profilo, i nomi dei file di configurazione e gli altri nomi presenti nella rete
- L'ubicazione del focal point per l'inoltro delle segnalazioni
- Le stazioni di lavoro a disposizione che è possibile continuare ad utilizzare e la quantità di nuove stazioni di lavoro necessarie
- Il ruolo che si desidera attribuire a ciascuna stazione di lavoro inclusa nella rete
- Il pacchetto da installare su ciascuna stazione di lavoro per soddisfare il ruolo ad essa assegnato.
- Le risorse hardware e software a disposizione che si desidera conservare ed aggiornare
- Le nuove risorse hardware e software necessarie per implementare la pianificazione della rete

- Il metodo per la gestione della rete e delle relative risorse
- Il numero ed il tipo di collegamenti host e le stazioni di lavoro da collegare agli host mediante il gateway e la relativa definizione

I passi illustrati nella sezione “Implementazione delle configurazioni Communicati” a pagina 183 forniscono una procedura che consente di stabilire queste informazioni relative alla rete. Se si dispone già di una procedura corretta, è possibile utilizzarla ma, prima di farlo, si consiglia di consultare la procedura riportata nel capitolo.

Convenzioni utilizzate in questo manuale

Nel manuale vengono utilizzate le convenzioni riportate di seguito.

Convenzioni relative al testo

Grassetto	Il grassetto indica quanto segue: • Verb, funzioni, parole chiavi e parametri che è possibile utilizzare in un programma oppure ad una richiesta comandi. Questi valori sono sensibili alle maiuscole/minuscole e devono essere immessi così come appaiono nel testo. • I nomi di controlli di finestre, come elenchi, caselle di controllo, campi di immissione, pulsanti ed opzioni di menu.
Corsivo	Il corsivo indica quanto segue: • Una variabile per la quale l'utente deve fornire un valore. • Titoli di pubblicazioni. • Una lettera viene utilizzata come lettera o una parola viene utilizzata come parola. **Esempio**: Quando viene riportato *a*, verificare che non rappresenti la preposizione *a*.
Corsivo grassetto	Il corsivo grassetto viene utilizzato per enfatizzare una parola.
UPPERCASE	Le lettere maiuscole indicano costanti, nomi di file ed opzioni che è possibile utilizzare in un programma oppure ad una richiesta comandi. Questi valori possono essere immessi con lettere maiuscole o minuscole.
Doppi apici	I doppi apici indicano i messaggi visualizzati in una finestra. Un esempio è rappresentato dai messaggi che vengono visualizzati nell'OIA (operator information area) di una sessione di emulazione.
`Esempio`	L'esempio indica le informazioni che è necessario immettere ad una richiesta comandi o in una finestra.

Convenzioni numeriche

Numeri binari	Vengono rappresentati come B'xxxx xxxx' o B'x' tranne che in alcuni esempi in cui vengono rappresentate nel formato testo (“Un valore binario xxxx xxxx è...”).
Posizione dei bit	Iniziano con 0 partendo dall'estrema destra (bit meno significativo).
Numeri decimali	I numero decimali composti da più di 4 cifre vengono rappresentati con lo stile metrico. Per separare i gruppi composti da 3 cifre, viene utilizzato uno spazio invece di una virgola. Ad esempio, il numero sedicimilacentoquarantasette viene scritto 16 147.
Numeri esadecimali	Vengono rappresentati nel formato testo come hex xxxx oppure X'xxxx' (“L'indirizzo del nodo adiacente è hex 5D, che viene specificato come X'5D'.”)

Reperimento delle informazioni

Per ulteriori informazioni, consultare la *Guida operativa* che contiene una descrizione completa della libreria di Communications Server e delle relative pubblicazioni.

L'home page di Communications Server disponibile su Internet contiene informazioni generali sul prodotto ed informazioni di servizio relative all'APAR ed alle correzioni. E' possibile accedere alla home page nei due modi seguenti:

1. In Communications Server, selezionare l'icona **Access Home Page**
2. Utilizzando un browser Internet, consultare il seguente URL:

   http://www.software.ibm.com/enetwork/commserver/about/csnt.html

Panoramica

Introduzione alle funzioni di Communications Server

Questo capitolo fornisce una panoramica delle funzioni per le comunicazioni supportate da Communications Server e dei metodi attraverso i quali configurare i sistemi per eseguire queste funzioni. I capitoli finali di questa pubblicazione descrivono più dettagliatamente le funzioni ed i metodi di configurazione.

Funzioni supportate

In questa sezione vengono descritte le seguenti funzioni di Communications Server:

- Supporto delle comunicazioni SNA
- APPC (Advanced Program-to-Program Communications), che include APPN (Advanced Peer-to-Peer Networking)
- API (application programming interface) a 32 bit
  - CPI-C
  - APPC
  - LUA RUI
  - LUA SLI sul server
  - API per servizi di gestione
  - API per servizi comuni
  - API per operazioni nodo
- HPR (High performance routing)
- Compressione dati SNA
- Discovery dei fornitori di servizi
- LUA (LU application) convenzionale
- DLUR (Dependent logical unit requester)
- Gateway SNA
- Supporto AnyNet
  - SNA Anynet su TCP/IP (nodo di accesso e gateway)
  - Socket AnyNet su SNA (nodo di accesso e gateway)
- Server TN3270E
- Server TN5250
- Accesso ai dati legacy
  - AS/400 OLE DB provider
  - Host Publisher
  - Server delle cartelle condivise AS/400
- Supporto client API SNA
- Supporto client Novell IntranetWare per SAA
- Supporto della configurazione e della gestione
- Distribuzione del carico
- Sicurezza dati

- Supporto adattatore
- Supporto DLC (Data Link Control)
- Supporto APPN MIB
- Hot Standby
- Funzioni di emulazione di base

Supporto delle comunicazioni SNA

Communications Server può agire come nodo SNA (Systems Network Architecture) 2.0 e 2.1. Questo supporto consente di scrivere i programmi per le comunicazioni con molti altri prodotti IBM SNA.

APPC/APPN

Communications Server fornisce alle stazioni di lavoro il supporto del nodo di rete e del nodo finale APPN (Advanced Peer-to-Peer Networking), che consente loro di comunicare in modo più flessibile con gli altri sistemi presenti nella rete. Inoltre, la funzione Branch Extender consente di isolare i rami in modo da evitare i traffici CP-CP non necessari.

Communications Server fornisce un protocollo APPC (advanced program-to-program communications) per il supporto delle comunicazioni tra programmi di elaborazione distribuiti, chiamati TP (transaction programs). I TP possono trovarsi su qualsiasi nodo nella rete che fornisce l'APPC. L'APPC utilizza il protocollo LU 6.2 per lo scambio dei dati tra i programmi ubicati su LU (logical unit) differenti. Inoltre, l'APPC supporta più collegamenti simultanei e sessioni parallele. L'APPC consente anche il supporto della sicurezza delle conversazioni o delle sessioni tra i programmi di comunicazione.

Communications Server fornisce alte prestazioni delle APPC in ambienti LAN più complessi e supporta i seguenti tipi di collegamento:

Tabella 1. Collegamenti APPC supportati

Protocolli	Collegamento	Tipo di collegamento
Canale	• CDLC (OEM) • MPC	
LAN (802.2)	• Token-Ring • Ethernet • Frame Relay • ATM Lan Emulation	
SDLC	• Sincrono • Autosincrono • Modem	• A composizione automatica, a composizione DTR, permanente • A composizione automatica • A composizione automatica, permanente • A composizione automatica
X.25	• Sincrono • Hayes** AutoSync • Rete X.25	• A composizione automatica, semipermanente • A composizione automatica, permanente • A composizione automatica
IP	SNA su IP	Collegamenti forniti da IP
IP	HPR su IP	Collegamenti forniti da IP

Nota: L'APPC/APPN dispone anche di una funzione di compressione dati. Per ulteriori informazioni sulla compressione dati, fare riferimento alla sezione “Compressione dati” a pagina 59. Inoltre, per informazioni sulla crittografia, consultare la sezione “Crittografia a livello sessione SNA” a pagina 62.

Supporto SNA LU 6.2

La LU 6.2 è un'architettura per le comunicazioni tra programmi. Communications Server supporta le seguenti funzioni SNA LU 6.2 facoltative:

- Comunicazioni di base e mappate
- Livello di sincronia della conferma
- Supporto della sicurezza a livello di sessione e conversazione
- LU multiple
- Sessioni parallele, inclusa la capacità di utilizzo di un sistema remoto per la modifica del numero di sessioni
- Transazioni in modo unidirezionale o simultaneo bidirezionale
- Collegamenti simultanei multipli con sessioni SSCP-PU, ciascuna della quali può essere collegata ad una rete di subarea

Per un elenco completo delle funzioni, fare riferimento a *Communications Server Programming Guide and Reference*.

Potenziamenti della configurazione APPC

La configurazione di base del nodo finale richiede solo quattro parametri: ID di rete, nome nodo locale, tipo di collegamento ed indirizzo di destinazione. La definizione del sistema è ridotta da:

- Modi forniti dalla IBM
- Creazione implicita della LU partner e definizioni del modo durante l'assegnazione di una comunicazione
- Inizializzazione implicita dei limiti di sessione (la funzione CNOS), che elimina la necessità di inizializzare esplicitamente i limiti della sessione prima dell'assegnazione delle comunicazioni
- Eliminazione dei limiti di sessione per le LU locali e partner per ottenere una maggiore libertà nella configurazione e nell'inizializzazione dei limiti di sessione del modo
- Valori predefiniti per i nomi, le operazioni ed il tipo di TP (transaction program), in modo da eliminare la necessità di configurare le definizioni TP (transaction program) per i programmi applicabili
- Aggiornamenti della configurazione dinamica
- Definizioni della stazione di lavoro implicita del gateway SNA
- Possibilità di editare un file .ACG contenente i parametri di configurazione
- Possibilità di ricercare le informazioni relative alla definizione del sistema mediante il protocollo Discovery

Poiché la configurazione SNA viene memorizzata come file di testo, è possibile modificare in modo rapido e semplice il file utilizzando un editor o un programma scritto da un utente. E' quindi possibile verificare ed aggiornare dinamicamente una configurazione attiva (senza arrestare Communications Server).

A questo punto è possibile configurare collegamenti su più host, con la possibilità di avere più collegamenti attivi allo stesso tempo. I collegamenti possono essere impostati su Avvio su richiesta oppure in seguito ad un hot standby non riuscito.

Il supporto Discovery di Communications Server consente ad un nodo di rilevare dinamicamente il nome CP (control point), l'indirizzo MAC (medium access control) e l'indirizzo SAP (service access point) di un altro server del nodo di rete Communications Server su una LAN Ethernet o Token-Ring. Ciò significa che non è necessario che l'utente conosca il nome CP (control point), gli indirizzi MAC e SAP di una macchina partner per poter definire un collegamento. Al momento, gli utenti di Client Access/400 e Personal Communications possono utilizzare questa funzione.

Concetti APPC fondamentali

Questa sezione introduce ai concetti ed alla terminologia APPC.

TP (Transaction Programs): Un TP è un programma o parte di un programma applicativo, che utilizza le funzioni delle comunicazioni APPC. I programmi applicativi utilizzano queste funzioni per comunicare con i programmi applicativi presenti su altri sistemi che supportano l'APPC.

Communications Server fornisce l'APPC API e supporta le chiamate CPI-C (Common Programming Interface for Communications) SAA (Systems Application Architecture) dell'IBM per i TP (transaction programs).

I TP (transaction programs) inviano parametri APPC per richiamare le funzioni APPC. Un ***parametro*** è una richiesta formattata che viene inviata da un TP (transaction program) ed eseguita dall'APPC. Un programma utilizza le sequenze di parametri APPC per comunicare con un altro programma. Due programmi che comunicano tra loro possono trovarsi su sistemi differenti o sullo stesso sistema. L'APPC API è la stessa in entrambi i casi.

Quando un TP (transaction program) scambia i dati con un altro TP, questo TP è chiamato TP ***partner***.

I TP possono inviare chiamate CPI-C. Queste chiamate consentono ai programmi applicativi di usufruire dei vantaggi forniti dalla SAA.

LU (Logical Units): Ogni TP (transaction program) accede ad una rete SNA mediante una ***LU*** (logical unit). La LU è un software SNA che accetta i parametri ricevuti dai programmi ed agisce su di essi. Un TP invia parametri APPC nella relativa LU. Questi parametri provocano il flusso dei comandi e dei dati attraverso la rete in una LU partner. Una LU agisce anche come intermediaria tra i TP e come rete per la gestione dello scambio dei dati tra i TP. Una LU singola può fornire servizi per più TP. Nel nodo possono essere attive più LU contemporaneamente.

Tipi di LU: Communications Server supporta i tipi di LU 0, 1, 2, 3 e 6.2. I tipi 0, 1, 2 e 3 supportano le comunicazioni tra programmi applicativi host e tipi differenti di periferiche, come terminali e stampanti.

La LU 6.2 supporta le comunicazioni tra due programmi ubicati nei nodi di subarea di tipo 5, nei nodi periferici di tipo 2.1 o entrambi e tra i programmi e le periferiche. L'APPC è un'implementazione dell'architettura LU 6.2.

Sessioni LU: Per abilitare le comunicazioni tra i TP, è necessario collegare le relative LU in una rapporto reciproco chiamato ***sessione***. Poiché una sessione collega due LU, viene chiamata sessione ***LU-LU***. La Figura 1 mostra questo rapporto di comunicazione.

Figura 1. Una sessione tra due LU (LU-LU)

Le sessioni agiscono come canali per la gestione degli spostamenti dei dati tra una coppia di LU in una rete SNA. In particolare, le sessioni gestiscono la quantità di dati trasmessi, la sicurezza dei dati, l'instradamento della rete e la congestione del traffico.

Le sessioni vengono gestite dalle LU. In generale, i TP (transaction programs) non operano con le caratteristiche delle sessioni. Tali caratteristiche vengono definite quando:

- Viene configurato il sistema
- Viene utilizzata l'applicazione **Operazioni nodo SNA**
- Vengono utilizzati i parametri di gestione

Comunicazioni tra TP (Transaction Program): La comunicazione tra TP viene chiamata ***conversazione***. Come nelle conversazioni telefoniche, un TP chiama un altro TP per iniziare a “conversare” comunicando uno alla volta, finché la conversazione non viene terminata da un TP. Una conversazione viene avviata quando un TP invia un parametro APPC oppure una chiamata CPI-C che assegna una conversazione. Le conversazioni vengono stabilite tra sessioni LU-LU.

L'assegnazione di una conversazione ad una sessione stabilisce un rapporto di inoltro-ricezione tra i TP collegati alla conversazione. Un TP invia i parametri per l'inoltro dei dati. L'altro TP invia i parametri per la ricezione dei dati. Quando il TP di inoltro termina l'inoltro dei dati, può trasferire il controllo dell'inoltro della conversazione al TP di ricezione. Le conversazioni possono scambiare dati ed informazioni sul controllo.

La Figura 2 mostra una conversazione tra due TP in una sessione.

Figura 2. Conversazione tra TP in una sessione

Una sessione può supportare solo una conversazione alla volta, ma ne può supportare diverse consecutive. Poiché più conversazioni possono riutilizzare le sessioni, una sessione è un collegamento di più lunga durata rispetto alla conversazione. Quando un programma assegna una conversazione e tutte le sessioni applicabili sono in uso, la LU colloca in una coda la richiesta di assegnazione in arrivo. Tale assegnazione viene completata quando una sessione viene resa disponibile.

Due LU possono stabilire anche sessioni parallele tra loro per il supporto di più conversazioni simultanee. Una sessione parallela viene stabilita quando uno dei TP assegna una conversazione ma la sessione esistente viene utilizzata da un'altra conversazione. La LU può richiedere una nuova sessione per soddisfare l'assegnazione.

La Figura 3 a pagina 9 mostra tre sessioni parallele tra due LU; in ciascuna sessione è in corso una conversazione.

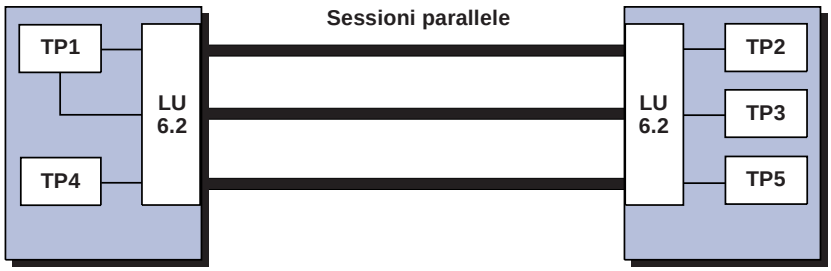


Figura 3. Sessioni parallele tra LU

APPN (Advanced Peer-to-Peer Networking)

APPN (Advanced peer-to-peer networking) è un insieme di funzioni, formati e protocolli che consentono di migliorare notevolmente la gestione di una rete SNA e l'utilizzo delle applicazioni APPC in esecuzione nella rete. Ciò è reso possibile mediante la riduzione dei requisiti di configurazione, le ricerche dinamiche delle directory, le funzioni di calcolo degli instradamenti e l'instradamento delle sessioni intermedie.

APPN consente di scrivere programmi senza conoscere i dettagli della rete sottostante. Tutto ciò che è necessario conoscere è il nome della LU partner e non la relativa ubicazione. SNA stabilisce l'ubicazione della LU partner ed il migliore percorso per l'instradamento dei dati. Una modifica alla rete sottostante, come la modifica dell'indirizzo fisico, l'aggiunta di un nuovo adattatore oppure il reindirizzamento di una macchina, non influisce sui programmi APPC.

Communications Server fornisce alle stazioni di lavoro il supporto del nodo di rete e del nodo finale APPN, che consente loro di comunicare in modo più flessibile con gli altri sistemi presenti nella rete. Inoltre, la funzione Branch Extender consente di isolare i rami in modo da evitare i traffici CP-CP non necessari.

- La funzione del nodo finale fornisce i seguenti servizi:
  - Collegamento del nodo locale ad un nodo di rete secondario per i servizi di instradamento e di directory
  - Riattivazione automatica delle sessioni CP-CP quando un nodo finale perde il server del nodo di rete.
- La funzione del nodo di rete fornisce i seguenti servizi:
  - Servizi di selezione dell'instradamento che consentono di calcolare l'instradamento migliore di una sessione in una rete APPN
  - Instradamento della sessione intermedia che consente a due LU su nodi non adiacenti di essere collegate alla stessa sessione, che attraversa uno o più nodi intermedi
  - I Directory Services che consentono di rilevare dinamicamente le ubicazioni della LU partner
  - Servizi di rete di collegamento per la LAN che consentono di rilevare gli indirizzi di destinazione LAN senza doverli configurare.

    Questa funzione consente ad un nodo di stabilire un collegamento direttamente con un altro nodo senza alcun indirizzo di destinazione LAN configurato.

– Supporto Branch Extender che consente di interconnettere una filiale dotata di LAN, nodi finali e nodi di rete che dispongono di LU dipendenti ed indipendenti e PU, come registratori di cassa, ad una o più WAN. Ciò consente il funzionamento di più nodi di rete come gateway per le filiali. Una LAN in ciascuna filiale può essere configurata come rete di collegamento.

Interfacce di programmazione

Il Communications Server supporta una vasta gamma di API (application programming interfaces) a 32 bit disponibile sul server per lo sviluppo di programmi applicativi. Queste API forniscono metodi convenienti per consentire ai programmi applicativi di accedere alle funzioni di Communications Server ed alle applicazioni di comunicare più agevolmente con i computer IBM e non. Inoltre, le interfacce fornite supportano protocolli SNA che garantiscono il rispetto degli standard.

Le API supportate includono:

- APPC (Advanced program-to-program communications)
- CPI-C (Common Programming Interface for Communications)
- LUA (LU Application Interface) RUI convenzionale e SLI
- HACL (Host Access Class Libraries)
- JCPI-C (Java CPI-C)
- WinSock (insieme con Socket AnyNet su SNA)
- Network Operator Facility
- Servizi di gestione
- Servizi comuni

Sui client viene fornita anche l'API EHNAPPC (Enhanced APPC).

Per gli sviluppatori di applicazioni è disponibile anche Communications Server Software Developers Tool Kit (che è possibile installare separatamente dal CD-ROM Communications Server). Il tool kit contiene esempi, file di intestazione, file di libreria e manuali in linea per ciascuna API.

Per ulteriori informazioni sulle interfacce di programmazione Communications Server, fare riferimento a *Client/Server Communications Programming* e *System Management Programming*
REFID='INSP1'.

HPR (High Performance Routing)

HPR (high performance routing) rappresenta un potenziamento dell'APPN che incrementa l'affidabilità e le prestazioni dell'instradamento dati e stabilisce un collegamento virtuale tra i nodi RTP (rapid transport protocol). HPR sostituisce l'instradamento delle sessioni intermedie, ovvero la tecnica di instradamento utilizzata nell'APPN.

HPR fornisce una trasmissione più rapida nei nodi intermedi, reinstrada le sessioni nei nodi e nei collegamenti non riusciti senza danneggiarle e regola il flusso del traffico prevedendo e riducendo la congestione nella rete.

Communications Server supporta i collegamenti HPR su Enterprise Extender (IP), SDLC (synchronous data link control), LAN, WAN, canale, MPC (Multi-Path Channel) ed i collegamenti X.25.

- Agire come convertitore di protocollo tra le stazioni di lavoro che utilizzano dei DLC per i collegamenti differenti dal DLC utilizzato per il collegamento host
- Ridurre la quantità di definizioni del sistema nell'host e nelle stazioni di lavoro
- Consentire la modifica dinamica delle definizioni di rete e l'aggiunta delle stazioni di lavoro
- Ridurre le risorse host ed il numero di collegamenti host mediante l'uso di LU in pool e mediante lo scollegamento automatico delle sessioni non utilizzate per un periodo di tempo specificato dall'utente.
- Migliorare l'affidabilità fornendo un collegamento host di backup

Il gateway SNA consente il supporto delle stazioni di lavoro che implementano le LU 0, 1, 2, 3 o la LU dipendente 6.2 (APPC) negli host S/390. Inoltre, esso supporta le LU 0, 1, 2 o 3 in un host AS/400. L'host AS/400 trasferisce i dati in un host della famiglia S/390.

Ciascun host interpreta il gateway SNA come nodo SNA PU 2.0, che supporta una o più LU per stazione di lavoro. Per l'host, tutte le LU appartengono alla PU del gateway SNA. Il gateway SNA può disporre di più collegamenti host simultanei ed indirizzare sessioni di stazioni di lavoro differenti su host specificati. Tuttavia, solo un host collegato ad una PU CP può agire come focal point ed il nome CP (control point) viene accodato a tutti gli NMVT (network management vector transports) instradati nel gateway.

Per le stazioni di lavoro supportate, il gateway SNA ha le funzioni di un'unità di controllo per comunicazioni SNA PU 4 ed inoltra messaggi host, quali BIND e UNBIND. Le LU di rete non riconoscono il gateway SNA. Il gateway SNA, tuttavia, riconosce tutte le LU delle stazioni di lavoro.

In realtà, il gateway SNA è un particolare tipo di PU 2.0. Finché una stazione di lavoro dipendente non è attiva, il gateway SNA implementa le funzioni LU per la stazione di lavoro, proprio come farebbe una vera PU 2.0. Tuttavia, non appena una stazione di lavoro è in linea con l'host, il gateway SNA consente alla stazione di lavoro di implementare le funzioni LU ed effettua il trasferimento dei dati tra le stazioni di lavoro e l'host.

Un gateway SNA consente alle applicazioni delle stazioni di lavoro supportate di accedere alle applicazioni remote in una rete di subarea senza richiedere un collegamento diretto separato a ciascun host in ogni stazione di lavoro. Da un punto di vista host, l'host dispone di un solo collegamento al gateway.

Per ulteriori informazioni sull'utilizzo di un gateway SNA, consultare la sezione “Pianificazione del gateway SNA” a pagina 115.

La Figura 4 mostra un esempio di collegamento che utilizza un gateway SNA.

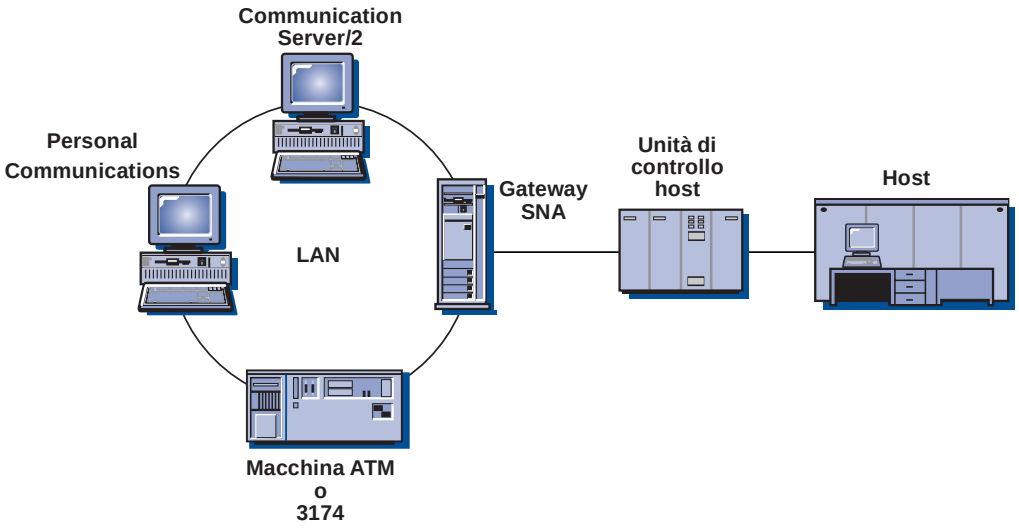


Figura 4. Esempio di collegamenti Gateway SNA

Supporto AnyNet

Communications Server incorpora le funzioni SNA su TCP/IP e Socket su SNA dalla famiglia di prodotti AnyNet. Questo supporto consente di estendere e semplificare la rete abilitando le comunicazioni tra applicazioni SNA in una rete TCP/IP e le comunicazioni Socket in una rete SNA senza alcuna modifica alle applicazioni.

SNA su TCP/IP

La funzione del nodo di accesso SNA su TCP/IP abilita le comunicazioni tra le applicazioni SNA che risiedono su una rete IP. Questa funzione supporta la LU 6.2 indipendente e le LU 0, 1, 2, 3 o 6.2 dipendenti con o senza DLUR (dependent LU requester). Inoltre, il nodo di accesso SNA su TCP/IP può essere utilizzato insieme con il gateway SNA per abilitare le sessioni gateway SNA su TCP/IP.

La funzione del gateway SNA su TCP/IP estende la portata delle applicazioni SNA consentendo alle applicazioni SNA di una rete SNA di comunicare con le applicazioni SNA di una rete IP. Il gateway SNA su TCP/IP supporta le sessioni LU 6.2 indipendente.

La Figura 5 a pagina 14 mostra le applicazioni SNA che comunicano mediante un gateway SNA su TCP/IP su reti IP e SNA.

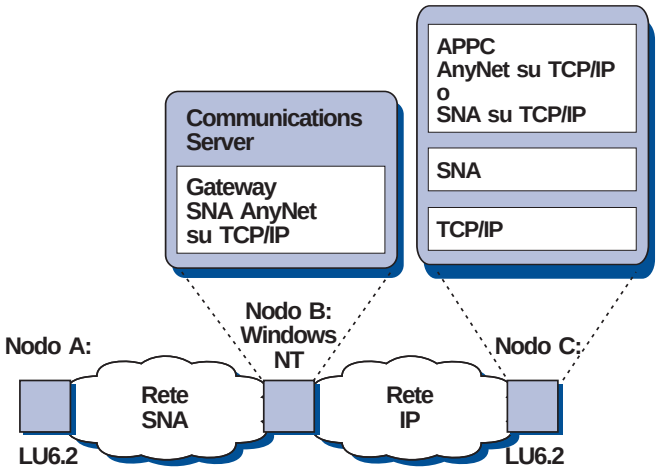


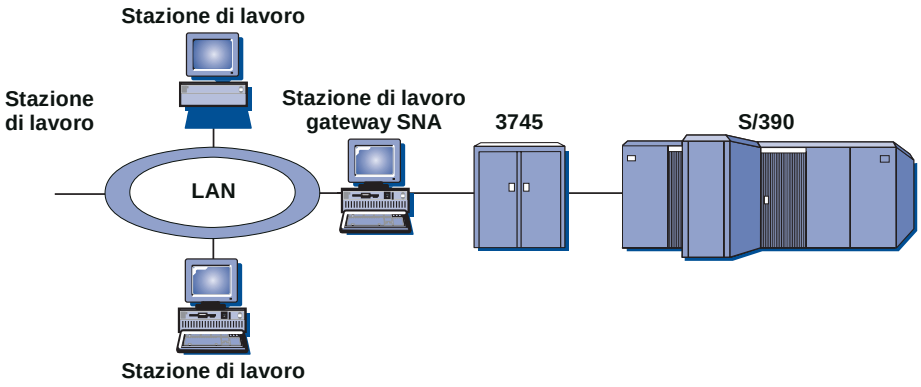
Figura 5. Gateway SNA su TCP/IP

Socket su SNA

La funzione del nodo di accesso Socket su SNA consente ai programmi applicativi TCP/IP che utilizzano l'interfaccia socket WinSock 1.1 e WinSock 2.0 di comunicare su una rete SNA.

La funzione del gateway Socket su SNA consente la comunicazione tra le applicazioni socket nelle reti SNA e TCP/IP. I gateway Socket su SNA vengono spesso utilizzati per collegare reti TCP/IP isolate utilizzando una rete backbone SNA.

La Figura 6 mostra le comunicazioni tra applicazioni Socket mediante la funzione del gateway Socket su SNA nelle reti IP e SNA.

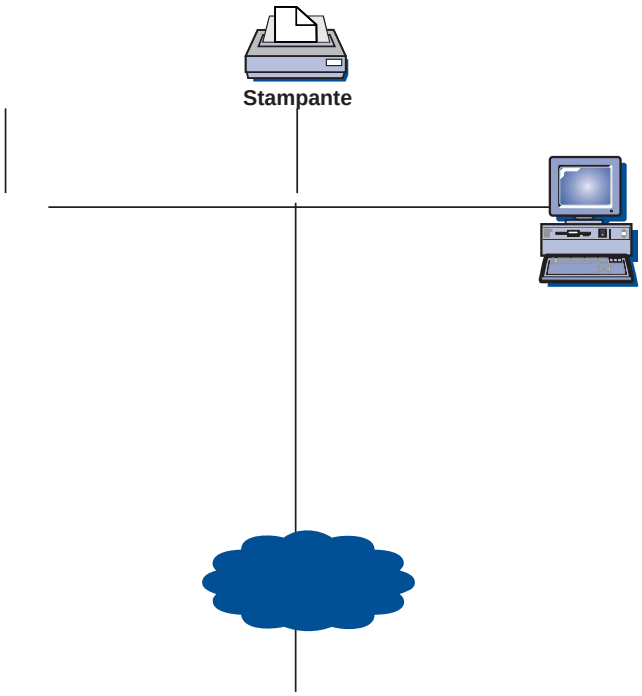


Communications Server supporta la distribuzione del carico per i collegamenti client di un server TN3270E collegato alle stesse risorse host, se il client è abilitato alla distribuzione del carico.

Il server TN3270E supporta il filtraggio di IP e nomi host, che consente l'accesso controllato alle LU senza alcuna modifica alle configurazioni client.

Il server TN3270E supporta anche l'autenticazione e la crittografia SSL (Secure Sockets Layer), che forniscono un accesso protetto alla rete TCP/IP. Se viene specificata la sicurezza, il server deve disporre di un certificato autenticato fornito da una CA (certificate authority) come Verisign. Communications Server fornisce un programma di utilità che genera e gestisce chiavi e certificati utilizzati dall'SSL Versione 3.

La Figura 7 mostra un esempio di collegamenti del server TN3270E.



Il server TN5250 supporta il filtraggio di IP e nomi host che consente la gestione centrale degli accessi al server e l'indirizzamento dei client su specifiche macchine AS/400.

Il server TN5250 supporta anche l'autenticazione e la crittografia SSL (Secure Sockets Layer), che forniscono un accesso protetto alla rete TCP/IP. Se viene specificata la sicurezza, il server deve disporre di un certificato autenticato fornito da una CA (certificate authority) come Verisign. Communications Server fornisce un programma di utilità che genera e gestisce chiavi e certificati utilizzati dall'SSL Versione 3.

La Figura 8 mostra un esempio di collegamenti del server TN5250.

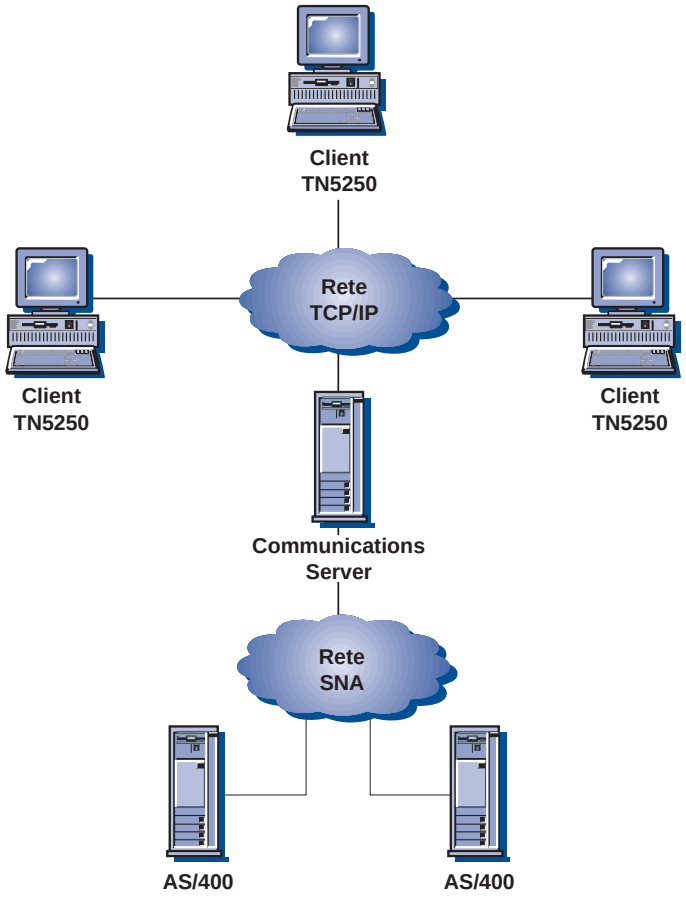


Figura 8. Collegamenti del server TN5250

Accesso ai dati legacy

Communications Server fornisce l'accesso ai dati presenti sulle macchine host, sulle macchine AS/400 e sulle stazioni di lavoro collegate a reti SNA, mediante le seguenti funzioni:

- AS/400 OLE DB provider
- Host Publisher
- Server delle cartelle condivise AS/400

AS/400 OLE DB Provider

La applicazioni che utilizzano OLE DB o ActiveX possono comunicare mediante Communications Server per l'accesso a livello di record ai file presenti in una stazione AS/400. La documentazione relativa a questa funzione e le informazioni sullo sviluppo di queste applicazioni mediante Client Access, sono disponibili nella directory `csnt\sdk\as400_oledb`.

Host Publisher

Host Publisher consente di accedere ai siti Web di grandi dimensioni con contenuto dinamico. Esso può essere utilizzato per accedere ai dati presenti sugli host S/390 o AS/400 e visualizzarli sulle pagine Web create dinamicamente in base ad un progetto personale.

Server delle cartelle condivise AS/400

Il sistema AS/400 utilizza una struttura chiamata cartella per la memorizzazione e l'organizzazione dei documenti, della posta e di altri oggetti correlati. Communications Server consente di creare sul server delle unità disco che comunicano con le cartelle AS/400 mediante l'IFS (Integrated File System) AS/400. Inoltre, se il server condivide queste unità disco, i client possono utilizzare la funzione NET USE per il collegamento. Più client possono collegarsi alle cartelle presenti nel sistema AS/400 come se fossero unità di stazioni di lavoro.

Le cartelle condivise possono essere utilizzate per:

- Utilizzare la sicurezza AS/400 per limitare l'accesso ai file delle stazioni di lavoro
- Condividere i dati con più utenti allo stesso tempo
- Eseguire il backup dei file delle stazioni di lavoro in una cartella AS/400

Supporto client di Communications Server

Communications Server fornisce il supporto per i client API SNA (disponibili sul CD-ROM) e per i client Novell IntranetWare per SAA.

Supporto client API SNA

Il supporto per il client API SNA di Communications Server consente ai client collegati tramite TCP/IP e IPX di accedere alle API SNA senza che siano richiesti protocolli SNA per le comunicazioni tra i client ed il server. Ciò consente di eseguire la maggior parte delle configurazioni SNA nel server centrale.

Communications Server supporta i client API SNA su Windows 95, Windows NT, Windows 3.1 e OS/2.

I client SNA forniscono il supporto per le interfacce CPI-C, APPC, EHNAPPC, LUA RUI, JCPI-C e HACL API e, contemporaneamente, l'elaborazione SNA sul server. Questi client vengono distribuiti come parte del server ma vengono installati e configurati nel client.

I client Windows e OS/2 a 32 bit dispongono di ulteriori potenziamenti:

- Crittografia tra client e server
- Formattazione più dettagliata delle tracce che rende più rapido il debug
- Possibilità di avviare ed arrestare la traccia quando il client è attivo

- Possibilità di reinstallare il client senza eseguire la disinstallazione

I client Windows NT e Windows 95 vengono eseguiti dallo stesso programma eseguibile che può essere installato su un'unità condivisa; tutte le correzioni vengono applicate ad entrambi i client. Il nuovo client Windows a 32 bit può comunicare con i Communications Server ed i server Novell IntranetWare o NetWare per SAA.

Per ulteriori informazioni sui client API in Communications Server, consultare la sezione “Pianificazione delle comunicazioni client/server” a pagina 95.

Supporto client Novell IntranetWare per SAA

Communications Server supporta i client collegati tramite IPX o TCP/IP che eseguono pacchetti software di emulazione che implementano l'architettura QEL/MU (Queue Element/Message Unit) della Novell per l'emulazione 3270, consentendo l'accesso dei client ai dati host mainframe. Sono supportate anche funzioni client comuni, incluse le categorie LU pubbliche, dedicate, e in pool, a cui si fa talvolta riferimento come tipi di risorsa.

Communications Server supporta i client Novell IntranetWare per SAA su Windows 95, Windows NT, Windows 3.1 e OS/2.

Per ulteriori informazioni sullo sviluppo di questi client, fare riferimento al manuale *Novell NetWare for SAA 3270 Client Interface Guide and Reference* P/N 100–002018–001.

Distribuzione del carico

Communications Server supporta la distribuzione del carico per tutti i tipi di client. La distribuzione del carico consente di distribuire sessioni LU da 0 a 3 e LU 6.2 nel Communications Server e nei server IntranetWare per SAA. Il server invia una notifica ai servizi, inclusi i fattori di carico che i client o i server possono raccogliere ed organizzare per la selezione di un server.

Utilizzo delle directory

E' possibile configurare più client da un'ubicazione centrale utilizzando l'LDAP (Lightweight Directory Access Protocol) per semplificare il processo di configurazione.

Per informazioni sull'utilizzo delle directory, fare riferimento a “Pianificazione delle comunicazioni client/server” a pagina 95.

Supporto per la configurazione e la gestione

Communications Server fornisce delle funzioni per la configurazione e la gestione delle risorse.

Configurazione di Communications Server

Questa sezione contiene una panoramica dei componenti per la configurazione di Communications Server e dei metodi utilizzati per crearli o modificarli. La configurazione si compone di un singolo file (ACG) memorizzato nella sottodirectory PRIVATE della directory in cui è installato il prodotto (ad esempio, C:\IBMCS\PRIVATE). Il file ACG può essere creato o modificato da **Configurazione nodo** oppure utilizzando un editor ASCII. E' disponibile un

programma di verifica che consente di controllare la validità del file ACG prima del relativo utilizzo.

E' possibile utilizzare i seguenti metodi per creare o modificare una configurazione Communications Server:

- **Configurazione nodo**
- Configurazione file di risposta

Configurazione nodo: Communications Server fornisce l'applicazione **Configurazione nodo** (PCSCFG) che consente di configurare le funzioni Communications Server utilizzando un'interfaccia grafica e fornisce valori predefiniti per semplificare tale configurazione mediante l'utilizzo di un numero minimo di parametri. Una volta completata una configurazione, una verifica automatica esamina la configurazione creata e, se non viene rilevato nessun conflitto, crea i file di configurazione necessari. In presenza di conflitti, gli errori vengono segnalati in modo da consentirne la correzione nella configurazione.

La configurazione locale è supportata sia a livello client che a livello server. La configurazione remota del server è supportata dai client Windows NT e Windows 95.

E' possibile creare la maggior parte delle configurazioni utilizzando l'applicazione **Configurazione nodo**. Tuttavia, alcune parole chiave ed alcuni parametri di parola chiave non sono supportati da **Configurazione nodo**.

Configurazione file di risposta: La configurazione del file di risposta consente di personalizzare un file di configurazione maschera in modo da soddisfare le esigenze di utenti specifici. Per ulteriori informazioni sull'utilizzo dei file di risposta per la configurazione, fare riferimento alla sezione “Configurazione con i file maschera e di risposta” a pagina 194.

Operazioni nodo SNA: **Operazioni nodo SNA** consente di creare e modificare le risorse selezionate.

Gestione di Communications Server

Communications Server fornisce le seguenti funzioni per la gestione delle risorse.

- **Operazioni nodo SNA**
- Programmi di utilità della riga comandi
- Gestione basata su Web
- Modulo Tivoli Plus

Per ulteriori informazioni sulle capacità di queste funzioni, fare riferimento alla sezione “Programmi per la gestione del sistema” a pagina 205.

Distribuzione del carico

La distribuzione del carico è una funzione di Communications Server che consente di assegnare dinamicamente le sessioni LU dipendente (host-stazione di lavoro) e le sessioni LU 6.2 indipendente, distribuendole sul server per le comunicazioni con il carico minore. Communications Server esegue la distribuzione del carico per i programmi API di Communications Server, per i programmi di emulazione 3270 non IBM collegati tramite i protocolli TCP/IP o per i programmi di emulazione

TN3270 e TN5250 non IBM. Le risorse su cui viene effettuata la distribuzione dipendono dal tipo di sessione:

- Per le sessioni LU dipendente, il carico viene distribuito sui server inclusi in un determinato pool di LU ed in un determinato ambito.
- Per le sessioni LU 6.2, il carico viene distribuito sui server disponibili in un determinato ambito o sui server selezionati all'interno di un determinato elenco di server.

Le capacità di distribuzione del carico di Communications Server vengono generate nelle API del client SNA. La distribuzione del carico viene configurata per i client mediante **Configurazione client SNA**.

Per le sessioni LU dipendente, i programmi di emulazione che utilizzano le API del client SNA possono partecipare alla distribuzione del carico. In caso contrario, è necessario acquistare un software di emulazione 3270, TN3270 o TN5250 non IBM che supporta la distribuzione del carico.

Per le sessioni LU 6.2, il collegamento iniziale stabilito da un client API SNA specifica il server che gestisce tutte le sessioni LU 6.2 successive.

Per ulteriori informazioni sulla distribuzione del carico, fare riferimento alla sezione “Pianificazione della distribuzione del carico” a pagina 147.

Sicurezza dati

Communications Server fornisce il supporto per la sicurezza di base ed avanzata a livello di sessione e conversazione. La sicurezza consiste nel limitare il numero di utenti Windows NT che possono accedere alle risorse SNA mediante i client API SNA. La sicurezza della conversazione include il supporto per la sostituzione della password. E' disponibile anche la sicurezza LU-LU avanzata.

Communications Server fornisce il supporto per la sicurezza basata su SSL (Secure Sockets Layer) nei collegamenti tra client TN e server TN3270E o TN5250. Tale sicurezza utilizza SSL Versione 3 per fornire la crittografia dei dati e l'autenticazione del server mediante l'utilizzo di certificati firmati.

Supporto adattatore

Communications Server fornisce un'interfaccia aperta che consente ai produttori di adattatori di creare soluzioni di connettività. Viene fornita un'interfaccia adattatore non programmabile per il funzionamento degli adattatori con lo stack di protocolli SDLC e X.25 di Communications Server ed un'interfaccia adattatore programmabile per la creazione di soluzioni di connettività mediante l'utilizzo dei controlli di collegamento dati forniti dai produttori.

Supporto DLC (Data Link Control)

Communications Server consente le comunicazioni sui seguenti DLC:

- AnyNet (SNA su TCP/IP)
- Biassiale (solo upstream)
- LAN (Qualsiasi adattatore di rete compatibile NDIS**)
- X.25 SDLC (sincrono, asincrono e AutoSync)

- OEM (supporto per adattatori non IBM)
- Canale (solo upstream)
- Multi-Path Channel (solo HPR)
- Enterprise Extender

DLC AnyNet (SNA su TCP/IP)

Per ulteriori informazioni sul DLC SNA AnyNet su TCP/IP, fare riferimento alla sezione “SNA su TCP/IP” a pagina 13.

DLC IBM MPC (Multi-Path Channel)

DLC MPC (Multi-Path Channel) fornisce collegamenti a fibre ottiche ad uno o più host compatibili MPC S/390 sull'adattatore ESCON Channel (P/N 9663 001). I collegamenti MPC forniscono alta velocità di trasmissione dati con backup trasparenti quando i collegamenti fisici vengono interrotti oppure non sono temporaneamente disponibili. Questo collegamento tra canali consente di fornire ai client LAN l'accesso alle risorse ed ai servizi S/390.

DLC MPC è disponibile solo negli US e in Canada.

DLC Enterprise Extender

Communications Server fornisce i collegamenti HPR su reti IP, mediante l'utilizzo dei pacchetti UDP/IP. Per la rete HPR, il backbone IP assume l'aspetto di un collegamento logico. Per la rete IP, il traffico SNA assume l'aspetto di datagrammi UDP. Questi datagrammi vengono instradati senza modifiche al backbone IP. Poiché il protocollo non viene trasformato ed i pacchetti vengono creati durante l'instradamento senza nessun altro livello di trasporto, i client SNA ed i client IP che accedono ai dati basati su SNA (ad esempio, i client TN3270 o i browser Web che utilizzano IBM Host on Demand) utilizzano in modo efficiente l'infrastruttura intranet.

Supporto MIB APPN

Communications Server supporta le richieste SNMP (simple network management protocol) per le informazioni sulla gestione APPN del sistema di gestione SNMP.

Hot Standby

In Communications Server, è possibile configurare determinati collegamenti host in modo da attivarli automaticamente in caso di malfunzionamento di un server strategico specificato. I collegamenti configurati in un host possono continuare a funzionare attivando i collegamenti alternativi in un server di backup. Questa funzione è chiamata Hot Standby.

I collegamenti presenti nella configurazione di un server strategico sul server di backup vengono attivati quando il server di backup rileva l'interruzione delle comunicazioni con il server strategico ed i costi relativi alle licenze per il server strategico vengono gestiti sul server di backup.

Nota: La funzione Hot Standby viene fornita solo per l'attivazione dei collegamenti host su un server di backup e dipende dall'utilizzo del software di emulazione che supporta l'instradamento alternativo sul server di backup quando un server strategico non è più attivo.

Per ulteriori informazioni sull'utilizzo della funzione Hot Standby per i collegamenti di backup, fare riferimento alla sezione “Pianificazione dei collegamenti host di backup” a pagina 151.

Funzioni del programma di emulazione di base

Communications Server include una versione di base del programma di emulazione 3270 e 5250 del Personal Communications per le funzioni di amministrazione. Questo programma di emulazione fornisce il supporto 5250 e 3270 di base sul server; tale supporto include un sottogruppo di caratteristiche e funzioni che vengono fornite nella famiglia di programmi di emulazione IBM Personal Communications con funzioni complete.

Le funzioni di emulazione di base fornite includono:

- Mappatura dei colori
- Trasferimento riga comandi (solo 3270)
- Serie completa di font
- Dimensioni video (mod. 2-5)
- Due sessioni

Sebbene il programma di emulazione di base non supporti la rimappatura grafica della tastiera, è possibile utilizzare i file di rimappatura generati dal programma di emulazione con funzioni complete.

Communications Server e SNA

Questo capitolo illustra le funzioni della rete SNA fornite da Communications Server e comprende gli argomenti riportati di seguito:

- Panoramica delle funzioni SNA
- Definizioni di DLC (Data link control)
- APPN (Advanced Peer-to-Peer Networking)
- HPR (High Performance Routing)
- Supporto LU
- Compressione dati
- Crittografia
- MS (Management services)
- Controllo flusso
- Supporto gateway SNA

Panoramica delle funzioni SNA

Questa sezione fornisce una panoramica del modo in cui Communications Server implementa SNA su una stazione di lavoro. Non si tratta di una discussione generale sulle funzioni SNA. Per informazioni più dettagliate su SNA, consultare i seguenti manuali:

- *Systems Network Architecture Concepts and Products*
- *Systems Network Architecture Technical Overview*
- *Systems Network Architecture Network Product Formats* (disponibile in linea nell'elenco della documentazione di Server)
- *Systems Network Architecture Format and Protocol Reference Manual: Architecture Logic for LU Type 6.2*

SNA definisce gli standard, i protocolli e le funzioni utilizzati dai dispositivi nella rete (dai mainframe ai terminali) per comunicare l'uno con l'altro. Tale comunicazione consente a questi dispositivi di condividere informazioni ed elaborare risorse in modo trasparente. In altre parole, non è necessario che un utente ad una stazione di lavoro sia a conoscenza delle esecuzioni in background per accedere alle informazioni contenute su un host o per comunicare con un altro utente.

Una rete SNA è organizzata come un sistema di nodi e collegamenti. E' importante ricordare che questa organizzazione è logica. SNA classifica i nodi in base alle loro funzioni e al controllo che hanno su altri nodi nella rete. Il tipo di nodo non è necessariamente associato ad un tipo specifico di hardware. Le funzioni di un nodo possono essere eseguite da dispositivi diversi. Una stazione di lavoro che agisce come un gateway può eseguire le stesse funzioni di un'unità di controllo per le comunicazioni. E' anche possibile che un singolo dispositivo contenga più di un nodo.

La rete SNA è responsabile del trasferimento dati tra due utenti finali in modo efficace, ordinato ed affidabile. Ad esempio, quando un utente di una stazione di

lavoro invia un messaggio ad un'altra stazione di lavoro, SNA effettua le seguenti operazioni:

- Crea pacchetti di messaggi in un formato che può essere utilizzato sul tipo di collegamento
- Indirizza il pacchetto
- Seleziona un instradamento per il messaggio
- Controlla la comunicazione per accertarsi che il messaggio giunga a destinazione
- Riconverte i messaggi in un formato che può essere utilizzato a destinazione

Queste attività vengono definite in SNA come livelli funzionali separati. Tali livelli non rientrano in questa specifica discussione, ma è importante ricordare che i livelli di SNA fanno parte di un collegamento logico.

Come si è già detto precedentemente, i nodi SNA vengono classificati in base alle loro capacità di comunicazione e al controllo che ha il nodo sugli altri nodi nella rete. I nodi SNA vengono interamente classificati come nodi subarea e nodi periferici. I nodi subarea hanno la funzione di hub e sono in grado di comunicare con i nodi periferici e con altri nodi subarea. I nodi subarea attivano e controllano le risorse ai nodi periferici. I nodi subarea vengono anche classificati come nodi del tipo 4 o del tipo 5. I nodi del tipo 5 contengono un SSCP (system service control point) che fornisce un CP (control point) centrale per i nodi del tipo 4 ad esso collegati. Un nodo del tipo 5 viene talvolta definito come nodo host. Un nodo periferico può soltanto comunicare direttamente con il nodo subarea a cui è collegato. Comunque, un nodo periferico può controllare i dispositivi a cui è collegato. Ad esempio, un'unità di controllo cluster che agisce come un nodo periferico è in grado di supportare i terminali che sono collegati ad esso. I nodi periferici vengono anche definiti come nodi del tipo 2 o del tipo 2.1.

Ogni nodo contiene delle NAU (network accessible units) che eseguono le funzioni di controllo e di comunicazione. Una di queste NAU è una PU (physical unit). La PU gestisce le risorse fisiche del nodo. Altre NAU chiamate LU (logical units) forniscono punti di accesso logici alla rete che consentono la comunicazione tra utenti ed applicazioni ad ogni nodo. La comunicazione tra LU viene definita sessione. Le sessioni non solo supportano la comunicazione tra utenti ed applicazioni, ma supportano anche la comunicazione tra applicazioni allo scopo di condividere l'elaborazione delle risorse. La comunicazione tra applicazioni è nota come APPC (advanced program-to-program communication). APPC è una serie di convenzioni e protocolli di programmazione che implementano la LU 6.2. (APPC è il nome dato alla funzione LU 6.2 in prodotti che implementano questo tipo di LU)

Profili DLC (Data Link Control)

DLC (Data link control) permette gli scambi corretti di dati tra due nodi tramite un collegamento logico. DLC fornisce i protocolli necessari per la distribuzione affidabile delle BTU (unità di trasmissione di base) tra una coppia di nodi nella rete SNA. E' necessario configurare i profili DLC di Communications Server adatti ad una stazione di lavoro per accedere ad una rete SNA.

Consultare il *Supporto Didattico* in linea per ulteriori informazioni sulla configurazione dei profili DLC adatti.

Advanced Peer-to-Peer Networking

APPN (Advanced Peer-to-Peer Networking) è una estensione di SNA che aggiunge funzioni per le comunicazioni oltre a quelle descritte nelle sezioni precedenti. I suoi elementi basilari comprendono:

- Tipi di nodo APPN
- CP (Control point)
- Branch extender
- DLC (Data link control)
- Collegamenti logici
- Directory services
- Servizi di selezione-instradamento e topologia

Tipi di nodo APPN

Questa sezione illustra i tre tipi di nodi implementati da Communications Server che possono far parte di una rete APPN :

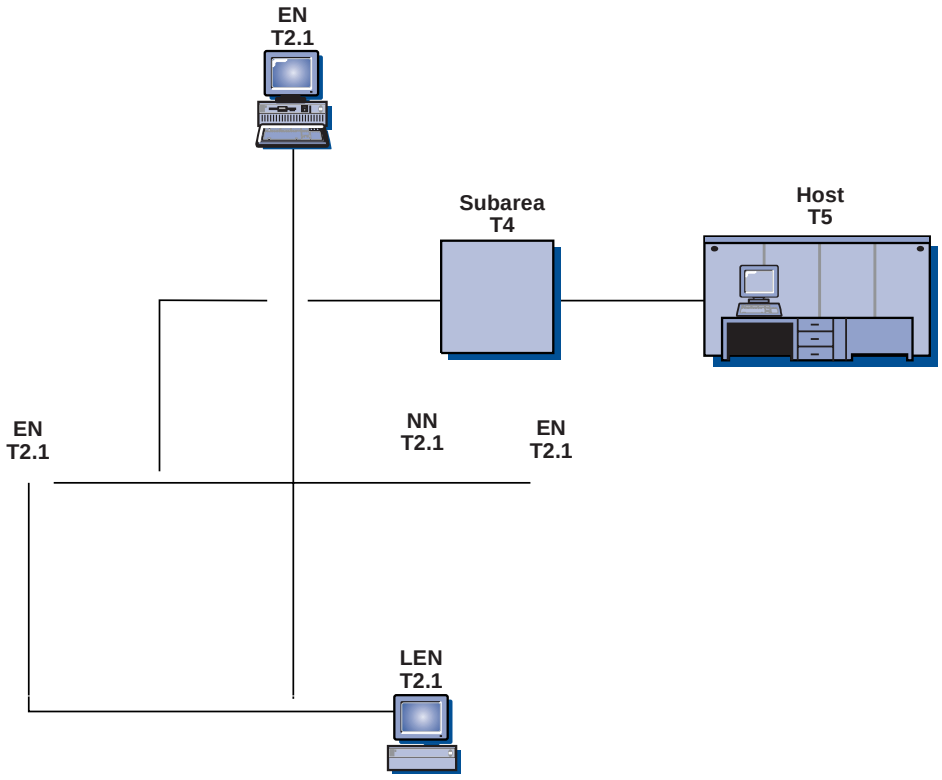
- Nodo di rete
- Nodo finale
- Nodo LEN (Low entry networking)

Inoltre, il branch extender è un'estensione di un nodo di rete. Sebbene fornisca servizi ai nodi finali come un nodo di rete, risulta nella rete come un nodo finale connesso ad altri nodi di rete.

Ogni nodo è distinto dagli altri nodi nella rete da un unico nome che consiste di due parti—un ID di rete e un nome di nodo locale (noto anche come nome CP [control point]). Il nome identifica ogni nodo rispetto a tutti gli altri nodi nella rete. Inoltre, il nodo può avere più nomi PU per un accesso simultaneo a più host PU T4/5.

E' possibile che un nodo venga configurato per essere un nodo finale o un nodo di rete, ma quando un nodo finale non dispone di sessioni CP-CP (consultare “Sessioni CP-CP” a pagina 28) in un nodo di rete APPN, agisce come un nodo LEN. Un nodo LEN non supporta le funzioni APPN.

I tipi di nodi vengono descritti più dettagliatamente nelle sezioni riportate di seguito. Figura 9 a pagina 26 mostra una rete APPN di esempio che comprende tutti questi tipi di nodi.


EN
T2.1
Subarea
T4
Host
T5
EN
T2.1
NN
T2.1
EN
T2.1
LEN
T2.1

- La funzione di instradamento MS (Management services) per l'inoltro di dati dei servizi di gestione (come le segnalazioni) tra un nodo finale assistito ed un FP (focal point) dei servizi di gestione.

Nodo finale

Un nodo finale opera in un ambiente peer per sessioni LU-LU (utilizzando protocolli LU 6.2) mentre fornisce funzioni APPN aggiuntive. Un nodo finale fornisce funzioni APPN come i directory services e i servizi di selezione instradamento agli utenti finali nel relativo nodo. Può partecipare nella rete APPN utilizzando i servizi di un server del nodo di rete collegato per richieste di sessione che coinvolgono dei nodi non direttamente collegati; può far questo scambiando richieste e risposte per i directory services con un nodo di rete adiacente (il relativo server) utilizzando sessioni CP-CP.

I nodi finali APPN possono registrare le LU locali nel proprio server del nodo di rete. Registrando i nodi finali, non è necessario che l'operatore di rete del server nodo di rete predefinisca i nomi delle LU per le LU in tutti gli nodo finale collegati per i quali il nodo di rete fornisce servizi.

Un APPN nodo finale può essere collegato a numerosi nodo di rete, ma può avere solo sessioni CP-CP attive con un nodo di rete alla volta —il relativo server nodo di rete. Gli altri nodo di rete possono essere utilizzati per fornire instradamento della sessione intermedia per l'nodo finale, oppure possono essere utilizzati come server del nodo di rete sostitutivo se il server del nodo di rete principale diviene inagibile. Le sessioni CP-CP non vengono mai stabilite tra due nodo finale.

Nodo LEN

Un nodo LEN è un nodo che implementa i protocolli T2.1 basilari senza i potenziamenti APPN. In un nodo LEN, tutti i potenziali collegamenti con le LU partner vengono predefiniti prima di avviare le relative sessioni. Un nodo LEN, collegato ad un APPN nodo di rete adiacente, utilizza le funzioni avanzate di APPN predefinendo i potenziali collegamenti con le LU partner come se esistessero in quel nodo di rete. Il nodo di rete, a sua volta, può agire automaticamente come il server nodo di rete del nodo LEN ed individuare la destinazione attuale della LU partner e selezionare l'instradamento migliore ad essa. Attraversando un nodo di rete, il nodo LEN può partecipare in una rete APPN senza richiedere collegamenti diretti a tutti i nodi.

CP (Control Point)

Il CP (control point) è responsabile della gestione del nodo e delle relative risorse. Per ottenere servizi di rete APPN, il CP in un nodo finale APPN deve comunicare con il CP in un nodo di rete adiacente. Inoltre, per gestire la rete, il CP in un APPN nodo di rete deve comunicare con i CP nei nodo di rete adiacenti. Il CP indirizza funzioni quali l'attivazione e la disattivazione dell'adattatore e l'attivazione e la disattivazione del collegamento, ed assiste le LU nell'avvio e nella chiusura della sessione.

Quando si imposta una stazione di lavoro, è necessario definire il nome del CP (noto anche come nome del nodo locale). Il CP è anche una LU, ed è possibile stabilire che la LU del CP sia l'unica LU definita sulla propria stazione di lavoro.

Sessioni CP-CP

Per eseguire i Directory services e servizi di selezione instradamento e topologia, i nodi adiacenti in tutta la rete APPN utilizzano una coppia di sessioni CP-CP parallele per lo scambio di informazioni di rete. I nodi di rete utilizzano le sessioni CP-CP per controllare i nodi in un collegamento di rete, come pure tracciare servizi di sessione e directory. Un nodo di rete stabilisce due sessioni parallele con ogni nodo di rete adiacente e con ogni nodo finale assistito. Un nodo finale APPN stabilisce due sessioni parallele con un singolo nodo di rete adiacente agendo come il relativo server corrente. I nodi LEN non supportano le sessioni CP-CP.

Una volta stabilito un collegamento, i nodi si scambiano informazioni relative all'identificazione (XID). In seguito, le sessioni CP-CP vengono avviate tra i control point nei nodi direttamente collegati. Le sessioni CP-CP utilizzano i protocolli LU 6.2 ed entrambe le sessioni di una determinata coppia devono essere attive affinché i CP partner comincino e mantengano le relative interazioni. Tutte le sessioni CP-CP vengono utilizzate per condurre ricerche di directory.

Una volta stabilite le sessioni CP-CP, i due nodi si scambiano messaggi sulle funzioni dei CP per informare ogni nodo sulle capacità dell'altro nodo. Quando entrambi i nodi sono dei nodo di rete, essi si scambiano messaggi TDU (topology database update). I messaggi TDU contengono informazioni di identificazione, caratteristiche del collegamento e del nodo, e numeri di sequenza risorse per identificare gli aggiornamenti più recenti per ognuna delle risorse descritte nel TDU.

Attivazione collegamento CP-CP

Una volta avviato, Communications Server tenta di attivare prima il collegamento al server NN preferito. Communications Server tenta di attivare tutti gli altri collegamenti definiti come ***attivazione all'avvio***. Se esiste un collegamento parallelo alternativo, invece di aspettare i risultati del tentativo di attivazione per il collegamento al server NN preferito prima di tentare un collegamento alternativo, Communications Server prova ad attivare le sessioni CP-CP sul collegamento alternativo.

Nota: Se il collegamento è stato disattivato dalla richiesta dell'operatore dal nodo locale, le sessioni CP-CP non vengono reindirizzate. Se il collegamento è stato disattivato dalla richiesta dell'operatore dal nodo remoto, le sessioni CP-CP vengono reindirizzate al nodo locale. Per i collegamenti tra i nodi NN, soltanto i collegamenti attivati su richiesta (collegamenti con un nome CP adiacente specificato e che non viene indicato come ***attivazione all'avvio***) vengono attivati.

Riattivazione collegamento CP-CP

Communications Server fornisce un supporto per la riattivazione del collegamento CP-CP. La perdita di sessioni CP-CP tra un nodo finale ed il relativo server del nodo di rete e tra nodi di rete adiacenti può interferire con il funzionamento di una rete APPN. Il supporto per la riattivazione del collegamento CP-CP migliora l'affidabilità di una rete APPN consentendo di ristabilire queste sessioni nel momento in cui vengono interrotte a causa di un errore o per la disattivazione del collegamento.

Un tentativo di riattivazione del collegamento CP-CP viene avviato per un'attivazione del collegamento CP-CP, per un errore di sessione CP-CP, oppure perché è scaduto il tempo previsto per eseguire i tentativi CP-CP di stabilire un

collegamento. Le sessioni CP-CP vengono avviate da Communications Server con il primo dei procedimenti riportati di seguito:

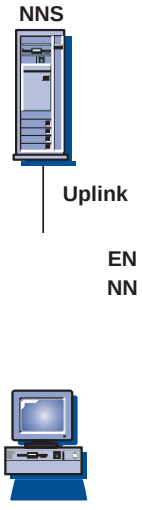
1. Utilizzo del CP-CP del server preferito (se non è già stato provato in precedenza).
2. Se DLUR è configurato, utilizzare un CP adiacente che supporta la registrazione di DLUR.
3. L'attivazione più recente degli NN che non è stata tentata, per la quale esiste un collegamento attivo.
4. Il primo di ogni altro NN di livello superiore per branch extender.

Nota: Se le connessioni CP-CP sono state interrotte per un errore di collegamento, Communications Server non riattiva il collegamento. E' possibile configurare un collegamento come ***riattivazione automatica*** (tentativo continuo) per mantenere attivi i collegamenti importanti.

Branch Extender

Il branch extender è un sottoinsieme del nodo a margine concepito per intercollegare una filiale ad una rete backbone WAN APPN. Le reti intercollegate possono essere native (cioè, dispongono dello stesso ID di rete) o non native. Un nodo che supporta il branch extender è un nodo di rete di ramo che solitamente presenta interfacce LAN e WAN e può anche includere DLUR e HPR.

I collegamenti al nodo che supportano il branch extender vengono definiti ***uplink di ramo*** o ***downlink di ramo***. Figura 10 fornisce un esempio del modo in cui un nodo di rete di ramo funziona in una rete. In questa figura, il nodo al centro è un nodo di rete di ramo. Tipicamente, il CP adiacente (nodo uplink di ramo) sarà l'NNS (network node server) per il nodo di rete di ramo, che sembra un nodo finale nel nodo uplink di ramo.

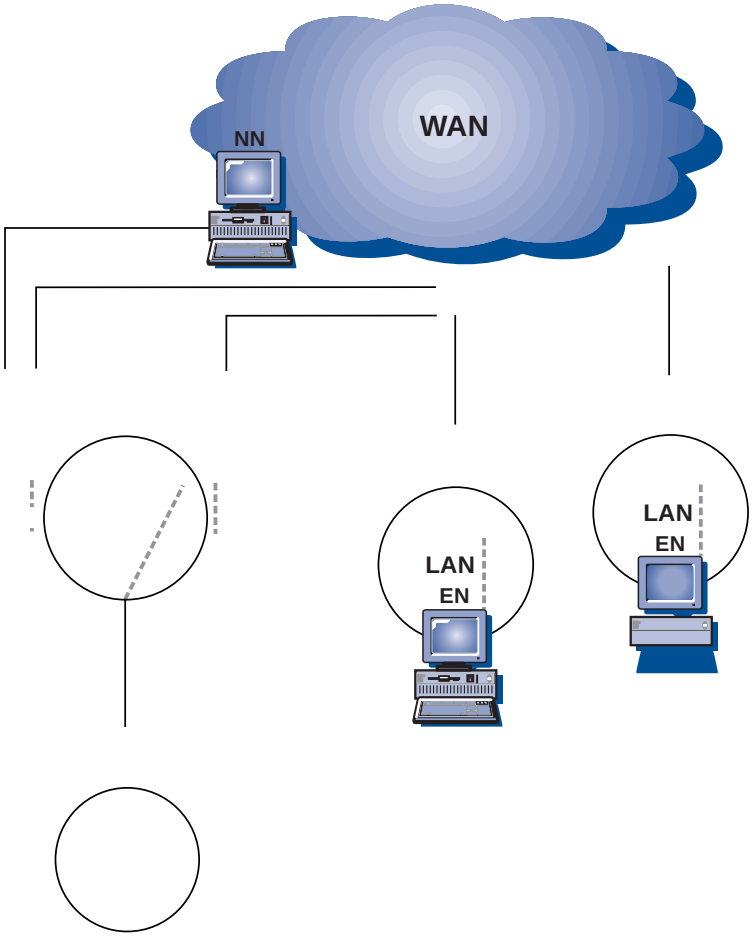


downlink di ramo sono solitamente collegamenti LAN (ma non è necessario che lo siano). E' possibile intendere i nodi finali collegati attraverso i downlink di ramo come risorse locali. Il nodo di rete di ramo è l'NNS per tali nodi finali. Sui downlink di ramo, fornisce servizi del nodo di rete per nodi finali di dominio, nodi finali LEN, nodi T2.0 dipendenti e nodi T2.1, LU locali e PU.

Un nodo di rete di ramo funziona come un NNS per il suo dominio. Conserva le informazioni topologiche su tutti i propri nodi downlink di ramo, ma non conserva le informazioni dettagliate sull'intera rete uplink. Se il nodo possiede delle informazioni insufficienti, trasmette le richieste di LOCATE al relativo NNS uplink, che potrebbe essere un altro nodo di rete di ramo o un nodo di rete APPN.

Il branch extender ottimizza l'ambiente di comunicazione peer-to-peer per i responsabili che desiderano collegare i rami basati sulla LAN alla WAN più estesta basata principalmente su una rete commutata. Il branch extender potenzia le prestazioni sulle reti APPN di vaste proporzioni. In particolare:

- Riduce il numero dei nodi di rete in reti APPN estese, consentendo in tal modo di aggiungere ulteriori reti di ramo
- Nasconde informazioni sulla topologia del ramo
- Permette la comunicazione peer-to-peer tra rami collegati alla stessa rete di collegamento APPN
- Permette che coesistano con server gateway PU
- Riduce il traffico delle sessioni CP-CP di uplink (traffico WAN)
- Isola la rete di ramo dal traffico WAN backbone


WAN
NN
LAN
EN
LAN
EN

- Per evitare un loop di ricerca, i nodi finali downlink devono essere nodi finali effettivi, non dei nodi che presentano un'immagine di nodo finale.
- Un nodo non può avere sessioni CP-CP con il nodo di rete di ramo tramite gli uplink e i downlink di ramo contemporaneamente.
- Un nodo di rete di ramo può avere sessioni CP-CP solo su un uplink di ramo alla volta; cioè, può avere sessioni CP-CP con al massimo un NNS.
- Il branch extender non fornisce supporto Twinax
- Un nodo del branch extender non può avere downstream delle sessioni DLUR.

Configurazione del Branch Extender

Per configurare il branch extender, è necessario configurare prima un nodo di rete di ramo. Quindi, è necessario configurare un DLC (per un collegamento implicito) o un nodo di rete di ramo. Un collegamento configurato per supportare il branch extender è un uplink di ramo. Su un nodo di rete di ramo, tutti i collegamenti non configurati per supportare la funzione sono downlink di ramo.

Se sono stati definiti collegamenti tra nodi di rete di ramo, è necessario che vengano definiti come collegamenti ***peer***, che conferiscono loro un tipo di collegamento **LEARN** nel file ACG. Altrimenti, è possibile definire il collegamento come **ACTIVATE_AT_STARTUP=1** in modo che il collegamento sia sempre attivo. Quando i nodi di ramo si collegano tra loro, si verificano dei loop nella topologia. Questo è ammissibile fino a che i collegamenti restano sempre attivi o vengono riconosciuti nel momento in cui sono attivati. Se i collegamenti vengono definiti tra i nodi di rete di ramo come collegamenti **END_NODE** o **NETWORK_NODE**, l'upstream segnalato dalla topologia potrebbe interpretare i collegamenti in maniera inappropriata e provocare degli errori di assegnazione.

Per configurare il branch extender è possibile utilizzare anche un file ACG.

Gestione del branch extender

Nelle seguenti sezioni viene descritto come verificare una configurazione e vengono riportate le limitazioni relative alla configurazione della rete.

Verifica della configurazione: E' possibile utilizzare **Operazioni nodo SNA** per un nodo che supporta Branch Extender per stabilire se un ramo locale è stato configurato correttamente. Durante il runtime, una finestra relativa alla topologia del nodo non deve contenere più di due nodi di rete, il nodo stesso ed il server del nodo di rete dell'uplink.

Nota: Soltanto un uplink è disponibile per CP-CP. Ciascuna stazione di lavoro deve essere configurata come nodo finale con il nodo di rete del ramo definito come server del nodo di rete preferito.

E' possibile utilizzare **Operazioni nodo SNA** per verificare se il DLC o il collegamento è stato configurato correttamente per supportare Branch Extender. Inoltre, esso può essere utilizzato per stabilire se un collegamento attivo è un uplink o un downlink di ramo. I nodi finali downstream registrati mediante AnyNet non registrano le proprie risorse.

Funzioni supportate

Communications Server supporta tutte le funzioni di base della Versione 2 di APPN (sia i nodi finali che i nodi di rete). Inoltre, sono supportate le opzioni seguenti:

- Nodo Finale

Serie di funzioni	Opzioni
008	Multiple TG
023	BIND Segmenting and Reassembly
041	Session Segmenting/Reassembly
081	Class-of-Service Manager
161	MS_CAPS Have Backup or Implicit FP
162	MS_CAPS Be Sphere of Control (SOC) EN
171	Problem Diagnosis Data in Alert
177	LAN Alert
178	SDLC/LAN LLC Alert
181	X.25 Alert
182	Held Alert for CPMS
1002	Adjacent Link Station Name
1004	Adjacent CP Name Change Support
1007	Parallel TGs
1011	Multiple Local Independent LUs
1012	CP=LU
1013	Interoperability with Peripheral Border Node
1015	CP-CP Session Activation Enhancements
1018	Delete EN Resources Before Registering
1067	Dependent LU Requester
1070	Session Cryptography
1107	Central Resource Registration (of LUs)
1116	DLUS-Served LU Registration
1200	Tree and TG Caching
1400	HPR Base (ANR)
1401	Rapid Transport Protocol
1402	Control Flows over RTP
1520	1Common Operations Services

- Nodo di rete

Serie di Funzioni	Opzioni
164	MS_CAPS Have a Subarea Focal Point
171	Problem Diagnosis Data in Alert

177	LAN Alert
178	SDLC/LAN LLC Alert
181	X.25 Alert
182	Held Alert for CPMS
1002	Adjacent Link Station Name
1004	Adjacent CP Name Change Support
1007	Parallel TGs
1011	Multiple Local Independent LUs
1012	CP=LU
1013	Interoperability with Peripheral Border Node
1015	CP-CP Session Activation Enhancements
1018	Delete EN Resources Before Registering
1067	Dependent LU Requester
1070	Session Cryptography
1100	Safe-Store of Directory Cache
1101	Preload Directory Cache
1107	Central Resource Registration (of LUs)
1116	DLUS-Served LU Registration
1118	EN TG Vector Registration
1121	Branch Extender Function
1200	Tree and TG Caching
1203	Detection and Elimination of TDU Wars
1301	Nonpaced Intermediate Session Traffic
11400	HPR Base (ANR)
1401	Rapid Transport Protocol
1402	Control Flows over RTP
1520	Common Operations Services

DLC (Data Link Control)

DLC fornisce i protocolli necessari per una distribuzione affidabile delle BTU (basic transmission units) tra una coppia di nodi nella rete APPN e per la gestione dei collegamenti logici tra i nodi.

Collegamenti

Una connessione collega una coppia di nodi adiacenti attraverso il DLC principale.

Collegamenti paralleli

E' possibile che il nodo locale abbia più collegamenti ad un nodo adiacente. Questa associazione viene definita come ***collegamenti paralleli***. A ciascuno dei collegamenti paralleli viene assegnato un numero univoco (numero del gruppo di trasmissione) e vengono attribuite caratteristiche di collegamento diverse. Per avere due collegamenti paralleli tra due nodi, le stazioni di collegamento possono coesistere su un singolo adattatore in un nodo ma devono trovarsi su adattatori separati nell'altro nodo; quindi, la combinazione del numero di adattatore e l'indirizzo della stazione di collegamento (o destinazione) adiacente deve essere univoca per ogni collegamento.

Attivazione collegamento

L'unità di messaggio che viene utilizzata per fornire le caratteristiche del nodo e del collegamento ad un nodo adiacente è definita come ***XID*** (Exchange Identification). Se **USE_PU_NAME_IN_XID=1**, il nome della PU viene utilizzato nel campo del nome del CP di XID. Altrimenti, il nome del CP viene utilizzato in quel campo. Le XID vengono scambiate tra i nodi prima e durante l'attivazione del collegamento per stabilire e negoziare le caratteristiche del collegamento e del nodo, e dopo l'attivazione del collegamento per comunicare le modifiche in tali caratteristiche.

I nodi APPN scambiano XID3 (XID format 3) con altri T2.1 o nodi a margine per eseguire uno scambio di ruoli. Per i collegamenti PU 2.0, utilizzare la parola chiave **LINK_STATION** per indicare un nome PU e un ID di nodo che vengono scambiati su XID3. Se **USE_PU_NAME_IN_XID=1**, il nome PU viene utilizzato nel campo del nome di XID. Altrimenti, il nome del CP viene utilizzato in quel campo. Le informazioni relative all'invio delle caratteristiche del nodo sono contenute in XID3, incluso il ruolo della stazione di collegamento (primario, secondario o negoziabile), il numero TG, il tipo di nodo, il numero di collegamento logico, la dimensione massima della BTU (unità di trasmissione di base) che può essere ricevuta, l'ID del nodo ed il nome della PU. Il nome della PU è, di solito, il nome del CP, ma nomi di PU e ID di nodo alternativi possono essere specificati nella parola chiave **LINK_STATION** per supportare collegamenti PU 2.0 simultanei.

Tipi di collegamento

I sei tipi di collegamenti riportati di seguito vengono propriamente definiti nei nodi di Communication Server:

- Accesso primario alla rete, attivato all'inizio (APPN o host)
- Accesso primario alla rete, collegamento host
- Accesso primario alla rete, sempre attivo (utilizzare quando richiesto)
- Accesso secondario alla rete, collegamento in entrata (caratteristiche di collegamento predefinite)
- Accesso secondario alla rete, uso limitato (definito anche come collegamento risorsa limitato)

La configurazione di Communications Server fornisce un modo per definire e controllare l'utilizzo di questi tipi di collegamento. Questa sezione descrive i parametri del nodo, di DLC, e della configurazione del collegamento utilizzati come pure le relazioni e le dipendenze che sussistono tra tali parametri. Vengono descritte le seguenti categorie:

- Parametri di attivazione e di definizione del collegamento
- Parametri di disattivazione del collegamento
- Altri parametri di collegamento

Vengono descritti i seguenti parametri:

- Parametri di attivazione e di definizione
  - Attivazione all'avvio
  - Attivazione su richiesta
  - Tentativo automatico di collegamento
  - Numero massimo dei tentativi di attivazione
  - Riattivazione richiesta dall'utente
- Parametri di disattivazione
  - Timeout inattività
  - Risorse limitate
- **Altri parametri di collegamento**
  - Rete di collegamento
  - Supporto sessioni CP-CP
  - Supporto HPR (High performance routing)
  - Tipo di nodo adiacente
  - NNS preferito
  - Sollecita sessioni SSCP
  - Nome PU (quando sollecita sessioni SSCP è pari a **1**)

Nota: Questi parametri si trovano nel file ACG e potrebbero non essere disponibili nelle finestre (**Configurazione nodo**).

Parametri di attivazione e di definizione del collegamento

Questa sezione descrive i parametri di attivazione e di definizione.

Attivazione all'avvio

Un collegamento ***attivazione all'avvio*** viene utilizzato, di solito, per i collegamenti di accesso primario alla rete che vengono attivati inizialmente quando si avvia Communications Server. Il collegamento viene attivato quando viene avviato Communications Server sulla propria macchina e rimane attivo finché Communications Server è in esecuzione.

Per definire un collegamento da attivare all'avvio, specificare **ACTIVATE_AT_STARTUP = 1** nella parola chiave **LINK_STATION** del file ACG. Generalmente i collegamenti vengono configurati per essere attivi all'avvio quando questi risultano importanti per la connettività della rete. Un collegamento importante può essere configurato anche per tentare il collegamento automaticamente (consultare “Tentativo automatico di collegamento” a pagina 38).

Il collegamento da un EN (end node) APPN al relativo NNS (network node server) preferito è un esempio di questo tipo di collegamento.

Un esempio di collegamento che non viene attivato all'avvio, codificato come **ACTIVATE_AT_STARTUP = 0**, potrebbe essere rappresentato da un collegamento host che non è richiesto appena viene avviato Communications Server, da un collegamento in entrata, le cui caratteristiche sarebbero controllate da un nodo, o da un collegamento che potrebbe risultare troppo costoso per essere mantenuto attivo tutto il tempo. Questi collegamenti vengono definiti in modo da non essere attivati all'avvio e vengono attivati quando le risorse di collegamento sono richieste da un'applicazione (consultare “Attivazione su richiesta”) o dal partner.

Attivazione su richiesta

Un collegamento ***attivazione su richiesta*** (definito anche come “attivazione automatica”) viene di solito utilizzato per l'accesso ad una LU partner che richiede un'attivazione dinamica del collegamento. Quando Communications Server viene avviato, il collegamento rimane inattivo. Comunque, è collocato nella topologia come collegamento disponibile se è specificato un nome di CP adiacente. Il collegamento viene attivato quando un TP (transaction program) richiede una connessione ad una LU remota che, a sua volta, richiede, che il collegamento sia attivo. Communications Server utilizza la LU partner completa definita per attivare il collegamento.

Per definire un collegamento ad attivazione su richiesta, **ACTIVATE_AT_STARTUP = 0** e **FQ_ADJACENT_CP_NAME**=(netid.cpname) devono essere configurati nella parola chiave **LINK_STATION** nel file ACG del nodo di origine. Se il partner non è **FQ_ADJACENT_CP_NAME**, configurare la parola chiave **PARTNER_LU**.

Frequentemente, un collegamento ad attivazione su richiesta viene anche configurato come una risorsa limitata (consultare “Risorse limitate” a pagina 40) o con un timeout di inattività (consultare “Timeout di inattività” a pagina 39) in modo che il collegamento venga disattivato nel momento in cui non è più richiesto.

Un esempio di collegamento ad attivazione su richiesta è costituito da un collegamento che definisce una connessione ad un partner il quale deve necessariamente essere attivo per un periodo limitato di tempo. Tale collegamento potrebbe costare più di quanto si sia disposti a pagare per mantenerlo attivo tutto il tempo. Se, ad esempio, si è in possesso di uno o più computer che riescono a stabilire regolari comunicazioni, a fine giornata, è possibile richiedere ad una delle macchine di attivare un collegamento a qualche macchina remota allo scopo di inviare i risultati giornalieri o per effettuare un backup dei dati.

Un altro esempio potrebbe essere rappresentato dalle connessioni ad un server di dati o ad un server di stampa. Il collegamento richiede alcune risorse sul server. Al fine di evitare delle limitazioni sul numero massimo delle stazioni di collegamento e di sessioni sul server, configurare un collegamento su richiesta per liberare le risorse presenti sul server dei dati dopo che le richieste relative al collegamento ad attivazione su richiesta sono state completate.

Un collegamento ad attivazione su richiesta non è necessariamente un collegamento di risorsa limitato, ma potrebbe essere definito come tale includendo il parametro **LIMITED_RESOURCE = 1** nella parola chiave **LINK_STATION** (consultare “Risorse limitate” a pagina 40).

Tentativo automatico di collegamento

Il tentativo automatico di collegamento è una funzione di recupero di un collegamento non riuscito a causa di un errore. Se è necessario riattivare un collegamento (senza l'intervento dell'utente) dopo un errore, è possibile utilizzare il tentativo automatico di collegamento. Il tentativo automatico di collegamento effettua dei tentativi di riattivazione automatica del collegamento se i parametri, riportati di seguito, sono stati specificati nelle parole chiave **LINK_STATION** o **PORT** :

- **DELAY_APPLICATION_RETRIES**
- **RETRY_LINK_ON_DISCONNECT**
- **RETRY_LINK_ON_FAILED_START**
- **RETRY_LINK_ON_FAILURE**.

Se uno di questi parametri viene specificato nella parola chiave **PORT**, i valori vengono utilizzati dalla parola chiave **LINK_STATION** se è stato indicato il parametro **INHERIT_PORT_RETRY_PARMS**.

Dopo un'attivazione riuscita, il timer di intervallo viene impostato nuovamente su 0.

Potrebbe rivelarsi vantaggioso utilizzare il tentativo automatico di collegamento su ciascuno dei tipi di collegamento elencati di seguito:

- Un collegamento ad un NN che viene attivato all'avvio. Se il collegamento non viene stabilito, viene riattivato solo un collegamento NNS (network node server).
- Collegamento host
- Un collegamento primario che dispone di un backup (definito, anche, come collegamento ad attivazione all'avvio)
- Qualsiasi collegamento che deve rimanere attivo sempre.

Numero massimo dei tentativi di attivazione

Il numero massimo dei tentativi di attivazione è un parametro di attivazione collegamento che fornisce un meccanismo in grado di impedire al traffico host della LU dipendente (ad esempio, un gateway LUA, 3270, LU 2 e/o DLUR che tenta di attivare un collegamento host per un'applicazione downstream) di effettuare un numero indefinito di tentativi di attivazione collegamento. Il parametro del numero massimo dei tentativi di attivazione **INHERIT_PORT_RETRY_PARMS** rappresenta il numero delle volte in cui viene tentata una richiesta di attivazione collegamento. Una volta raggiunto tale numero, le successive richieste vengono respinte fino a quando viene impostato di nuovo il numero di tentativi. Le richieste di attivazione collegamento della LU dipendente inoltrate dopo che è stato raggiunto il numero massimo dei tentativi di attivazione vengono respinte subito senza tentare effettivamente di attivare il collegamento. In tal caso, viene restituito un codice di ritorno primario di X'0003' e un codice secondario di X'00000005', un tentativo DLC, con un codice sense di X'00000000'. Le richieste di attivazione collegamento della LU indipendente inoltrate dopo che è stato raggiunto il numero massimo dei tentativi di attivazione restituisce insieme al codice di ritorno primario X'0003' e secondario X'00000005', un codice sense di 081C0001 per indicare che è stato raggiunto il limite massimo dei tentativi di attivazione.

Nota: Se un TP, come un'applicazione LUA, va in loop cercando di attivare una sessione sullo stesso host dell'applicazione LU dipendente, verrà raggiunto il numero massimo dei tentativi di attivazione prima che l'applicazione dipendente possa effettuare la sua prima richiesta.

Il numero massimo dei tentativi di attivazione viene reimpostato nel modo seguente:

- Quando un TP indipendente attiva il collegamento. I TP devono controllare il codice sense ed utilizzare un protocollo appropriato per l'attivazione del collegamento che non ritenta di effettuare l'attivazione all'infinito.
- Quando l'utente attiva il collegamento utilizzando **Operazioni nodo SNA**.
- Quando il collegamento viene attivato dall'altra direzione (ad esempio, dal partner).

Se **Operazioni nodo SNA** sta tentando l'attivazione di un collegamento, il numero massimo di tentativi di attivazione viene diminuito di 1 ed il risultato viene ignorato. Se il limite è stato superato su un collegamento host gateway, l'attivazione del collegamento verrà tentata dopo 30 minuti se è divenuto attivo un collegamento della stazione di lavoro. Questo comporta l'interruzione dei tentativi che vengono ripresi in seguito quando vengono riavviate le stazioni di lavoro. Quando gateway, LUA o **Operazioni nodo SNA** attivano un collegamento correttamente, il numero massimo di tentativi di attivazione viene impostato su 0.

Per configurare il numero massimo dei tentativi di attivazione su un collegamento, il parametro **MAX_ACTIVATION_ATTEMPTS**= n viene configurato nella parola chiave **LINK_STATION**, dove n è il numero dei tentativi da -1—127. -1 indica che dovrebbe essere utilizzato il valore nella parola chiave **PORT** e 0 indica un numero indefinito di tentativi.

Riattivazione richiesta dall'utente

La ***Riattivazione richiesta dall'utente*** si verifica quando l'utente richiede di riattivare un collegamento da **Operazioni nodo SNA** o dalla riga comandi utilizzando, ad esempio, Communications Server.

Parametri di disattivazione del collegamento

Le seguenti sezioni descrivono i parametri di disattivazione.

Timeout di inattività

Timeout di inattività è un parametro di disattivazione del collegamento SDLC che controlla quando i collegamenti vengono disattivati. Il valore del timeout di inattività indica il tempo (in secondi) in cui un collegamento può rimanere inattivo prima che sia disattivato. Questo è simile al **LINK_DEACT_TIMER** nella parola chiave **LINK_STATION**. La differenza consiste nel fatto che il **LINK_DEACT_TIMER** aspetta che tutte le sessioni vengano chiuse (il numero delle sessioni raggiunge lo 0) prima di disattivare il collegamento. **INACTIVITY_TIMER** ignora il numero delle sessioni e disattiva il collegamento dopo che è rimasto inattivo per il tempo specificato.

La funzione timeout di inattività è stata implementata per gestire la situazione in cui una sessione di emulazione, una connessione LUA, 3270, o LEN, è stata lasciata

attiva casualmente per lunghi periodi di tempo. Quando il nodo non rileva nessuna attività su questo tipo di collegamento per la durata di **INACTIVITY_TIMER**, il collegamento viene disattivato automaticamente, anche se esistono sessioni e comunicazioni attive sul collegamento. Per definizione, **LINK_DEACT_TIMER** non è considerato dannoso, mentre **INACTIVITY_TIMER** è considerato dannoso.

Note:

1. Il timeout di inattività può essere utilizzato su collegamenti a risorsa limitata o a risorsa non-limitata. Un collegamento è definito come risorsa limitata e le comunicazioni rimangono attive, il timeout a risorsa limitata non scade ed il collegamento verrà disattivato allo scadere del timeout di inattività. Se un collegamento è definito come risorsa non-limitata, il timeout di inattività viene utilizzato per disattivare il collegamento per liberare le risorse all'estremità remota.
2. Attualmente con HPR, il timeout di inattività viene ignorato. Questo accade perché HPR non è in grado di riconoscere il traffico presente sul collegamento e perché il protocollo keepalive HPR produce traffico sufficiente per mantenere il collegamento sempre attivo.

Per configurare il timeout di inattività su una connessione SDLC, il parametro **INACTIVITY_TIMER**= n è codificato nel parametro **LINK_STATION_SDLC_SPECIFIC_DATA** della parola chiave **LINK_STATION** nel file ACG, dove n è un valore compreso tra 40 e 160. Per configurare il timeout di inattività per un collegamento, il parametro **LINK_DEACT_TIMER**= n viene codificato nella parola chiave **LINK_STATION** del file ACG, dove n è un valore compreso tra 0 e 1 000. Lo 0 indica che non esiste un timeout (il collegamento resterà attivo). Il valore predefinito SDLC è 80 ed il valore predefinito per il collegamento è 10.

Risorse limitate

Un collegamento a risorse limitate è utilizzato, di solito, per i collegamenti di accesso primario alla rete ad uso limitato e per i collegamenti di accesso secondario alla rete. Un collegamento a risorse limitate è un collegamento che viene disattivato automaticamente quando il numero delle sessioni raggiunge lo 0. Il collegamento a risorse limitate può essere definito come **ACTIVATE_AT_STARTUP=1** o **ACTIVATE_AT_STARTUP=0**. Se il collegamento è **ACTIVATE_AT_STARTUP=1**, viene avviato all'avvio di Communications Server. Se il collegamento è **ACTIVATE_AT_STARTUP=0**, viene collocato nella topologia quando viene avviato Communications Server, se è specificato il nome del CP adiacente ed attivato quando i servizi vengono richiesti.

Nota: I collegamenti ad attivazione all'avvio non vengono collocati all'interno della topologia a meno che non siano attivi.

Per configurare un collegamento a risorse limitate, **LIMITED_RESOURCE = 1** viene specificato nella parola chiave **LINK_STATION** del file ACG. Il **LINK_DEACT_TIMER**= n è specificato nella parola chiave **LINK_STATION** ed il parametro **ADJACENT_NODE_TYPE=LEARN** deve essere specificato.

Nota: Se **CP_CP_SESSION_SUPPORT=1**, il collegamento non è un collegamento a risorse limitate. La verifica della configurazione indica questo come un'avvertenza. Le sessioni CP-CP attive impediscono la disattivazione del collegamento.

Reti di collegamento

Le reti di collegamento permettono ai nodi APPN in una LAN di avere collegamenti diretti tra loro senza richiedere definizioni di collegamento logico ad ogni nodo. Tale caratteristica riduce ampiamente la definizione del sistema senza dover instradare tutte le sessioni attraverso un nodo di rete. Consente inoltre, ai nuovi nodi che vengono aggiunti alla LAN di partecipare interamente alle comunicazioni APPC senza richiedere le modifiche di definizione a ciascun nodo.

Un nodo di rete nella rete di collegamento presume che tutti i nodi in una rete di collegamento possono avere collegamenti diretti tra loro. Quando si calcola l'instradamento per una sessione, il nodo di rete valuta il collegamento diretto e solitamente sceglie il collegamento diretto come instradamento ottimale. Avendo calcolato l'instradamento diretto, il nodo di rete invia, semplicemente, al nodo finale l'indirizzo del partner da utilizzare per l'attivazione del collegamento.

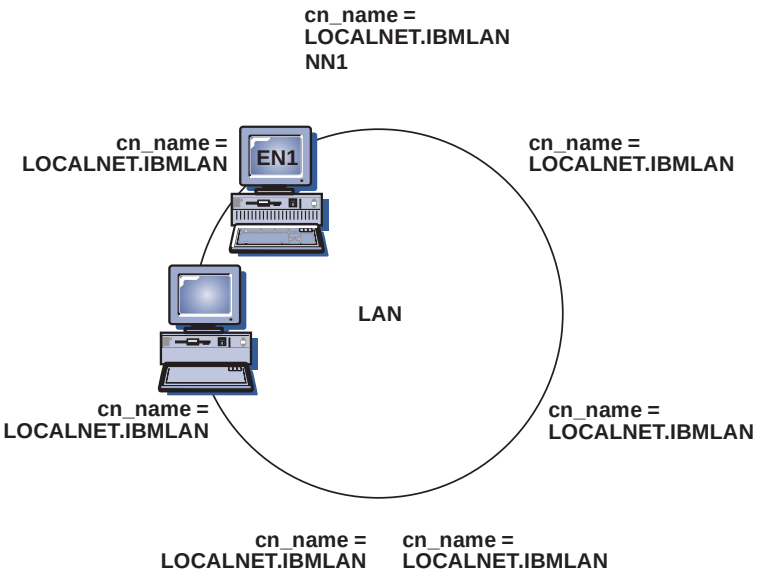
L'instradamento della rete di collegamento potrebbe non essere utilizzato quando la sicurezza della rete di collegamento è inferiore rispetto a quanto richiesto. Se DLC della rete di collegamento non è protetto e viene utilizzato un modo come #BATCHSC sul parametro **MODE_NAME**, il nodo di rete tenta di trovare un instradamento protetto, ignorando la rete di collegamento.

Se i bridge LAN vengono utilizzati, APPN visualizza tutta la LAN con bridge come una singola rete logica. Poiché i collegamenti possono essere attivati tra due sistemi qualsiasi sulla LAN, è necessaria soltanto una rete di collegamento. La rete di collegamento dovrebbe essere definita in tutti i sistemi APPN sulla LAN.

Un nodo di rete apprende le informazioni relative alla rete di collegamento durante la registrazione EN e le ricerche di directory APPN. Il server del nodo di rete, a questo punto, dispone di sufficienti informazioni per calcolare un collegamento diretto tra i nodi finali di sessioni senza l'instradamento attraverso dei nodi intermedi.

Solo i nodi finali ed i nodi di rete possono trarre vantaggio dalla rete di collegamento; i collegamenti ai nodi LEN devono essere chiaramente definiti.

Figura 12 a pagina 42 illustra una rete di collegamenti di esempio. Questa figura mostra una rete di collegamenti denominata LOCALNET.IBMLAN. Con questo tipo di definizione, qualsiasi EN è in grado di collegarsi direttamente a qualunque altro EN finché NN1 è l'NNs attivo per tutti i nodi di rete.


cn_name =
LOCALNET.IBMLAN
NN1
cn_name =
LOCALNET.IBMLAN
EN1
cn_name =
LOCALNET.IBMLAN
LAN
cn_name =
LOCALNET.IBMLAN
cn_name =
LOCALNET.IBMLAN
cn_name =
LOCALNET.IBMLAN
cn_name =
LOCALNET.IBMLAN

NNS preferito

L'NNS preferito indica se il nodo di rete adiacente deve essere utilizzato come l'NNS sul collegamento in fase di definizione.

Sollecita sessioni SSCP

Sollecita sessioni SSCP indica se le sessioni SSCP-PU sono o non sono richieste dall'host su cui si sta definendo il collegamento.

Directory Services

Un nodo di rete fornisce i directory services alle LU ubicate nel nodo di rete e alle LU nei nodi finali che il nodo di rete utilizza. Il nodo di rete consente ai directory services forniti da altri nodi di rete nella rete di rispondere positivamente alle richieste di ricerca directory ricevute quando la risorsa specificata viene trovata nella directory locale. La directory locale associa un nome di LU al nome del CP del nodo dove è ubicata la LU. Se il CP di destinazione è un LEN o un nodo finale, la directory include il nome del nodo di rete necessario.

Il componente Directory Services risiede in ogni nodo; comunque, lo scopo e le relative funzioni variano a seconda del livello di supporto directory nel nodo.

Un nodo finale gestisce una directory locale che contiene voci per le LU residenti localmente. Inoltre, il nodo finale gestisce voci di directory per le LU in nodi adiacenti con i quali il nodo finale è stato in sessione. Per una sessione LU-LU con un nodo peer adiacente, una ricerca della directory locale restituisce il CP di destinazione corretto associato con la LU ricercata, consentendo che venga selezionato il collegamento logico appropriato.

In un nodo LEN, tutte le LU partner vengono immesse nella directory, come mostra l'esempio in Figura 13 a pagina 44. Quelle che non si trovano all'interno di un nodo finale peer adiacente, ma all'esterno di una rete APPN vengono associate nella relativa directory al proprio server nodo di rete indicato. Il nodo LEN invia una richiesta (BIND) di attivazione della sessione LU-LU al proprio server nodo di rete per qualsiasi LU associata nella relativa directory al proprio server; il server individua automaticamente la LU di destinazione ed inoltra il BIND correttamente. Il nodo di rete può inviare una ricerca Locate, attendere la risposta e poi inviare il BIND.

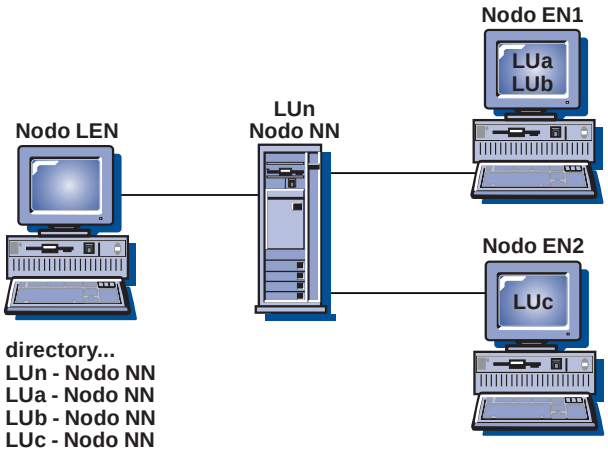


Figura 13. Directory del nodo LEN. La directory del nodo LEN deve contenere tutte le LU con le quali comunica. Poiché l'NN (network node) adiacente serve il nodo LEN anche senza le sessioni CP-CP, è necessario che il nodo LEN definisca il CP del nodo di rete come "CP in comunicazione" di tutte le LU, comprese le LU individuate negli EN (end node).

Quando una LU non è rappresentata in una directory del nodo finale, il nodo finale comincia una ricerca Locate per trovare la LU desiderata. Per attivare la ricerca, il nodo finale richiama i servizi del proprio server nodo di rete. In Figura 14 viene mostrato un esempio di directory del nodo finale.

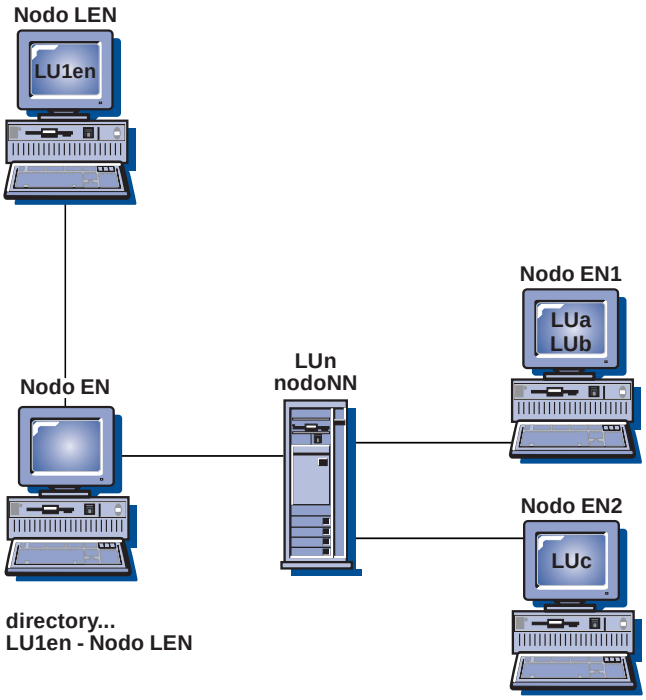


Figura 14. Directory del nodo finale. L'EN (end node) utilizza i servizi del proprio server nodo di rete per trovare l'ubicazione delle LU. Nessuna delle LU nella rete APPN deve essere definita nel nodo finale. La LU del nodo LEN adiacente, comunque, deve essere definita in quanto non è collegata al nodo di rete e non appartiene alla rete APPN.

Un nodo di rete fornisce i Directory Services distribuiti ai propri nodo finale utilizzati con tutti gli altri nodo di rete nella rete APPN. Il nodo di rete di origine riceve il nome di una LU di destinazione in una richiesta di ricerca Locate da un nodo finale, o il nome di una LU secondaria in un BIND da un nodo LEN. Il nodo di rete verifica

l'attuale ubicazione della LU se è rappresentata nella directory del nodo di rete (ma non è nel nodo di rete stesso). La verifica viene effettuata inviando una ricerca orientata al server nodo di rete di destinazione.

Se la LU non si trova nella directory del nodo di rete di origine, il nodo di rete inizia una ricerca della rete. La ricerca viene avviata inviando una ricerca broadcast ad ogni nodo di rete adiacente, ciascuno dei quali a turno diffonde la broadcast e restituisce risposte che denotano la riuscita o l'errore. Per le necessità future, un nodo di rete memorizza nella cache le informazioni ottenute da ricerche broadcast riuscite.

Un nodo finale APPN può anche ricevere (e rispondere alle) richieste di ricerca Locate dal proprio server nodo di rete per ricercare o per garantirne la presenza continua di LU specifiche nel nodo finale.

Ogni nodo finale può registrare le proprie LU con il relativo server nodo di rete inviando un messaggio di registrazione al nodo di rete. Se il nodo finale viene registrato con l'NNS, il nodo di rete gestisce le informazioni della directory attuale che si riferiscono agli nodo finale nel relativo dominio.

La Figura 15 mostra un esempio di una directory del nodo di rete.

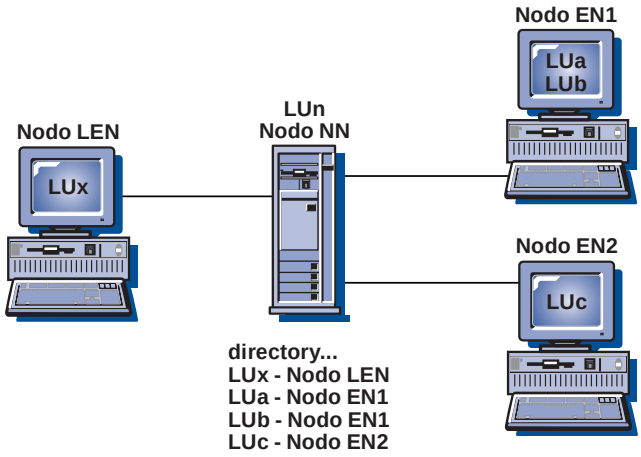


Figura 15. Directory del nodo di rete. La directory del NN (network node) contiene tutte le LU che serve. Gli EN (end node) registrano le proprie LU; è necessario configurare la LU del nodo LEN.

Servizi di selezione-instradamento e topologia

Un nodo di rete fornisce servizi di selezione-instradamento a sé stesso e agli nodo finale utilizzati. Gestisce un database della topologia di rete interna che dispone di informazioni sulla topologia attuali e complete relative alla rete. Queste informazioni sulla topologia sono costituite dalle caratteristiche di tutti i nodi di rete nella rete e da tutti i collegamenti tra i nodo di rete. Tutti i nodo di rete contengono una copia del database della topologia .

Un nodo di rete utilizza il database della topologia di rete per elaborare instradamenti per le sessioni che hanno origine nelle LU presenti e nei nodi finali utilizzati. Ciascun instradamento elaborato dal nodo di rete rappresenta l'instradamento corrente meno complesso dal nodo contenente la LU di origine al

nodo contenente la LU di destinazione. Per fornire un percorso appropriato attraverso la rete, l'algoritmo utilizzato per selezionare l'instradamento assegna, innanzitutto, delle priorità ai collegamenti ed ai nodi. L'algoritmo di priorità calcola un valore scalare per ogni nodo e collegamento logico, in base al rispettivo significato delle caratteristiche per la classe di servizio richiesta.

Database topologia

Il database della topologia in un nodo di rete contiene delle informazioni su tutti i nodo di rete e tutti i gruppi di trasmissione intercollegati ad essi. Si tratta di un database interamente replicato che viene condiviso tra tutti i nodo di rete nella rete ed utilizzato per la selezione dell'instradamento. La gestione del database richiede aggiornamenti broadcast tra tutti i nodo di rete. Gli aggiornamenti vengono realizzati attraverso messaggi TDU (topology database update), che contengono informazioni sull'identificazione del nodo, sulle caratteristiche del nodo e del collegamento e sui numeri di sequenza di aggiornamento per identificare le modifiche più recenti per ciascuna delle risorse descritte in un TDU.

Un database della topologia locale in un nodo finale contiene soltanto informazioni su sé stesso e sui nodi direttamente collegati.

Un componente di servizi di instradamento e topologia utilizza le sessioni CP-CP tra i nodo di rete per scambiare informazioni per creare e gestire un database della topologia. Tale database della topologia nei nodo di rete viene aggiornato utilizzando degli aggiornamenti che vengono trasmessi tra tutti i nodo di rete qualora una risorsa (nodo o collegamento) sia attivata o disattivata, o si modificano le caratteristiche di una risorsa esistente.

Un database della configurazione locale ed un database della topologia di rete vengono gestiti su ogni nodo di rete come mostrato in Figura 16 a pagina 48. Il database della configurazione locale è univoco sul nodo, mentre il database della topologia di rete è replicato su tutti i nodo di rete.

Tabella 2 mostra le informazioni contenute nel database della configurazione nel nodo di rete locale.

Tabella 2 (Pagina 1 di 2). Databse della configurazione NN locale

Nodo	Collegamenti	Connessione
NN5	e	NN5—EN1
	a	NN5—NN7
	b	NN5—NN6
NN7	a	NN7—NN5
	d	NN7—NN8
NN6	b	NN6—NN5
	f	NN6—EN2
	c	NN6—NN8
	g	NN6—EN3

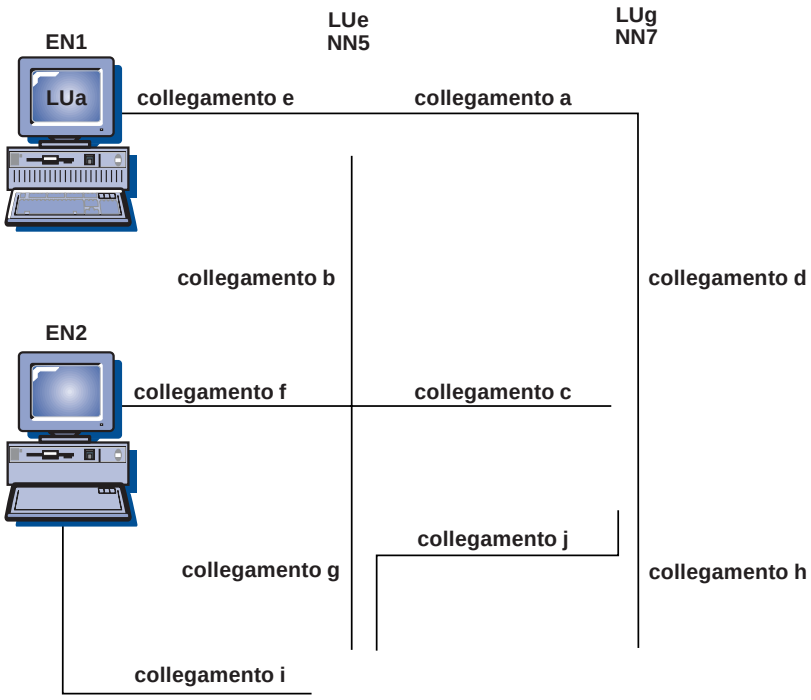
Tabella 2 (Pagina 2 di 2). Databse della configurazione NN locale

Nodo	Collegamenti	Connessione
NN8	c	NN8—NN6
	d	NN8—NN7
	j	NN8—EN3
	h	NN8—EN4

Tabella 3 mostra le informazioni contenute nel database della topologia di rete nel nodo di rete locale.

Tabella 3. Database della topologia di rete NN locale

Nodo	Collegamenti	Connessione
NN5, NN6, NN7, NN8	a	NN5—NN7
	a	NN7—NN5
	b	NN5—NN6
	b	NN6—NN5
	c	NN6—NN8
	c	NN8—NN6
	d	NN7—NN8
	d	NN8—NN7


LUe
NN5
LUg
NN7
EN1
LUa
collegamento e
collegamento a
collegamento b
collegamento d
EN2
collegamento f
collegamento c
collegamento j
collegamento g
collegamento h
collegamento i

Quando una sessione attraversa sia una rete APPN che una rete di subarea, utilizza due classi di servizio:

- Nella rete APPN, la sessione utilizza COS (class of service) definita per il modo utilizzato dal programma di transazione. Tale definizione si trova nella configurazione attiva della stazione di lavoro. Questa COS viene utilizzata per instradare la sessione nella rete APPN.

  Se non viene immesso alcun valore, la COS associata è #CONNECT.

- Nella rete subarea, il nome di COS può essere scritto nella tabella del modo di collegamento, nella voce per il nome del modo usato dalla sessione. Questo nome di COS viene utilizzato dal programma VTAM per instradare la sessione attraverso la rete subarea.

  Se non si immette alcun valore o se non si definisce nessuna COS in una voce della relativa tabella del modo di collegamento, la COS non viene impostata automaticamente su nessuna voce nella tabella ISTSDCOS.

In entrambi i casi, ogni rete utilizza il nome del modo per trovare il nome della COS, ma i nomi delle due COS non sono necessariamente uguali.

Priorità della trasmissione SNA

La priorità della trasmissione è un valore indicato nella classe di servizio. La priorità della trasmissione viene inviata nel BIND nel vettore di controllo del COS/TPF (Class of Service/Transmission Priority). Una volta che la sessione viene stabilita, i dati della sessione successiva confluiscono nella priorità di trasmissione indicata nel vettore di controllo COS/TPF.

Il flusso dei dati sulle sessioni che utilizzano una classe di servizio ad alta priorità può trasferire dei dati su sessioni a bassa priorità. E' necessario dare priorità alle sessioni che trasmettono il traffico interattivo dove il tempo di risposta è importante, ad esempio, per le sessioni di emulazione. Alle sessioni che trasmettono grosse quantità di dati, ad esempio i trasferimenti file per NetView Distribution Manager, è necessario dare priorità più bassa. Il supporto di priorità della trasmissione impedisce alle sessioni ad alto volume il blocco del traffico sulle sessioni interattive.

Le quattro priorità di trasmissione sono rete, alto, medio e basso. La priorità di rete viene utilizzata per i dati del controllo di rete quali la topologia ed i directory services. Le altre priorità vengono utilizzate per i dati dell'utente.

Communications Server supporta la priorità della trasmissione per i collegamenti LAN, SDLC e X.25. Il vantaggio è più evidente quando la rete contiene dei collegamenti a bassa velocità congestionati.

Selezione Instradamento

Dopo che il server nodo di rete riceve una risposta dalla ricerca locate, il componente dei servizi di instradamento e topologia calcola l'instradamento dal nodo di origine al nodo di destinazione per le COS richieste. Poiché il componente dei servizi di instradamento e topologia invia e riceve aggiornamenti del database della topologia come caratteristiche di qualsiasi modifica delle risorse, ogni instradamento viene calcolato con le informazioni più recenti.

Selezione instradamento per utenti VTAM

Per instradare il traffico APPC attraverso una subarea, le stazioni di lavoro collegate alla subarea devono essere definite come nodi di rete in Communications Server. In ogni nodo di rete, viene definita una connessione che collega il nodo alla subarea. Per il nodo di rete, le LU partner sull'altra parte della subarea vengono definite come se fossero ubicate sull'host (un nodo LEN). Per host, ciascun nodo di rete collegato alla subarea deve essere definito in un programma VTAM con una macro PU. Tutte le unità logiche delle LU 6.2 di destinazione all'interno della rete APPN per un collegamento particolare vengono definite nella PU (il nodo di rete) come se fossero veramente collocate nella PU. Comunque, le LU possono essere effettivamente ubicate in altri nodi all'interno della rete APPN collegata al nodo di rete. L'host visualizza soltanto la PU del nodo di rete. La PU del nodo di rete può anche essere una PU del gateway. Il traffico SETN (**CP_CP_SESS_SUPPORT=NO**) non è consentito quando il parametro è impostato su YES in NCP e non c'è nessuna sessione CP o PU.

Se il nome della PU nella definizione VTAM è lo stesso del nome del CP definito in Communications Server, l'utente non è autorizzato a definire il CP come una LU nelle definizioni VTAM. I nomi devono essere univoci nel programma VTAM, sia che si tratti di nomi di LU che di PU.

La macro PU deve contenere **XID=YES** per utilizzare uno scambio XID durante l'attivazione della PU. Questo parametro viene codificato nel nodo principale NCP. Non deve trovarsi nell'istruzione PU di un nodo principale commutato.

Per i dispositivi SNA commutati, è possibile utilizzare un nuovo parametro nella macro PU: **CPNAME**=cccccccc. Indica il nome del CP del nodo di rete collegato alla subarea. Sia **CPNAME** che **IDBLK** e **IDNUM** devono essere specificati su un'istruzione di definizione PU commutata. Possono essere specificati entrambi. Il nodo di rete fornisce il nome del CP al programma VTAM nello scambio XID durante la sequenza del collegamento. Il programma VTAM utilizza il nome del CP per individuare la macro PU corrispondente. Se non c'è nessuna macro PU con il nome CP corrispondente, il programma VTAM utilizza **IDNUM** e **IDBLK** per individuare la macro PU.

Per instradare il traffico APPC da una rete APPN attraverso la subarea e all'esterno verso un'altra porzione della rete APPN, il nome di rete (**NETID**) del proprio VTAM deve corrispondere all'ID di rete della rete APPN. In Communications Server, l'ID di rete (del nodo di rete collegato alla subarea) può essere rintracciato utilizzando il profilo delle caratteristiche del nodo locale SNA.

Instradamento sessione intermedia

L'instradamento sessione intermedia è una funzione eseguita da un nodo di rete. Tale funzione consente ad un nodo di rete di ricevere ed instradare dei dati destinati ad un altro nodo. L'origine e la destinazione dei dati può essere o un nodo finale, o un nodo di rete, o un nodo LEN. La parte della sessione tra due nodi adiacenti viene definita stage di sessione.

Supporto HPR (High Performance Routing)

Communications Server supporta i collegamenti HPR (high performance routing) su Enterprise Extender (IP), SDLC (synchronous data link control), LAN, WAN, canale, MPC (Multi-Path Channel) ed i collegamenti X.25.

ANR (automatic network routing) di HPR riduce la memoria ed i requisiti di elaborazione nei nodi intermedi e costituisce una soluzione migliore rispetto ad ISR (intermediate session routing) APPN per le reti ad alta velocità con una bassa percentuale di errori.

HPR migliora l'instradamento SNA grazie a queste caratteristiche principali:

- Nodi intermedi stateless

  I nodi intermedi stateless ignorano i collegamenti che passano attraverso essi.

  Un nodo intermedio HPR non necessita di alcun blocco di controllo o pool di buffer per supportare i collegamenti che passano attraverso esso. Non necessita neanche di tabelle di instradamento perché le informazioni sull'instradamento vengono fornite in ogni pacchetto. Utilizzando ANR, un nodo intermedio HPR riceve semplicemente un pacchetto, esamina l'intestazione del pacchetto per trovare un identificativo per il collegamento logico al nodo successivo e invia il pacchetto su quel collegamento.

- Un nodo intermedio HPR:
  - Non ripristina i pacchetti perché gli end point del collegamento HPR rilevano e recuperano i pacchetti persi utilizzando RTP (rapid transport protocol).

    Se la propria LAN presenta un'alta percentuale di errori è anche possibile scegliere un supporto ERP (error recovery protocol) a livello di collegamento. In ogni modo, questo non dovrebbe essere necessario sui collegamenti a bassa percentuale di errori.
  - Non rimonta pacchetti segmentati per poi segmentarli nuovamente, in quanto gli end point del collegamento HPR selezionano automaticamente la dimensione di un pacchetto supportato da tutti i nodi intermedi nell'instradamento.
  - Non gestisce effettivamente i buffer e previene le congestioni perché gli end point del collegamento HPR usano gli algoritmi del controllo del flusso che impediscono la congestione nei nodi intermedi.
  - Non stabilisce l'instradamento di un pacchetto eseguendo una ricerca delle tabelle perché gli end point del collegamento HPR eseguono un istradamento di origine e creano le informazioni di instradamento del pacchetto utilizzando etichette scelte per un'esecuzione ottimale da ogni nodo intermedio.

  Per ottenere nodi intermedi stateless:
  - Gli end point dell'instradamento devono possedere capacità buffer che riflettano la combinazione del ritardo dell'instradamento e dell'esecuzione dell'applicazione, un valore che dipende dalla propria configurazione di rete.
  - I collegamenti dei dati devono supportare le dimensioni del campo d'immissione sufficientemente ampie per contenere le intestazioni degli HPR e trasmettere ancora i dati dell'applicazione in modo efficiente.

  - I collegamenti dei dati devono essere molto affidabili perché un alta percentuale di errori influirebbe negativamente sulla prestazione di HPR.

  Per le configurazioni in cui tali condizioni non possono essere riscontrate, APPN senza HPR rappresenta ancora una valida scelta di implementazione. La tecnologia di HPR è un'opzione APPN e APPN senza HPR è ancora disponibile e supportata.

- Come evitare la congestione

  Una rete HPR consente di raggiungere un elevato numero di collegamenti. Utilizzando una tecnica chiamata controllo del flusso ARB (automatic rate based), gli end point del collegamento HPR rilevano automaticamente le congestioni di rete e riducono il carico della trasmissione. Questo impedisce la perdita dei pacchetti che, in altri algoritmi di instradamento, potrebbe essere provocata dalla mancanza di buffer disponibili nei nodi intermedi.

- Reinstradamento automatico senza danni

  Quando un end point del collegamento HPR rileva che un instradamento non è riuscito, calcola automaticamente un nuovo instradamento, ristabilizza il collegamento e ripristina eventuali pacchetti che sono andati persi a causa dell'errore. Poiché i nodi intermedi HPR sono stateless (cioè, ignorano i collegamenti che passano attraverso essi), non partecipano a questo protocollo di ripristino. Poiché nessun pacchetto viene perso se l'instradamento è commutato correttamente, le applicazioni che utilizzano l'instradamento non vengono danneggiate dall'errore.

- Il Software compatibile con l'hardware

  HPR è un estensione software di APPN; è possibile utilizzare HPR sugli adattatori LAN o WAN esistenti e sui collegamenti frame relay. Poiché HPR non cerca di fornire larghezza di banda dedicata e trasporto in tempo reale garantito (lasciando questo livello di funzione al Broad Band Networking Services), i limiti delle prestazioni relativi ai ritardi di inoltro dei pacchetti sono gli stessi per APPN senza HPR. I protocolli del CP utilizzati da HPR sono gli stessi di APPN di base con minori aggiunte, così i nodi HPR possono essere installati in numero sempre maggiore entro una rete APPN esistente senza una precedente pianificazione o coordinazione.

RTP (Rapid Transport Protocol)

RTP è un insieme di formati e protocolli dei messaggi progettati per utilizzare supporti di comunicazione di dati moderni, ridurre le difficoltà nei nodi intermedi e commutare automaticamente i percorsi quando un collegamento nel percorso non riesce.

I collegamenti RTP vengono stabiliti all'interno di una ***sottorete HPR*** e sono utilizzati per il trasporto del traffico delle sessioni. Una sottorete HPR è una porzione di una rete APPN che è in grado di stabilire collegamenti RTP e trasferire il traffico delle sessioni HPR. I collegamenti RTP possono essere intesi come dei ***pipe di trasporto*** sui quali vengono trasmesse le sessioni. Tali collegamenti possono trasmettere dei dati ad altissima velocità utilizzando un instradamento intermedio di basso livello e ridurre il traffico sui collegamenti per il ripristino degli errori e il controllo del flusso. Tali flussi vengono gestiti dagli end point del collegamento RTP.

Un percorso fisico di collegamento RTP può essere commutato automaticamente in modo da reinstradare dati su un nodo o un collegamento non riuscito senza danneggiare le sessioni. I dati nella rete al momento della mancata riuscita vengono ripristinati automaticamente.

RTP effettua il ripristino degli errori su una base end-to-end, invece che su una base a livello di collegamento. La prestazione viene migliorata riducendo il numero di flussi richiesti per effettuare il ripristino degli errori. Gli ERP (error recovery protocols) a livello di collegamento vengono anche supportati per tutti i collegamenti. ERP rappresenta un metodo per rilevare un pacchetto perso all'estremità di un collegamento e per ripristinarlo chiedendo all'altra estremità del collegamento di ritrasmettere il pacchetto. Se viene utilizzato ERP, i pacchetti HPR vengono inviati come frame di informazioni numerati, cioè come I-FRAMES. Quando si perde un frame, DLC rileva la perdita ed il mittente ritrasmette il frame. Se non viene utilizzato ERP, i pacchetti HPR vengono inviati come frame di informazioni non numerati, detti UI-FRAMES. Quando si perde un frame, DLC non può rilevare la perdita e RTP (rapid transport protocol) di HPR deve rilevare e ripristinare i pacchetti persi negli end point di collegamento.

In entrambi i casi, RTP rileva e ripristina sempre i pacchetti persi negli end point di collegamento. Per qualsiasi connessione, non esistono restrizioni sul numero dei collegamenti che utilizzano ERP, o che non utilizzano ERP.

ERP può essere attivato o disattivato su una base link-by-link. Poiché RTP rileva e ripristina i pacchetti persi negli end point di collegamento, è possibile utilizzare sia i collegamenti ERP che i collegamenti non-ERP quando si crea una rete. Questo consente di specificare ERP a livello di collegamento su collegamenti che presentano un alto tasso di pacchetti persi e di incrementare il numero dei collegamenti specificando che non utilizzano ERP a livello di collegamento. Generalmente, l'uso di ERP non è consigliato nelle LAN.

Nota: ERP viene sempre attivato in un ambiente WAN (wide area network).

Il controllo del flusso ed il controllo della congestione vengono anche effettuati da RTP su base end-to-end. RTP utilizza una tecnica chiamata controllo del flusso ARB (automatic rate based) per utilizzare interamente la larghezza di banda della rete, quando possibile. RTP incrementa la velocità con cui vengono inviati i pacchetti quando la rete supporta tale velocità di inoltro aumentata. La congestione viene riconosciuta automaticamente e, quando si verifica, diminuisce, di conseguenza, la velocità di invio. Le effettive funzioni configurate dei collegamenti nel percorso di connessione vengono utilizzate per stabilire sia la velocità di inoltro iniziale che l'incremento della velocità di inoltro.

Il supporto per i CF (control flow) sui collegamenti RTP non è disponibile con HPR nel Communications Server. Precedentemente, i flussi di controllo, compreso le sessioni CP-CP ed i messaggi di impostazione instradamento, hanno utilizzato i collegamenti APPN mentre i flussi di dati hanno utilizzato collegamenti HPR. A questo punto, entrambi i flussi di controllo e di dati possono utilizzare i collegamenti RTP. Il vantaggio di tale supporto comprende la commutazione automatica del percorso per le sessioni CP-CP.

I flussi di controllo fluiscono automaticamente su RTP se entrambi gli endpoint del collegamento supportano tale funzione.

ANR (Automatic Network Routing)

ANR (Automatic network routing) è una tecnica di instradamento stateless attivata da RTP per la quale viene visualizzato un messaggio con un'etichetta che identifica unicamente l'hop successivo nel percorso. A causa della sua semplicità, ANR può essere eseguito ad un basso livello pur ignorando i collegamenti che utilizzano il percorso. ANR riduce al minimo i cicli ed i requisiti di memoria per instradare i pacchetti attraverso i nodi intermedi.

La funzione di commutazione veloce del pacchetto ANR migliora le prestazioni nei nodi intermedi effettuando l'instradamento ad un livello più basso di APPN ed eseguendo il ripristino degli errori, la segmentazione, il controllo del flusso ed il controllo della congestione nel nodo finale, invece che nel nodo intermedio.

I nodi ANR intermedi ignorano le sessioni SNA o i collegamenti RTP. Le informazioni sull'instradamento per ciascun pacchetto vengono trasmesse in un'intestazione di rete con il pacchetto. Ogni nodo elimina le informazioni che ha utilizzato nell'intestazione prima di inoltrare il pacchetto, in modo che il nodo successivo riesca a trovare le relative informazioni per l'instradamento in un posto stabilito nell'intestazione. Non è necessario mantenere le tabelle di instradamento per i connettori di sessioni come in APPN di base, così la commutazione dei pacchetti attraverso i nodi può essere effettuata più rapidamente.

Supporto LU

SNA definisce i tipi di LU 0, 1, 2, 3, 4, 6.0, 6.1, 6.2, e 7. I tipi di LU 0, 1, 2, 3, 4, e 7 supportano le comunicazioni tra i programmi di applicazione e i generi diversi di stazioni di lavoro. I tipi di LU 6.0 e 6.1 forniscono le comunicazioni tra i programmi ubicati nei nodi subarea del tipo 5. Il tipo di LU 6.2 supporta le comunicazioni tra due programmi collocati nei nodi subarea del tipo 5 o nodi periferici del tipo 2.1, o entrambi e tra i programmi e le periferiche.

Communications Server supporta i tipi di LU 0, 1, 2, e 3, i quali supportano le comunicazioni con le applicazioni host che supportano periferiche come:

Tipo di LU 0 Terminali per transazioni di tipo bancario 3650 e 4700

Tipo di LU 1 Stampanti 3270

Tipo di LU 2 Video interattivi 3270

Tipo di LU 3 Stampanti 3270

La comunicazione si verifica solo tra le LU dello stesso tipo di LU. Ad esempio, una LU 2 comunica con un'altra LU 2; non comunica con una LU 3. Communications Server supporta anche il tipo di LU 6.2 o APPC.

Le funzioni SNA di Communications Server consentono alle applicazioni di utilizzare l'API (application programming interface) APPC per fornire una funzione di elaborazione della transazione distribuita in cui due o più programmi cooperano per ricavare una funzione di elaborazione. Tale funzione comporta la comunicazione tra due programmi in modo che possano condividere le risorse come i cicli di processori, i database, le code di lavoro e le interfacce fisiche come le tastiere e i video.

Communications Server supporta APPC attraverso API di APPC. Per ulteriori informazioni, consultare le seguenti pubblicazioni:

- *Client/Server Communications Programming*
- *System Management Programming*

Le funzioni di Communications Server riportate di seguito supportano vari tipi di LU:

- Gateway SNA

  Il gateway SNA consente agli host IBM System/370 (S/370), o i computer host ad architettura System/390 (S/390), o entrambi, di supportare le stazioni di lavoro collegate alla LAN che utilizzano i tipi di LU 0, 1, 2, 3, o 6.2 per comunicare attraverso una stazione di lavoro gateway SNA.

  Il gateway SNA supporta anche i tipi di LU 1, 2, o 3 per i computer host AS/400, i quali possono elaborare i dati o trasmetterli attraverso i computer host ad architettura S/370 o S/390.

- LUA (Applicazione LU convenzionale)

  La LUA è costituita da un software di sistema che offre delle routine di servizi per supportare le LU 0, 1, 2, e 3.

Supporto SDDLU

Il supporto SDDLU (self-defining dependent LU) permette all'utente di definire ed attivare una LU dipendente sull'host (VTAM). In VTAM, questo è noto come DDLU (dynamic definition of dependent LU). SDDLU viene abilitato in Communications Server codificando un'istruzione LU_MODEL su una definizione di LU.

Per attivare la funzione DDDLU in VTAM, codificare l'operando LUGROUP sull'istruzione di definizione per la PU e codificare un nodo principale del gruppo delle LU. Per utilizzare la routine di uscita SDDLU fornita dall'IBM che genera i nomi delle LU per l'utente, è preferibile codificare anche l'operando LUSEED sull'istruzione della PU.

L'operando del LUGROUP indica il nome del gruppo di definizione della LU modello che il VTAM utilizza quando definisce le LU in modo dinamico per questa PU. Il nodo principale del gruppo di LU contiene le istruzioni di definizione del modello. Le definizioni dinamiche per le LU vengono create utilizzando le definizioni della LU modello contenute in questo nodo principale.

L'operando LUSEED fornisce un nome campione che viene utilizzato con la routine di uscita SDDLU al fine di produrre un nome per le LU create in maniera dinamica. Una volta che sono state aggiunte le istruzioni corrette all'istruzione della PU e che è stato codificato il nodo principale del gruppo di LU, è necessario che questi nodi principali siano attivi per abilitare la funzione SDDLU.

Supporto DLUR (Dependent Logical Unit Requester)

DLUR (Dependent Logical Unit Requester) è un'architettura volta a fornire un supporto LU dipendente in una rete APPN. Communications Server supporta tutte le funzioni DLUR di base e le funzioni facoltative riportate di seguito:

- Supporto SDDLU (Self-defining dependent LU)

Utilizzando il supporto SDDLU le LU supportate dal DLUR possono essere definite in maniera dinamica in VTAM, eliminando in tal modo la necessità di predefinire tali LU.

- Supporto TakeOver/GiveBack

  Tale supporto permette alle sessioni LU-LU di rimanere attive anche quando non riesce il collegamento tra i nodi DLUR e DLUS. Il collegamento può essere ristabilito con lo stesso o con un altro DLUS, senza che vengano mai danneggiate le sessioni LU-LU.

- Supporto MultiSubnet

  Questo supporto permette al nodo DLUR, al nodo DLUS ed al nodo contenente l'applicazione di trovarsi in sottoreti diverse.

- Registrazione LU assistita da DLUS

  Un nodo finale DLUR registra le proprie LU in modo che il nodo di rete possa collocare tali LU senza dover trasmettere le richieste locate a DLUR.

- Supporto DLUS della copia di backup

  Quando il collegamento a DLUS primario non riesce o non diviene attivo, Communications Server tenta automaticamente di stabilire un collegamento con DLUS della copia di backup.

Utilizzo di DLUR

Per utilizzare la funzione DLUR, si configura una definizione **DLUR_DEFAULTS** e si usa il nome del collegamento da quella definizione come il collegamento host per le relative definizioni LUA, LU 6.2 dipendente, o gateway. Communications Server invia PUNAME, CPNAME e NODEID al DLUS. PUNAME viene inviato come parte dell'informazione di segnalazione (CV X'0E').

- Se DLUS è di livello superiore (supporta il controllo del CV X'0E' su REQACTPU) utilizza PUNAME nel relativo algoritmo di ricerca. Questo è disponibile in VTAM 4.3 con PTF o superiore.
- Se DLUS è di livello inferiore, ignora il CV X'0E'.
- Se non c'è corrispondenza su PUNAME o DLUS è di livello inferiore, DLUS tenta poi di individuare una PU con un nome CP corrispondente o NODEID (IDBLK/IDNUM) o predefinito in un nodo principale di commutazione VTAM o creato in modo dinamico utilizzando l'uscita ISTEXCCS.

I collegamenti alla rete che utilizzano la connettività di propria scelta (Token Ring, SDLC, AnyNet e così via) devono essere configurati e resi attivi prima che possa essere stabilito il collegamento DLUR-to-DLUS. Una volta che esiste un collegamento APPN tra DLUR e DLUS, viene stabilita una coppia di sessioni di controllo tra DLUR e DLUS utilizzando un modo speciale, CPSVRMGR. Questa coppia di sessioni di controllo viene anche definita come pipe CP-SVR e risulta come un collegamento a Communications Server. Pertanto, essa può essere attivata, disattivata e visualizzata utilizzando **Operazioni nodo SNA**.

Una volta che è attivato il pipe, il supporto SSCP-to-PU e SSCP-to-LU può essere fornito alle PU e alle LU che hanno definito il pipe come collegamento host relativo. Le sessioni LU-to-LU non utilizzano il pipe, ma utilizzano il percorso migliore disponibile sulla rete.

In ambiente DLUR, qualunque numero di PU dedicate può essere definito sulle sessioni LU 6.2. Questo consente ai gateway di fornire accesso alla gestione di rete attraverso le PU dedicate alle stazioni di lavoro downstream senza richiedere numerosi collegamenti all'host.

In Figura 17 viene mostrata una stazione di lavoro Communications Server che agisce come un gateway DLUR sia per una stazione di lavoro sia per un'unità di controllo 4702.

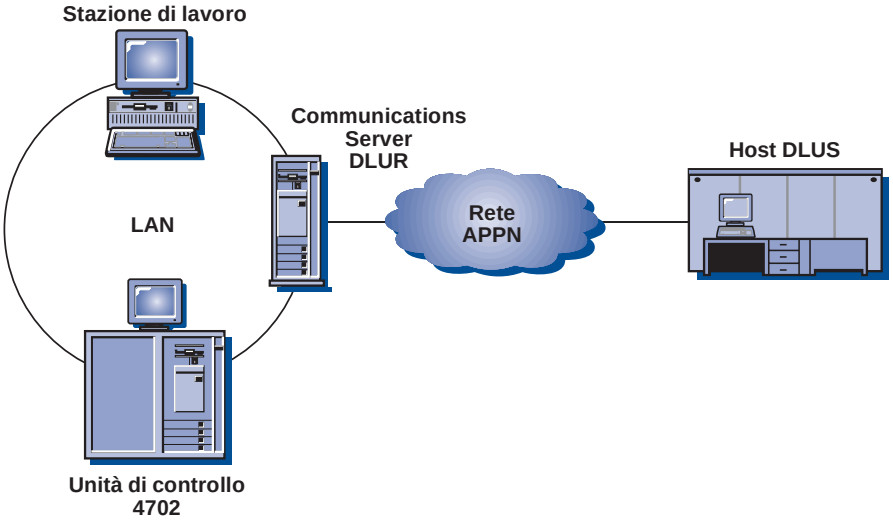


Figura 17. Collegamento DLUR ad un Host tramite un Gateway di Communications Server

Sessioni LU-LU

Le LU di Communications Server possono avviare sessioni e rispondere alle richieste di avviamento sessione. Una LU avvia e risponde alle richieste secondo il tipo di LU: indipendente o dipendente.

LU indipendente

Una LU indipendente è in grado di attivare una sessione LU-LU (cioè, invia una richiesta BIND) senza assistenza da SSCP; perciò, non dispone di una sessione SSCP-LU. Una LU indipendente è in grado di inviare e ricevere dei BIND. Il mittente del BIND viene definito come PLU (primary LU); il destinatario del BIND viene definito come SLU (secondary LU).

Soltanto una LU 6.2 può essere una LU indipendente. Communications Server supporta i protocolli di LU indipendenti su altri nodi del tipo 2.1 e nodi di subarea di tipo 5 a livello di rete di base.

Le LU indipendenti possono avere delle sessioni parallele tra la stessa coppia di LU e possono disporre di più sessioni tra una LU e diverse altre LU. I loro limiti di sessione vengono stabiliti su una base nome di modo, che può essere da 1 a 32 767.

In Figura 18 a pagina 58 viene mostrato in che modo le sessioni multiple e parallele possono essere stabilite da una LU indipendente. La LUx supporta le sessioni parallele con la LUy e una sessione singola con la LUz. La direzione delle frecce della sessione mostra la relazione PLU-SLU. La LUx agisce come la PLU

per la sessione con la LUz e per una delle sessioni con la LUy. La LUx agisce anche come la SLU per una delle sessioni parallele con LUy.

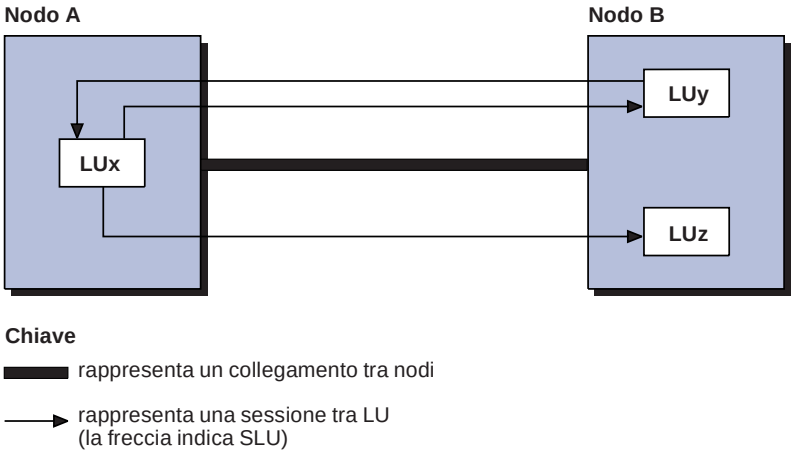


Figura 18. Sessioni multiple e parallele

LU dipendente

Una LU dipendente è una LU controllata da un sistema host SNA. Per attivare una sessione LU-LU, una LU dipendente richiede l'assistenza da parte di un SSCP. Richiede una sessione SSCP-LU per inviare un BIND. I protocolli delle LU dipendenti sono supportati da Communications Server, ma solo sui nodi subarea del tipo 5 che utilizzano i protocolli del tipo 2.0, non su altri nodi periferici del tipo 2.1. Le LU dipendenti agiscono solo come le SLU ed hanno un limite di sessione LU-LU di 1. Comunque, il supporto PU multiplo in Communications Server permette di stabilire più sessioni SSCP-PU simultanee con le sessioni LU dipendenti.

La funzione DLUR (dependent LU requester) consente a Communications Server di trarre vantaggio dal supporto SSCP potenziato fornito da un DLUS (dependent LU server). Alcuni dei vantaggi di tale funzione sono:

- Le LU dipendenti possono risiedere in nodi che non sono adiacenti all'host.
- La logica della ricerca APPN individua il percorso migliore per le sessioni LU-LU.
- Le LU dipendenti SNA possono ottenere i vantaggi di una rete APPN.

Per utilizzare DLUR, configurare un parametro **DEFINE_DEPENDENT_LU_SERVER** ed usare il nome del collegamento da quella definizione per le definizioni LUA, LU 6.2 dipendente o del gateway.

LU 6.2

Le LU indipendenti vengono definite nel programma VTAM codificando LOCADDR=0. Possono esistere tutte le LU che si desiderano definite con LOCADDR=0. Si tenga presente, comunque, che non tutte le LU 6.2 sono LU indipendenti.

Quando si definiscono le LU di una parte della rete APPN nel programma VTAM, è necessario definirle come se si trovassero nel nodo di rete che collega questa parte della rete APPN alla rete subarea. Seguendo la definizione della PU di tale nodo di

rete, definire ogni LU che si desidera raggiungere dall'altra parte della rete APPN. Non dimenticare che i CP sono delle LU.

Una LU deve essere definita in VTAM per stabilire una sessione con un'altra LU se tale sessione passa attraverso la rete di subarea. Non è possibile ottenere ciò in nessun altro modo (neanche con i caratteri globali di APPN); VTAM deve necessariamente conoscere il nome di ciascuna LU di destinazione.

Poiché una rete APPN viene intesa per modificarsi facilmente, è preferibile definire le LU della rete APPN in un nodo principale speciale ove ciò sia possibile. E' anche possibile definire, in VTAM, le LU che non esistono ancora.

Altre LU

Se il nodo di rete utilizza il collegamento relativo alla rete di subarea per l'emulazione 3270, le LU del tipo 2 di LU dell'emulazione 3270 vengono definite nella stessa macro PU come le LU del tipo 6.2 di LU della rete APPN. Il collegamento viene anche utilizzato per la connessione tra l'emulazione 3270 e l'host.

Nodo di rete APPN e supporto T2.1

APPN costituisce un potenziamento a SNA dell'IBM e all'architettura di nodo del T2.1 (tipo 2.1). APPN consente l'interconnessione di sistemi dalle dimensioni ampiamente differenti in reti di topologia dinamica. Una rete APPN risulta più facile da usare, è più affidabile e fornisce una flessibilità maggiore rispetto alle reti SNA tradizionali.

Consultare *3174 APPN Implementation Guide* per ulteriori informazioni sui nodi di rete.

Compressione dati

La compressione dei dati consiste nel comprimere i byte ripetuti o le stringhe di dati ripetute per ridurre la lunghezza di record e blocchi. Ciò riduce il tempo di trasferimento necessario per le comunicazioni. Diminuendo la quantità di dati trasferiti tra le sessioni host e della stazione di lavoro, è possibile incrementare la prestazione su linee a bassa velocità e abbassare il costo per bit sulle linee costose.

Il risultato della prestazione, valutato in base al numero di byte trasferiti, che è possibile aspettarsi utilizzando la compressione dati è spesso un rapporto di circa 2:1. Ciò significa che, con la compressione dati attiva, vengono salvati i byte di ogni secondo circa nei buffer necessari per la conversione protocollo di livello inferiore.

La compressione dati è utile per coloro che richiedono:

- Tempi di risposta ottimali, specialmente su linee a bassa velocità
- Costi ridotti su linee in cui le tariffe si basano sul volume dei dati
- Meno linee dedicate

Comunque, la compressione dati non dovrebbe essere applicata ad ogni sessione in esecuzione poiché esistono degli svantaggi che vanno considerati:

- La compressione e la decompressione necessita di cicli CPU aggiuntivi

- Si renderà necessario un incremento della memoria dati (32 byte a 9.0 KB)
- La compressione dati richiede un collegamento sicuro come precisato nella relativa tabella COS (class-of-service) APPN.
- E' necessario richiedere l'impostazione della dimensione dell'RU per ottenere la prestazione migliore. Ciascuna RU viene compressa e poi inviata. Se i pacchetti sono stati inviati, una dimensione di RU maggiore sul modo consentirà l'invio di più pacchetti pieni.

  Nota: La quantità di memoria aumentata dipende dall'algoritmo di compressione che si utilizza. Tale aumento si aggiunge alla memoria richiesta per il messaggio.

Per avere delle descrizioni tecniche e dettagliate sui diversi algoritmi di compressione consultare le seguenti pubblicazioni:

- *Formati SNA*
- *Better OPM/L Text Compression IEEE Transactions on Communications, vol COM-34, no 12, pgs 1176-1182,1986*
- *IBM ITSC VTAM V3R4 and V3R4.1 Planning Guide*
- *A Technical Guide to ESA/390 Compression*

Le seguenti sezioni descrivono l'implementazione di Communications Server e la compressione a livello sessione SNA.

Architettura della Compressione a livello sessione SNA

La compressione a livello sessione SNA implementa la compressione dati nella mezza sessione LU-LU. Con Communications Server essa è disponibile per tutti i tipi di LU supportati, cioè: tipi di LU 0, 1, 2, 3, e 6.2. La compressione dati a livello sessione fornisce i vantaggi riportati di seguito:

- Risulta più utile comprimere i dati prima di crittografarli
- Gli algoritmi diversi sono più efficaci per tipi di dati diversi.
- I programmi di applicazione non devono fornire la propria logica di compressione.

Due algoritmi vengono generalmente definiti per la compressione a livello sessione SNA, RLE (Run length encoding) e un formato di LZ (Lempel-Ziv). Communications Server supporta la compressione a livello sessione SNA utilizzando i seguenti algoritmi:

- compressione NO.
- compressione RLE; RLE è l'algoritmo più semplice e più ampiamente conosciuto, sostituendo le stringhe o byte identici con stringhe codificate più brevi.
- compressione LZ9; LZ9 è un algoritmo di compressione dinamica che comprime le stringhe visualizzate precedentemente (nelle RU attuali o precedenti) in un codice di 9 bit che rappresenta l'indice di origine zero di una voce nella tabella compressione/decompressione. Le voci delle tabelle memorizzano le stringhe visualizzate precedentemente.
- compressione LZ10; LZ10 è un algoritmo di compressione dinamica che comprime le stringhe visualizzate precedentemente (nelle RU attuali o

precedenti) in un codice di 10 bit che rappresenta l'indice di origine zero di una voce nella tabella compressione/decompressione. Le voci delle tabelle memorizzano le stringhe visualizzate precedentemente.

Solitamente, LZ comprime i dati meglio di RLE, ma con un costo superiore di memoria e funzione CPU.

La compressione a livello sessione SNA visualizza la sessione in due direzioni, PLU-SLU e SLU-PLU. PLU (primary logical unit) è la LU responsabile dell'attivazione della sessione. SLU (secondary logical unit) è la LU che risponde. PLU attiva una sessione inviando una richiesta di sessione BIND (Bind Session) alla SLU, che risponde con un BIND. Ciò significa che diversi algoritmi di compressione possono essere utilizzati nelle direzioni PLU-SLU e SLU-PLU. Questo è eseguibile attraverso la negoziazione di BIND dei livelli di compressione. La LU 6.2 può utilizzare qualsiasi combinazione di livelli di compressione per una sessione (ad esempio, PLU potrebbe usare RLE e SLU-PLU potrebbe utilizzare LZ9). Tutti gli altri tipi di LU hanno la compressione attivata o disattivata. Quando è attivata, il livello di compressione PLU-SLU è LZ9 e SLU-PLU è RLE.

Compressione dati di Communications Server

Communications Server supporta la compressione dei dati a livello sessione SNA con gli algoritmi di compressione RLE, LZ9, e LZ10. Con Communications Server, è possibile specificare l'utilizzo della compressione dati per le comunicazioni sulle sessioni CPI-C (attraverso le sessioni APPC), le sessioni APPC (LU 6.2) e sessioni LUA (LU 0, LU 1, LU 2, e LU 3).

Una configurazione divisa in due parti viene utilizzata per attivare la compressione dati. Il nodo di Communications Server deve essere attivato per la compressione dati e la LU (APPC e LUA) deve essere attivata per prima. I due campi di compressione nodo (livello e token) si trovano sulla finestra delle caratteristiche del nodo locale (la parola chiave **NODE** nel file .ACG).

Il campo di livello di compressione imposta il livello massimo mediante il quale si può avviare qualsiasi sessione: NONE, RLE, LZ9, o LZ10. Questo campo ha priorità su tutti i livelli di compressione configurati o tentati (l'unica eccezione è rappresentata da DTF indipendente, il quale non richiede la definizione di nodo). Se si sta configurando una sessione utilizzando LUA (LU 0, LU 1, LU 2, e LU 3) per supportare l'emulazione 3270 o le stampanti, viene richiesto l'LZ9 per la compressione dati. Gli altri livelli di compressione non permettono la compressione dati per questi tipi di LU.

La dimensione della RU (request unit) predefinita per modi compressi è pari al doppio della dimensione della BTU (basic transmission unit) di collegamento. Se si sta utilizzando la commutazione di pacchetto, è possibile che non si desideri utilizzare tale dimensione predefinita; utilizzare, allora, una dimensione maggiore e segmentare i pacchetti.

La compressione della LU 6.2 può essere attivata:

- Utilizzando i modi forniti con Communications Server
  - #INTERC
  - #BATCHC
  - #BATCHCS

  - #INTERCS
- Modificando o aggiungendo i modi con la compressione attivata

I tre campi di compressione modi, l'esigenza di compressione, il livello di compressione PLU->SLU e il livello di compressione SLU->PLU vengono visualizzati nel pannello relativo alla definizione del modo (parola chiave **MODE** nel file .ACG).

La compressione dispone di due valori.

Prohibited Nessuna compressione.

Requested Utilizzare questo valore per richiedere la compressione dati con i valori definiti nel livello di compressione PLU->SLU e nel livello di compressione SLU->PLU. Il livello richiesto potrebbe non essere ottenuto per le seguenti ragioni:

- Le impostazioni del nodo hanno limitato il livello consentito
- La SLU ha negoziato i livelli

L'SLU considera i livelli di compressione richiesti dalla PLU, a meno che non sia limitata dalle relative impostazioni di compressione del nodo.

Per ulteriori informazioni sulla compressione di Communications Server, fare riferimento al testo della guida in linea del prodotto oppure a *Configuration File Reference*.

Crittografia a livello sessione SNA

La crittografia a livello sessione SNA consente di crittografare tutti i dati o i dati selezionati che vengono trasferiti tra la stazione di lavoro e l'host. Se si desidera proteggere qualsiasi tipo di dati della stazione di lavoro utilizzando la crittografia, anche l'host deve essere configurato per utilizzare la crittografia.

Per abilitare la riservatezza dei dati, è necessario installare sul server un adattatore IBM SecureWay 4758 PCI Cryptographic Coprocessor (definito anche come IBM 4758). Tale adattatore deve essere avviato seguendo le istruzioni fornite con esso.

In Communications Server, la crittografia a livello sessione LU 6.2 viene configurata in base alla descrizione del modo utilizzata per un determinato programma di transazione. Esistono due livelli di crittografia:

- livello sessione APPC

  Rigorosamente tra due LU, nessun CP viene coinvolto nelle chiavi di transazioni

- conversione chiave della sessione APPN

  Il CP della LU di origine (EN o NN) ed eventualmente il relativo NN server convertono le chiavi oltre alla LU di origine.

Per configurare un modo per la crittografia, visualizzare la finestra relativa alle funzioni SNA e selezionare **MODI**. In seguito, all'interno della finestra relativa alla definizione del modo, selezionare **Imposta...**. Compare la finestra relativa al supporto crittografia a livello sessione e alla compressione. I parametri per la configurazione della crittografia sono divisi in due parti:

- Per la crittografia a livello sessione, è possibile indicare se la crittografia è facoltativa (la negoziazione delle LU) o obbligatoria (è necessario utilizzare la crittografia).

  Nota: La crittografia da Communications Server ad un host viene sempre impostata in modo da essere obbligatoria.

- Per la conversione chiave della sessione APPN, è possibile specificare che soltanto la LU converte la chiave, che soltanto l'EN converte la chiave di sessione, o che l'EN ed il relativo NN convertono la chiave.

Communications Server richiede degli altri prodotti per la memorizzazione e la conversione delle chiavi. Un prodotto CCA (common cryptographic architecture) viene richiesto per la memorizzazione delle chiavi, gestita dalle funzioni fornite con l'adattatore 4758 IBM. Communications Server richiama un prodotto CCA, che interagisce con l'adattatore 4758 IBM per ottenere le chiavi e codificare i dati.

Utenti VTAM:

Communications Server non codifica la sessione SNASVCMG. E' necessario specificare ENCR=OPT nell'istruzione APPL della definizione di applicazione VTAM. Lavorando con VTAM, è necessario avere la crittografia specificata sull'istruzione MODEENT. Ad esempio:

```
ENCR=B'0011' FOR MANDATORY ENCRYPTION
```

Per utilizzare la crittografia VTAM, PCF (Programmed Cryptographic Facility) IBM deve essere avviato prima di avviare VTAM.

Se si inizia con VTAM V3R4.1, VTAM utilizza una nuova interfaccia in ICSF/MVS (Integrated Cryptographic Service Facility/MVS) per i servizi di crittografia, come fornire crittografia a livello sessione. Questa interfaccia è conforme a CCA (Common Cryptographic Architecture) se implementato da ICSF/MVS. Grazie a questo supporto, è possibile avviare ed arrestare il servizio di crittografia dopo che è stato avviato VTAM ed è possibile modificare la chiave principale senza danneggiare VTAM o attivare le sessioni LU-LU.

Per informazioni su come definire la crittografia dei dati, consultare *OS/390 eNetwork Communications Server: SNA Network Implementation*.

Management Services

MS (management services) di Communications Server sono funzioni distribuite tra i componenti di rete per operare, gestire e controllare una rete. Tale funzione si basa sull'architettura di MS SNA documentata in *Systems Network Architecture Management Services Reference*.

Focal Point, Service Point ed Entry Point

Communications Server fornisce un supporto relativo alla programmazione che attiva l'installazione delle applicazioni FP (focal point), SP (service point) ed EP (entry point) di MS. Le applicazioni SP MS rappresentano semplicemente una variazione delle applicazioni EP MS e differiscono solo nei generi di funzioni che esse forniscono; altrimenti, interagiscono con un FP MS come applicazioni EP MS.

Focal Point Un FP MS costituisce un punto centrale di controllo per la gestione di una rete. Da un SP MS o un'applicazione EP MS, l'FP MS può richiedere alcuni dati relativi alle operazioni di una rete come i dati sulle prestazioni e i problemi o identificazione del prodotto.

L'FP MS può anche accettare alcuni dati MS non richiesti dai nodi che gestisce che si basa sulla categoria dei dati MS. Un esempio di categoria MS è costituito dalle segnalazioni MS. Un FP MS è in grado di gestire una o più categorie di dati MS e possono esserci uno o più FP MS in una rete. Communications Server IBM, il programma NetView IBM ed il sistema operativo OS/400 IBM rappresentano esempi di prodotti che forniscono la funzione FP MS.

Service Point Un SP MS è la funzione in un nodo che può richiedere e prendere dei dati dalle periferiche che, da sole, non possono servire da EP MS, come le periferiche collegate dai protocolli LAN (ma non protocolli SNA di livello superiore) al nodo SP MS. Oltre a raccogliere dei dati non locali, un SP MS funziona come un EP MS in relazione all'FP MS. I prodotti IBM NetView/PC ed IBM LAN Network Manager costituiscono esempi di applicazioni EP MS che forniscono funzioni SP MS e funzioni EP MS.

Entry Point Un EP MS rappresenta la funzione in un nodo che cattura dati MS locali e li invia ad un FP MS per l'elaborazione, sia su richiesta che non. Communications Server fornisce la funzione EP MS per inviare segnalazioni al focal point MS delle segnalazioni. Tali segnalazioni possono avere origine all'interno di Communications Server o con i DLC che utilizza. Communications Server fornisce anche supporti di programmazione per le applicazioni, come i prodotti IBM NetView/PC e IBM LAN Network Manager, fornendo segnalazioni da inviare al focal point MS delle segnalazioni.

Livelli di architettura MS SNA

Un prodotto SNA implementa un livello particolare (o creazione) dell'architettura MS SNA ed alcuni prodotti supportano vari livelli dell'architettura. Communications Server può inviare dati MS ai prodotti SNA, e ricevere dati MS da questi, che implementano uno qualunque dei tre livelli dell'architettura MS. Tali livelli sono:

Livello MDS (Multiple Domain Support) Un prodotto SNA che implementa il livello MDS dell'architettura MS, come Communications Server e IBM NetView Versione 2 Rilascio 2 (o successivi). Può inviare e ricevere MDS-MU (MDS message units). IBM NetView Versione 2 Rilascio 2 fornisce i livelli MDS come una LU subarea, non fornisce un CP (control point) e utilizza le sessioni modo SNASVCMG per trasferire le MDS-MU. Come focal point, supporta relazioni FP-EP esplicite, implicite (primarie) e implicite (backup). NetView Versione 2 Rilascio 2 continua anche a supportare la relazione FP-EP host su prodotti EP che non dispongono del supporto di livello MDS.

Livello di migrazione Un prodotto SNA che implementa il livello precedente dell'architettura MS, come IBM OS/400 Versione 1 Rilascio 3 livello di modifica (o precedenti). Un prodotto con livello di migrazione è in grado di supportare delle relazioni FP-EP esplicite, predefinite e di dominio. La relazione di dominio FP-EP si ottiene quando le sessioni CP-CP vengono attivate in un nodo di livello di migrazione. Un livello di migrazione utilizzato da un NN (network node) non invia le funzioni MS

per la notifica FP agli EN (end node) utilizzati e un EN utilizzato con livello di migrazione non accetta le funzioni MS per la notifica FP dal nodo di rete utilizzato. Può inviare e ricevere CP-MSU ma non MDS-MU. Come focal point, supporta soltanto la categoria MS di segnalazione.

Livello NMVT (Network Management Vector Transport) Un prodotto SNA che implementa il livello NMVT dell'architettura MS SNA, come IBM NetView versione 2 rilascio 1 (o successivi). NMVT è una RU (request unit) MS che agisce in una sessione attiva tra MS di PU ed MS di CP (control point). Se un NMVT viene instradato da una stazione di lavoro attraverso un gateway, in seguito il gateway aggiunge il proprio nome CP a NMVT.

Controllo flusso

Per gestire il flusso di dati in una rete, Communications Server utilizza il pacing di adattamento a livello sessione. Il pacing si verifica tra ogni coppia di nodi adiacenti che partecipano all'instradamento della sessione. Il pacing tra due nodi adiacenti è indipendente dal pacing utilizzato tra altri nodi adiacenti nell'instradamento.

Pacing a livello sessione

Il pacing di adattamento a livello sessione utilizza uno schema con finestre, in cui un mittente può inviare soltanto un numero limitato, o ***finestra***, di RU (request units) per autorizzazioni esplicite a procedere. La dimensione della finestra può essere modificata in base alle condizioni del destinatario. Tale funzione consente ad un nodo di controllare la quantità di dati che è stata inviata e ricevuta durante una normale operazione di sessione. Il controllo della finestra consente al nodo ricevente di gestire la propria velocità per la ricezione dei dati nei propri buffer di sessione. Il pacing di adattamento a livello sessione fornisce ad un nodo che supporta molte sessioni un mezzo dinamico per assegnare delle risorse ad una sessione che ha una notevole attività e per richiedere delle risorse inutilizzate dalle

Pacing BIND di adattamento

Il traffico BIND può causare interruzioni, in particolare all'avvio della rete o del nodo. Perciò, il pacing BIND di adattamento esiste per controllare il flusso dei BIND tra due nodi adiacenti. Viene impiegato lo stesso algoritmo della finestra utilizzato per il pacing a livello sessione.

Segmentazione e riassemblaggio

Per trasmettere le RU più a lungo rispetto alla dimensione massima della BTU (unità di trasmissione di base) consentita da un particolare collegamento, Communications Server supporta la segmentazione ed il riassemblaggio. Tali segmenti vengono riassemblati in tutte le RU nel nodo partner. Questa operazione consente alla dimensione definita della RU per una sessione di essere indipendente dal collegamento che viene utilizzato per l'instradamento.

Pacing HPR (High Performance Routing)

HPR (high performance routing) fornisce un nuovo metodo di controllo del flusso definito controllo congestione ARB (adaptive rate-based). ARB regola il flusso del traffico prevedendo la congestione nella rete, riducendo la velocità di invio del nodo nella rete e prevenendo la congestione piuttosto che tentare di risolverla in seguito.

Pacing fisso

Il pacing fisso consente di condividere un collegamento fisico tra due sessioni. Senza il pacing fisso, i dati che devono essere trasmessi vengono inseriti in una coda DLC (data link control) comune e i dati interattivi seguono i dati messi in coda precedentemente. Il pacing fisso riduce anche la quantità di spazio di memoria che può essere utilizzato per collocare i dati nella coda DLC. Il pacing a due vie fisso può essere utilizzato con un NCP per evitare di definire il pacing fisso di host. Comunque, in generale, il pacing di adattamento rappresenta il metodo più efficace di trasferimento dati tra nodi.

La priorità di trasmissione, come il pacing fisso, permette la condivisione di un collegamento fisico tra sessioni. Ad ogni modo, blocca la memoria appena i dati vengono collocati sulle code DLC, ma non richiede le risposte di pacing ulteriori che sono richieste per il pacing fisso.

Partizione delle LU tra gli host

Quando si definiscono più connessioni host di subarea, viene richiesto che il traffico dal dominio di un host determinato si immetta soltanto su un collegamento logico. E' importante notare che le connessioni a composizione manuale risultano essere un singolo collegamento. E' necessario definire una PU diversa per supportare ogni host differente. Solo i collegamenti host definiti sul control point dispongono di sessioni CP-CP e sono parte integrante della rete APPN. I collegamenti che hanno **USE_PU_NAME_IN_XID=1** non possono disporre di sessioni CP-CP. Diversamente, i collegamenti host possono avere sessioni CP-CP e possono anche partecipare alle comunicazioni APPN. La parola chiave **LINK_STATION** indica il nome PU ed il collegamento logico che deve essere utilizzato per la PU. Se i collegamenti paralleli sono richiesti (in situazioni in cui ci sono più di 254 LU dipendenti), uno dei collegamenti deve disporre del supporto sessione CP-CP impostato su No.

Ciascuna LU dipendente può essere definita come associata solo ad una PU. La parola chiave **LOCAL_LU** indica il nome collegamento host utilizzato per una LU dipendente del tipo 6.2. La parola chiave **LU_0_TO_3** denota il nome collegamento host per LUA ed il profilo 3270 specifica il collegamento host per ciascuna sessione di emulazione 3270.

Il CP (control point) definisce automaticamente una PU con lo stesso nome del control point. Le LU dipendenti che vengono definite in una subarea SSCP possono essere associate alla PU del control point. (Infatti, la LU definita automaticamente per il control point può essere anche specificata come dipendente.) Ogni PU 2.0 ulteriore per un diverso host di subarea richiede un collegamento separato e una definizione di PU. Una PU viene definita indicando PU sulla parola chiave **LINK_STATION**. Questo non è necessario se tutte le LU sono indipendenti.

Se la sessione SSCP-PU deve inviare segnalazioni all'host, definire il collegamento del focal point con la parola chiave **NODE** nel file .ACG. Se un host deve ricevere le segnalazioni, indicare un collegamento logico per il control point sull'host. Se il collegamento a quell'host non è disponibile, Communications Server registra le segnalazioni. Le uniche richieste di gestione di rete che vengono accettate da un host PU 2.0 sono quelle per la PU del control point. Le risposte vengono inviate allo stesso host che utilizza la PU del control point.

Ogni LU dipendente deve avere un indirizzo locale configurato che è lo stesso di quello configurato sull'host. Comunque, l'utilizzo del gateway SNA permette la conversione dell'indirizzo del gateway. Una LU 6.2 dipendente può agire come una LU indipendente in un nodo peer; cioè, è dipendente solo nella subarea. Una LU di questo tipo non dovrebbe essere parte di una rete APPN con qualunque altro collegamento alla stessa subarea, cioè, la subarea che contiene SSCP di controllo. E' permesso soltanto un collegamento di subarea per una rete APPN, a meno che le subarea siano indipendenti. Sebbene un gateway possa avere dei collegamenti paralleli alla stessa subarea, uno soltanto può disporre di sessioni CP-CP e traffico APPN.

SSCP nella rete di subarea attiva le LU dipendenti che controlla dopo che il collegamento ad esso viene stabilito. Fino a quando una LU non viene attivata, la LU non può avviare una sessione. Quando APPC viene interrotto, è richiesto lo scollegamento da ogni host attivo in sessione con una PU nel nodo. Ciascun host libera il collegamento dopo aver disattivato prima le LU e poi le PU sulle sessione SSCP-PU.

Supporto Gateway SNA

Communications Server fornisce un gateway SNA (Systems Network Architecture) con funzioni complete. Il gateway consente alle stazioni di lavoro multiple collegate alla LAN di accedere agli host System/370 o System/390 attraverso uno o più collegamenti fisici ad uno o più host. Questo aiuta a ridurre il costo per stazione di lavoro di collegamenti host.

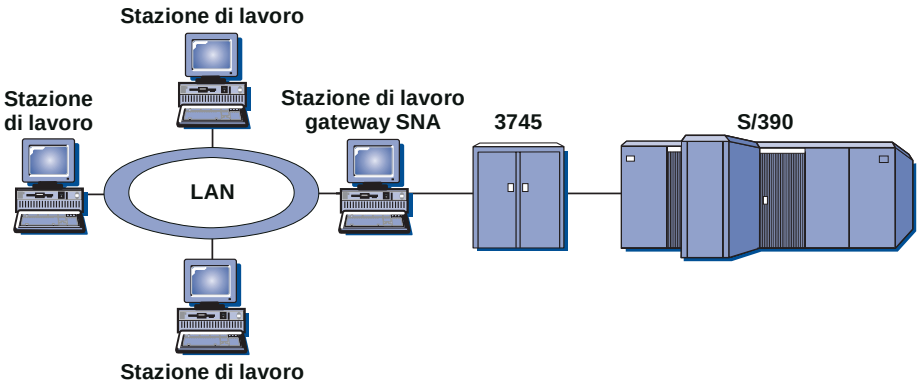


Figura 19. Esempio di configurazione gateway SNA

Il gateway Communications Server supporta le LU 0, 1, 2, 3 dei protocolli SNA e la LU 6.2 (APPC) dipendente. Con la funzione AnyNet SNA su TCP/IP, le stazioni di lavoro downstream ora sono in grado di comunicare con il gateway SNA in una rete IP. Inoltre il gateway supporta le LU 0, 1, 2, o 3 su un host AS/400 utilizzando pass-through SNA. L'host AS/400 trasmette i dati tramite un host System/390.

Un gateway è anche in grado di agire come un convertitore di protocolli tra stazioni di lavoro collegate ad una LAN e una linea host WAN.

Le LU definite nel gateway possono essere dedicate ad una stazione di lavoro particolare o in pool tra più stazioni di lavoro. L'inserimento in pool consente alle stazioni di lavoro di condividere le LU comuni, incrementando l'efficienza delle LU e riducendo i requisiti di avvio e configurazione sull'host. E' possibile, inoltre, definire pool di più LU, ogni pool viene associato ad una applicazione specifica. Ed è possibile definire i pool comuni che sono associati a più host. Quando un client si collega al gateway, il gateway recupera una LU dal pool per stabilire una sessione. La LU viene restituita al pool per accedere da altre stazioni di lavoro quando la sessione viene chiusa.

Inoltre, un gateway SNA può supportare l'inoltro di NMVT (network management vector transport) tra le stazioni di lavoro e l'host.

Ciascun host interpreta il gateway SNA come nodo SNA PU 2.0, che supporta una o più LU per stazione di lavoro. Per l'host, tutte le LU appartengono alla PU del gateway SNA. Il gateway SNA può disporre di più collegamenti host contemporaneamente ed indirizzare sessioni di stazioni di lavoro differenti ad host specifici.

Alle stazioni di lavoro supportate, il gateway SNA appare come un'unità di controllo delle comunicazioni SNA PU 4 ed inoltra tali richieste host come BIND e UNBIND. Le LU della stazione di lavoro ignorano il gateway SNA. Il gateway SNA, tuttavia, riconosce tutte le LU delle stazioni di lavoro.

Le applicazioni downstream che utilizzano i protocolli di connettività SNA standard per LU 0, 1, 2 e 3 e dipendente 6.2 e che comunicano tramite un gateway SNA con l'host, sono supportate da Communications Server. Tabella 4 a pagina 69 riassume le funzioni del gateway SNA.

Tabella 4. Riepilogo gateway SNA

Funzione	Descrizione
Stazioni di lavoro attive	254 (LAN) per adattatore 128 (X.25)
DLC	AnyNet (SNA su TCP/IP) Biassiale (solo upstream) LAN (qualsiasi adattatore di rete compatibile NDIS**) X.25 SDLC (sincrono, asincrono e AutoSync) OEM Channel (solo upstream) MPC Channel (solo upstream, richiede il DLUR) Enterprise Extender
Stazioni di lavoro downstream	Qualsiasi prodotto che supporta i protocolli di connettività SNA standard per LU 0, 1, 2, 3 e 6.2.
Modifiche e aggiunte dinamiche	Sì
Supporto stazione di lavoro implicita	Sì
Inserimento in pool di LU	Sì
Numero massimo di LU	254 per PU; nessun limite sul numero di PU
Funzionamento	Molteplici PU downstream (non evidenti all'host). PU non visibili all'host (se non attraverso DLUR)
Supporto PU multiple	Sì
Supporto segmentazione	Sì
Tipi di LU supportati	LU 0, 1, 2, 3 e dipendente 6.2

Pianificazione ed installazione

Pianificazione del supporto AnyNet

Communications Server fornisce due tipi di supporto AnyNet:

- Gateway e nodo di accesso SNA AnyNet su TCP/IP
- Gateway e nodo di accesso Socket AnyNet su SNA

La funzione SNA AnyNet su TCP/IP di Communications Server consente alle applicazioni SNA di comunicare su reti IP e SNA interconnesse.

La funzione del nodo di accesso SNA su TCP/IP abilita le comunicazioni tra le applicazioni SNA che si trovano su una rete IP. Questa funzione supporta la LU 6.2 indipendente e le LU 0, 1, 2, 3 o 6.2 dipendenti con o senza DLUR (dependent LU requester). Inoltre, il nodo di accesso SNA su TCP/IP può essere utilizzato insieme con il gateway SNA per abilitare le sessioni gateway SNA su TCP/IP.

La funzione gateway SNA su TCP/IP estende la portata delle applicazioni SNA consentendo alle applicazioni SNA di una rete SNA di comunicare con le applicazioni SNA di una rete IP. Il gateway SNA su TCP/IP supporta le sessioni LU 6.2 indipendente.

Per ulteriori informazioni sulla configurazione di SNA AnyNet su TCP/IP, consultare la sezione “Configurazione di SNA AnyNet su TCP/IP”.

La funzione del nodo di accesso Socket su SNA consente ai programmi applicativi TCP/IP che utilizzano l'interfaccia socket WinSock 1.1 e WinSock 2.0 di comunicare su una rete SNA.

La funzione del gateway Socket su SNA consente le comunicazioni tra le applicazioni socket nelle reti SNA e TCP/IP. I gateway Socket su SNA vengono spesso utilizzati per collegare reti TCP/IP isolate utilizzando una rete backbone SNA.

Per ulteriori informazioni sulla configurazione di Socket su SNA, fare riferimento alla sezione “Configurazione di Socket AnyNet su SNA” a pagina 86.

Configurazione di SNA AnyNet su TCP/IP

Questa sezione contiene informazioni dettagliate sulla configurazione di SNA AnyNet su TCP/IP.

Mappatura di risorse SNA sugli indirizzi IP

Uno dei passi più importanti per l'abilitazione delle comunicazioni SNA su TCP/IP non viene eseguito nelle finestre di Communication Server. Prima di poter stabilire collegamenti o sessioni SNA, è necessario che SNA su TCP/IP stabilisca l'indirizzo IP del partner. A questo scopo è necessario associare l'identificativo SNA del partner ad un indirizzo IP effettuando le seguenti operazioni:

1. SNA su TCP/IP riceve l'identificativo SNA da Communications Server in uno dei seguenti formati:
   - Per i nomi LU, `netid.luname`
   - Per i nomi CP, `netid.cpname`

- Per i valori IDBLK e IDNUM, configurati come `ID nodo adiacente`, con due campi: `ID blocco` e `ID unità fisica`.

2. SNA su TCP/IP assume l'identificativo e genera un nome di dominio:
   - Per i nomi LU, `luname.netid.snasuffix`
   - Per i nomi CP, `cpname.netid.snasuffix`
   - Per i valori IDBLK e IDNUM , `bbbnnnnn.snasuffix`

     Nota: Il valore predefinito per `snasuffix` è **SNA.IBM.COM**. Per ulteriori informazioni sul suffisso del nome di dominio SNA, fare riferimento alla guida in linea.

   In Figura 20 vengono mostrati degli esempi di nomi di dominio generati da SNA su TCP/IP.

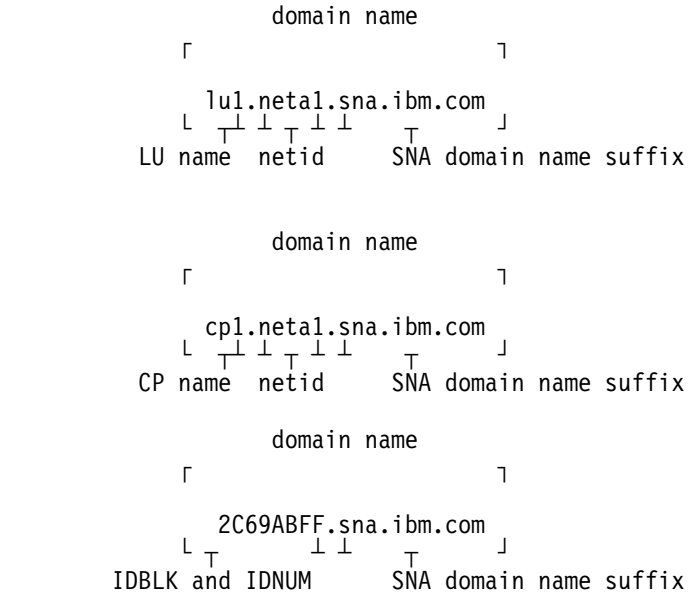


Figura 20. Formati dei nomi di dominio creati da SNA su TCP/IP

3. SNA su TCP/IP richiede che il nome di dominio venga convertito in un indirizzo IP.
4. TCP/IP utilizza il file HOSTS o il server dei nomi di dominio per convertire il nome di dominio in un indirizzo IP (ad esempio, `9.67.192.28`).

Quando la rete IP include gateway SNA su TCP/IP, tenere presente i seguenti punti relativi alla mappatura degli indirizzi:

- Se è possibile raggiungere la LU partner mediante un gateway, il nome di dominio del partner deve essere associato all'indirizzo IP del gateway. In presenza di gateway paralleli, il nome di dominio deve essere associato a ciascun indirizzo IP del gateway.
- Per ridurre al minimo le informazioni sulla mappatura degli indirizzi necessarie per AnyNet, utilizzare una convenzione per la creazione dei nomi grazie alla quale il nome LU risulta identico al nome host TCP/IP. Ad esempio, supposto che il nome host dell'elaboratore sia PATR.ANYNET.OURCORP.COM, se si

utilizza il nome LU PATR e l'ID di rete ANYNET e poi si imposta il suffisso del nome di dominio SNA su OURCORP.COM, AnyNet richiede al TCP/IP di risolvere il nome PATR.ANYNET.OURCORP.COM. Questo nome deve essere già presente nel server dei nomi di dominio.

Definizione dei nomi di dominio e degli indirizzi IP

Questa sezione descrive la funzione di risoluzione del nome TCP/IP, utilizzata da AnyNet per associare le risorse SNA agli indirizzi IP. Tale funzione interroga sia il file HOSTS locale che i server dei nomi di dominio per la conversione di un nome di dominio (ad esempio, `lu1.neta1.sna.ibm.com`) in un indirizzo IP (ad esempio, 10.1.1.1).

File HOSTS E' possibile utilizzare i file TCP/IP HOSTS per associare nomi di dominio ad indirizzi IP per la rete. Tuttavia, con l'aumentare delle dimensioni della rete e dei tempi di gestione dei file HOSTS su ciascuna stazione di lavoro per utenti finali, si consiglia di utilizzare un server dei nomi di dominio.

Nel file HOSTS (nella sottodirectory dei driver\ecc della directory di sistema Windows NT) sono elencati:

- Indirizzo IP
- Nome di dominio
- Altri alias per il nome di dominio

Ad esempio, se l'indirizzo IP è 10.1.1.1, l'ID di rete è NETA1, il nome della risorsa SNA è LUA1 ed il suffisso del nome di dominio SNA è quello predefinito (`sna.ibm.com`), immettere quanto segue nel file HOSTS:

```
10.1.1.1      lua1.neta1.sna.ibm.com
```

Server dei nomi di dominio I nomi di dominio e gli indirizzi IP possono essere definiti anche nel database del server dei nomi di dominio.

Ciascun identificativo SNA viene associato ad un indirizzo IP corrispondente da un server dei nomi di dominio. L'ubicazione di questi server viene configurata nella sezione Rete del Pannello di controllo.

Per ulteriori informazioni sui file HOSTS e sui server dei nomi di dominio, fare riferimento alla documentazione TCP/IP. Se la stazione di lavoro utilizza il supporto TCP/IP fornito in Windows NT, fare riferimento alla documentazione TCP/IP in linea inclusa nel prodotto Windows.

Considerazioni sul gateway SNA su TCP/IP

Le seguenti informazioni si riferiscono ai gateway e non alle funzioni del nodo di accesso.

Definizione dei nomi CP univoci e dei nomi di rete di collegamento

Per le configurazioni che dispongono di due o più gateway SNA su TCP/IP che collegano una rete SNA ad una o più reti IP, è necessario definire un nome CP (control point) SNA univoco ed un nome di rete di collegamento SNA univoco per ciascuna rete IP.

Tutte le LU che si trovano su nodi di accesso nella rete IP si presentano su un nodo con questo nome CP.

Utilizzare il file dei dati invertiti del server dei nomi di dominio oppure il file HOSTS per definire il nome CP ed il nome della rete di collegamento per una determinata rete IP. Associare l'indirizzo IP 127.0.0.3 al nome CP e l'indirizzo IP 127.0.0.4 al nome della rete di collegamento.

Il seguente esempio mostra le voci del file dei dati invertiti. Per una rete IP con ID di rete SNA NETA, nome CP MYCPNAME e nome di rete di collegamento MYCNET, viene definito quanto segue:

```
127.0.0.3       NETA.MYCPNAME.
127.0.0.4       NETA.MYCNET.
```

Note:

1. Alla fine del nome è necessario un punto solo se la definizione si trova nel file dei dati invertiti DNS. Nelle definizioni del file HOSTS non viene utilizzato nessun punto.
2. Non includere il suffisso del nome di dominio SNA.

La funzione SNA AnyNet su TCP/IP di Communications Server fornisce un nome CP predefinito ($ANYNET.$GWCP) ed un nome di rete di collegamento predefinito ($ANYNET.$GWCNET). Nelle configurazioni in cui è presente una rete IP, è possibile utilizzare il valore predefinito non definendo un nome CP o un nome di rete di collegamento. Nelle configurazioni con più gateway che collegano più reti IP, una rete IP può utilizzare il valore predefinito. Tuttavia, è necessario definire un nome CP univoco ed un nome di rete di collegamento per tutte le altre reti IP.

Figura 21 a pagina 77 mostra come definire il nome CP e il nome di rete di collegamento per una configurazione in cui sono presenti due reti IP.

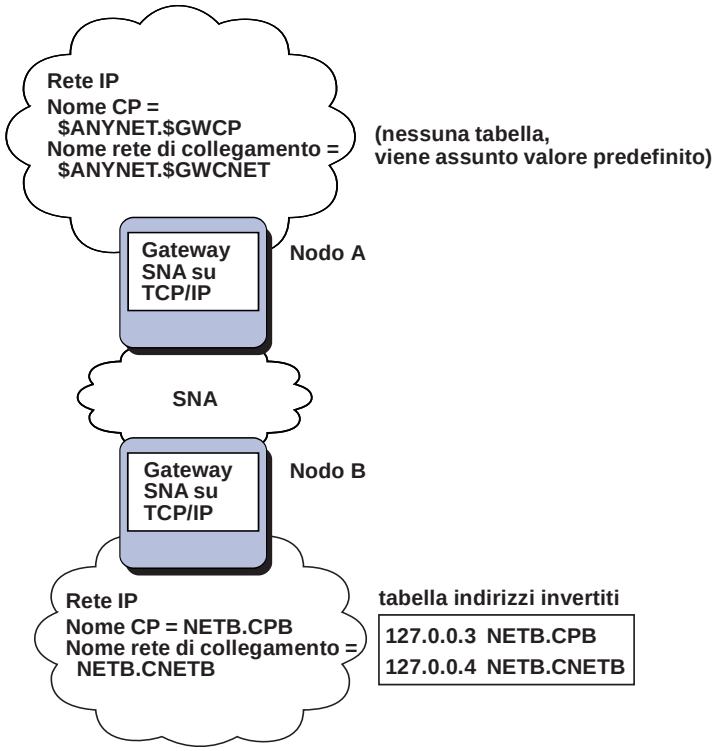


Figura 21. Definizione di un nome CP e di una nome di rete di collegamento

Utilizzo dei caratteri globali nelle definizioni del server dei nomi di dominio

Se si utilizza il gateway SNA su TCP/IP e la configurazione soddisfa le seguenti restrizioni sulla creazione dei nomi, è possibile ridurre il numero di voci del server dei nomi di dominio definendo una voce di nome di dominio per ciascun ID di rete SNA a cui è possibile accedere mediante uno o più gateway SNA su TCP/IP.

- Ciascuna rete SNA deve disporre di un ID di rete SNA univoco tra tutte le reti SNA.
- Ciascuna rete IP deve disporre di un ID di rete SNA univoco tra tutte le reti IP.
- Una rete SNA ed una rete IP possono avere lo stesso ID di rete SNA.

Codificando una singola voce di nome di dominio per ciascun ID di rete SNA, non è necessario definire una voce di nome di dominio per ciascuna LU inclusa nella rete SNA con cui si desidera comunicare nella rete IP. E' possibile utilizzare un carattere globale (*) per specificare il nome LU di tutte le LU che hanno lo stesso ID di rete SNA. Sostituendo *luname* con un carattere globale, viene definita una singola voce del server dei nome di dominio che rappresenta tutte le LU incluse in quella particolare rete.

Nota: Se si utilizza un carattere globale, è necessario che sia completo. I caratteri globali parziali, come LUA*, non sono validi.

Il carattere globale viene associato all'indirizzo IP del primo gateway SNA su TCP/IP utilizzato per raggiungere la rete con quell'ID di rete SNA. Come mostrato in Figura 22 a pagina 78, le unità logiche SNAAPPL1, APPC1, APPC2 e LU5 si trovano nella rete NETB e possono essere raggiunte solo dalla rete IP mediante un gateway SNA su TCP/IP con indirizzo IP IPgwg. Se il suffisso del nome di dominio

SNA è SNA.IBM.COM, viene definita la seguente voce nel server dei nomi di dominio:

```
*.NETB.SNA.IBM.COM        IPgwg
```

Questa voce viene utilizzata per le quattro unità logiche.

Nota: L'utente può scegliere di definire ciascuna unità logica individualmente.

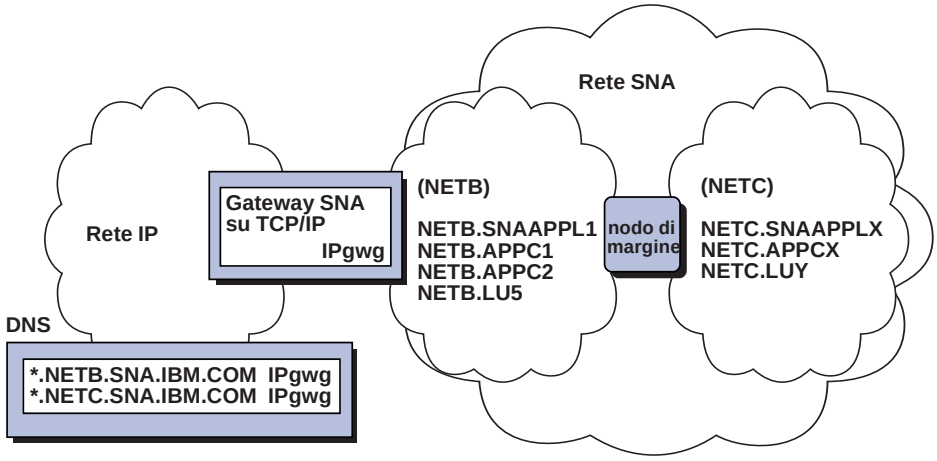


Figura 22. Definizioni del server dei nomi di dominio per un singolo gateway collegato ad una rete SNA con due ID di rete

In ciascuna rete SNA deve essere contenuta una voce univoca. Come illustrato in Figura 22, se nella rete NETC sono presenti anche SNAAPPLX, APPCX e LUY, che è possibile raggiungere solo mediante il gateway SNA su TCP/IP con l'indirizzo IP IPgwg, le voci del server dei nomi di dominio sono le seguenti:

```
*.NETB.SNA.IBM.COM        IPgwg
*.NETC.SNA.IBM.COM        IPgwg
```

Inoltre, in ciascun gateway deve essere contenuta una voce univoca. Se all'esempio precedente viene aggiunto un gateway parallelo SNA su TCP/IP, come illustrato nella Figura 23 a pagina 79, con indirizzo IP IPgwh, le voci del server dei nomi di dominio sono le seguenti:

```
*.NETB.SNA.IBM.COM        IPgwg
*.NETC.SNA.IBM.COM        IPgwg
*.NETB.SNA.IBM.COM        IPgwh
*.NETC.SNA.IBM.COM        IPgwh
```

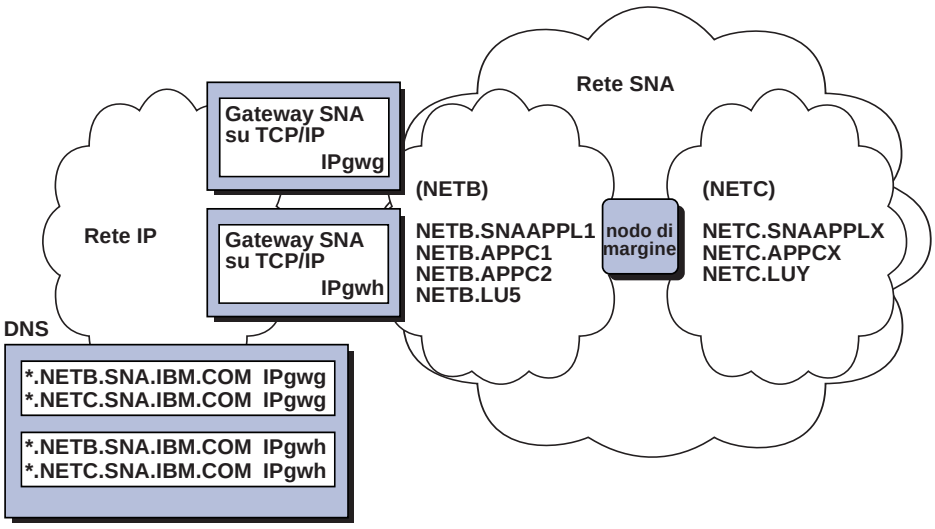


Figura 23. Definizioni del server dei nomi di dominio per gateway paralleli collegati ad una rete SNA con due ID di rete

Considerazioni sulla funzione del nodo di accesso SNA su TCP/IP

Le seguenti informazioni si riferiscono solo ai nodi di accesso e non ai gateway.

Instradamento delle sessioni SNA su SNA AnyNet su TCP/IP

Quando un'applicazione SNA avvia una sessione, Communications Server deve stabilire prima il tipo di trasporto da utilizzare - SNA, IP o una combinazione dei due.

Il trasporto preferito viene configurato impostando la preferenza di instradamento. Tale preferenza può essere impostata per l'intero nodo mediante la preferenza di instradamento predefinita sulla periferica AnyNet su TCP/IP o su base LU quando vengono definite le LU partner.

La tabella delle preferenze di instradamento viene utilizzata solo per le nuove sessioni. Le sessioni esistenti in precedenza utilizzano lo stesso tipo di trasporto e non vengono chiuse e reinstradate se la tabella delle preferenze di instradamento viene modificata.

Nota: La preferenza di instradamento per un nodo gestisce solo le sessioni che vengono avviate dal nodo (sessioni del nodo di accesso). La preferenza di instradamento non influisce sulle sessioni di un nodo.

E' possibile impostare o modificare la preferenza di instradamento predefinita su una delle seguenti opzioni:

Primo nativo Le richieste vengono instradate su SNA. Se non è disponibile nessun instradamento SNA, le richieste vengono instradate su TCP/IP.

Primo non nativo Le richieste vengono instradate su TCP/IP. Se non è disponibile nessun instradamento TCP/IP, le richieste vengono instradate su SNA.

Solo nativo Le richieste vengono instradate solo su SNA. Se non è disponibile nessun instradamento SNA, il collegamento avrà esito negativo.

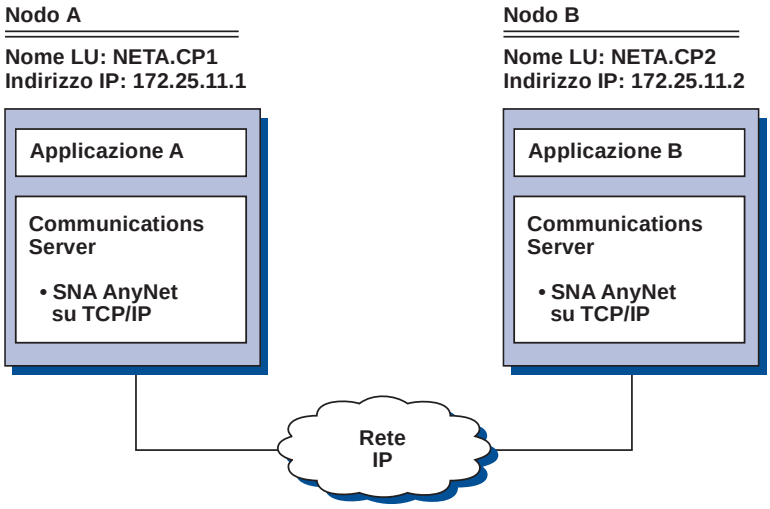
Solo non nativo Le richieste vengono instradate solo su TCP/IP. Se non è disponibile nessun instradamento TCP/IP, il collegamento avrà esito negativo.

Esempi di configurazione SNA AnyNet su TCP/IP

In questa sezione sono inclusi esempi di comunicazione SNA su IP abilitata da AnyNet. Le seguenti istruzioni di configurazione possono considerarsi complete solo per il sistema operativo Windows NT. In tutti gli esempi, il suffisso del nome di dominio SNA è SNA.IBM.COM.

Per ulteriori informazioni sulla configurazione di AnyNet per le altre piattaforme citate in questa sezione (come VTAM o AS/400), fare riferimento alla documentazione appropriata sul prodotto.

Esempio 1. Esecuzione di applicazioni APPC o CPI-C su una rete TCP/IP



Passi

Attenersi ai passi riportati di seguito per stabilire delle comunicazioni tra due nodi Windows NT. Tenere presente che in questo esempio, i nomi CP vengono utilizzati come nomi LU.

Per il Nodo A, effettuare le seguenti operazioni:

1. Aggiungere la seguente voce al file HOSTS locale:

   ```
   172.25.11.2  CP2.NETA.SNA.IBM.COM
   ```

2. Utilizzare **NETA.CP1** come nome CP (control point) durante l'impostazione del nodo. Verificare che l'instradamento delle sessioni sia stato impostato su TCP/IP. Per ulteriori informazioni, fare riferimento alle finestre della guida di **Configurazione nodo**.

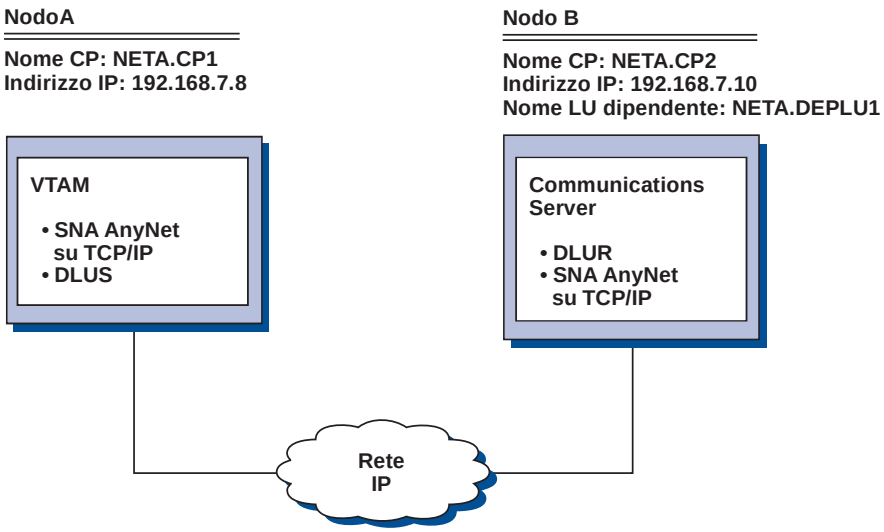
Per il Nodo B, effettuare le seguenti operazioni:

1. Aggiungere la seguente voce al file HOSTS locale:

   ```
   172.25.11.1  CP1.NETA.SNA.IBM.COM
   ```

2. Utilizzare **NETA.CP2** come nome CP (control point) durante l'impostazione del nodo. Verificare che la preferenza di instradamento sia impostata sull'instradamento delle sessioni su TCP/IP. Per ulteriori informazioni, fare riferimento alle finestre della guida di **Configurazione nodo**.

Esempio 2. Emulazione 3270 via DLUR su una rete TCP/IP



Passi

Attenersi ai passi riportati di seguito per stabilire delle comunicazioni tra il Nodo A ed il Nodo B.

Per il Nodo B, effettuare le seguenti operazioni:

1. Aggiungere la seguente voce al file HOSTS locale:

```
192.168.7.8    CP1.NETA.SNA.IBM.COM
```

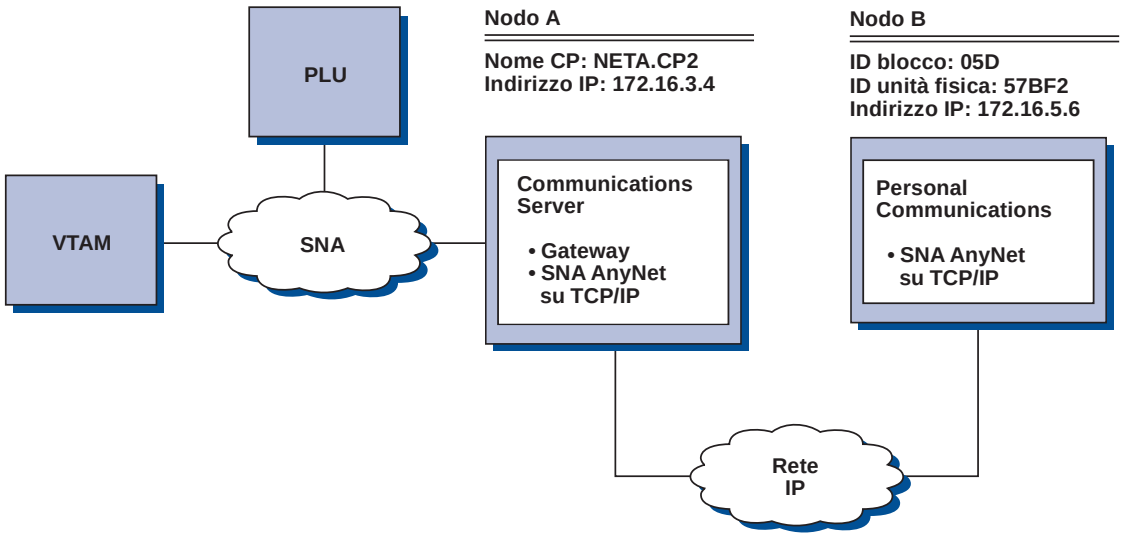
2. Utilizzare **NETA.CP2** come nome CP (control point) durante l'impostazione del nodo e **NETA.CP1** come nodo DLUS durante la configurazione delle PU DLUR. Verificare che sia stato impostato l'instradamento delle sessioni su TCP/IP. Per ulteriori informazioni, fare riferimento alle finestre della guida di **Configurazione nodo**.

Per il Nodo A, aggiungere le seguenti voci al file HOSTS:

```
192.168.7.10    CP2.NETA.SNA.IBM.COM
192.168.7.10    DEPLU1.NETA.SNA.IBM.COM
```

Tenere presente che SNA AnyNet MVS su TCP/IP richiede DLUS/DLUR per le comunicazioni delle LU dipendenti.

Esempio 3. Utilizzo di un gateway SNA per l'abilitazione dell'emulazione 3270 tra reti SNA e TCP/IP



Passi

Attenersi ai passi riportati di seguito per stabilire delle comunicazioni tra il Nodo B e l'host VTAM.

Per il Nodo A, effettuare le seguenti operazioni:

1. Aggiungere la seguente voce al file HOSTS locale:

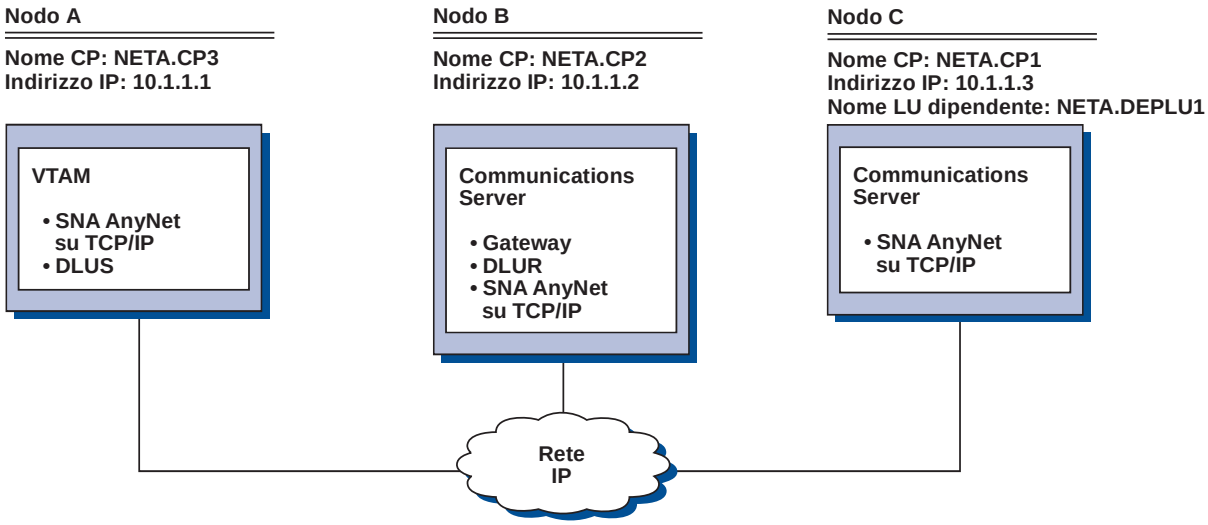
   ```
   172.16.5.6 05D57BF2.SNA.IBM.COM
   ```

2. Utilizzare **NETA.CP2** come nome CP (control point) durante l'impostazione del nodo ed utilizzare la periferica ANYNET per l'assegnazione di maschere implicite durante la definizione dei client. Per ulteriori informazioni, fare riferimento alle finestre della guida di **Configurazione nodo**.

Per il Nodo B, aggiungere quanto segue al file HOSTS locale:

```
172.16.3.4  CP2.NETA.SNA.IBM.COM
```

Esempio 4. Utilizzo di un gateway SNA per l'emulazione 3270 su una rete TCP/IP



Passi

Attenersi ai passi riportati di seguito per stabilire delle comunicazioni tra il Nodo C ed il Nodo A.

Per il Nodo B, effettuare le seguenti operazioni:

1. Aggiungere la seguente voce al file HOSTS locale:

   ```
   10.1.1.3  CP1.NETA.SNA.IBM.COM
   ```

2. Utilizzare **NETA.CP2** come nodo CP (control point) durante l'impostazione del nodo, **NETA.CP1** come nome CP adiacente durante la definizione del collegamento SNA AnyNet su TCP/IP e **NETA.CP3** come nome DLUS durante l'assegnazione del DLUS ad una maschera client. Verificare che la preferenza di instradamento sia impostata su non-nativo per NETA.CP3. Per ulteriori informazioni, fare riferimento alle finestre della guida di **Configurazione nodo**.

Per il Nodo C, effettuare le seguenti operazioni:

1. Aggiungere la seguente voce al file HOSTS:

   ```
   10.1.1.2    CP2.NETA.SNA.IBM.COM
   ```

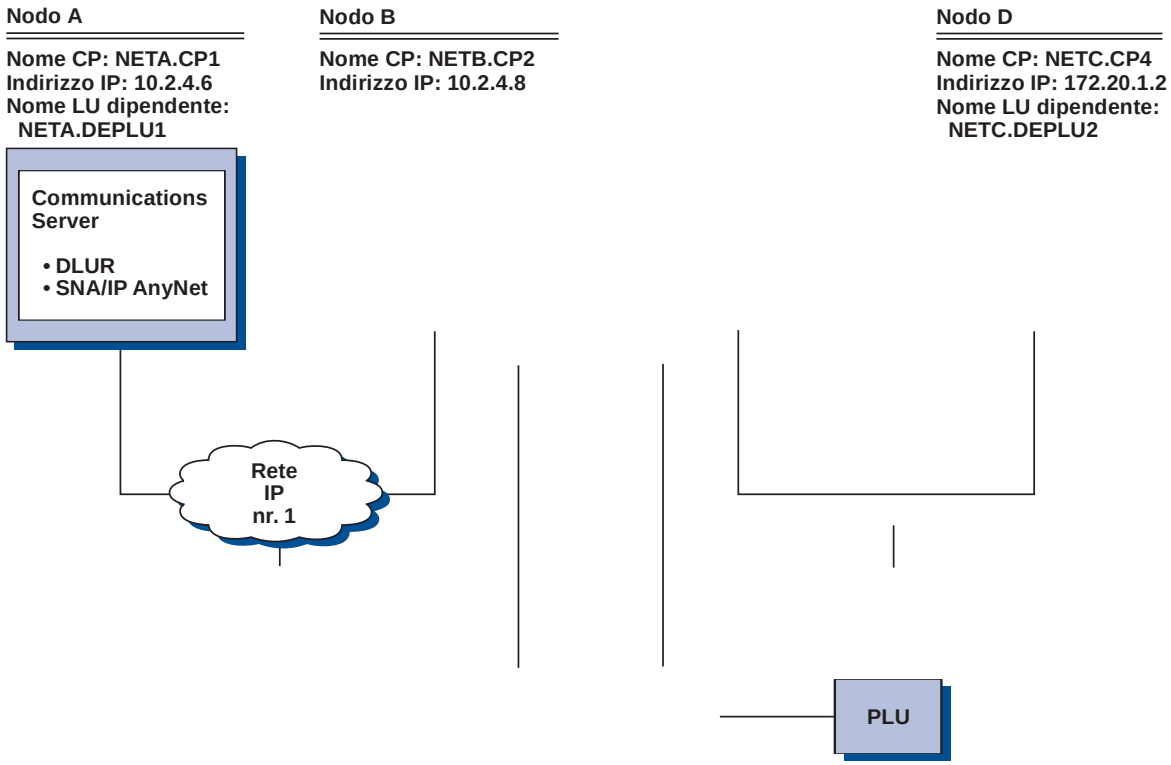
2. Utilizzare **NETA.CP1** come nome CP (control point) durante l'impostazione del nodo e **NETA.CP2** come nome CP adiacente durante la definizione del collegamento SNA AnyNet su TCP/IP. Per ulteriori informazioni, fare riferimento alle finestre della guida di **Configurazione nodo**.

Per il Nodo A, aggiungere la seguente voce al file HOSTS:

```
10.1.1.2   CP2.NETA.SNA.IBM.COM
10.1.1.2   DEPLU1.NETA.SNA.IBM.COM
```

Esempio 5. Emulazione 3270 da due stazioni di lavoro Windows NT su reti IP differenti

Informazioni su SNA AnyNet su TCP/IP



```
10.2.4.6    CP1.NETA.SNA.IBM.COM
127.0.0.2   DEPLU1.NETA.SNA.IBM.COM
10.2.4.6    DEPLU1.NETA.SNA.IBM.COM
127.0.0.4   IPNET1.GWCNET
127.0.0.3   IPNET1.CP1
```

Per il Nodo C, aggiungere le seguenti voci al file HOSTS:

```
172.20.1.2  CP4.NETC.SNA.IBM.COM
127.0.0.2   DEPLU2.NETC.SNA.IBM.COM
172.20.1.2  DEPLU2.NETC.SNA.IBM.COM
127.0.0.4   IPNET2.GWCNET
127.0.0.3   IPNET2.CP2
```

Per il Nodo D, effettuare le seguenti operazioni:

1. Aggiungere la seguente voce al file HOSTS locale:

   ```
   172.20.1.1  CP5.NETB.SNA.IBM.COM
   127.0.0.4   IPNET2.GWCNET
   127.0.0.3   IPNET2.CP2
   ```

2. Utilizzare **NETC.CP4** come nome CP (control point) durante l'impostazione del nodo e **NETB.CP5** come nodo DLUS durante la configurazione delle PU DLUR. Verificare che la preferenza di instradamento per NETB.CP5 sia impostata su non nativo. Per ulteriori informazioni, fare riferimento alle finestre della guida di **Configurazione nodo**.

Suggerimenti utili

In questa sezione sono contenuti suggerimenti utili sulle impostazioni, la connettività TCP/IP via SLIP o PPP e gli indirizzi IP dinamici.

Ricerca del collegamento

Se è possibile accedere ad una LU mediante più gateway SNA su TCP/IP ed il nome LU è stato messo in corrispondenza di più indirizzi IP, aumentare il valore dei parametri **CONN_RETRY_SECS** e **CONNWAIT_SECS** della parola chiave **ANYNET_COMMOM_PARAMETERS** durante la configurazione dei parametri di base AnyNet. In questo modo è possibile assicurarsi che i collegamenti TCP vengano tentati con tutti gli adattatori ed i gateway possibili. Il tempo impiegato perché un collegamento TCP con un indirizzo IP inattivo non riesca, non può essere superiore a 90 secondi.

Indirizzi IP dinamici

In generale, SNA AnyNet su TCP/IP dipende dalle risorse SNA (ad esempio, nomi LU, nomi CP o idblk/num) associati in modo statico agli indirizzi IP. Tuttavia, in base al tipo di configurazione in uso ed al modo in cui i collegamenti sono stati avviati, dovrebbe essere possibile utilizzare SNA AnyNet su TCP/IP negli ambienti in cui gli indirizzi IP vengono assegnati in modo dinamico (ad esempio, DHCP).

Applicazioni APPC o CPIC: Un nodo di accesso SNA su TCP/IP con un indirizzo IP assegnato in modo dinamico può sempre avviare delle sessioni su un altro nodo di accesso SNA su TCP/IP o su un gateway che dispone di un indirizzo IP statico.

Il solo modo in cui un nodo di accesso SNA su TCP/IP o un gateway con un indirizzo IP statico (nodo A) può avviare una sessione su un partner con un indirizzo IP dinamico (nodo B) è il seguente:

1. Il Nodo B ha avviato prima una sessione sul/attraverso il Nodo A.
2. La sessione avviata al Passo 1 è ancora attiva.

Applicazioni delle LU dipendenti

Nota: Le informazioni riportate in questa sezione fanno riferimento alle LU 0, 1, 2, 3 o alle applicazioni 6.2 dipendenti.

I nodi di accesso SNA su TCP/IP con indirizzi IP assegnati in modo dinamico possono supportare comunicazioni di LU dipendenti se vengono soddisfatti i seguenti criteri:

- La comunicazione della LU dipendente è stata stabilita attraverso un gateway SNA oppure attraverso:
  - Communications Server/2 4.1 con APAR JR10461 installato
  - Communications Server/2 V5
  - Communications Server per Windows NT 5.01 o versione successiva
- Il nodo di accesso SNA su TCP/IP con un indirizzo IP assegnato in modo dinamico avvia i collegamenti su un gateway SNA che dispone di un indirizzo IP statico.

Le comunicazioni delle LU dipendenti attraverso DLUS/DLUR su SNA AnyNet su TCP/IP non sono supportate se nel nodo DLUR è presente un indirizzo IP assegnato in modo dinamico.

Configurazione di Socket AnyNet su SNA

Questa sezione contiene informazioni sulla configurazione di Socket su SNA.

La funzione del nodo di accesso Socket su SNA di Communications Server consente alle applicazioni conformi a WinSock di comunicare sulle reti SNA. La funzione del gateway Socket su SNA consente le comunicazioni tra le applicazioni socket nelle reti SNA e IP.

Funzionamento di Socket su SNA

In Figura 24 a pagina 87 viene mostrata la struttura di un nodo Windows NT che esegue Socket su SNA ed illustra il funzionamento dei programmi applicativi socket e di Socket su SNA su un nodo Windows NT.

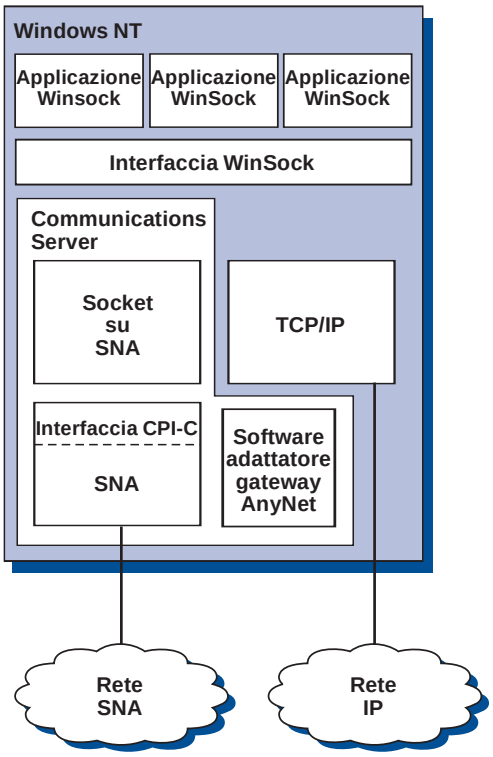


Figura 24. Struttura di un nodo Windows NT che esegue Socket su SNA

WinSock è un'API che consente di eseguire le applicazioni socket in un ambiente Windows.

Socket su SNA non fornisce un'interfaccia WinSock e non elabora le chiamate socket. Le applicazioni WinSock utilizzano invece l'interfaccia WinSock dello stack TCP/IP nativo. Il codice del gateway Socket su SNA consente a queste applicazioni di comunicare in una rete SNA.

Il gateway Socket su SNA consente alle applicazioni socket in esecuzione in una rete IP di comunicare con applicazioni socket in esecuzione sui nodi Socket su SNA. Ciò è possibile mediante l'instradamento dei pacchetti tra reti SNA e IP e la trasformazione tra i protocolli SNA ed IP. Il driver del gateway AnyNet guida l'utente durante l'instradamento dei pacchetti tra reti TCP/IP ed SNA ed il codice Socket su SNA esegue la conversione tra i due protocolli.

Generazione di una chiamata LU 6.2 da una chiamata socket

Per consentire l'instradamento su SNA delle informazioni TCP/IP, Socket su SNA mette in corrispondenza gli indirizzi IP con i nomi completi delle LU per la rete SNA. Quando un programma applicativo richiama Socket su SNA per stabilire un collegamento stream con un altro programma applicativo, Socket su SNA stabilisce due comunicazioni LU 6.2 half-duplex per il collegamento stream.

Socket su SNA stabilisce una comunicazione LU 6.2 per tutti i datagrammi inviati ad una singola destinazione. Le comunicazioni dedicate al traffico dei datagrammi vengono annullate se queste non vengono utilizzate per un periodo di tempo specificato.

Mappatura di un indirizzo IP con un nome di rete SNA

Quando un programma applicativo richiama Socket su SNA per comunicare con un altro programma applicativo, esso fornisce l'indirizzo IP del nodo di destinazione. Socket su SNA deve mettere in corrispondenza l'indirizzo IP con un indirizzo SNA per immettere una chiamata LU 6.2 appropriata. A ciascun indirizzo IP che identifica un nodo corrisponderà un nome di rete SNA.

La “Panoramica sull'instradamento e la mappatura” a pagina 89 mostra il funzionamento della mappatura degli indirizzi e fornisce istruzioni e requisiti per l'impostazione della mappatura degli indirizzi IP-LU.

Instradamento e mappatura dei dati su reti SNA e IP

I gateway Socket su SNA consentono le comunicazioni tra i programmi applicativi socket nelle reti IP e SNA mediante la combinazione della funzione di instradamento del TCP/IP con le funzioni di conversione dei protocolli e di mappatura degli indirizzi di Socket su SNA.

La conversione dei protocolli e la mappatura degli indirizzi sono necessari quando i dati vengono instradati tra nodi che utilizzano protocolli di comunicazione differenti. Il gateway Socket su SNA eseguono la conversione automatica dei protocolli dopo aver stabilito il tipo di comunicazione associato all'indirizzo IP di destinazione. Per un riepilogo dei processi di instradamento e di mappatura, consultare la sezione “Instradamento e mappatura dei dati del gateway Socket su SNA” a pagina 91.

Supporto dei programmi applicativi fornito da Socket su SNA

Socket su SNA supporta le applicazioni WinSock 1.1 e WinSock 2.0 (solo Windows NT 4.0) che utilizzano i socket AF_INET.

Socket su SNA non supporta le applicazioni che utilizzano le trasmissioni di tipo broadcast.

Se si desidera utilizzare il gateway Socket su SNA per l'instradamento delle informazioni in/da un nodo MVS/ESA configurato con la funzione VTAM V3R4.2 Socket su SNA, è necessario installare prima la funzione `route` sul nodo MVS/ESA. Per installare la funzione `route` su MVS/ESA, installare il PTF (program temporary fix) UW03567. I PTF sono disponibili da una delle seguenti fonti:

- Accesso alle informazioni
- SoftwareXcel Extended
- IBMLink (ServiceLink)

Se non si dispone di accesso a queste fonti, rivolgersi al supporto IBM.

Pianificazione di Socket su SNA

In questa sezione sono indicati i punti che un programma di pianificazione di rete dovrebbe considerare prima di procedere alla configurazione di una rete mediante Socket su SNA.

Panoramica sull'instradamento e la mappatura

In questa sezione vengono illustrati i concetti di base sull'indirizzamento Internet e sul rapporto tra questi concetti, l'instradamento e la mappatura. Esso contiene le seguenti informazioni:

Indirizzamento Internet

A ciascun host viene assegnato almeno un indirizzo IP (Internet Protocol) univoco che viene utilizzato per l'instradamento dei dati nella rete.

Nota: Nella serie di protocolli IP, ***host*** si riferisce ad un sistema finale e può essere qualsiasi stazione di lavoro; non deve essere un mainframe.

L'indirizzo IP assegnato all'host non definisce un host nella rete ma piuttosto un'interfaccia per una rete. Ad esempio, l'indirizzo dell'interfaccia di rete SNA identifica un collegamento del nodo alla rete SNA.

Un host gateway dispone di un indirizzo IP univoco per ciascuna interfaccia di rete. Poiché il gateway Socket su SNA instrada i dati SNA e TCP/IP, è necessario impostare indirizzi IP univoci per le interfacce TCP/IP e SNA.

Nella sezione successiva vengono descritti il formato dell'indirizzo IP, le classi di indirizzo e le maschere di rete. Per informazioni più dettagliate, consultare la documentazione TCP/IP.

Formato e classi degli indirizzi IP: Un indirizzo IP è costituito da un campo a 32 bit distinto in due parti:

- La prima parte del campo indirizzo contiene l'indirizzo di rete; la seconda parte contiene l'indirizzo host.
- Il numero di bit utilizzati per le porzioni rete e host di un indirizzo IP è variabile e dipende dalla classe dell'indirizzo IP.
- Una maschera di rete consente l'utilizzo di una parte della porzione host dell'indirizzo IP come indirizzo di sottorete.

In Tabella 5 sono riportate le maschere di rete predefinite.

Tabella 5. Maschere degli indirizzi IP supportate da Socket su SNA

Per un indirizzo IP decimale con punti nel formato *a.b.c.d*, l'intervallo di valori per *a* è:	**Maschera di rete predefinita**
1–127	255.0.0.0
128–191	255.255.0.0
192–223	255.255.255.0

Maschere utilizzate da Socket su SNA: Socket su SNA utilizza due tipi di maschere:

- **Maschera di sottorete**

  La maschera di sottorete viene utilizzata per l'instradamento e viene specificata durante la configurazione degli instradamenti e del nodo locale. E' possibile accettare la maschera di sottorete predefinita oppure specificare un valore diverso da quello predefinito per definire gli indirizzi di sottorete.

- **Maschera di indirizzo**

  La maschera di indirizzo viene utilizzata per la mappatura dell'indirizzo IP-LU generato e viene specificata durante la configurazione.

Tabella di instradamento IP

Ciascun host dispone di una tabella di instradamento IP che memorizza le informazioni relative alle destinazioni possibili ed al modo per raggiungerle. Le voci di instradamento vengono aggiunte quando:

- L'indirizzo IP locale è definito. Per ulteriori informazioni, consultare la guida in linea.
- Le istruzioni per l'instradamento vengono definite dalla finestra **Configurazione nodo**. Fare clic su **Configura socket AnyNet** e poi su **Instradamenti**. Per ulteriori informazioni, consultare la guida in linea.
- Viene trovato un instradamento con un numero di hop inferiore. Ciò si verifica quando il gateway Socket su SNA riceve un'istruzione di reindirizzamento ICMP o un messaggio RIP. Per ulteriori informazioni, consultare la “Funzione di ricerca dell'instradamento (Discovery)” a pagina 92.

Per un esempio di tabella di instradamento, vedere la Figura 25 a pagina 91.

ID di rete SNA utilizzato da Socket su SNA

A ciascun instradamento definito mediante l'interfaccia SNA (sna0) deve corrispondere un ID di rete SNA con cui l'indirizzo di rete IP è mappato. Il numero degli ID di rete SNA definito dipende da come si desidera eseguire la mappatura della rete IP con la rete SNA.

Ad esempio, se le applicazioni socket che utilizzano l'SNA vengono configurate per utilizzare le sottoreti IP 9.67.0.0 e 9.77.0.0, è possibile definire un ID di rete SNA che corrisponde a ciascuna sottorete IP oppure è possibile definire un ID di rete SNA che corrisponde ad entrambe le sottoreti. Socket su SNA non richiede una mappatura esatta ed univoca tra un indirizzo di rete IP ed un ID di rete SNA.

Mappatura di un indirizzo IP con un nome LU

Per mappare gli indirizzi IP con i nomi LU SNA, è possibile utilizzare la mappatura esplicita o quella generata:

- Nella mappatura esplicita, vengono definiti tutti i nomi LU e ciascun indirizzo host IP viene assegnato ad un nome LU SNA specifico durante la configurazione.
- Nella mappatura generata, i nomi LU vengono generati automaticamente. Durante la configurazione, vengono specificati i valori relativi all'indirizzo IP di rete, alla maschera di indirizzo, all'ID di rete ed alla maschera LU.

Socket su SNA utilizza la maschera di indirizzo per eseguire la mappatura della porzione di rete dell'indirizzo IP con l'ID di rete SNA e la porzione host con il nome LU SNA. Il valore della maschera LU viene utilizzato per stabilire i caratteri e le posizioni dei caratteri utilizzati per il nome LU.

E' possibile visualizzare il nome LU generato per un determinato indirizzo IP mediante l'utilizzo del programma di utilità della riga comandi **sxmap**. La sintassi per questo programma di utilità è:

```
  sxmap convert
<indirizzo IP> <maschera di indirizzo> <maschera LU>
```

Instradamento e mappatura dei dati del gateway Socket su SNA

I passi riportati di seguito descrivono brevemente in che modo il gateway Socket su SNA stabilisce se instradare i dati su SNA o TCP/IP e gestisce la mappatura degli indirizzi:

1. Socket su SNA ricerca la relativa tabella di instradamento per individuare un instradamento che consenta ai dati di raggiungere l'indirizzo IP di destinazione. Se Socket su SNA non trova gli instradamenti corrispondenti, la richiesta di collegamento viene inoltrata allo stack TCP/IP nativo.
2. Se Socket su SNA trova un instradamento corrispondente, la voce relativa all'instradamento indica come è possibile raggiungere la destinazione:
   a. Se l'indirizzo router è l'indirizzo di un'interfaccia di rete locale, come sna0, è possibile raggiungere direttamente la rete di destinazione, la sottorete o l'indirizzo host.
   b. Se l'indirizzo router è l'indirizzo di un gateway o di un router, è possibile raggiungere la destinazione solo mediante quel gateway o router intermedio.

   La Figura 25 mostra un esempio di tabella di instradamento IP.

```
Indirizzo IP destin.  Maschera destin. Indirizzo IP gateway  Uso
------------------------------------------------------------------------
1.2.3.4               255.255.255.255  199.245.253.1        10
10.0.0.0              255.0.0.0        199.245.253.2        0
10.11.0.0             255.255.0.0      199.245.253.113      37
127.0.0.1             255.255.255.255  127.0.0.1            8
128.1.0.0             255.255.0.0      199.245.253.3        0
199.245.253.0         255.255.255.0    199.245.253.113      368
```

Figura 25. Esempio di pannello di instradamento IP

3. Se non viene trovato nessun instradamento nella tabella di instradamento Socket su SNA, Socket su SNA assume che la destinazione TCP/IP possa essere raggiunta mediante una rete IP nativa. Per ulteriori informazioni sull'instradamento dei dati con TCP/IP, fare riferimento alla documentazione relativa al protocollo TCP/IP.
4. Se l'instradamento scelto indica che i dati devono essere trasmessi mediante l'interfaccia SNA (sna0), Socket su SNA ricerca l'indirizzo dell'hop successivo nella tabella di mappatura IP-LU:
   a. Se Socket su SNA rileva una voce corrispondente, viene stabilito un collegamento LU 6.2.

b. Se Socket su SNA non rileva nessuna voce corrispondente, il tentativo di collegamento ha esito negativo.

c. Socket su SNA inoltra l'indirizzo di destinazione ed i dati a Communications Server.

5. Tutti gli instradamenti definiti in Socket su SNA sono riflessi nello stack TCP/IP nativo in modo da poter instradare i pacchetti dell'IP su SNA.

Funzione di ricerca dell'instradamento (Discovery): La funzione di ricerca dell'instradamento (Discovery) fornita dal gateway Socket su SNA consente di instradare il traffico TCP/IP in modo più efficiente e ridurre il numero di istruzioni di instradamento definite esplicitamente nella rete. Questa funzione non deve essere selezionata o configurata.

Uno dei problemi relativi all'utilizzo di reti di grandi dimensioni è quello di individuare l'aggiunta di nuove reti o sottoreti ed il router da utilizzare per raggiungere la nuova rete o sottorete. Socket su SNA risolve questo problema facendo in modo che tutti i nodi utilizzino inizialmente un router predefinito che comunica la presenza di altri nodi quando viene individuato un instradamento più diretto. Questo metodo risulta più efficace rispetto all'utilizzo della tipica soluzione TCP/IP che consiste nell'esecuzione di una trasmissione di tipo broadcast delle informazioni relative all'instradamento.

Nota: Per utilizzare correttamente questa funzione, è necessario utilizzare la mappatura algoritmica degli indirizzi IP con i nomi LU ed una rete backbone APPN. In caso contrario, è necessario che i nodi definiscano esplicitamente i nomi LU e gli indirizzi IP per tutti i nodi remoti con cui essi comunicano.

La Figura 26 mostra un esempio di configurazione.

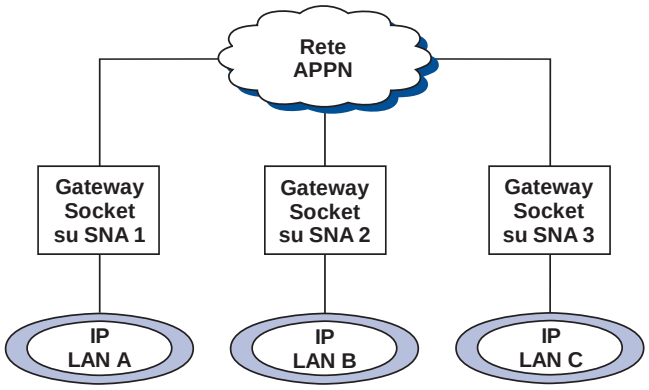


Figura 26. Esempio di una rete che utilizza la funzione Discovery per l'instradamento di Socket su SNA

In questo scenario:

- I Gateway 1, 2 e 3 sono gateway Socket su SNA collegati alle LAN degli IP. Questi gateway collegano le LAN degli IP ad una rete backbone APPN.
- Il Gateway 1 è l'unico gateway in cui viene gestita una tabella di instradamento completa e permanente.

  I Gateway 2 e 3 definiscono il Gateway 1 come router predefinito. Se una rete o una sottorete remota viene riconosciuta dal Gateway 1, i Gateway 2 e 3 non devono definire esplicitamente questi instradamenti.

- Quando i Gateway 2 e 3 instradano i dati su reti o sottoreti non definite, queste richieste vengono inviate al router predefinito, Gateway 1.

  Se la rete o la sottorete viene riconosciuta dal Gateway 1 ed è disponibile un percorso più diretto, il Gateway 1 invia un messaggio di reindirizzamento ICMP al richiedente che indica il percorso da utilizzare successivamente. Questo messaggio di reindirizzamento ICMP aggiorna la tabella di instradamento del richiedente. Pertanto, i Gateway 2 e 3, creano dinamicamente le relative tabelle di instradamento per le reti e le sottoreti remote, come necessario.
- Se vengono aggiunti nuovi gateway, aggiornare la tabella di instradamento permanente del Gateway 1. Per i Gateway 2 e 3 non sono necessarie istruzioni di instradamento esplicite.

Definizione dei modi Socket su SNA

Socket su SNA utilizza le comunicazioni LU 6.2 per consentire le comunicazioni tra i programmi applicativi socket. Quando viene stabilita una comunicazione LU 6.2, Socket su SNA definisce le caratteristiche del modo e della sessione associata del collegamento. Communications Server utilizza il nome del modo per identificare le caratteristiche del collegamento tra i due nodi Socket su SNA.

Il modo predefinito per Socket su SNA è BLANK. E' possibile utilizzare tale modo predefinito oppure definirne un altro. Per modificare il modo predefinito per Socket su SNA, dalla finestra **Configurazione nodo**, fare clic su **Configura Socket AnyNet su SNA** e poi fare clic su **Modi**. E' possibile definire un altro modo predefinito per tutto il traffico TCP/IP ed assegnare uno modo specifico ad una determinata porta TCP/IP.

Se viene specificato un modo alternativo che non è definito da Communications Server, è necessario definire le caratteristiche della sessione associate a quel modo in Communications Server.

Modifica dell'intervallo di timeout inattività

L'opzione di avvio del timeout di inattività consente di regolare il numero di secondi di inattività prima che Socket su SNA chiuda la comunicazione del datagramma. Questo intervallo consente di bilanciare l'utilizzo delle risorse di sistema per la conservazione di una comunicazione esistente del datagramma e di disporre di più tempo per ristabilire una nuova comunicazione del datagramma. Ad esempio, se questo intervallo viene impostato su un valore basso, le comunicazioni del datagramma non utilizzate terminano più velocemente ma l'inoltro del successivo datagramma richiede più tempo. L'intervallo di timeout inattività predefinito è 90 secondi.

Per modificare l'opzione di avvio, dalla finestra **Configurazione nodo**, fare clic su **Configura Socket AnyNet su SNA**, poi su **Visualizza/Cambia/Aggiungi**, sul separatore **Avanzato** e selezionare un nuovo valore per questa opzione.

Pianificazione delle comunicazioni client/server

Questo capitolo contiene informazioni sulla pianificazione dei client API SNA per Communications Server e Novell IntranetWare per SAA.

Client API SNA

Questa sezione contiene informazioni specifiche per i client API SNA.

Installazione e configurazione

Per informazioni sull'installazione e la configurazione dei client API SNA di Communications Server, fare riferimento al manuale *Guida operativa*.

LDAP (Lightweight Directory Access Protocol)

LDAP (Lightweight Directory Access Protocol) fornisce una modalità standard di accesso ai directory services. LDAP consente di leggere, ricercare, aggiungere e cancellare le informazioni dai database centralizzati o distribuiti. Esso è simile al precedente X.500 DAP (Directory Access Protocol), ma non presenta alcuni dei suoi svantaggi (come i livelli OSI di presentazione e di sessione). E' possibile utilizzare **LDAP Client Configuration** per eseguire la configurazione delle informazioni relative ai client API SNA e memorizzarle in un server LDAP.

LDAP Client Configuration mostra l'organizzazione e le relazioni logiche tra i client e le relative configurazioni., and consists of three major areas:

- Gerarchia dei client
- Gerarchia delle configurazioni
- Pulsanti di azione per le definizioni

Per ulteriori informazioni sull'utilizzo di queste aree principali, fare riferimento ai pannelli di aiuto relativi a **LDAP Client Configuration**.

DIT (Directory Information Tree)

DIT (Directory Information Tree) collega tutti i DSA (Directory Service Agent) in un modello predefinito. Il modello è una struttura gerarchica estensibile composta da diversi oggetti di base. Un DIT LDAP tipico è costituito da un root, in cui sono definiti le ***countries*** (c). Al di sotto delle nazioni (country) si trovano generalmente le ***organizations*** (o) e al di sotto delle organizzazioni si trovano gli ***individuals***, ((cn) o (uid)), o le ***organizational units*** (ou). Ad esempio, una voce LDAP distinta viene specificata come segue:

```
c=US, o=company.com, ou=Sales, cn=temp
```

Gerarchia dei client

La gerarchia dei client si riferisce al DIT LDAP con cui si è effettuato il collegamento. E' possibile aggiungere oppure eliminare utenti o unità organizzative alla/dalla gerarchia client.

DIT (Directory Information Tree): DIT (Directory Information Tree) collega tutti i DSA (Directory Service Agents) in un modello predefinito. Il modello è una struttura gerarchica estensibile composta da diversi oggetti di base. Un DIT LDAP tipico è

costituito da un root, in cui sono definiti le ***countries*** (c). Al di sotto delle nazioni (country) si trovano generalmente le ***organizations*** (o) e al di sotto delle organizzazioni si trovano gli ***individuals***, ((cn) o (uid)), o le ***organizational units*** (ou). Ad esempio, una voce LDAP distinta viene specificata come segue:

```
c=US, o=company.com, ou=Sales, cn=temp
```

Gerarchia delle configurazioni

La gerarchia delle configurazioni mostra uno schema logico della configurazione client e di tutte le relazioni tra le definizioni di configurazione, utilizzando una vista grafica ad albero. Tale gerarchia consente la creazione, la modifica o la rimozione delle definizioni.

Pulsanti di azione delle definizioni

I pulsanti di azione per le definizioni agiscono sulla gerarchia delle configurazioni e vengono abilitati in base alla configurazione correntemente selezionata nella gerarchia. Sono disponibili pulsanti di azione per le definizioni che consentono di:

- Creare una nuova definizione del tipo selezionato nella gerarchia delle configurazioni
- Modificare una definizione esistente del tipo selezionato nella gerarchia delle configurazioni
- Eliminare una definizione selezionata

  Nota: Prima dell'eliminazione della risorsa non viene visualizzato nessun messaggio di conferma.

- Eliminare più definizioni

  Dall'elenco delle definizioni nel pannello relativo alla gerarchia delle configurazioni, selezionare le definizioni che si desidera eliminare. Fare clic su **OK** per eliminare le definizioni selezionate. Se si desidera eliminare tutte le definizioni contenute nell'elenco, è possibile fare clic su **Select all**.

Common API Client per Communications Server per Windows NT ed IntranetWare per SAA

Il client fornito con Communications Server consente ai client di individuare nella rete gli IBM Communications Server ed i server IWSAA (IntranetWare for SAA) ed accedervi.

Opzioni di installazione per l'ubicazione della configurazione

Durante l'installazione del client, l'utente può scegliere l'ubicazione per la configurazione del client. Sono disponibili tre scelte:

- Configurazione del file INI, che è il metodo utilizzato con le versioni precedenti di Communications Server e quello predefinito durante l'installazione del client API SNA fornito con Communications Server
- NDS (Netware Directory Services), che è il metodo utilizzato con le versioni precedenti di IWSAA e quello predefinito durante l'installazione del client API SNA fornito con IntranetWare per SAA
- LDAP (Lightweight Directory Access Protocol)

L'ubicazione della configurazione contiene elenchi server, nomi utente e tutte le altre informazioni relative alla configurazione client.

Ubicazioni di configurazione

Dal momento che le informazioni sulla configurazione sono indipendenti dal tipo di server (Communication Server per Windows NT o IntranetWare per SAA), è possibile memorizzare le informazioni nelle ubicazioni NDS, INI o LDAP. Ad esempio, è possibile memorizzare i nomi e gli indirizzi dei Communication Server nelle ubicazioni NDS, INI o LDAP per il client API. Poiché i programmi di gestione NDS vengono forniti solo con IntranetWare per SAA, per configurare le informazioni sul client API SNA nell'NDS è necessario che il prodotto IntranetWare per SAA sia presente nella rete. Il Common SNA API consente di integrare in modo semplice i diversi tipi di server nella stessa rete.

Programma di utilità per la configurazione

Utilizzare il programma di utilità **Set Configuration Options** per modificare l'ubicazione della configurazione client (INI, NDS o LDAP) in seguito all'installazione.

Individuazione dei server

Il client consente all'utente di individuare ed accedere agli IBM Communications Server ed ai server IWSAA mediante i protocolli di comunicazione TCP/IP e SPX.

TCP/IP: Il metodo utilizzato per l'individuazione dei server mediante il protocollo di comunicazione TCP/IP è identico. Il responsabile della rete può controllare l'accesso ai server mediante la configurazione del server. Per ulteriori informazioni, consultare la sezione “Pianificazione degli ambiti TCP/IP” a pagina 148.

SPX: I metodi utilizzati per l'individuazione dei server mediante il protocollo di comunicazione SPX sono differenti. L'individuazione degli IBM Communications Server e dei server IWSAA richiede più tempo della sola individuazione degli IBM Communications Server o dei server IWSAA.

Il client API SNA di Communications Server tenta di individuare prima gli IBM Communication Server e poi i server IWSAA. Se nella rete non è presente alcun server IWSAA oppure non è possibile accedervi, l'utente può impostare una variabile di ambiente per impedire l'individuazione dei server IWSAA. L'impostazione della variabile consente di migliorare le prestazioni in un ambiente in cui il protocollo di comunicazione SPX accede solo agli IBM Communication Server. La variabile di ambiente è **SNA_API_CLIENT_NO_CC**. L'impostazione di tale variabile non influisce sull'ubicazione del server che utilizza il protocollo di comunicazione TCP/IP.

Assegnazione di una LU locale predefinita

E' possibile assegnare a ciascun utente un alias predefinito per la LU locale utilizzando la configurazione del file INI o la configurazione LDAP per i client API SNA Windows a 32 bit.

I programmi APPC possono utilizzare un alias predefinito per la LU locale invece di specificarne uno direttamente. Quando un programma APPC emette un verb TP_START con il campo relativo all'alias per la LU locale impostato su zero binari o su tutti spazi ASCII, l'API APPC utilizza l'alias predefinito per la LU locale configurato.

I programmi EHNAPPC possono utilizzare un alias predefinito per la LU locale invece di specificarne uno direttamente. Quando il campo relativo alla LU locale nel

pannello di configurazione AS/400 viene lasciato vuoto, viene utilizzato l'alias predefinito configurato per la LU locale.

I programmi CPI-C possono utilizzare un alias predefinito per la LU locale invece di specificarne uno direttamente. Quando il campo relativo all'alias della LU locale nel record CPI-C viene lasciato vuoto e non sono stati definiti valori utilizzando la variabile di ambiente APPCLLU, l'API CPI-C utilizza l'alias predefinito configurato per la LU locale durante l'avvio di una conversazione.

I programmi avviati da Attach Manager possono utilizzare un alias predefinito per la LU locale invece di specificarne uno direttamente. Quando il campo relativo all'alias della LU locale nel record Attach Manager viene lasciato vuoto, Attach Manager utilizza l'alias predefinito configurato per la LU locale durante l'elaborazione delle richieste di conversazione in arrivo.

Assegnazione di una LU partner predefinita

E' possibile assegnare a ciascun utente un alias predefinito per la LU partner utilizzando la configurazione del file INI oppure la configurazione LDAP per i client API SNA Windows a 32 bit.

I programmi APPC possono utilizzare un alias predefinito per la LU partner invece di specificarne uno direttamente. Quando un programma APPC emette un verb ALLOCATE con i campi relativi all'alias LU partner ed alla LU partner completa impostati su zero binari o su tutti spazi ASCII, l'API APPC utilizza l'alias predefinito configurato per la LU partner.

I programmi CPI-C possono utilizzare un alias predefinito per la LU partner invece di specificarne uno direttamente. Quando il campo relativo all'alias LU partner nel record dell'ubicazione CPI-C viene lasciato vuoto, l'API CPI-C utilizza l'alias predefinito configurato per la LU partner durante l'avvio di una conversazione.

Assegnazione di un nome di sessione LUA predefinito

E' possibile assegnare a ciascun utente un alias predefinito per la LU partner utilizzando la configurazione del file INI oppure la configurazione LDAP per i client API SNA per Windows a 32 bit.

I programmi LUA, come i programmi di emulazione 3270, possono utilizzare un nome di sessione LUA predefinito invece di specificarne uno direttamente. Quando un programma LUA emette un verb RUI_INIT o SLI_OPEN con il campo relativo al nome LU LUA impostato su zero binari o su tutti spazi ASCII, l'API RUI/SLI utilizza il nome predefinito configurato per la sessione LUA.

Crittografia dei dati client/server

La crittografia dei dati client/server consente al client di richiedere la crittografia dei dati applicativi nelle comunicazioni tra client API SNA e Communications Server.

Tale crittografia può essere attiva, non attiva o facoltativa. La crittografia facoltativa dei dati indica che la crittografia viene utilizzata solo se è supportata dal server.

Sicurezza client/server

Communications Server consente ai client API SNA per Windows 95 e per Windows NT di utilizzare la sicurezza del dominio Windows NT per l'autenticazione del collegamento client al server evitando la nuova immissione dell'ID utente e della password. Il client deve appartenere ad un dominio Windows NT, partecipando ad un dominio Communications Server oppure eseguendo il collegamento in locale con una password ed un ID utente sincronizzati.

Agli utenti del client API SNA esterni al dominio Windows NT viene richiesto di fornire l'ID utente e la password, utilizzando una richiesta oppure memorizzando questi valori nel file di configurazione del client.

Gli utenti autorizzati all'utilizzo client/server vengono memorizzati nel gruppo locale IBMCSAPI, che si trova direttamente in Communications Server o nell'unità di controllo del dominio a cui appartiene Communications Server. Tale gruppo di utenti viene creato durante l'installazione e può essere gestito utilizzando l'applicazione User Manager di Windows NT.

E' possibile stabilire se l'ID utente e la password sono necessari per il collegamento al server impostando il valore **LogonControl** del server su zero (0), in modo da eliminare dal client il requisito relativo all'ID utente ed alla password.

I record relativi alla registrazione dell'attività di rete dei collegamenti client al server vengono tracciati nella registrazione eventi di Windows NT. E' possibile visualizzare i record utilizzando il Visualizzatore eventi di Windows NT nella registrazione **Applicazione**. Se non si desidera tracciare i collegamenti client al server, è possibile modificare il valore **AuditTrail** sul server impostandolo su zero (0).

E' possibile accedere ai valori **LogonControl** e **AuditTrail** utilizzando l'Editor del registro di Windows NT con la chiave:
`HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/IBM SNA Client Services`.

Client Novell IntranetWare per SAA

Communications Server supporta i client collegati tramite IPX o TCP/IP che eseguono pacchetti software di emulazione che implementano l'architettura QEL/MU (Queue Element/Message Unit) della Novell per l'emulazione 3270, consentendo l'accesso dei client ai dati host mainframe. Sono supportate anche funzioni client comuni, incluse le categorie LU pubbliche, dedicate, e in pool, a cui si fa talvolta riferimento come tipi di risorsa.

Communications Server supporta i client Novell IntranetWare per SAA sulle piattaforme Windows 95, Windows NT, Windows 3.1 ed OS/2.

Per le comunicazioni tra i client Novell IntranetWare per SAA e Communications Server sono necessari i protocolli TCP/IP, IPX/SPX o entrambi. Se si esegue IPX, è anche necessario che il seguente software sia abilitato sul server:

- Gateway Service per Netware
- Agente SAP
- NWLink IPX/SPX o un protocollo compatibile

Se Communications Server viene eseguito su un'unità di controllo primaria o di backup, è necessario assegnare diritti di utente nel gruppo IBMCSAPI per eseguire il collegamento in locale al server.

Pianificazione dell'accesso ai dati legacy

Questo capitolo contiene informazioni sulle funzioni di Communications Server che consentono di accedere alle informazioni host.

AS/400 OLE DB Provider

Le applicazioni che utilizzano OLE DB o ActiveX possono comunicare mediante Communications Server per l'accesso a livello di record ai file presenti sulle stazioni AS/400. L'accesso ai file AS/400 richiede la definizione della stazione AS/400 remota, in cui sono memorizzati i file, come LU partner.

AS/400 OLE DB Provider può essere installato come componente di Communications Server oppure come componente del client API SNA per Windows 95. Inoltre, può essere installato come componente del client API SNA per Windows NT; tuttavia, esso richiede Windows NT Workstation o Server 4.0 o versione successiva. Se MDAC (Microsoft Data Access Components) Versione 1.5 non è installato, Communications Server lo installerà durante l'installazione di questo componente.

Se AS/400 OLE DB Provider viene installato su una macchina su cui è già installato Client Access Versione 3 Rilascio 2 MD (o precedente), alcune funzioni di Client Access verranno disabilitate, incluso il supporto per i programmi ActiveX e OLE DB che utilizzano Client Access per accedere alle code di dati AS/400, i comandi remoti, le chiamate ai programmi distribuiti, le procedure memorizzate e le istruzioni SQL.

Se si desidera continuare ad utilizzare queste funzioni mediante Client Access, non installare il componente AS/400 OLE DB Provider durante l'installazione di Communications Server. Se tale componente viene installato e si desidera ripristinare le funzioni di Client Access, è possibile eseguire la reinstallazione di Client Access. Tuttavia, se Client Access viene reinstallato, non sarà possibile utilizzare AS/400 OLE DB Provider con Communications Server.

Quando Client Access viene installato in seguito all'installazione di Communications Server, le informazioni relative al registro vengono sovrascritte. Se si desidera utilizzare il componente AS/400 OLE DB Provider con Communications Server dopo aver eseguito l'installazione di Client Access, è possibile eseguire il programma REGSVR32.EXE sui file cwbzzodb.dll e cwbzzidx.dll in modo da ripristinare le informazioni sul registro AS/400 OLE DB Provider.

AS/400 OLE DB Provider può essere utilizzato per eseguire il collegamento dei client Windows 95 e Windows NT 4.0 mediante Communications Server ad una o più stazioni AS/400, come illustrato nella Figura 27 a pagina 102. Questa configurazione fornisce ai client su cui è installato il componente AS/400 OLE DB Provider l'accesso a record specifici all'interno dei file presenti sulla stazione AS/400.

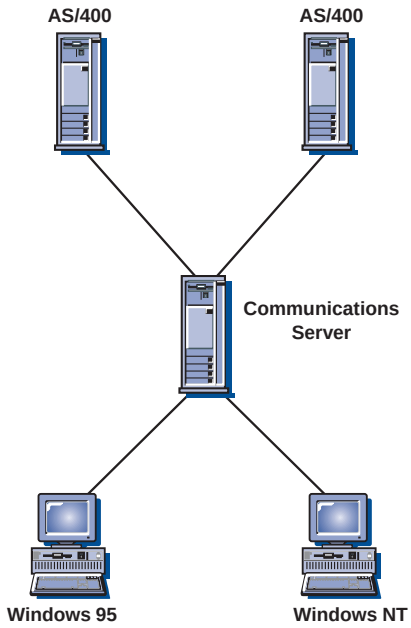


Figura 27. AS/400 OLE DB Provider

Su entrambi i client rappresentati in questa figura è installato il componente AS/400 OLE DB Provider. In alternativa, è possibile installare ed utilizzare la funzione dal server.

La documentazione relativa a questa funzione e le informazioni sullo sviluppo delle applicazioni OLE DB e ActiveX mediante Client Access, sono disponibili nella directory `csnt\sdk\as400_oledb`.

Server delle cartelle condivise AS/400

E' possibile creare sul server delle unità disco che comunicano con le cartelle AS/400 mediante ISF (Integrated File System) AS/400. Se il server condivide queste unità disco, i client possono collegarsi a queste unità ed utilizzarle in modo da ottenere l'accesso alle unità AS/400 senza un'ulteriore configurazione o installazione del codice sulla macchina client. Più client possono collegarsi alle cartelle presenti nel sistema AS/400 come se fossero unità di stazioni di lavoro.

L'applicazione **Configurazione nodo** abilita il supporto delle cartelle condivise. Quando un'unità disco è disponibile all'utente, questa agisce come unità disco supportata dal sistema. Utilizzare le interfacce fornite da Windows NT per controllare l'unità. Gli utenti possono condividere l'unità nella rete conservando i propri diritti di accesso.

Il server delle cartelle condivise AS/400 richiede OS/400 Versione 3.1 o versione successiva.

Host Publisher

Host Publisher consente di accedere ai siti Web di grandi dimensioni con contenuto dinamico. Esso può essere utilizzato per accedere ai dati presenti sugli host S/390 o AS/400 e visualizzarli sulle pagine Web create dinamicamente in base ad un progetto personale.

Host Publisher include diversi componenti. Per le descrizioni dei componenti e le informazioni sull'installazione di Host Publisher, fare riferimento alla *Guida operativa* in linea.

Tre valori di registro abilitano il controllo basato sul registro sull'utilizzo di qualsiasi JIT presente ed un percorso classe specifico per Host Publisher. Potenzialmente le implementazioni Java incompatibili possono risiedere sulla stessa macchina su cui risiede Host Publisher.

JITCompiler Questo valore indica il nome del programma di compilazione JIT da utilizzare per la creazione delle istanze Host Publisher per la VM. Esso imposta la proprietà di sistema **java.compiler** che gestisce il modo in cui VM carica ed utilizza i JIT.

EnableJIT Questo valore booleano indica se il JIT specificato da **JITCompiler** viene utilizzato.

Classpath Questo valore indica il percorso classe specificato nella VM. Se il valore non è specificato o è specificato come nullo, viene utilizzata la variabile dell'ambiente di sistema.

E' possibile accedere ai valori **JITCompiler**, **EnableJIT** e **Classpath** mediante l'Editor del registro di Windows NT con la chiave:
`HKEY_LOCAL_MACHINE/Software/IBM/Host Publisher/Config`.

Dal momento che Java VM viene inizializzata durante l'inizializzazione di Host Publisher, PageServer ed Integrator devono essere riavviati per rendere effettive le modifiche apportate al registro.

Elaborazione delle pagine Web

Dopo aver creato una libreria Web utilizzando **Integrator**, è necessario implementare la libreria in modo che i client possano utilizzare un browser Web per la visualizzarla sul Web.

Quando un client fa clic su un pulsante nella pagina Web, viene inviata una richiesta dal sistema client ad un server Web. Il server Web contatta l'**Adattatore** che stabilisce che la richiesta è associata ad una pagina Web dinamica, memorizzata come file della libreria Web in una macchina di rete su cui è presente **PageServer**.

Dispatcher stabilisce che **PageServer** deve soddisfare la richiesta e l'**Adattatore** instrada la richiesta al **PageServer** consigliato.

PageServer colloca la pagina in una delle sue librerie e ne inizia l'elaborazione. Esso ricerca le tag DYNA nel file.

- Se vengono rilevate delle tag DYNA, **PageServer** esegue una ricerca nella libreria Web per identificare l'ubicazione degli Integration Object associati alle tag DYNA ed elabora i comandi in modo da estrarre il contenuto dinamico.

PageServer risolve l'elaborazione degli script del server rilevati nella pagina, sostituisce le tag DYNA con le tag HTML, incluse le informazioni estratte dall'origine, e restituisce la pagina all'**Adattatore**.

- Se non vengono rilevate tag DYNA, **PageServer** crea un file e lo invia all'**Adattatore**.

L'**Adattatore** invia la pagina al server Web, che la invia alla macchina client.

Configurazioni Host Publisher

E' possibile installare diverse configurazioni Host Publisher, in base a fattori quali la potenza delle macchine utilizzate e le prestazioni dell'origine dati a cui si è acceduto.

Per una configurazione di base, server Web, **PageServer**, **Adattatore** e **Dispatcher** si trovano tutti sulla stessa macchina.

Per una configurazione estesa, è necessario disporre di un server Web indipendente, di più **PageServer** indipendenti ed il **Dispatcher** deve trovarsi sulla stessa macchina su cui si trova **PageServer** o server Web.

Per una configurazione migliore, è necessario disporre di un server Web indipendente, di più **PageServer** indipendenti, di un **Dispatcher** primario indipendente e di un **Dispatcher** secondario indipendente.

In Figura 28 viene mostrato un esempio delle modalità di utilizzo di un browser Web con Host Publisher per l'accesso alle informazioni di un'applicazione 3270 presente su un host.

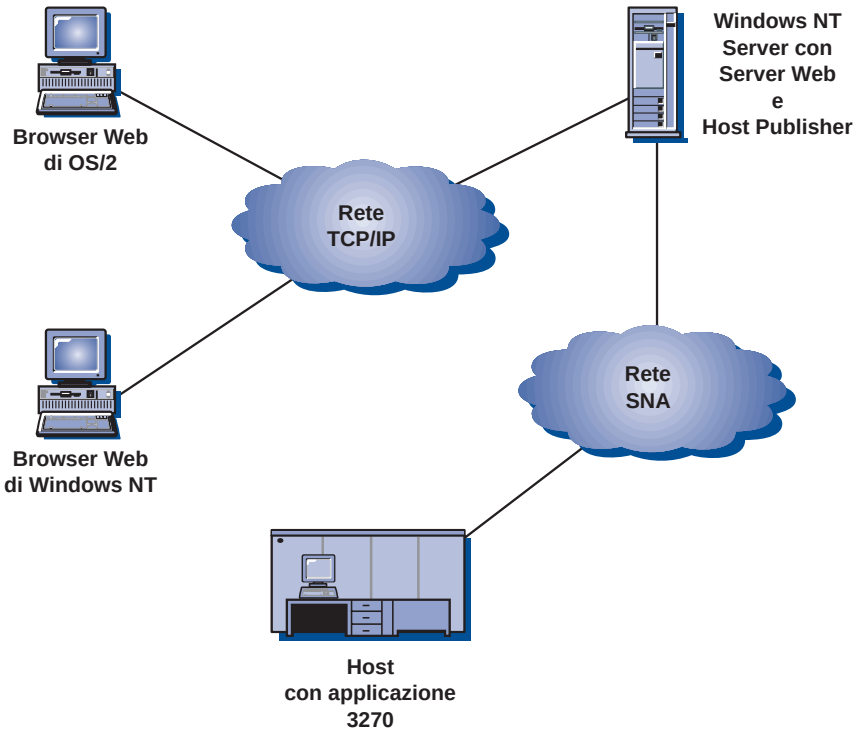


Figura 28. Host Publisher ed un'applicazione host integrata in un ambiente Web

Configurazione per applicazioni ad alta disponibilità

E' possibile estendere il sito Web in caso di aumento del volume di attività. Per accertarsi che i client funzionino in un ambiente con tolleranza agli errori, Host Publisher consente di configurare il **Dispatcher** in modo esso possa continuare a lavorare con i componenti standby.

Il **Dispatcher** può essere configurato in modo da disporre di istanze primarie e secondarie. Se, per qualsiasi motivo, il **Dispatcher** primario viene eseguito con esito negativo, l'**Adattatore** ed i **PageServer** provano immediatamente a collegarsi al **Dispatcher** secondario. Ciascun **Dispatcher** può supportare diversi server Web.

E' possibile replicare le librerie Host Publisher su diversi **PageServer**. Il **Dispatcher** opera con i **PageServer** per l'esecuzione della distribuzione del carico e l'assegnazione delle risorse. Le richieste client vengono inviate al **PageServer** su cui sono presenti le risorse più disponibili. Con l'aumento delle richieste client, è possibile avviare ulteriori **PageServer**.

Collegamento di Client Access agli host CICS

Il software per i client CICS per Windows NT viene fornito con Communications Server in modo da consentire il collegamento dei client agli host CICS mediante Communications Server.

In Figura 29 viene mostrato un esempio di configurazione di un client CICS per l'accesso alle informazioni contenute in un database CICS di un host.

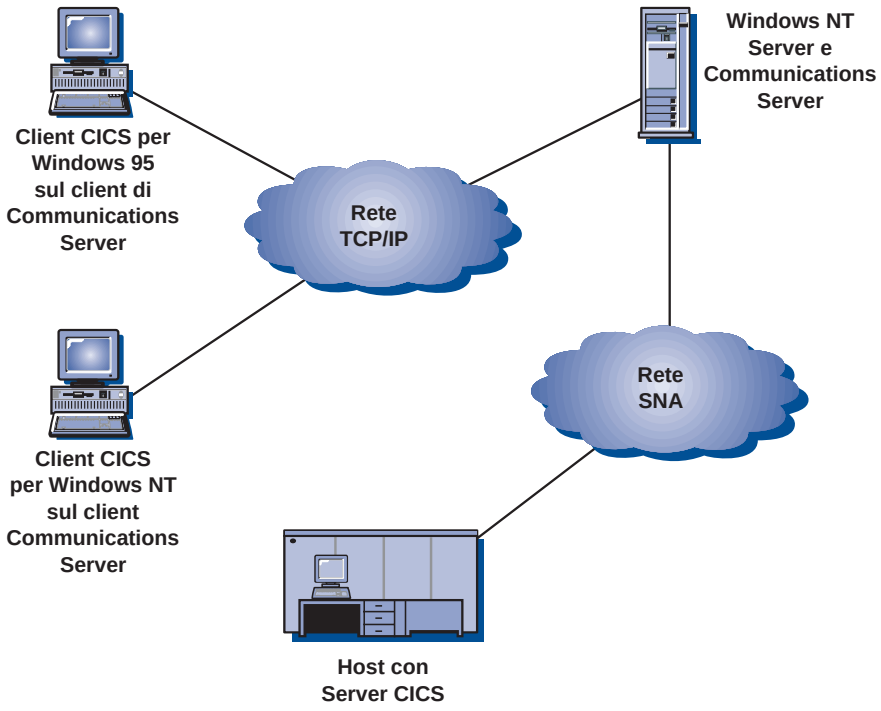


Figura 29. Ambiente client CICS

Per ulteriori informazioni sulla configurazione dei client CICS, fare riferimento a *CICS Clients Administration*. Questo manuale è disponibile su Internet al seguente indirizzo:

http://www.software.ibm.com/ts/cics/library

Collegamento di Client Access agli host MQSeries

Il software per i client MQSeries per Windows NT viene fornito con Communications Server in modo da consentire il collegamento dei client agli host MQ mediante Communications Server.

In Figura 30 viene mostrato un esempio di configurazione di un client MQSeries per l'accesso alle informazioni contenute in un database MQSeries di un host.

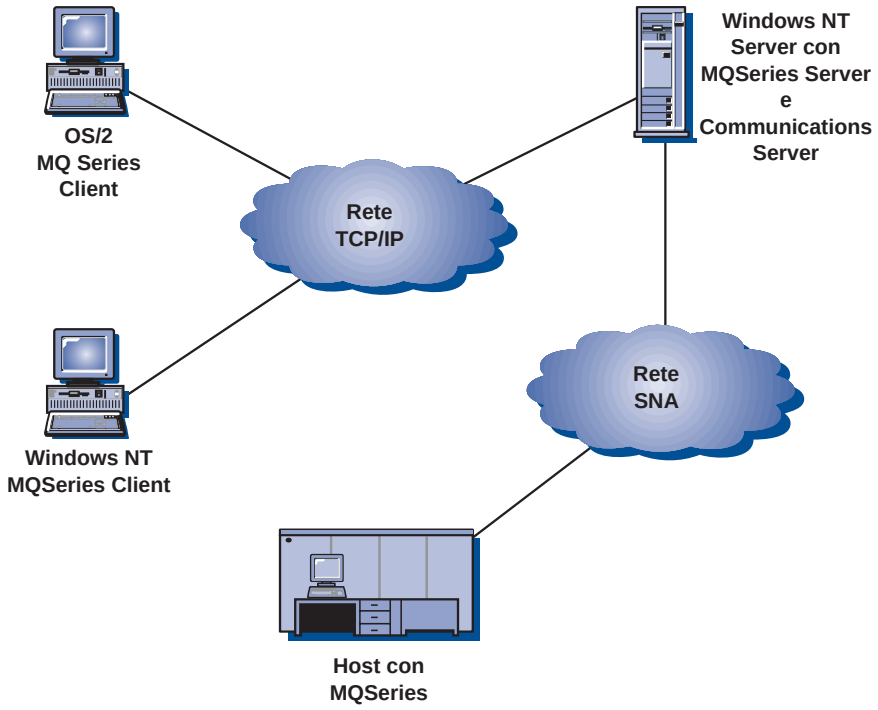


Figura 30. Ambiente client MQSeries

Per ulteriori informazioni sulla configurazione dei client MQ, fare riferimento a *MQSeries Intercommunication*. Questo manuale è disponibile su Internet al seguente indirizzo:

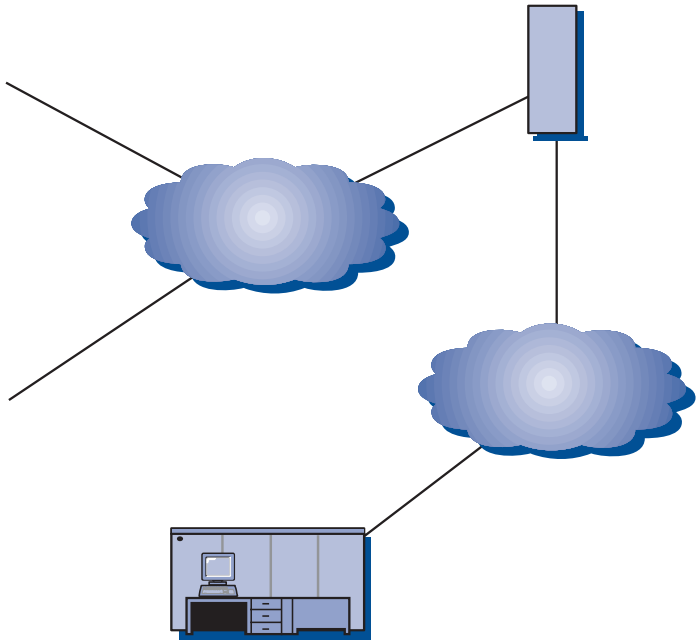
http://www.software.ibm.com/ts/mqseries/library

Collegamento di Client Access agli host DB2

Communications Server include un software “try and buy” per DB2 Connect Enterprise Edition, un prodotto per la connettività multiutenza all'host. DB2 Connect Enterprise Edition può essere installato su un server Windows NT.

Communications Server include anche DB2 CAE (Client Application Enabler) che fornisce un collegamento client access all'host. DB2 CAE può essere installato su una macchina client su cui vengono eseguiti Windows 3.1, Windows 95, Windows NT o OS/2.

La Figura 31 a pagina 107 mostra un esempio di configurazione di DB2 Connect Enterprise Edition per l'accesso alle informazioni contenute in un database DB2 di un host.



Pianificazione di HPR

Communications Server supporta i collegamenti HPR (high performance routing) su Enterprise Extender (IP), SDLC (synchronous data link control), LAN, WAN, canale, MPC (Multi-Path Channel) ed i collegamenti X.25.

Communications Server supporta i collegamenti HPR su

L'ANR (automatic network routing) HPR riduce al minimo i requisiti di memoria e di elaborazione nei nodi intermedi e rappresenta un potenziamento rispetto all'ISR (intermediate session routing) APPN per le reti ad alta velocità con bassi indici di errore.

Il supporto HPR di Communications Server include il supporto RTP (rapid transport protocol) e ANR (automatic network routing).

Caratteristiche dei collegamenti HPR

Per usufruire delle suddette funzioni, HPR assume che i collegamenti dei dati forniscano indici bassi di frame perduti. HPR risolve le condizioni che provocano una perdita di frame, ma se tali condizioni persistono per lunghi periodi, HPR assume che vi sia un'eccessiva congestione della rete e la produttività HPR viene ridotta. Il raggiungimento di una buona produttività HPR in un determinato collegamento è indice di una configurazione corretta del nodo di inoltro, delle funzioni che costituiscono il collegamento tra i due nodi e del nodo ricevente.

Nota: Nei casi in cui le funzioni della linea LAN presentano una perdita elevata di frame, è possibile impostare i valori ERP.

Nodo di inoltro

I tipici adattatori utilizzati con HPR inviano frame alla linea con bassi indici di errore. Per Ethernet, le prestazioni HPR si riducono se nella LAN vengono caricate molte collisioni (ad esempio, se il carico è superiore del 30% - 40% alla velocità Ethernet nominale). Per i collegamenti frame relay, le funzioni devono essere configurate in modo che i singoli collegamenti raggiungano la velocità della linea di accesso senza provocare condizioni di congestione nella rete frame-relay.

Funzioni di linea

Le funzioni LAN possono essere caratterizzate da una sostanziale complessità, che può essere determinata da grandi numeri di stazioni che condividono un singolo segmento LAN, bridge tra segmenti LAN, talvolta con collegamenti nascosti a bassa velocità e segmenti LAN simulati che funzionano su sottoreti complesse. E' necessario soddisfare il requisito di bassa perdita di frame. Ad esempio, i collegamenti WAN tra bridge suddivisi devono utilizzare funzioni con bassi indici di errore oppure devono compensare utilizzando il ripristino degli errori a livello di collegamento tra i bridge. Come altro esempio, è necessario evitare condizioni che provochino un'eccessiva produzione di buffer di bridge (interferenze di trasmissioni di tipo broadcast o grandi raffiche di frame broadcast).

Nodo di ricezione

I tipici adattatori utilizzati con HPR ricevono frame dalla linea con bassi indici di errore. Alcuni adattatori, tuttavia, non riescono a ricevere frame quando dei frame consecutivi arrivano troppo velocemente. E' possibile realizzare le migliori prestazioni HPR quando l'adattatore di ricezione può gestire il traffico senza alcuna perdita di frame in arrivo.

Se la rete è caratterizzata da una velocità di errori elevata, i responsabili di sistema possono osservare una produttività inferiore a quella prevista nei collegamenti HPR.

Considerazioni sull'HPR

E' possibile utilizzare le funzioni HPR includendo ulteriori informazioni nelle intestazioni frame. Se non è necessario utilizzare tali funzioni, le ulteriori operazioni possono ridurre le prestazioni della rete. Le funzioni HPR rappresentano un vantaggio in tutti i casi in cui sono presenti nodi intermedi o instradamenti alternativi. Tuttavia, se sono richieste elevate prestazioni tra due nodi collegati da un singolo collegamento in assenza di ripristino senza interruzione durante un errore di collegamento, è necessario disabilitare l'HPR quando viene configurato tale collegamento.

HPR implementa l'accodamento prioritario. In generale, il traffico interattivo viene trasmesso nella rete ad una velocità maggiore di quella del traffico batch a più bassa priorità. Gli adattatori che accodano i frame, eseguono questa operazione senza considerare le priorità, con la possibilità dunque di interferire con l'accodamento prioritario dell'HPR. Potrebbe risultare necessario ridurre il numero di accodamenti dell'adattatore per evitare che il traffico a bassa priorità provochi dei ritardi nel traffico ad alta priorità. Per le istruzioni sull'impostazione di accodamento dell'adattatore, consultare la documentazione relativa all'adattatore.

Molti PC dispongono di funzioni avanzate di gestione dell'alimentazione che consentono di sospendere l'alimentazione nei dispositivi (come le unità disco) e ridurre la velocità di clock di una CPU, per risparmiare energia nel caso in cui la tastiera o il mouse non vengano utilizzati. Su una stazione di lavoro questa funzione risulta utile e su una piattaforma server può essere utilizzata durante l'instradamento dei dati da un adattatore all'altro e quando non si sta verificando nessuna attività disco. Per Communications Server, disabilitare la funzione di gestione avanzata dell'alimentazione e di gestione dell'alimentazione hardware immettendo la configurazione BIOS durante l'avvio (generalmente premendo F1 durante l'inizializzazione dell'hardware) e poi disabilitare queste opzioni.

HPR utilizzerà una maggiore quantità di memoria dell'adattatore LAN a causa dell'incremento delle prestazioni e dell'accodamento. Molti adattatori con RAM condivisa utilizzano per impostazione predefinita 8 kilobyte di memoria condivisa. E' necessario che la quantità di memoria RAM condivisa sia 16 kilobyte. Per modificare questa configurazione, fare riferimento al manuale relativo alla configurazione dell'adattatore. Questa impostazione si trova sulla macchina BIOS o nelle impostazioni per l'attivazione dell'adattatore.

Nota: Se la RAM condivisa non viene aumentata a 16 kilobyte, le prestazioni della rete saranno ridotte.

Non impostare la RAM condivisa su un valore superiore a 16, l'impostazione migliore per la memoria dell'adattatore.

Se i collegamenti HPR non vengono eseguiti correttamente durante grossi traffici, è possibile impostare i timer di ricezione su un valore superiore. Ciò fornisce più tempo ai collegamenti per la ricezione di una conferma dei frame inviati.

Per i collegamenti SDLC, tale valore è PRT (Primary Receive Timer). Il timer di ricezione può essere impostato su DLC o su un'istruzione di collegamento logico.

Per calcolare il valore minimo per il timer di ricezione in decimi di secondo, utilizzare la seguente formula:

```
[(send_window_count * max_i_field_size * 8) /actual line speed]* 10
```

Considerazioni sull'impostazione dei parametri sui DLC LAN

E' possibile specificare otto parametri per regolare la velocità con cui Communications Server gestisce il ripristino e gli errori dei collegamenti LAN. Potrebbe risultare necessario modificare questi parametri in modo da ottenere risultati migliori se si utilizzano collegamenti a bassa velocità, HPR o i collegamenti dell'host di backup.

E' necessario considerare i seguenti parametri durante la definizione di un dispositivo LAN in **Configurazione nodo**:

Nel separatore **Avanzato**:

Intervallo tentativi verifica L'intervallo dei tentativi di verifica specifica il tempo che intercorre tra i tentativi per il rilevamento della stazione del collegamento adiacente nella LAN (local area network). Il numero di tentativi effettuati si basa sul valore specificato per il limite di tentativi di verifica.

Il valore predefinito è 8.

Limite tentativi verifica Il limite dei tentativi di verifica specifica il numero massimo di tentativi per il rilevamento della stazione di collegamento adiacente nella LAN (local area network) in assenza di una conferma ricevuta nel tempo impostato dal valore relativo all'intervallo di tentativi di verifica.

Il valore predefinito è 5.

Dimensione massima PIU La dimensione massima PIU (path information unit) rappresenta il numero massimo di byte contenuti nel buffer dei dati utilizzato dalle sessioni SNA per questo collegamento. Se tale valore supera la dimensione frame supportata dal driver della periferica locale, il valore verrà ridotto in modo da corrispondere a tale dimensione.

Il valore predefinito è 65535.

Nel separatore **Prestazioni**:

Timeout inattività Il timeout di inattività specifica l'intervallo di tempo che il driver della periferica LAN attende per ricevere un frame prima di dichiarare non operativo il collegamento.

Il valore predefinito è 30 secondi.

Ritardo conferma Il ritardo della conferma specifica l'intervallo di tempo in cui il dispositivo LAN conserva una risposta ad un frame ricevuto allo scopo di consentire la ricezione e la conferma di più frame con lo stesso RR (Request Ready).

Il valore predefinito è 100 millisecondi.

Timeout risposta POLL

Il timeout di risposta poll specifica l'intervallo di tempo in cui il dispositivo LAN attende una risposta ad un frame inviato con il bit POLL impostato.

Il valore predefinito è 8 000 millisecondi.

Trasmissioni in sospeso previste Le trasmissioni in sospeso previste specificano il numero massimo di frame accodati dal dispositivo LAN ad una stazione di collegamento prima dell'inoltro di un RNR (Receive Not Ready) alla stazione di collegamento adiacente.

Il valore predefinito è 16 frame.

Numero buffer di ricezione Il numero dei buffer di ricezione specifica il numero di buffer riservati nella memoria per la memorizzazione dei dati ricevuti dall'host fino alla relativa elaborazione. Ciascun buffer rappresenta la dimensione PIU.

Il valore predefinito è 32 buffer.

Elaborazione commutazione percorso HPR

HPR fornisce una funzione sicura di commutazione del percorso che consente di passare ad un collegamento differente in caso di esito negativo di un collegamento. Prima di effettuare la commutazione di percorso, viene ritentato il collegamento non riuscito. Di seguito è riportata una spiegazione dei parametri utilizzati per stabilire se un collegamento non è riuscito e l'intervallo di tempo necessario per avviare la commutazione di percorso.

Una volta raggiunto il valore specificato per l'opzione **Timeout inattività**, viene inviato un frame di tipo keepalive. Il valore predefinito per **Timeout inattività** è 30 secondi.

Il valore specificato per **Timeout risposta POLL** stabilisce l'intervallo di tempo in cui il dispositivo attende una risposta ad un frame di tipo keepalive. Il valore predefinito per **Timeout risposta POLL** è otto secondi (8000 millisecondi). Un frame di tipo keepalive viene ritentato 10 volte. Questo numero di tentativi non può essere modificato.

Se non si riceve nessuna risposta al frame keepalive, vengono inviati i comandi TEST al sistema partner. Il valore specificato per **Intervallo tentativi verifica** stabilisce l'intervallo di tempo tra i tentativi del comando TEST ed il valore specificato per **Limite tentativi verifica** stabilisce il numero massimo di tentativi del comando TEST. Il valore predefinito per **Intervallo tentativi verifica** è 8 secondi mentre il valore predefinito per **Limite tentativi verifica** è cinque.

Il calcolo riportato di seguito indica il tempo necessario per stabilire se un collegamento non è riuscito ed avviare la commutazione di percorso:

```
(Timeout inattività) + (Timeout risposta POLL * 10 tentativi) +
          (Intervallo tentativi verifica * Limite tentativi verifica) + 1
```

Se vengono utilizzati i valori predefiniti per i parametri, il tempo necessario per stabilire l'esito negativo di un collegamento ed avviare una commutazione di percorso può raggiungere un valore massimo pari a 151 secondi.

```
(30 secondi) + (8 secondi * 10 tentativi) +
           (8 secondi * 5 tentativi) + 1 = 151 secondi
```

Se, in caso di esito negativo del collegamento, si verificano errori o lunghi intervalli di tempo per la commutazione di percorso da parte dell'HPR, è possibile ridurre tali intervalli di tempo diminuendo i valori relativi ai parametri del calcolo.

The time Communications Server allows before failing an activation attempt is ???. This is two minutes for the default value of the test retry limit(?).

The time Communications Server allows for a response before failing a link is (test retry interval * test retry limit)(?) seconds. This is the number of (test retry interval?) time intervals for the original transmission plus test retry limit(?) retries. This is ??? seconds for the default values of test retry interval and test retry limit(?).

To maintain a link where responses are taking a long time, increase the poll response timeout(?). For example, you might change the Group 1 response timer (test retry parameter to 45 (9 seconds). oppure conservare il tempo richiesto per l'esito negativo di un collegamento riducendo il parametro RT. Ad esempio, se il parametro RT è impostato su 2, il collegamento avrà esito negativo dopo (2 + 1) * 9 = 27 secondi. Ciò potrebbe ridurre gli errori di collegamento dovuti ai frame rifiutati.

Se, in caso di esito negativo di un collegamento, si verificano errori o lunghi intervalli di tempo per la commutazione del percorso da parte dell'HPR, è possibile ridurre questi intervalli di tempo. Il collegamento potrebbe non avere un esito negativo immediato e la commutazione del percorso da parte dell'HPR potrebbe ritornare sullo stesso collegamento. Tentare di ridurre il tempo di inattività(?) su un valore 127 (25 secondi) e verificare il limite dei tentativi(?) per 3 volte. In tal modo Communications Server aumenterà la velocità per rendere inattivo il collegamento.

Se si stanno utilizzando collegamenti host di backup, il collegamento attivazione su richiesta o del supporto di rete con HPR impiega un paio di minuti(???) prima che Communications Server non riesca ad attivare il collegamento. Due minuti rappresenta il timeout predefinito per la commutazione del percorso per alcune sessioni. Consider reducing the test retry limit(?) parameter to 1 or 2. This will reduce the amount of time Communications Server spends trying to activate a link

Pianificazione del gateway SNA

Il gateway SNA supporta:

- Diversi protocolli SNA
- Diverse stazioni di lavoro downstream
- Diversi tipi di collegamento tra gateway e host
- Pool delle LU (sessioni) nel gateway
- Definizione delle stazioni di lavoro implicite
- Modifica e aggiunta dinamica delle definizioni per le stazioni di lavoro non attive
- Diversi host simultanei
- Diversi tipi di collegamento (che è possibile combinare) tra le stazioni di lavoro ed il gateway

La configurazione di un gateway SNA mediante l'applicazione **Configurazione nodo** richiede la creazione di solo due profili:

- Profilo gateway—host e pool di LU host
- Profilo gateway—stazioni di lavoro che utilizzano il gateway (un profilo per ogni LU che si trova in ciascuna stazione di lavoro esplicita supportata) oppure gateway—stazioni di lavoro implicite che utilizzano il profilo gateway o entrambi i profili

Per le istruzioni sulla configurazione del gateway SNA mediante la **Configurazione nodo**, fare riferimento a *Guida operativa*.

Invece di utilizzare la **Configurazione nodo** per configurare il gateway SNA, è possibile utilizzare un editor di testo per editare la parola chiave **LINK_STATION** nel file .ACG.

Per ulteriori informazioni sull'utilizzo del file .ACG per la configurazione del gateway SNA, consultare il manuale *Configuration File Reference*.

Other profiles must exist before the SNA gateway can function. These include the define logical links parameters required to connect the computer implementing the SNA gateway to the supported workstations and to the host. If you want to use the gateway computer as a workstation, the profiles required to give it the functions you want must also be configured.

Refer to the online *Tutorial* for details on configuring these profiles.

Collegamenti alle stazioni di lavoro supportati

Il gateway SNA supporta le stazioni di lavoro collegate mediante:

- Connettività LAN
  - Token ring
  - Ethernet
  - ATM (Emulazione LAN)

- Frame Relay
- SDLC
  - Asincrono
  - Sincrono
  - Hayes Autosync
  - Multipoint Primary
- Rete X.25
- TCP/IP AnyNet (per connettività supportate da Microsoft TCP/IP)
- Enterprise Extender IP (per connettività supportate da Microsoft IP)
- Collegamenti ISDN
- Collegamenti HPR

Il gateway SNA può supportare 254 LU per ciascuna PU definita. E' possibile definire una PU differente per ciascun collegamento host. Le LU vengono utilizzate dalle stazioni di lavoro downstream per eseguire il collegamento all'host. Il numero di stazioni di lavoro downstream supportate dipende da diversi fattori, incluso il tipo di connettività ed il numero di adattatori presenti sul gateway. Ad esempio, se sul gateway è presente un adattatore LAN, un collegamento host con 254 LU può essere utilizzato contemporaneamente da 253 stazioni di lavoro downstream. Con due adattatori, è possibile raddoppiare il numero di stazioni di lavoro downstream.

Con i collegamenti X.25, possono essere attive simultaneamente 128 stazioni di lavoro che condividono le 254 LU.

Collegamenti delle stazioni di lavoro SDLC

E' possibile scegliere di eseguire il collegamento utilizzando l'SDLC nelle configurazioni point-to-point e Multipoint. Una volta completata la configurazione, è possibile eseguire l'SDLC tra la stazione di lavoro ed il gateway.

Durante l'impostazione delle stazioni di lavoro multidrop, tenere presente i diversi fattori che controllano i tempi di risposta dell'interrogazione ciclica. Limitazioni fisiche influiscono sulla rapidità con cui la stazione primaria può eseguire l'interrogazione ciclica della stazione secondaria più lontana. La definizione di tutte le stazioni di lavoro secondarie mediante l'utilizzo degli stessi parametri consente di semplificare il seguente calcolo.

Per calcolare il tempo minimo di inattività in secondi, utilizzare la seguente formula:

```
     NS * (SW + RW) * (IS + 2) / (LS / 8)
dove:
     NS  =  Numero di stazioni
     SW  =  Dimensioni della finestra di inoltro
     RW  =  Dimensioni della finestra di ricezione
     IS  =  Dimensioni del campo di immissione
     LS  =  Velocità della linea in bps
```

Se questi valori non sono identici per tutte le stazioni di lavoro secondarie, è necessario effettuare un calcolo separato per ciascun gruppo o stazione di lavoro ed aggiungerlo in modo da ottenere il valore corretto per il timer di inattività.

Ad esempio, per un collegamento multidrop con 16 stazioni di lavoro secondarie alla velocità di 14.4 Kbps, con ciascuna stazione di lavoro impostata su dimensioni di finestra di inoltro pari a 7, dimensioni di finestra di ricezione pari a 7 e dimensioni di campo di immissione pari a 521, il calcolo per il timer di inattività è il seguente:

```
16 * (7 + 7) * (521 + 2) / (14400 / 8) = 65.1 secondi
```

Nota: Aggiungere sempre dei secondi supplementari per un buffer.

Collegamenti delle stazioni di lavoro X.25

Se il gateway SNA viene configurato in modo da utilizzare solo i collegamenti X.25 PVC (permanent virtual circuit) tra il gateway e le stazioni di lavoro, si consiglia di configurare tutti i PVC della stazione di lavoro e del gateway con ruoli di collegamento negoziabili. In caso contrario, le stazioni di lavoro potrebbero non riuscire a stabilire i collegamenti X.25 PVC al gateway.

Per ulteriori informazioni sui collegamenti PVC e sulla configurazione, consultare la sezione Pianificazione della rete X.25.

Collegamenti agli host supportati

Il gateway SNA supporta i seguenti collegamenti ad un host:

- Connettività LAN
  - Token ring
  - Ethernet
  - ATM (Emulazione LAN)
- Frame Relay
- SDLC
  - Sincrono
  - Hayes Autosync
- Rete X.25
- Biassiale (su AS/400)
- TCP/IP AnyNet (per connettività supportate da Microsoft TCP/IP)
- Enterprise Extender (per connettività supportate da Microsoft IP)
- Canale (CDLC)
- Canale (MPC) con un collegamento DLUR
- Collegamenti ISDN
- Collegamenti DLUR e HPR

Se sono disponibili collegamenti a più host dal gateway utilizzato dal traffico della LU dipendente, solo il collegamento host con il nome PU CP (control point) può effettuare quanto segue:

- Agire come focal point host
- Avere sessioni CP-CP con l'host
- Essere utilizzato per le funzioni APPN

I collegamenti che vengono definiti con un nome PU che non corrisponde al nome CP (control point) possono essere utilizzati solo per ulteriori collegamenti LU dipendente.

Se un collegamento host gateway viene definito come collegamento di risorsa limitata, esso invierà una richiesta di scollegamento all'host in seguito all'uscita dell'ultima sessione LU-LU. Il gateway quindi trasferisce le DACTLU alla stazione di lavoro ed una DACTPU alle stazioni di lavoro che sono connesse solo a quel collegamento host. Quando la stazione di lavoro collegata al gateway viene definita come risorsa limitata, il collegamento della stazione di lavoro viene interrotto se non sono presenti altre sessioni. In Communications Server è possibile designare una stazione di lavoro come risorsa limitata durante la definizione del collegamento del client esplicito.

Tuttavia, se la stazione di lavoro dispone di un'applicazione o di un programma di emulazione che riattiva automaticamente il collegamento host, il gateway riattiva il collegamento gateway all'host quando la stazione di lavoro attiva il collegamento al gateway. Ciò significa che le definizioni di stazione di lavoro che non sono compatibili inibiscono completamente la funzione di risorsa limitata nel gateway.

Considerazioni sull'host

Durante la pianificazione del collegamento host è necessario tenere presente i seguenti punti:

- Se l'ambiente utilizza un NCP (network control point), l'NCPGEN 37*xx*, la macro **LINE** ed il valore **MAXLU** devono corrispondere almeno al numero di LU su Communications Server.
- Gli utenti VTAM possono controllare l'intervallo di tempo durante il quale il VTAM memorizza i dati prima di inviarli all'unità di controllo (accodamento). Quando in una definizione PU viene specificato il parametro di accodamento VTAM **DELAY = 0**, è possibile che i tempi di inoltro delle risposte host risultino più veloci comportando però un maggiore lavoro da parte del processore host.

  Quando viene specificato un valore per DELAY che non è pari a zero, il processore non dovrà eseguire delle istruzioni ma i tempi di ricezione delle risposte sulla stazione di lavoro Communications Server risulteranno più lenti.

  Per l'accodamento, iniziare con il valore predefinito 0.2. Un secondo ritardo 0.2 influisce moderatamente sui tempi di risposta, ma se la velocità è di circa una transazione al secondo o superiore, si verifica l'operazione di accodamento.
- Anche se ciascuna stazione di lavoro SNA downstream sulla LAN implementa una PU con la relativa serie di LU, il gateway SNA viene implementato in modo che l'host riconosca solo la PU gateway. Pertanto, nell'host viene codificata una sola definizione PU. Tale definizione PU contiene le LU relative a ***tutte*** le stazioni sulla LAN che eseguono il collegamento all'host mediante questo gateway.

  E' possibile utilizzare le SDDLU (self-defining dependent LU), se supportate dal VTAM host. Durante la configurazione delle LU host, specificare un modello di LU oppure fornire un nome di modello di LU che corrisponda al valore dell'operando LUSEED definito nel nodo principale commutato VTAM ed utilizzato dalla routine di uscita VTAM SDDLU.

Configurazione dell'indirizzo di destinazione LAN

Se viene utilizzato uno dei collegamenti LAN supportati tra il gateway e l'host oppure tra il gateway ed una stazione di lavoro definita in modo esplicito, è necessario fornire un indirizzo di destinazione. Gli indirizzi di destinazione corretti da immettere in ciascun profilo devono essere stabiliti dal gateway SNA. In Figura 32 viene mostrata la prospettiva corretta per la definizione degli indirizzi.

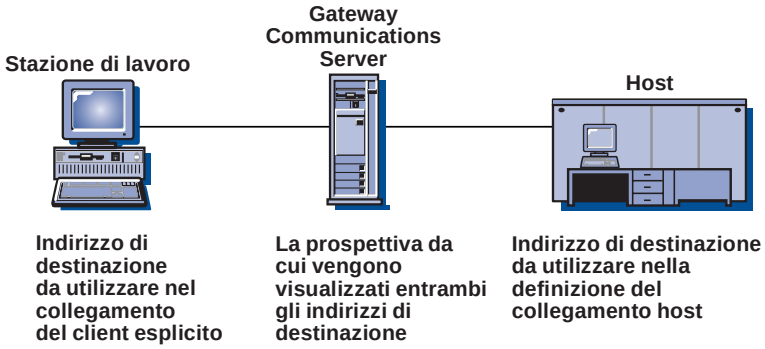


Figura 32. Prospettiva delle voci relative all'indirizzo di destinazione

In alternativa, è possibile configurare il collegamento per la stazione di lavoro specificando un nome CP adiacente o l'ID del nodo adiacente invece dell'indirizzo di destinazione. I collegamenti specificati senza un indirizzo di destinazione possono essere attivati solo dalla stazione di lavoro.

Nota: Quando viene specificato un indirizzo di destinazione, il formato dell'indirizzo (ad esempio, Ethernet o token ring) ed il SAP (service access point) remoto devono corrispondere.

Pianificazione delle definizioni LU gateway

Il gateway SNA supporta le LU host ***in pool*** e le LU host ***dedicate***. Quando le LU vengono configurate per ciascun collegamento host presente nel gateway SNA, è possibile suddividerle in pool. La creazione dei pool offre spesso i seguenti vantaggi:

- Se non tutte le sessione delle stazioni di lavoro devono comunicare con l'host simultaneamente, la creazione dei pool consente di preservare le risorse del sistema. Le sessioni di una stazione di lavoro sulla LAN possono condividere le stesse LU ma non simultaneamente. Mediante questa funzione è possibile disporre di un numero di LU configurate sul gateway SNA per le sessioni della stazione di lavoro che risulta superiore al numero di LU configurate tra host e gateway, in modo da ridurre i requisiti di risorsa host, le definizioni della stazione di lavoro host ed accelerare le procedure di riavvio.
- I pool possono essere gestiti e configurati in modo più semplice. Le dimensioni di un pool possono essere regolate aggiungendo o eliminando LU, senza modificare le altre definizioni.

  Le LU in pool non sono dedicate a nessuna stazione di lavoro in particolare e non devono essere dedicate all'utilizzo da parte dei soli utenti del gateway downstream. Un singolo pool può essere condiviso dagli utenti del TN3270 downstream e dalle stazioni di lavoro del gateway SNA, come pure dai client API SNA e dalle sessioni di emulazione locale. Se si desidera configurare un

pool (ad esempio, PUBLIC) per tutti gli usi della LU dipendente, non è necessario sapere come verranno distribuiti gli utenti tra questi tipi.

- I pool possono fornire una maggiore disponibilità per le stazioni di lavoro downstream se le LU vengono definite da più collegamenti presenti nello stesso pool. Se solo uno dei collegamenti è attivo, gli utenti possono accedere alle LU del collegamento attivo.

Tenere presente i seguenti scenari:

- Communications Server dispone di due collegamenti host con 100 LU definite in ciascun collegamento, tutte appartenenti al pool A. Il primo collegamento viene configurato come *attivazione all'avvio* ed è operativo. Tutte le stazioni di lavoro utilizzano tale collegamento con le relative LU. Il secondo collegamento viene configurato come *attivazione automatica*. Questa combinazione di pool con configurazione di collegamento può fornire una maggiore disponibilità nei seguenti due modi. Se il primo collegamento non riesce, le sessioni dipendenti di ripristino attivano automaticamente il secondo collegamento. Se il primo collegamento esaurisce le LU definite, il collegamento di backup viene attivato automaticamente quando viene richiesta la successiva LU (la 101esima).
- La combinazione di pool e configurazione di collegamento può essere utilizzata anche per fornire la distribuzione del carico alle stazioni di lavoro downstream nei collegamenti host disponibili. Un esempio di ciò è quando Communications Server dispone di due collegamenti host con 100 LU definite in ciascun collegamento, tutte appartenenti al pool A. Entrambi i collegamenti vengono configurati come *attivazione all'avvio* e sono operativi. Le stazioni di lavoro messe in corrispondenza con il pool di LU verranno distribuite su entrambi i collegamenti in modo da condividerne il carico.

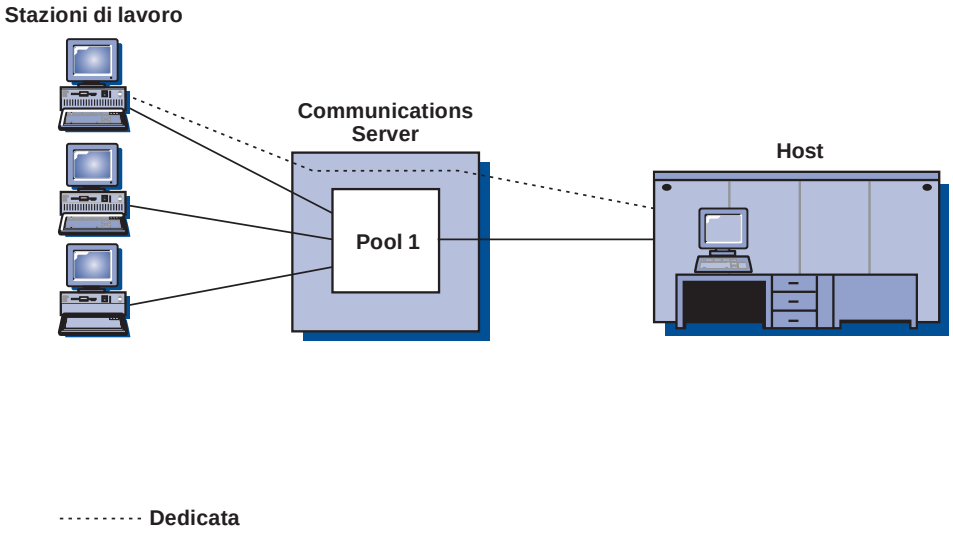
For example, the Communications Server has two host connections with 100 LUs defined on each connection, all belonging to pool A. The first link is configured as *activate at startup* and is operational. Tutte le stazioni di lavoro utilizzano tale collegamento con le relative LU. Il secondo collegamento viene configurato come *attivazione automatica*. Questa combinazione di pool con configurazione di collegamento può fornire una maggiore disponibilità nei seguenti due modi. Se il primo collegamento viene eseguito con esito negativo, le sessioni dipendenti di ripristino attivano automaticamente il secondo collegamento. If the first link depletes its defined LUs, the backup link will be automatically activated when the next LU is required.

You can also use the combination of pools and link configuration to provide load balancing for downstream workstations across available host connections. For example, the Communications Server has 2 host connections with 100 LUs defined on each connection, all belonging to pool A. Both links are configured as *activate at startup* and are operational. The workstations that are mapped to the pool will be distributed across the connections.

Il gateway SNA assegna le LU in pool alle sessioni della stazione di lavoro quando la stazione di lavoro downstream viene collegata al gateway. Le sessioni della stazione di lavoro possono essere definite in modo da utilizzare le LU, dedicate o in pool, presenti su host differenti.

Le LU dedicate non appartengono ad un pool. Una LU dedicata può essere configurata in modo da essere utilizzata da un client definito in modo esplicito.

In Figura 33 a pagina 121 viene mostrata una configurazione semplice con stazioni di lavoro che utilizzano LU dedicate, LU in pool o entrambi i tipi di LU. (Le linee di collegamento rappresentano le LU.)



Per le stazioni di lavoro implicite, gli utenti collegati al gateway devono conoscere

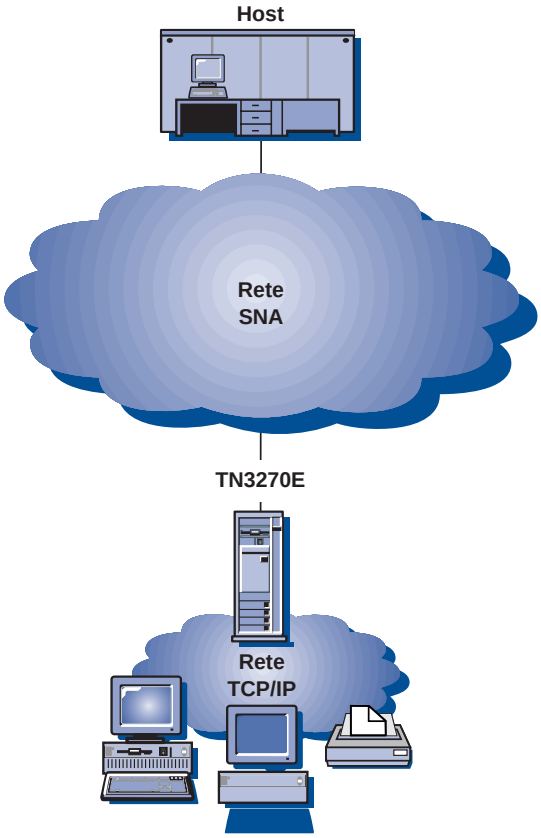
messi in corrispondenza con il DLUS. Tale configurazione risulta più semplice poiché non richiede alcuna conoscenza delle LU downstream presenti sul gateway e fornisce la più elevata visibilità delle unità downstream al VTAM, dal momento che questo riconosce le PU.

Se non si desidera che il VTAM riconosca le PU downstream, è possibile configurare una PU interna sul gateway (invece di un collegamento host) e mettere in corrispondenza le stazioni di lavoro downstream con tale PU interna.

Se una stazione di lavoro downstream, come Personal Communications, supporta il DLUR, potrebbe essere necessario instradare la stazione di lavoro mediante Communications Server utilizzando il nodo di rete invece del gateway SNA.

Pianificazione del server TN3270E

Il server TN3270E consente di configurare la rete come illustrato in Figura 34 o in Figura 35 a pagina 126.



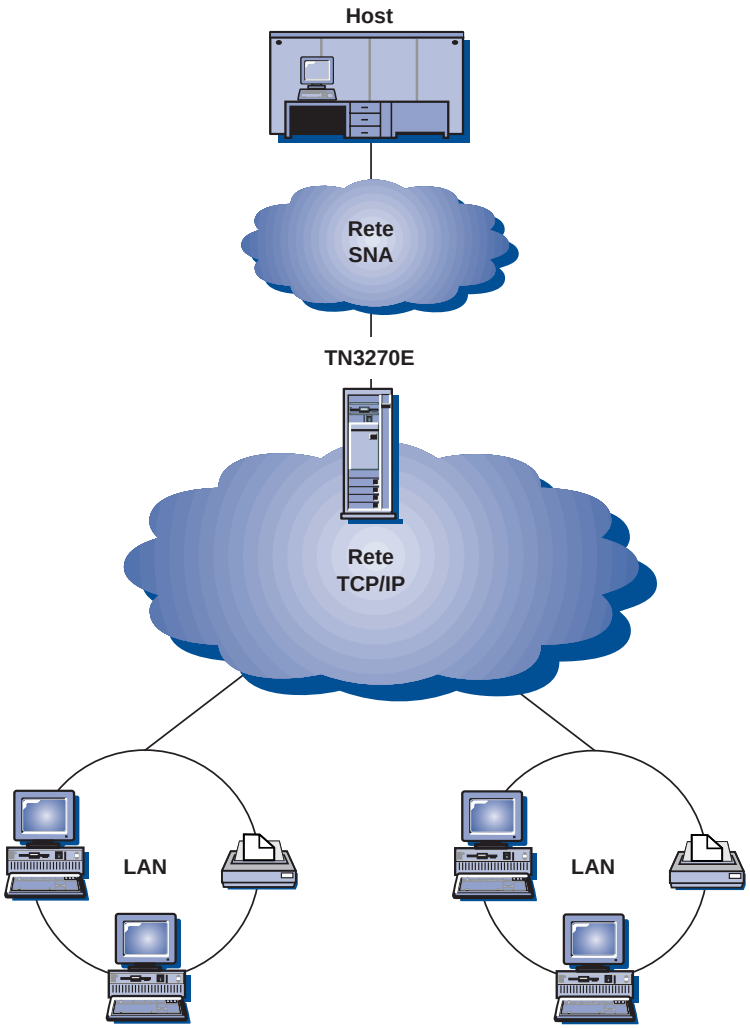


Figura 35. Communications Server configurato come Server TN3270E con TCP/IP WAN

Il server TN3270E supporta:

- emulazione LU

  Il server TN3270E supporta la LU 2, che consente agli utenti di eseguire programmi applicativi video 3270 interattivi.

- Stampa host

  Le estensioni standard TN3270E (Telnet 3270) consentono agli utenti di eseguire la stampa dalle applicazioni host su stampanti collegate alla stazione di lavoro. Queste stampanti possono essere collegate in locale oppure alla rete. Sono supportate le sessioni LU 1 e LU 3.

  Il server TN3270E implementa i protocolli indicati in RFC 1646 e RFC 1647, consentendo al server di inoltrare i dati della sessione LU 1 e LU 3 ai client abilitati al TN3270E, attendere la conferma del client relativa alla richiesta di stampa e rispondere all'host.

- filtraggio IP

  Communications Server supporta la specifica dei filtri del client TCP/IP, mediante l'utilizzo degli indirizzi IP, delle sottoreti, dei nomi host o dei nomi di dominio. Questa funzione consente la gestione centrale dei client che possono

collegarsi al server TN3270E e la specifica dei nomi LU e dei pool a cui possono accedere i client.

- Gestione delle risposte

  I client abilitati al TN3270E possono trasmettere risposte positive e negative, che il server TN3270E invia all'host. Il server TN3270E genera le risposte alle richieste per i client TN3270 standard.

- Gestione delle chiavi ATTN e SYSREQ

  Il server TN3270E può convertire ed inoltrare le informazioni all'host quando il client invia una chiave ATTN o SYSREQ. Sebbene i client che non sono abilitati al TN3270E non dispongano di definizione esplicita per ATTN e SYSREQ, il server TN3270E utilizza i seguenti comandi Telnet per l'implementazione di queste funzioni:

Tabella 6. Equivalenti dei comandi

Telnet	TN3270E	TN3270 standard
IP	ATTN	SYSREQ
AO	SYSREQ	SYSREQ
BREAK	N/A	ATTN

- Classi di LU

  Communications Server suddivide in categorie i collegamenti utente utilizzando classi di LU. Tali classi sono costituite da LU configurate con caratteristiche comuni; ad esempio, quelle che richiedono un collegamento host specifico. Ciò consente di semplificare l'accesso utente, raggruppare gli utenti in base alle applicazioni richieste e massimizzare le risorse host.

- Sicurezza basata su SSL (Secure Sockets Layer)

  I collegamenti tra client TN e server TN3270E utilizzano l'SSL Versione 3 per fornire la crittografia dei dati e l'autenticazione del server mediante l'utilizzo dei certificati firmati.

Il server TN3270E supporta il Telnet 3270 standard ed esteso. I programmi client tipici emulano un video 3270. I client che supportano il protocollo TN3270E possono emulare le stampanti LU 1 e LU 3.

Per le istruzioni sulla configurazione del server TN3270E, fare riferimento alla *Guida operativa*.

Stazioni di lavoro client supportate dal server TN3270E

Il server TN3270E supporta qualsiasi client TN3270E o TN3270 conforme a RFC 1576, 1646 o 1647.

Caratteristiche principali

Questa sezione fornisce ulteriori informazioni su alcune funzioni che è possibile configurare per il server TN3270E.

Modifica del numero di porta predefinito

E' possibile configurare il numero di porta che il server utilizza per i nuovi collegamenti dalla finestra relativa alle opzioni TN3270E. Il numero di porta predefinito è 23, ma questa porta può essere utilizzata anche da altre applicazioni Telnet, come il supporto per il server TN5250. In questo caso, è necessario utilizzare un'altra porta.

Se il numero di porta viene modificato, evitare i numeri utilizzati da altre applicazioni. Se due applicazioni utilizzano lo stesso numero di porta, una delle applicazioni non verrà eseguita correttamente.

Se il numero di porta viene modificato, utilizzare un numero maggiore di 1 024. I numeri inferiori a 1 024 sono riservati. Per ulteriori informazioni sui numeri di porta riservati, consultare il seguente indirizzo su Internet:

http://www.ds1.internic.net

Al momento della pubblicazione di questo documento, l'RFC più recente per i numero assegnati è RFC1700.

Quando il numero di porta viene modificato è necessario avvisare gli utenti del client TN3270E, poiché essi dovranno configurare le applicazioni di emulazione in modo da creare una corrispondenza.

Gestione del traffico di sistema

Sono disponibili due metodi per il controllo della frequenza con cui i collegamenti non utilizzati vengono scollegati: l'elaborazione keepalive e lo scollegamento automatico.

Per impostazione predefinita, il server TN3270E non utilizza l'elaborazione keepalive. Se viene utilizzata questa elaborazione, è possibile scegliere NOP o il contrassegno di tempo.

- L'elaborazione NOP invia un comando NOP di Telnet dopo una frequenza keepalive specificata. Ciò provoca la trasmissione dei dati nel collegamento, che comporta il rilevamento da parte del TCP/IP dell'interruzione del collegamento. Il server non attende una risposta dal client. Il rilevamento dell'interruzione di un collegamento da parte del TCP/IP può richiedere un intervallo di tempo non prevedibile.
- L'elaborazione contrassegno di tempo invia un comando di contrassegno di tempo Telnet al client. Se il client non risponde entro il periodo di tempo specificato, il collegamento viene chiuso.

L'elaborazione contrassegno di tempo provoca un traffico maggiore sul sistema rispetto all'elaborazione NOP, ma consente di chiudere più rapidamente i collegamenti non utilizzati.

Se si sceglie di eseguire lo scollegamento automatico, il server scollega tutte le sessioni in cui non è presente un traffico per il periodo di tempo specificato. Il

traffico dell'elaborazione keepalive non mantiene aperto il collegamento; i dati devono essere inviati all'/dall'host. Le sessioni della stampante non vengono scollegate automaticamente.

Se i programmi di emulazione del client vengono configurati in modo da eseguire l'elaborazione keepalive, è possibile che l'utente desideri disattivarla nel server e, se questa viene eseguita sul server, è possibile che l'utente desideri disattivarla nel client allo scopo di ridurre il traffico della rete.

Filtraggio IP

Communications Server consente di configurare i filtri TN3270E in modo da specificare i client TCP/IP che è possibile collegare al server. I client possono essere specificati mediante l'utilizzo di indirizzi IP individuali, sottoreti IP, nomi host TCP/IP o nomi di dominio.

Supporto SSL (Secure Sockets Layer)

E' possibile configurare il numero di una porta protetta che il server utilizza per i collegamenti protetti dalla finestra relativa ai parametri del server TN3270E oppure da un file di risposta.

Per abilitare la sicurezza, Communications Server fornisce un programma di utilità **Gestione file di chiavi** che consente di generare il certificato e le chiavi richieste da SSL. Per ulteriori informazioni, fare riferimento alla sezione “Pianificazione della sicurezza basata su SSL (Secure Sockets Layer)” a pagina 137.

Una volta configurata ed abilitata la sicurezza, i client TN3270E che supportano SSL Versione 3 possono collegarsi ad un numero di porta protetta e stabilire collegamenti protetti.

Configurazione dei collegamenti SNA

Prima di utilizzare il server TN3270E, è necessario configurare il collegamento host e le LU host. Per una tabella di descrizione e spiegazione dei parametri host, fare riferimento a *Guida operativa*.

Inserimento in pool

Sono disponibili quattro classi di definizioni LU specifiche per il server TN3270E: stazione di lavoro implicita, stazione di lavoro esplicita, stampante implicita e stampante esplicita. Questi classi corrispondono alle classi terminale-generico, terminale-specifico, stampante-generica e stampante-specifica specificate in RFC 1647.

Le definizioni relative alla ***stazione di lavoro implicita*** vengono definite in un pool utilizzato dal server TN3270E per soddisfare le richieste di collegamento. Il pool predefinito può essere configurato in modo da soddisfare le richieste in cui il client non specifica una LU o un nome pool. Tutti gli altri pool devono essere richiesti in base al nome.

E' anche possibile definire un insieme di definizioni LU utilizzate per soddisfare le richieste relative ad un nome LU specifico. Queste definizioni di ***stazione di lavoro***

esplicita assicurano che un terminale necessario ad un'applicazione host non venga assegnato ad un client che non lo richiede in modo specifico.

In modo simile, è possibile definire un pool di definizioni di stampante che verranno utilizzate per soddisfare le richieste di collegamento che non richiedono nomi LU specifici (***stampante implicita***) ed un insieme utilizzato per soddisfare le richieste relative ad un nome LU specifico (***stampante esplicita***).

Alle definizioni di stazione di lavoro implicita ed esplicita possono essere associate delle stampanti. A ciascun definizione di terminale può essere assegnata una stampante ed a ciascuna stampante può essere associata una definizione di terminale. Queste stampanti non sono incluse nelle definizioni di stampante esplicita o implicita.

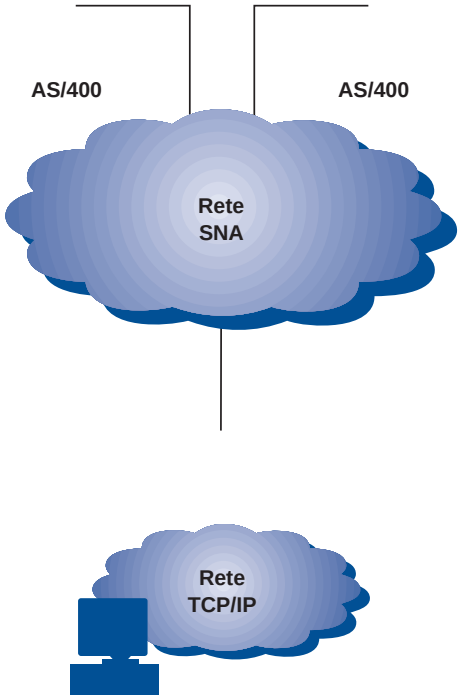
E' possibile accedere alle definizioni della ***stampante associata*** solo facendo riferimento al nome LU del terminale. Esse riducono la quantità di informazioni di cui necessita l'utente del client a cui è richiesta solo la conoscenza del nome LU del terminale da collegare alle sessioni del terminale e della stampante.

Distribuzione del carico dei server TN3270E

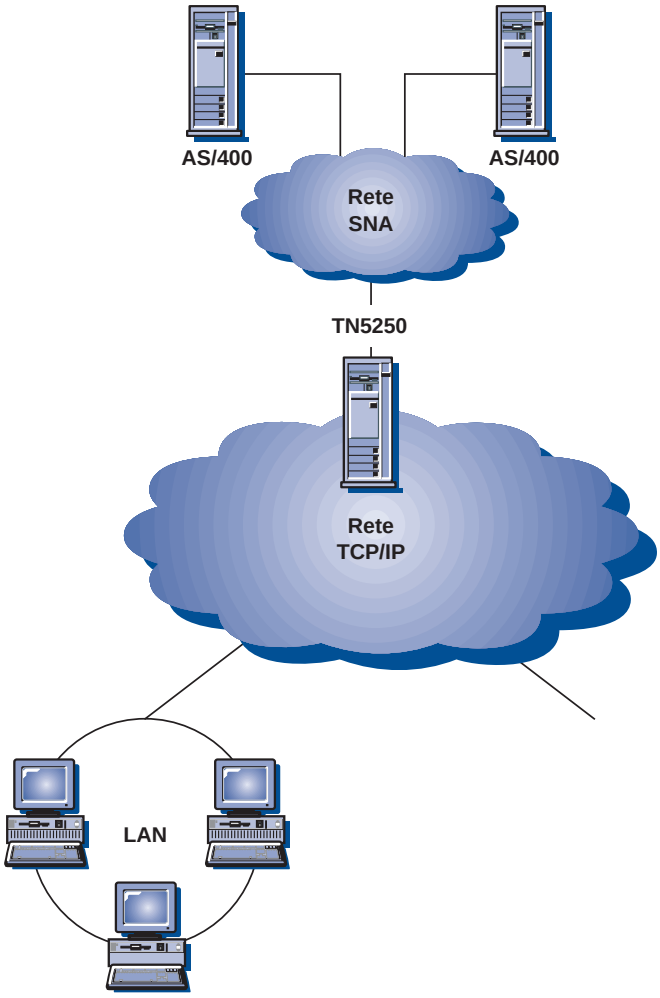
Communications Server supporta anche la distribuzione del carico dei client TN3270 su più server TN3270E. Per ulteriori informazioni, fare riferimento alla sezione “Pianificazione della distribuzione del carico” a pagina 147.

Pianificazione del server TN5250

Il server TN5250 consente di configurare la rete come illustrato nella Figura 36 o nella Figura 37 a pagina 132.



Pianificazione del server TN5250



I collegamenti tra client TN e server TN3270E utilizzano SSL Versione 3 per fornire la crittografia dei dati e l'autenticazione del server mediante l'utilizzo dei certificati firmati.

Per le istruzioni sulla configurazione di un server TN5250, fare riferimento alla to *Guida operativa*.

Stazioni di lavoro client supportate nel server TN5250

Il server TN5250 supporta qualsiasi client TN5250 conforme a RFC 1205.

Caratteristiche principali

Questa sezione fornisce ulteriori informazioni su alcune funzioni che è possibile configurare per il server TN5250.

Modifica del numero di porta predefinito

Quando viene configurato il supporto per il server TN5250, viene definita una porta predefinita con il numero 23; questa porta può essere utilizzata anche da altre applicazioni Telnet, come il supporto per il server TN3270E. In questo caso, è necessario utilizzare un'altra porta.

Se il numero di porta viene modificato, evitare i numeri utilizzati da altre applicazioni. Se due applicazioni utilizzano lo stesso numero di porta, una delle applicazioni non verrà eseguita correttamente.

Se il numero di porta viene modificato, utilizzare un numero maggiore di 1 024. I numeri inferiori a 1 024 sono riservati. Per ulteriori informazioni sui numeri di porta riservati, consultare il seguente indirizzo su Internet:

http://www.ds1.internic.net

Al momento della pubblicazione di questo documento, l'RFC più recente per i numero assegnati è RFC1700.

Quando il numero di porta viene modificato è necessario avvisare gli utenti del client TN5250, poiché essi dovranno configurare le applicazioni di emulazione in modo da creare una corrispondenza.

Gestione del traffico di sistema

Sono disponibili due metodi per il controllo della frequenza con cui i collegamenti non utilizzati vengono scollegati: l'elaborazione keepalive e lo scollegamento automatico.

Per impostazione predefinita, il server TN5250 non utilizza l'elaborazione keepalive. Se viene utilizzata questa elaborazione, è possibile scegliere NOP o il contrassegno di tempo.

- L'elaborazione NOP invia un comando Telnet NOP dopo una frequenza keepalive specificata. Ciò provoca la trasmissione dei dati nel collegamento, che comporta il rilevamento da parte del TCP/IP dell'interruzione del collegamento. Il server non attende una risposta dal client. Il rilevamento

dell'interruzione di un collegamento da parte del TCP/IP può richiedere un intervallo di tempo imprevedibile.

- L'elaborazione contrassegno di tempo invia un comando di contrassegno di tempo Telnet al client. Se il client non risponde entro il periodo di tempo specificato, il collegamento viene chiuso.

L'elaborazione contrassegno di tempo provoca un traffico maggiore sul sistema rispetto all'elaborazione NOP, ma consente di chiudere più rapidamente i collegamenti non utilizzati.

Se si sceglie di eseguire lo scollegamento automatico, il server scollega tutte le sessioni in cui non è presente un traffico per il periodo di tempo specificato. Il traffico dell'elaborazione keepalive non mantiene aperto il collegamento; i dati devono essere inviati all'/dall'host.

Se i programmi di emulazione del client vengono configurati in modo da eseguire l'elaborazione keepalive, è possibile che l'utente desideri disattivarla nel server e, se questa viene eseguita nel server, è possibile che l'utente desideri disattivarla nel client allo scopo di ridurre il traffico della rete.

Specifica dell'accesso alle stazioni AS/400 con più porte

Communications Server consente di configurare più di una stazione AS/400 e più di una porta dalla quale il server TN5250 attende i collegamenti in arrivo. Quando viene configurata una nuova porta del server TN5250, è possibile specificare la stazione AS/400 a cui associarla. I collegamenti TCP/IP in arrivo ricevuti su tale porta dal server TN5250 accederanno alla stazione AS/400 ad essa associata.

Segnalare agli utenti del client TN5250 i numeri di porta da configurare per il collegamento delle applicazioni di emulazione a specifiche stazioni AS/400.

Filtraggio IP

Communications Server consente di configurare i filtri TN5250 per specificare i client TCP/IP che è possibile collegare al server. I client possono essere specificati mediante l'utilizzo di indirizzi IP individuali, sottoreti IP, nomi host TCP/IP o nomi di dominio.

E' anche possibile configurare una stazione AS/400 con un filtro in modo da specificare una stazione AS/400 differente da quella associata alla porta. Questa può essere utilizzata per indirizzare i client associati ad un filtro ad una specifica stazione AS/400.

In un filtro è possibile specificare più di una stazione AS/400. Se il tentativo di collegamento di un client alla prima stazione AS/400 specificata non riesce, vengono eseguiti dei tentativi di collegamento alle altre stazioni AS/400 specificate nel filtro.

Supporto SSL (Secure Sockets Layer)

Quando viene configurata una nuova porta server TN5250, è possibile specificare che tale porta venga utilizzata per i collegamenti protetti. E' possibile specificare più di una porta protetta.

Per abilitare la sicurezza, Communications Server fornisce un programma di utilità **Gestione file di chiavi** che consente di generare il certificato e le chiavi richieste

da SSL. Per ulteriori informazioni, fare riferimento alla sezione “Pianificazione della sicurezza basata su SSL (Secure Sockets Layer)” a pagina 137.

Una volta configurata ed abilitata la sicurezza, i client TN5250 che supportano SSL Versione 3 possono collegarsi ad un numero di porta protetta e stabilire collegamenti protetti.

Configurazione della rete SNA

Per consentire il collegamento del server TN5250 alle stazioni As/400, è necessario configurare la rete SNA. Per le informazioni sulla configurazione della rete SNA per il server TN5250, fare riferimento alla *Guida operativa*.

Distribuzione del carico dei server TN5250

Communications Server supporta anche la distribuzione del carico dei client TN5250 su più server TN5250. Per ulteriori informazioni, fare riferimento alla sezione “Pianificazione della distribuzione del carico” a pagina 147.

Pianificazione della sicurezza basata su SSL (Secure Sockets Layer)

E' possibile utilizzare la sicurezza basata su SSL (Secure Sockets Layer) nei collegamenti tra client TN e server TN3270E o TN5250. Tale sicurezza utilizza SSL Versione 3 per fornire la crittografia dei dati e l'autenticazione del server mediante l'utilizzo dei certificati firmati.

E' possibile configurare specifiche porte per il supporto della sicurezza basata su SSL. Se viene specificata la sicurezza, il server deve disporre di un certificato autenticato fornito da una CA (certificate authority). Communications Server fornisce un programma di utilità che genera e gestisce chiavi e certificati utilizzati dall'SSL Versione 3.

In questo capitolo viene fornita una panoramica della pianificazione della sicurezza basata su SSL (Secure Sockets Layer). La sicurezza basata su SSL viene fornita come opzione durante la configurazione dei server TN3270E e TN5250.

Funzionamento della sicurezza SSL

SSL (secure sockets layer) è un protocollo standard che utilizza la tecnologia di crittografia delle chiavi simmetriche e delle chiavi pubbliche. La crittografia delle chiavi simmetriche utilizza la stessa chiave per crittografare e decrittografare i messaggi. La crittografia delle chiavi pubbliche utilizza una coppia di chiavi: una chiave pubblica ed una chiave privata. La chiave pubblica di ciascun server viene pubblicata e la chiave privata viene mantenuta secreta. Per inviare un messaggio protetto al server, il client esegue la crittografia del messaggio utilizzando la chiave pubblica del server. Quando il server riceve il messaggio, ne esegue la decrittografia utilizzando la relativa chiave privata.

SSL fornisce tre servizi di sicurezza di base:

- Riservatezza dei messaggi

  La riservatezza dei messaggi è resa possibile mediante una combinazione di crittografia di chiave pubblica e di chiave simmetrica. Tutto il traffico tra un client SSL ed un server SSL viene crittografato utilizzando una chiave ed un algoritmo di crittografia negoziato durante l'impostazione della sessione.

- Integrità dei messaggi

  Il servizio di integrità dei messaggi assicura che il traffico della sessione SSL non venga modificato durante l'instradamento alla destinazione finale. SSL utilizza una combinazione di chiavi pubbliche/private e funzioni di indirizzamento casuale per assicurare l'integrità dei messaggi.

- Autenticazione

  L'autenticazione è il processo in base al quale il client ed il server riconoscono le proprie identità. Le identità del client e del server vengono codificate nei certificati della chiave pubblica. Un certificato della chiave pubblica contiene i seguenti componenti:

  – Nome distinto dell'argomento

  – Nome distinto dell'issuer

  - Chiave pubblica dell'argomento
  - Firma dell'issuer
  - Periodo di validità
  - Numero di serie

Nota: Communications Server supporta l'autenticazione server. Solo il Secure Server richiede l'autenticazione da parte di una CA (certificate authority) per stabilire un collegamento TN3270E o TN5250.

Supporto SSL di Communications Server

Communications Server supporta i seguenti componenti per la sicurezza SSL:

- Sessioni SSL protette tra il server TN3270E e qualsiasi client TN3270 e TN3270E che supporti SSL Versione 3
- Sessioni SSL protette tra il server TN5250 e qualsiasi client TN5250 che supporti SSL Versione 3
- SSL Versione 3
- Riservatezza ed integrità dei messaggi
- Autenticazione server

Configurazione della sicurezza SSL

Durante la configurazione dei server TN3270E e TN5250, vengono specificate le porte che utilizzeranno la sicurezza SSL per i propri collegamenti. Per ulteriori informazioni sulla configurazione delle porte protette, consultare le sezioni “Pianificazione del server TN3270E” a pagina 125 e “Pianificazione del server TN5250” a pagina 131.

Per consentire la sicurezza SSL con l'autenticazione server, è necessaria una serie di chiavi pubbliche/private ed un certificato autenticato della chiave pubblica associato. Communications Server fornisce il programma di utilità **Gestione file di chiavi** che consente di creare, gestire e memorizzare le chiavi pubbliche/private ed i certificati richiesti da SSL.

Quando viene utilizzato questo programma di utilità, è necessario effettuare una delle seguenti operazioni:

- Creare una coppia di chiavi pubblica/privata ed ottenere un certificato da una delle CA (certificate authority) predefinite riconosciute e poi memorizzarlo.

  Questa procedura richiede meno passi di impostazione poiché il file del database del file di chiavi viene preconfigurato con i certificati root CA necessari per l'identificazione delle CA da cui viene emesso il certificato.
- Creare una coppia di chiavi pubblica/privata, definire una CA non riconosciuta ottenendo il certificato root CA e memorizzandolo nel file del del database del

Nota: Per garantire un'adeguata sicurezza al proprio sito, è necessario utilizzare l'autocertificazione solo per eseguire prove controllate.

Programma di utilità Gestione file di chiavi

Il programma di utilità **Gestione file di chiavi** di Communications Server consente di creare, gestire e memorizzare le chiavi pubbliche/private ed i certificati necessari per le comunicazioni SSL tra Communications Server e client. Prima di iniziare la configurazione delle comunicazioni SSL, è necessario aprire il file del database del file di chiavi di Communications Server. Per aprire il file, procedere nel modo seguente:

1. Selezionare **File database chiavi** dal menu principale e selezionare **Apri** per aprire un database del file di chiavi esistente.
2. Dalla finestra **Apri**, scegliere la sottodirectory **private** della directory in cui è installato il prodotto (ad esempio, C:\IBMCS\PRIVATE).
3. Selezionare **ibmcs.kdb** come database del file di chiavi
4. Quando viene richiesto, immettere la password.

   Nota: La password viene inizialmente impostata su **ibmcs**. Per una sicurezza adeguata, è ***necessario*** modificare la password prima di eseguire qualsiasi attività di **Gestione file di chiavi**.

Modifica della password

Per modificare la password del database corrente, effettuare i seguenti passi:

1. Selezionare **File database chiavi** dal menu e poi **Modifica password** per modificare la password del database del file di chiavi per il database corrente. Viene visualizzata la finestra di dialogo **Modifica password**.
2. Immettere la nuova password che si desidera utilizzare.
3. Immettere nuovamente la stessa password per verifica.
4. Se si desidera impostare una scadenza per la password, fare clic su **Imposta scadenza**. Tale scadenza è necessaria se si desidera garantire una sicurezza adeguata.
5. Se si desidera impostare una scadenza per la password, specificare il numero di giorni che mancano a tale scadenza.
6. Fare clic su **Nascondi password** per nascondere la password del database corrente.

Configurazione SSL mediante una CA di garanzia riconosciuta

Per impostare la sicurezza SSL utilizzando un certificato emesso da una CA riconosciuta, eseguire le procedure riportate in questa sezione. I seguenti certificati del firmatario CA sono già memorizzati nel database del file di chiavi e contrassegnati come certificati di garanzia:

- Integrion Certification Authority Root
- IBM World Registry Certification Authority
- Thawte Personal Premium CA
- Thawte Personal Freemail CA

- Thawte Personal Basic CA
- Thawte Premium Server CA
- Thawte Server CA RSA secure server CA (rilasciato anche da VeriSign)
- VeriSign class 4 public primary CA
- VeriSign class 3 public primary CA
- VeriSign class 2 public primary CA
- VeriSign class 1 public primary CA

Per impostare la sicurezza SSL utilizzando una CA riconosciuta, è necessario effettuare le seguenti procedure:

- Creare una chiave ed una richiesta di certificato
- Inviare una richiesta di certificato alla CA
- Ottenere un certificato e memorizzarlo nel database del file di chiavi del server

Creazione di una chiave e di una richiesta di certificato

Per creare le chiavi pubblica/privata e la richiesta di certificato, effettuare i seguenti passi nel programma di utilità **Gestione file di chiavi**:

1. Selezionare **Richieste di certificati personali** dall'elenco a discesa del menu principale e fare clic su **Nuovo** per creare una nuova coppia di chiavi ed una richiesta di certificato. Viene visualizzata la finestra di dialogo **Crea nuova chiave e richiesta di certificato**.
2. Immettere il nome (etichetta) utilizzato per identificare la chiave ed il certificato all'interno del database.
3. Immettere il numero relativo alle dimensioni della chiave che si desidera utilizzare. L'utilizzo di dimensioni di chiave elevate comporta una maggiore sicurezza ma richiede una maggiore elaborazione sul client e sul server per stabilire un collegamento.
4. Immettere il nome host TCP/IP del Communications Server come nome comune (ad esempio, wtr05306.raleigh.ibm.com).
5. Immettere un nome di società.
6. Immettere un'unità organizzativa (facoltativo).
7. Immettere una città o una località (facoltativo).
8. Immettere uno stato o una provincia (facoltativo).
9. Immettere un C.A.P. (facoltativo).
10. Immettere un codice di paese. E' necessario specificare almeno 2 caratteri (ad esempio, US).
11. Immettere il nome del file relativo alla richiesta di certificato oppure utilizzare il nome file predefinito.

Quando si fa clic su **OK**, le informazioni fornite vengono elaborate. Vengono creati due file:

ibmcs.rdb File di chiavi private

certreq.arm Si tratta del nome predefinito del file relativo alla richiesta di certificato. Se è stato assegnato un nome file, viene creato un file con tale nome. Il file della richiesta di certificato è un file di tipo PKCS 10 nel formato 64 protetto.

Non provare a modificare o spostare questi file. Se non è possibile trovare il file **ibmcs.rdb** oppure è stato danneggiato durante il tentativo di immissione del certificato nel database del file di chiavi , sarà necessario inviare nuovamente la richiesta di certificato alla CA.

Invio di una richiesta di certificato

Avviare un browser Web ed accedere alla pagina Web relativa alla CA. Seguire le istruzioni fornite per l'invio di una richiesta di certificato. Di seguito sono riportati gli URL relativi ad alcune CA riconosciute:

- VeriSign: **http://www.verisign.com/**
- Thawte: **http://www.thawte.com/**

In base alla CA scelta, inviare una e-mail della richiesta di certificato generato dal programma di utilità **Gestione file di chiavi** oppure incorporare la richiesta di certificato nel modulo o nel file fornito dalla CA.

Dopo aver inviato una richiesta di certificato ad una CA, è possibile abilitare la sicurezza SSL creando e memorizzando un'autocertificazione. Tale autocertificazione deve essere utilizzata solo per eseguire prove controllate. Per ulteriori informazioni, fare riferimento alla sezione “Creazione di un'autocertificazione” a pagina 144.

Memorizzazione di un certificato nel database del file di chiavi

Quando si riceve un certificato da una CA, utilizzare il programma di utilità **Gestione file di chiavi** per inserire il certificato nel file del database del file di chiavi , **ibmcs.kdb**, ubicato sul server.

1. Selezionare **Certificati personali** dall'elenco a discesa del programma di utilità **Gestione file di chiavi** e fare clic su **Ricevi** per ricevere la coppia di chiavi e la richiesta di certificato. Viene visualizzata la finestra di dialogo **Ricevi certificato da un file**.
2. Verificare che il tipo di dati sia **Dati ASCII codificati BASE64** (formato 64 protetto).
3. Immettere il nome del file del certificato.
4. Immettere l'ubicazione (nome percorso) del certificato. Fare clic su **OK**. Il certificato memorizzato viene visualizzato come prima voce.
5. Evidenziare il certificato memorizzato e fare clic su **Visualizza/Modifica**. Viene visualizzata la finestra di dialogo **Informazioni sulle chiavi**.
6. Fare clic su **Imposta il certificato come predefinito**. La chiave selezionata diventa la chiave predefinita.

Configurazione SSL mediante una CA non riconosciuta

Per impostare la sicurezza SSL utilizzando una CA non riconosciuta (non ancora definita nel database), è necessario procedere nel modo seguente:

- Creare una chiave ed una richiesta di certificato
- Inviare una richiesta di certificato alla CA
- Ottenere il certificato root CA ed il proprio certificato e memorizzarli nel database del file di chiavi del server

Creazione di una chiave e di una richiesta di certificato

Per creare le chiavi pubblica/privata e la richiesta di certificato, effettuare i seguenti passi nel programma di utilità **Gestione file di chiavi**:

1. Selezionare **Richieste di certificati personali** dall'elenco a discesa del menu principale e fare clic su **Nuovo** per creare una nuova coppia di chiavi ed una richiesta di certificato. Viene visualizzata la finestra di dialogo **Crea nuova chiave e richiesta di certificato**.
2. Immettere il nome (etichetta) utilizzato per identificare la chiave ed il certificato all'interno del database.
3. Immettere il numero relativo alle dimensioni della chiave che si desidera utilizzare. L'utilizzo di dimensioni di chiave elevate comporta una maggiore sicurezza ma richiede una maggiore elaborazione sul client e sul server per stabilire un collegamento.
4. Immettere il nome host TCP/IP del Communications Server come nome comune (ad esempio, wtr05306.raleigh.ibm.com).
5. Immettere un nome di società.
6. Immettere un'unità organizzativa (facoltativo).
7. Immettere una città o una località (facoltativo).
8. Immettere uno stato o una provincia (facoltativo).
9. Immettere un C.A.P. (facoltativo).
10. Immettere un codice di paese. E' necessario specificare almeno 2 caratteri (ad esempio, US).
11. Immettere il nome del file relativo alla richiesta di certificato oppure utilizzare il nome file predefinito.

Quando si fa clic su **OK**, le informazioni fornite vengono elaborate. Vengono creati due file:

ibmcs.rdb File di chiavi private

certreq.arm Si tratta del nome predefinito del file relativo alla richiesta di certificato. Se è stato assegnato un nome file, viene creato un file con tale nome. Il file della richiesta di certificato è un file di tipo PKCS 10 nel formato 64 protetto.

Non provare a modificare o spostare questi file. Se non è possibile trovare il file **ibmcs.rdb** oppure è stato danneggiato durante il tentativo di immissione del certificato nel database del file di chiavi , sarà necessario inviare nuovamente la richiesta di certificato alla CA.

Invio di una richiesta di certificato

Per inviare la richiesta di certificato, seguire le procedure indicate dalla CA non riconosciuta.

In base alla CA scelta, inviare una e-mail della richiesta di certificato generato dal programma di utilità **Gestione file di chiavi** oppure incorporare la richiesta di certificato nel modulo o nel file fornito dalla CA.

Dopo aver inviato una richiesta di certificato ad una CA, è possibile abilitare la sicurezza SSL creando e memorizzando un'autocertificazione. Tale autocertificazione deve essere utilizzata solo per eseguire prove controllate. Per ulteriori informazioni, fare riferimento alla sezione “Creazione di un'autocertificazione” a pagina 144.

Memorizzazione di un certificato nel database del file di chiavi

Quando si riceve un certificato da una CA, rivolgersi alla CA per ottenere il relativo certificato root. Tale certificato deve essere memorizzato nel database del file di chiavi prima di procedere alla memorizzazione del certificato richiesto. Il certificato root CA convalida il certificato richiesto. Utilizzare il programma di utilità **Gestione file di chiavi** per memorizzare il certificato root CA.

1. Selezionare **Certificati firmatario** dall'elenco a discesa e fare clic su **Ricevi** per ricevere la coppia di chiavi e la richiesta di certificato. Viene visualizzata la finestra di dialogo **Ricevi certificato da un file**.
2. Verificare che il tipo di dati sia **Dati ASCII codificati BASE64** (formato 64 protetto).
3. Immettere il nome del file del certificato.
4. Immettere l'ubicazione (nome percorso) del certificato. Fare clic su **OK**. Il file viene contrassegnato come file ***di garanzia*** e quindi memorizzato.

Per memorizzare il certificato richiesto, utilizzare il programma di utilità **Gestione file di chiavi** per inserire il certificato nel file del database del file di chiavi , **ibmcs.kdb**, ubicato sul server.

1. Selezionare **Certificati personali** dall'elenco a discesa del menu principale e fare clic su **Ricevi** per ricevere la coppia di chiavi e la richiesta di certificato. Viene visualizzata la finestra di dialogo **Ricevi certificato da un file**.
2. Verificare che il tipo di dati sia **Dati ASCII codificati BASE64** (formato 64 protetto).
3. Immettere il nome del file del certificato.
4. Immettere l'ubicazione (nome percorso) del certificato. Fare clic su **OK**. Il certificato memorizzato viene visualizzato come prima voce.
5. Evidenziare il certificato memorizzato e fare clic su **Visualizza/Modifica**. Viene visualizzata la finestra di dialogo **Informazioni sulle chiavi**.
6. Fare clic su **Imposta il certificato come predefinito**. La chiave selezionata diventa la chiave predefinita.

Creazione di un'autocertificazione

Per ricevere un certificato da una CA di garanzia riconosciuta potrebbero essere necessarie tre settimane. Finché non si riceve il certificato del server pubblico, è possibile creare un'autocertificazione per abilitare le sessioni SSL tra i client ed il server. Tale autocertificazione deve essere utilizzata solo per eseguire prove controllate. Per garantire un'adeguata sicurezza al proprio sito, è necessario non utilizzare tale autocertificazione in un ambiente di produzione. Per impostare il sito in modo da utilizzare un'autocertificazione mediante il programma di utilità **Gestione file di chiavi**, effettuare i seguenti passi:

1. Selezionare **Nuova autocertificazione** dall'opzione di menu **Crea** per creare una nuova autocertificazione. Viene visualizzata la finestra di dialogo **Crea nuova autocertificazione**.
2. Immettere il nome (etichetta) utilizzato per identificare la chiave ed il certificato all'interno del database. Selezionare **X509 V3** come versione di certificato.
3. Immettere il numero relativo alle dimensioni della chiave che si desidera utilizzare. L'utilizzo di dimensioni di chiave elevate comporta una maggiore sicurezza ma richiede una maggiore elaborazione sul client e sul server per stabilire un collegamento.
4. Immettere il nome host TCP/IP del Communications Server come nome comune (ad esempio, wtr05306.raleigh.ibm.com).
5. Immettere un nome di società.
6. Immettere un'unità organizzativa (facoltativo).
7. Immettere una città o una località (facoltativo).
8. Immettere uno stato o una provincia (facoltativo).
9. Immettere un C.A.P. (facoltativo).
10. Immettere un codice di paese. E' necessario specificare almeno 2 caratteri (ad esempio, US).
11. Immettere il numero di giorni di validità dell'autocertificazione.
12. Fare clic su **OK**.
13. Fare clic su **Sì** per impostare la chiave come chiave predefinita nel relativo database.

Se viene utilizzato IBM eNetwork Host On-Demand o qualsiasi altro client SSL che richiede la designazione dell'autocertificazione, utilizzando il programma di utilità **Gestione file di chiavi**, effettuare i seguenti passi:

1. Selezionare **Certificati personali** dall'elenco a discesa, evidenziare la propria autocertificazione e fare clic su **Estrai certificato**. Viene visualizzata la finestra di dialogo **Estrai certificato per un file**.
2. Selezionare **Dati DER binari** come tipo di dati.
3. Immettere il nome del file del certificato. Il file deve essere di tipo **der** (ad esempio, ibmcs.der).
4. Immettere l'ubicazione (nome percorso) del certificato.
5. Fare clic su **OK**.

Il file del certificato deve essere fornito a ciascun client autorizzato al collegamento al server. Per le istruzioni sulla memorizzazione dell'autocertificazione come certificato root CA nel file di classe client o nel file del database del file di chiavi , fare riferimento alla documentazione relativa al client.

Pianificazione della distribuzione del carico

In questo capitolo viene fornita una panoramica della pianificazione della distribuzione del carico e viene descritta la pianificazione della distribuzione del carico della LU dipendente e della LU 6.2.

Distribuzione del carico della LU dipendente

La distribuzione del carico consente di distribuire le sessioni host dipendenti tra i server. Essa è supportata per le applicazioni API LUx mediante i client API SNA, i programmi di emulazione 3270 e TN3270.

Quando Communications Server risponde alle richieste del client, esso ordina i server che supportano il pool richiesto in base al carico.

Il carico per le LU dipendenti rappresenta una percentuale di risorse disponibili di un particolare server. La percentuale di carico viene calcolata dividendo il numero di collegamenti di applicazioni attive per il numero totale di LU (da 0 a 3) disponibili.

E' possibile influire sul carico calcolato specificando un fattore di carico da LU 0 a 3 (fattore di carico delle sessioni host) per compensare le differenze tra i due server, come la memoria disponibile, la velocità del processore e l'utilizzo della CPU. E' anche possibile utilizzare il fattore di carico LU da 0 a 3 per distribuire i carichi tra i Communications Server ed i server Novell IntranetWare per SAA.

Note:

1. I server che partecipano alla distribuzione del carico vengono stabiliti dai membri del pool di LU e dai membri dell'ambito. Tutti i Communications Server che dispongono di LU in pool dello stesso nome sono soggette alla distribuzione del carico.
2. I client che utilizzano il protocollo TCP/IP possono partecipare alla distribuzione del carico. Tuttavia, i client TCP/IP possono distribuire il carico solo tra IBM Communications Server. La distribuzione del carico viene stabilita da ambiti configurati.

In Communications Server, se i pool di LU ubicati su server differenti hanno lo stesso nome, funzionano come singolo pool per la distribuzione del carico. Durante l'assegnazione delle LU ad un pool di LU, effettuare selezioni dai collegamenti host su un server ed assegnare le LU dal collegamento host selezionato al pool di LU. Queste LU non devono essere dello stesso tipo. Inoltre, il pool ottenuto può contenere LU appartenenti a più collegamenti.

Distribuzione del carico della LU 6.2

La distribuzione del carico consente di distribuire sessioni LU 6.2 indipendente su

limite massimo cumulativo di sessioni per tutte le LU locali. Il limite massimo di sessioni è il limite di sessioni LU 6.2 specificato durante la configurazione. Se il limite massimo di sessioni viene specificato come zero (0), per indicare che non è previsto nessun limite di sessioni, per il calcolo del carico viene utilizzato il limite massimo di sessioni locali predefinito pari a 512 per LU locale. Tale limite può essere specificato anche durante la configurazione.

E' possibile influire sul carico calcolato specificando un fattore di carico LU 6.2 (fattore di carico delle sessioni APPC) per compensare le differenze tra due server, come la memoria disponibile, la velocità del processore e l'utilizzo della CPU. E' anche possibile utilizzare il fattore di carico LU6.2 per distribuire i carichi tra i Communications Server ed i server Novell IntranetWare per SAA.

Nota: I client che utilizzano il protocollo TCP/IP possono partecipare alla distribuzione del carico LU 6.2.

Pianificazione degli ambiti TCP/IP

Ambito è un parametro utilizzato per il controllo e la gestione degli accessi dei client TCP/IP ai server presenti in una rete. Esso equivale all'ambito SLP (service location protocol) a cui si fa riferimento in RFC 2165. L'ambito SLP viene utilizzato da Communications Server per implementare la distribuzione del carico basata su TCP/IP.

L'ambito di controllo fornito è necessario per due motivi:

- Per l'aumento delle dimensioni della rete, l'ambito di controllo è indispensabile per ridurre il traffico nella rete a causa del numero crescente dei client che tentano di accedere a quei server.
- L'ambito di controllo consente ai responsabili di organizzare gli utenti ed i server in gruppi di gestione.

Il significato dei valori dell'ambito viene definito dal responsabile della rete. Tali valori possono rappresentare qualsiasi entità. Generalmente, rientrano in linee dipartimentali, geografiche o organizzative.

Una volta configurati, i client possono raggiungere la rete SNA mediante server configurati con lo stesso ambito oppure senza alcun ambito associato (servizi o server ***senza ambito***).

Nota: Se un server viene configurato come non inserito in un ambito, esso risponde sia alle richieste inserite in un ambito SLP **che** a quelle che non lo sono. Se il client API SNA è configurato in modo da collegarsi ai server non inseriti in un ambito, risponderanno solo i server non inseriti in un ambito.

Sicurezza client/server e ambiti

Communications Server consente ai client Novell IntranetWare per SAA di utilizzare la sicurezza del dominio Windows NT per autenticare il collegamento client al server senza immettere nuovamente l'ID utente e la password. Il client deve appartenere ad un dominio Windows NT, partecipando ad un dominio Communications Server oppure eseguendo il collegamento in locale con una password ed un ID utente sincronizzati.

Gli utenti autorizzati all'utilizzo client/server vengono memorizzati nel gruppo locale IBMCSAPI, che si trova direttamente in Communications Server o nell'unità di controllo del dominio a cui appartiene Communications Server. Tale gruppo di utenti viene creato durante l'installazione e può essere gestito utilizzando l'applicazione User Manager di Windows NT.

Gli utenti del client Novell IntranetWare per SAA esterni al dominio Windows NT devono ripetere l'ID utente e la password in tutti i server configurati con lo stesso ambito.

Ubicazione della configurazione dell'ambito

Ciascun server viene assegnato ad uno o più ambiti mediante la **Configurazione nodo**. I client che utilizzano questi server devono essere configurati in modo da eseguire il collegamento ai server inclusi in un singolo ambito specifico o ai server non inseriti in un ambito. Per ulteriori informazioni sulla configurazione dei client, fare riferimento a *Client/Server Communications Programming*.

Relazione tra ambito ed SLP

L'ambito di Communications Server si rapporta direttamente all'ambito SLP (service location protocol). Pertanto, gli agenti della directory SLP possono risiedere nella rete che supporta gli ambiti Communications Server configurati. Se si desidera consentire ai client l'individuazione dei servizi di Communications Server basati sugli ambiti, è necessario tenere presente la relazione tra l'ambito e l'intera rete. Se in una rete in cui vengono utilizzati anche gli ambiti sono presenti servizi senza ambito, tali servizi possono soddisfare qualsiasi richiesta con ambito, con la possibilità di causare problemi agli agenti dei servizi e delle directory che supportano servizi senza ambito.

Nota: Se il client API SNA è configurato in modo da collegarsi ai server non inseriti in un ambito, risponderanno solo i server non inseriti in un ambito.

Se gli agenti delle directory devono essere utilizzati nelle rete del sito per eseguire una scalatura verso l'alto, è necessario configurarli in modo da gestire ambiti identici a quelli configurati per Communications Server. Inoltre, se i servizi senza ambito devono essere utilizzati nelle reti che dispongono di agenti di directory, è necessario configurare almeno un agente di directory senza ambito.

Communications Server include un agente di servizio SLP che viene installato su ciascun server su cui è presente Communications Server. Nella rete non è necessario installare nessun supporto SLP aggiuntivo per il corretto funzionamento della distribuzione del carico TCP/IP e del supporto Discovery di Communications Server.

Traccia del carico corrente

Utilizzando l'applicazione Performance Monitor di Windows NT , è possibile tracciare il carico corrente delle LU dipendenti e delle LU 6.2. Il Performance Monitor può essere avviato dalla selezione **Strumenti di amministrazione (Comune)** del menu **Programmi**.

Dal pannello di Performance Monitor, selezionare **Aggiungi al grafico** dal menu a discesa **Modifica**. Nel campo **Oggetto**, selezionare **IBM SNA Distribuzione del carico**. I due contatori elencati sono:

Carico LU0/LU3 Utilizzare questo contatore per tracciare il carico delle LU dipendenti.

Carico LU6.2 Utilizzare questo contatore per tracciare il carico delle LU 6.2.

I risultati delle tracce del carico possono essere salvati per un riferimento futuro.

Pianificazione dei collegamenti host di backup

Per gli ambienti in cui può essere importante fornire collegamenti host di backup ai collegamenti primari utilizzati dalle sessioni di emulazione della stazione di lavoro, Communications Server fornisce delle opzioni che consentono di configurare i collegamenti host che vengono attivati in risposta a condizioni di malfunzionamento. Le opzioni che è possibile utilizzare dipendono dal livello di backup che si desidera fornire:

- Per abilitare il backup completo del sistema tra i nodi server che supportano le sessioni di emulazione delle stazioni di lavoro IPX o IP basate su LAN, includere la funzione Hot Standby nell'ambiente.
- Per abilitare il backup completo del sistema tra i nodi server che supportano le sessioni di emulazione delle stazioni di lavoro diverse da quelle IP o IPX basate su LAN, non includere la funzione Hot Standby nell'ambiente. Configurare un'altra installazione di Communications Server sul sistema di backup.
- Per abilitare il backup in un nodo server, non utilizzare la funzione Hot Standby. Utilizzare le opzioni normali per le definizioni del collegamento nell'ambiente di backup.

Queste opzioni vengono illustrate nelle sezioni che seguono.

Pianificazione dei collegamenti di backup tra i server utilizzando la funzione Hot Standby

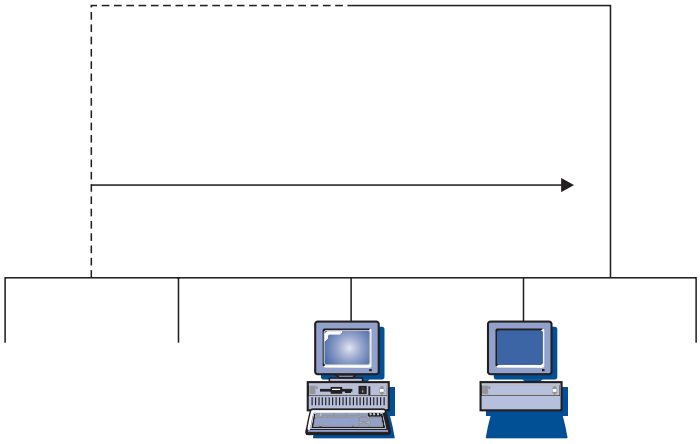
In Communications Server, è possibile configurare i collegamenti host da attivare automaticamente in caso di malfunzionamento di un server strategico. I collegamenti configurati in un host possono continuare a funzionare attivando collegamenti alternativi in un server di backup. Questa funzione è chiamata Hot Standby.

Per l'utente di una sessione di emulazione di una stazione di lavoro che dispone di una macchina host il cui collegamento iniziale ha esito negativo a causa di un malfunzionamento di Communications Server, la funzione Hot Standby consente di eseguire un successivo tentativo allo scopo di ristabilire il collegamento con la macchina host, eseguendo l'instradamento automatico mediante un Communications Server alternativo. Il server iniziale che fornisce il collegamento viene chiamato ***server strategico***. Il server alternativo che fornisce un collegamento alla macchina host in seguito al malfunzionamento del server strategico viene chiamato ***server di backup***. Il server di backup fornisce collegamenti che vengono avviati automaticamente in seguito al rilevamento di un malfunzionamento del server strategico ed i costi per la licenza relativi alla connettività host del server strategico vengono gestiti automaticamente sul server di backup.

Un server può essere contemporaneamente un server strategico ed un server di backup. Ciascun server può eseguire il backup dell'altro.

La funzione Hot Standby abilita il supporto del server di backup per le sessioni di emulazione IPX o IP basate su LAN e non fornisce tale supporto per l'ambiente SNA.

In Figura 38 a pagina 152, il server di backup viene configurato con un collegamento di backup completo per HOSTCON1, che fornisce la connettività host primaria sul server strategico. Le linee tratteggiate tra il server di backup ed i client di emulazione della stazione di lavoro non sono attive durante il funzionamento del server strategico.



In caso di malfunzionamento del server strategico, il ripristino viene effettuato come segue:

1. Il server di backup, l'host ed il software di emulazione della stazione di lavoro rilevano quasi contemporaneamente il malfunzionamento sulla stazione di lavoro.
2. I collegamenti presenti nella configurazione del server strategico del server di backup vengono attivati automaticamente e ne viene stabilita la connettività con la macchina host.
3. La stazione di lavoro apre una nuova sessione con il server di backup che ha appena attivato i collegamenti del relativo server strategico.
4. La stazione di lavoro contatta la macchina host e visualizza una richiesta di logon per l'utente.

Nota: Una volta riattivato il server strategico, i collegamenti del server di backup attivati non vengono disattivati automaticamente. E' necessario disattivarli manualmente.

Utilizzo di un server di produzione o di backup dedicato per la funzione Hot Standby

Non è possibile installare le stesse licenze Communications Server su più di un server in esecuzione sulla stessa rete. Installare Communications Server su più server acquistando un altro pacchetto Communications Server per ciascun server aggiuntivo.

Prima di configurare Communications Server per la funzione Hot Standby, decidere se si desidera eseguire Communications Server sia come server di produzione che come server di backup o come server di backup dedicato.

Utilizzo di un server di produzione

Un ***server di produzione*** è un Communications Server che si occupa dei requisiti di comunicazione quotidiani. Questo ambiente configura Communications Server con collegamenti host che vengono attivati all'esterno di uno scenario di malfunzionamento del server strategico. L'attivazione e l'utilizzo di tali collegamenti richiede l'acquisto delle licenze appropriate. Non è possibile installare le stesse licenze Communications Server su più di un server. Per installare Communications Server in modo da utilizzarlo come server di produzione su più sistemi, è necessario acquistare un altro pacchetto Communications Server per ciascuna installazione serevr aggiuntiva.

Quando un Communications Server viene utilizzato sia come server di produzione che come server di backup, non è necessario fare nessuna considerazione speciale sulle licenze. E' necessario installare Communications Server e le licenze acquistate per l'utilizzo di Communications Server come server di produzione.

Il ruolo di Communications Server come server di backup non richiede nessuna ulteriore licenza oltre a quella di base acquistata per i server strategici che esso deve controllare. Per il server di backup non è necessario fare nessuna considerazione speciale sulle licenze. Quando il server di backup rileva il malfunzionamento di un server strategico, il server di backup attiva automaticamente i collegamenti configurati per il server strategico e modifica le licenze del server di backup in base a quelle in uso per il server strategico.

Communications Server gestisce la licenza per la funzione Hot Standby senza richiedere l'intervento dell'utente.

Tuttavia, se i collegamenti configurati per il server strategico sono stati già attivati all'esterno di uno scenario di malfunzionamento del server strategico, la modifica del server di backup in base alle licenze del server strategico non viene eseguita ed è necessaria una licenza separata per il server di backup.

Utilizzo di un server dedicato

Un server di backup ***dedicato*** non funziona come server di produzione e non attiva i collegamenti esterni ad uno scenario di malfunzionamento del server strategico. Non è possibile attivare su di esso nessun collegamento all'avvio oppure manualmente. La sua funzione è quella di controllare uno o più server strategici.

Un server di backup dedicato non richiede nessuna licenza aggiuntiva oltre a quella di base acquistata per i server strategici che esso deve controllare. Communications Server gestisce la licenza per la funzione Hot Standby senza richiedere l'intervento dell'utente.

Pianificazione dell'ambiente hot standby completo

Gli scenari per l'utilizzo della funzione Hot Standby includono i normali scenari funzionali di Communications Server per il supporto dei client di emulazione su IP o IPX basati su LAN, con alcune operazioni hot standby specifiche.

Per configurare un ambiente hot standby, è necessario quanto segue:

- Due o più Communications Server devono essere configurati in modo da fornire collegamenti compatibili ad una macchina host. Il server utilizzato come backup deve essere configurato con una configurazione per server strategico per il server che fornisce la connettività primaria alla macchina host.
- Il software del client di emulazione della stazione di lavoro utilizzato per collegarsi mediante il server in modo da fornire agli utenti sessioni di emulazione sulla macchina host deve supportare delle funzioni che consentono di intervenire sull'instradamento alternativo in caso di malfunzionamento del server strategico.

E' possibile che alcuni client di emulazione non forniscano l'instradamento alternativo. La pianificazione di un'ambiente hot standby richiede un'attenta valutazione del software di emulazione e del tipo di connettività utilizzato tra client e server. Di seguito sono riportate alcune opzioni per l'instradamento alternativo:

- **Hot rollover** - Si riferisce al supporto in un client di emulazione per la configurazione di più server da contattare, in un ordine specifico, per stabilire un collegamento mediante server alla macchina host per una sessione di emulazione. L'hot rollover consente di configurare il server di backup da contattare quando i tentativi effettuati per contattare il server strategico non hanno esito positivo. Quando si verifica un malfunzionamento nel server strategico e le risorse del server di backup vengono attivate, il client di emulazione contatta il server di backup e stabilisce un instradamento alternativo mediante questo server per eseguire il collegamento alla macchina host.
- **Pool di LU** - Si riferisce alla possibilità in un client di emulazione di stabilire dinamicamente il collegamento alla macchina host per una sessione di emulazione mediante il server che al momento risponde alle interrogazioni

relative alle LU disponibili da un determinato pool. Il supporto pool di LU consente al server di backup ed ai server strategici di fornire LU allo stesso pool. Il server di backup viene definito inizialmente ma non è attivo. Quando si verifica un malfunzionamento del server strategico e le risorse sul server di backup vengono attivate, il server di backup risponde alle richieste di una LU del pool inviate dal client di emulazione e stabilisce un instradamento alternativo mediante questo per eseguire il collegamento alla macchina host. L'opzione pool di LU include i seguenti tipi di supporto client per i pool di LU:

  - Supporto pre-SLP: prima del supporto SLP di Communications Server, l'accesso client dei pool di LU è stato casuale oppure in un ordine server specificato.
  - Supporto SLP: il supporto SLP di Communications Server fornisce l'accesso client dei pool di LU, distribuendo il carico della sessione tra i server che fanno parte del pool.

- **Sessioni di emulazione multiple** - Si riferisce al supporto in un client di emulazione per la configurazione di più sessioni di emulazione, che consente all'utente di configurare sessioni separate utilizzando il server di backup ed i server strategici per il collegamento alla macchina host. L'utilizzo di più sessioni di emulazione non è semplice come il supporto dell'hot rollover o dei pool di LU, poiché richiede l'intervento manuale dell'utente del programma di emulazione che, in caso di malfunzionamenti, deve fornire assistenza mediante l'instradamento alternativo. Quando il collegamento del server strategico non viene eseguito correttamente, l'utente avvia manualmente la sessione configurata per utilizzare il server di backup in modo da ristabilire il collegamento alla macchina host.

Il supporto di IBM Personal Communications per i client di emulazione TN3270E, TN5250, API o QEL/MU fornisce delle opzioni per l'instradamento alternativo mediante una o più delle opzioni hot rollover, pool di LU o sessioni di emulazione. Alcuni fornitori di client di emulazione forniscono opzioni per l'instradamento alternativo.

Configurazione Hot Standby sul server di backup

Dal pannello avanzato **Configurazione nodo**, utilizzare l'opzione di configurazione Configura server strategici hot standby per configurare la funzione Hot Standby sul server di backup.

Sul server strategico non è necessario eseguire nessuna configurazione hot standby, ma il server di backup richiede una configurazione hot standby. Utilizzando l'opzione avanzata **Configurazione nodo**, configurare il server di backup con le definizioni di server strategico. Una definizione di server strategico specifica il nome del server strategico controllato dal server di backup ed i nomi dei collegamenti attivati quando si verifica un malfunzionamento del server strategico. E' possibile configurare più definizioni di server strategico, consentendo ad un server di backup di controllare e fornire il backup per più server strategici. Dopo aver configurato le definizioni di server strategico sul server di backup, riavviare il nodo del server di backup per rendere effettive le modifiche apportate. Per informazioni dettagliate sulla configurazione hot standby, consultare la guida in linea relativa alla **Configurazione nodo**.

Configurazione di un ambiente hot standby

Per configurare un ambiente hot standby, effettuare i seguenti passi:

1. **Configurare il server strategico:** Il server strategico viene configurato senza nessuna configurazione hot standby. Configurare la connettività host in modo che essa corrisponda all'opzione di instradamento alternativo utilizzata con i client di emulazione.
2. **Configurare il server di backup:** La configurazione del server di backup comporta due concetti principali:
   a. La configurazione della connettività host sul server di backup è simile a quella sul server strategico, con l'eccezione che i collegamenti host vengono configurati per l'avvio manuale.
   b. La configurazione del server strategico sul server di backup definisce i collegamenti host avviati quando viene rilevato un malfunzionamento del server strategico.
3. **Configurare i client di emulazione:** I client di emulazione della stazione di lavoro vengono configurati in modo da corrispondere ad un'opzione di instradamento alternativa alla connettività fornita dai server.
4. **Avviare i nodi del server strategico e del server di backup:** Avviare i nodi in modo normale. **Operazioni nodo SNA** può verificare lo stato hot standby del server strategico e di quello di backup.
5. **Malfunzionamento del server strategico:** Quando si verifica un malfunzionamento del server strategico, il ripristino viene eseguito come segue:
   a. Il server di backup, l'host ed il software di emulazione della stazione di lavoro sul client rilevano quasi contemporaneamente il malfunzionamento.
   b. I collegamenti presenti nella configurazione del server strategico sul server di backup vengono attivati e viene stabilita la connettività con la macchina host.
   c. Il client di emulazione della stazione di lavoro apre una nuova sessione con il server di backup. Il server di backup instrada delle sessioni sulla macchina host mediante il collegamento attivato sul server di backup in seguito al malfunzionamento del server strategico.
   d. La stazione di lavoro contatta la macchina host e visualizza una richiesta di logon per l'utente.
6. **Server strategico nuovamente attivo:** Una volta riattivato il server strategico, nuove sessioni di emulazione della stazione di lavoro utilizzano la connettività host del server strategico. Le sessioni di emulazione esistenti della stazione di lavoro instradate mediante il server di backup continuano a funzionare fino a quando non vengono chiuse le sessioni.

   I collegamenti del server di backup devono essere disattivati manualmente, durante le ore di non attività. Prima di eseguire la disattivazione dei collegamenti, è necessario avvisare gli utenti delle sessioni di emulazione della stazione di lavoro che dispongono del server di backup.

Pianificazione dei collegamenti di backup tra i server senza utilizzare la funzione Hot Standby

Dal momento che la funzione Hot Standby è limitata agli ambienti che supportano sessioni di emulazione di una stazione di lavoro IP o IPX basate su LAN, alcuni ambienti non possono utilizzare tale funzione per la connettività di backup. Molte considerazioni relative alla pianificazione di un ambiente di backup senza la funzione Hot Standby sono simili a quelle relative alla pianificazione di un ambiente di backup con l'utilizzo di tale funzione. Per configurare un ambiente di backup senza utilizzare la funzione Hot Standby, effettuare i passi riportati di seguito:

1. Sul server di backup, installare un pacchetto Communications Server acquistato separatamente con le licenze appropriate in modo da fornire i collegamenti host di backup al server primario.
2. Sul server di backup, configurare i collegamenti host utilizzati come backup da attivare su richiesta.
3. Configurare i client di emulazione della stazione di lavoro in modo da fornire l'instradamento automatico alle risorse presenti sul server di backup quando si verifica un malfunzionamento del server primario. Tuttavia, è necessario limitare l'accesso dell'instradamento al server di backup solo se viene rilevato un malfunzionamento del server primario.
4. Entrambi i nodi vengono avviati ma solo il nodo primario con i relativi collegamenti upstream attivi fornisce inizialmente la connettività all'host.
5. Quando si verifica un malfunzionamento del server primario, i client di emulazione della stazione di lavoro tentano di eseguire collegamenti successivi mediante il server di backup. I collegamenti host sul server di backup vengono attivati.
6. La licenza duplicata installata sul server di backup fornisce la disponibilità del server di backup ai client precedentemente instradati mediante il server primario.
7. Una volta riattivato il server primario, i collegamenti sul server di backup vengono disattivati manualmente.

Pianificazione dei collegamenti di backup in un solo server

La funzione Hot Standby per la connettività di backup non può essere utilizzata in un solo server poiché essa è applicabile solo agli ambienti che dispongono di collegamenti di backup tra i server. Tuttavia, alcune considerazioni relative alla pianificazione di un ambiente di backup in un solo server sono simili a quelle per la pianificazione di un ambiente di backup mediante l'utilizzo della funzione Hot Standby. Le differenze vengono riassunte dai seguenti passi relativi ai collegamenti di backup in un solo server:

1. Sul server che funziona come gateway per l'host, configurare i collegamenti primari e di backup che forniscono le LU allo stesso pool di LU, ma con il collegamento di backup configurato in modo da essere attivato su richiesta.
2. Configurare i client di emulazione della stazione di lavoro in modo da eseguire il collegamento mediante il pool di LU.

3. Quando si verifica un malfunzionamento del collegamento primario oppure quando le LU nel pool vengono esaurite, un tentativo di collegamento al pool avvia l'attivazione del collegamento di backup.
4. Una volta riattivato il server primario, i collegamenti sul server di backup vengono disattivati manualmente.

Pianificazione della rete X.25

La configurazione X.25 deve essere pianificazione attentamente. E' necessario considerare quanto segue:

- Per utilizzare una PSDN pubblica, è necessario richiedere una sottoscrizione alla rete per ciascuna linea (collegamento) richiesta. Dal momento che potrebbe essere necessario del tempo per ottenere una linea, è consigliabile eseguire prima un controllo accurato con il fornitore della rete X.25.
- Le funzioni disponibili sulla rete X.25 e quelle richieste. Il fornitore della rete generalmente fornisce una guida tecnica relativa alla rete che l'utente deve ottenere e consultare.
- Raccogliere le informazioni relative ai canali logici necessarie per i collegamenti PVC ed SVC.
  - E' possibile definire fino a 16 gruppi di 256 canali logici.
  - Il numero di gruppi può essere compreso tra 0 e 15.
  - Il numero di canale logico all'interno del gruppo può essere compreso tra 0 e 255.

    Moltiplicando il numero di gruppo per 256 ed aggiungendo il numero di canale logico si ottiene un numero compreso nell'intervallo da 0 a 4095, che identifica in modo univoco un canale logico. A questa combinazione viene talvolta fatto riferimento come numero di canale logico.

    Note:

    1. Se CCITT viene specificato come 1984 o 1988, il massimo numero di canali logici è 4095.
    2. Se CCITT viene specificato come 1980, il massimo numero di canali logici è 1024.
  - I gruppi di canali logici possono essere solo in arrivo (riservati per le chiamate da altri DTE), solo in uscita (riservati per le chiamate ad altri DTE), o in entrambe le direzioni.
- La quantità di circuiti virtuali richiesti dall'SNA
- I PVC richiesti
- L'alternanza di canali logici solo in arrivo, solo in uscita e nelle due direzioni
- Le dimensioni massime del pacchetto richieste e quelle supportate dalla rete X.25.
- I dettagli dei programmi X.25 facoltativi che verranno utilizzati dai programmi applicativi X.25.

  Le raccomandazioni CCITT X.25 definiscono un numero di programmi facoltativi che la rete può supportare.

  In alcuni programmi sono definiti dei parametri che possono essere specificati o negoziati da un programma applicativo durante l'impostazione e la cancellazione della chiamata mediante i campi dei programmi nei pacchetti relativi alla richiesta di chiamata, chiamata accettata e cancellazione della richiesta.

Il collegamento X.25 può essere configurato in modo da supportare i seguenti programmi durante l'impostazione della chiamata:

- CUG (closed user group)
- Identificazione utenti di rete
- Negoziazione dimensioni finestra e pacchetto
- Chiamate a carico

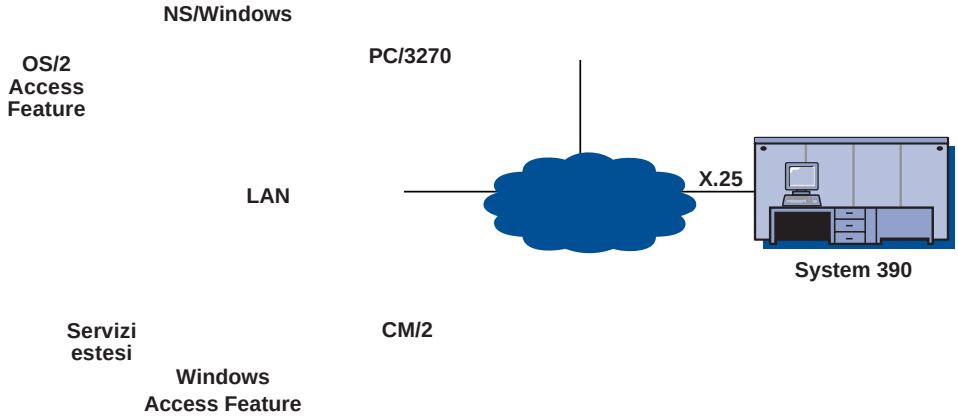
Definire i programmi durante la configurazione DLC X.25.

- I dettagli relativi ai requisiti speciali per i parametri dei frame e dei pacchetti. I valori predefiniti per questi parametri di configurazione sono stati scelti attentamente in modo da poterli adattare alla maggior parte delle situazioni. Tuttavia, il fornitore della rete potrebbe richiedere o consigliare alcuni valori.

  Per evitare problemi, i parametri di configurazione devono corrispondere ai dettagli relativi alla sottoscrizione alla rete. Ad esempio, se sono stati configurati 20 canali logici SVC ma è stata effettuata la sottoscrizione solo a 10 di essi, il DCE rileva una condizione di errore quando si tenta di utilizzare l'undicesimo canale logico.

Collegamenti X.25 possibili

In Figura 40 viene mostrato il modo in cui una rete X.25 può fornire un collegamento da un gateway SNA ad un host.



Questi costi dipendono dai programmi offerti dal fornitore della rete. Ad esempio, è possibile che l'utente debba pagare dei costi relativi a ciascun programma di rete opzionale per il quale ha fornito una sottoscrizione. E' anche possibile che debba pagare dei costi per ciascun canale logico disponibile. I collegamenti PVC generalmente costano più di quelli SVC poiché richiedono l'utilizzo di risorse di rete dedicate.

- Costi di utilizzo

  Questi costi dipendono dalla durata del collegamento logico alla rete, possibilmente soggetto a costi minimi.

- Costi relativi al volume

  Questi costi si riferiscono alla quantità di dati trasmessi nella rete durante un periodo di fatturazione.

Configurazione della connettività host

E' possibile collegarsi a stazioni di lavoro che eseguono Communications Server su host System/390 (incluso System/370) o AS/400. Molti dei valori specificati per la configurazione di Communications Server vengono utilizzati anche per la configurazione dell'host. In questo capitolo viene descritta la mappatura dei parametri di configurazione specificati durante la configurazione di Communications Server ed i parametri specificati negli host. Inoltre, vengono riportate tabelle in cui sono elencati i parametri che è possibile utilizzare per eliminare i parametri comuni in ciascuna macro, da emettere tra Communications Server e host.

Nota: Molti dei parametri NCP emessi dalle macro LINE, PU e LU possono essere specificati nella macro GROUP per poterne consentire la lettura ed una semplice codifica. Questa corrispondenza di parametri elimina la necessità di includere parametri comuni in ciascuna macro successiva e, quando necessario, consente di eseguire anche la sovrapposizione.

NTRI (NCP Token Ring) con VTAM e Communications Server

In Tabella 7, i parametri host vengono confrontati con i parametri Communications

Tabella 8 (Pagina 2 di 2). Riferimento incrociato parametri host/PC: Rete commutata VTAM Rete Token-Ring IBM

VTAM	Profilo/Parametri Communications Server	Osservazioni
IDNUM=	Nodo di configurazione ID nodo locale **ID unità fisica**	L'IDNUM dell'host deve corrispondere agli ultimi 5 caratteri esadecimali dell'**ID nodo locale**. Specificare questo parametro quando si utilizzano linee commutate oppure ometterlo se si utilizza CPNAME=.
CPNAME=	Definizione nodo Configura nodo **Nome CP completo** (secondo campo)	Specificare questo parametro quando si utilizzano linee commutate oppure ometterlo quando si utilizzano IDBLK= e IDNUM=.
LOCADDR	Configura LU host **Indirizzo NAU**	Questi parametri devono avere lo stesso valore. Per le LU indipendenti, il VTAM consiglia la creazione di una definizione CDRSC oppure l'utilizzo dell'operando DYNLU invece della codifica LOCADDR=0. Per ulteriori informazioni sulla codifica delle definizioni CDRSC per le LU indipendenti, fare riferimento alla *VTAM Network Implementation Guide* Se viene utilizzata la SDDLU o la definizione dinamica per le LU indipendenti su VTAM 3.4 o versione successiva, non sono necessarie definizioni host per le LU dipendenti.
MAXDATA	Configura periferiche LAN **Dimensione massima PIU** (265–65535)	Questi valori non devono corrispondere.
MAXOUT	Configura periferiche LAN **Numero buffer di ricezione** (2–64)	Il **Numero buffer di ricezione** in Communications Server deve essere uguale al parametro MAXOUT presente sull'host.

Adattatore 9370 Rete Token-Ring IBM e Communications Server

In Tabella 9, i parametri host 9370 vengono confrontati con i parametri Communications Server per i collegamenti Rete Token-Ring IBM.

Tabella 9. Riferimento incrociato parametri host/PC: Rete Token-Ring IBM 9370 VTAM LAN

VTAM	Profilo/Parametri Communications Server	Osservazioni
VBUILD TYPE = LAN	Tipo DLC: LAN	
PORT MACADDR=	Configura collegamenti LAN **Indirizzo di destinazione**	L'indirizzo di destinazione specificato nella personalizzazione Communications Server deve essere l'indirizzo dell'adattatore 9370 IBM Token-Ring.
PORT SAPADDR=04	Configura collegamenti LAN **SAP remoto**	Questi valori devono corrispondere.
+ADDR=04 (solo in uscita)	Configura collegamenti LAN **SAP locale**	Questi valori devono corrispondere.

Unità di controllo 3174 e Communications Server

In Tabella 10, vengono confrontati i parametri dell'unità di controllo 3174 con i parametri Communications Server per i collegamenti IBM Token-Ring.

Tabella 10. Corrispondenza parametri tra 3174 Token Ring e Communications Server

3174	Profilo/Parametri Communications Server	Osservazioni
Indirizzo limite superiore maggiore di 104: CUA	Tipo DLC: LAN	
Indirizzo Token-Ring per gateway	Configura collegamenti LAN **Indirizzo di destinazione**	Questi valori devono corrispondere.
Definizione trasmissione Ring. W= window maxout, F=0, W = 1-7, F=1, W = 1-7, F=2, W = 1-4, F=3, W = 1-2	Configura periferiche LAN **Numero buffer di ricezione** (1–8)	Il **Numero buffer di ricezione** in Communications Server deve essere uguale a 3174 W.

PU VTAM dell'unità di controllo 3174 e Communications Server

Nella Tabella 11 vengono confrontati i parametri PU VTAM dell'unità di controllo 3174 con i parametri Communications Server per i collegamenti IBM Token-Ring.

Tabella 11. Riferimento incrociato parametri host/PC: Rete Token-Ring IBM PU VTAM dell'unità di controllo 3174 e Communication

VTAM	Profilo/Parametri Communications Server	Osservazioni
CUADDR (locale) o ADDR (remoto)	(nessuno)	Associato dall'unità di controllo 3174 all'indirizzo IBM Token-Ring
MAXDATA (solo remoto)	Configura periferiche LAN **Dimensione massima PIU** (99–65535)	Il valore Dimensione massima PIU impostato sulla stazione di lavoro Communications Server deve corrispondere al valore impostato sull'host.
MAXOUT (solo remoto)	Configura periferiche LAN **Numero buffer di ricezione** (2–64)	Il **Numero buffer di ricezione** in Communications Server deve essere uguale a MAXOUT.
LOCADDR	Configura LU host **Indirizzo NAU**	Questi parametri devono avere lo stesso valore. Per le LU indipendenti, il VTAM consiglia la creazione di una definizione CDRSC oppure l'utilizzo dell'operando DYNLU invece della codifica LOCADDR=0. Per ulteriori informazioni sulla codifica delle definizioni CDRSC per le LU indipendenti, fare riferimento alla *VTAM Network Implementation Guide* Se viene utilizzata la SDDLU o la definizione dinamica per le LU indipendenti su VTAM 3.4 o versione successiva, non sono necessarie definizioni host per le LU dipendenti.

Ethernet con rete commutata VTAM e Communications Server

In Tabella 12, i parametri host vengono confrontati con i parametri Communications Server per i collegamenti della rete Ethernet che utilizzano una rete commutata VTAM.

Tabella 12. Riferimento incrociato parametri host/PC: Rete Ethernet con rete commutata VTAM

VTAM	Profilo/Parametri Communications Server	Osservazioni
IDBLK=	Configura nodo ID nodo locale **ID blocco**	L'IDBLK dell'host deve corrispondere ai primi 3 caratteri esadecimali dell'**ID nodo locale**, che viene impostato sul valore predefinito X'05D' per Communications Server. Specificare questo parametro quando si utilizzano linee commutate oppure ometterlo se si utilizza CPNAME=.
IDNUM=	Configura nodo ID nodo locale **ID unità fisica**	L'IDNUM dell'host deve corrispondere agli ultimi 5 caratteri esadecimali dell'**ID nodo locale**. Specificare questo parametro quando si utilizzano linee commutate oppure ometterlo se si utilizza CPNAME=.
CPNAME=	Definizione nodo Configura nodo **Nome CP completo** (secondo campo)	Specificare questo parametro quando si utilizzano linee commutate oppure ometterlo quando si utilizzano IDBLK= e IDNUM=.
LOCADDR	Configura LU host **Indirizzo NAU**	Questi parametri devono avere lo stesso valore. Per le LU indipendenti, il VTAM consiglia la creazione di una definizione CDRSC oppure l'utilizzo dell'operando DYNLU invece della codifica LOCADDR=0. Per ulteriori informazioni sulla codifica delle definizioni CDRSC per le LU indipendenti, fare riferimento alla *VTAM Network Implementation Guide* Se viene utilizzata la SDDLU o la definizione dinamica per le LU indipendenti su VTAM 3.4 o versione successiva, non sono necessarie definizioni host per le LU dipendenti.
MAXDATA	Configura periferiche LAN **Dimensione massima PIU** (265–65535)	Questi valori non devono corrispondere.
MAXOUT	Configura periferiche LAN **Numero buffer di ricezione** (2–64)	Il **Numero buffer di ricezione** in Communications Server deve essere uguale al parametro MAXOUT presente sull'host.

VTAM/NCP e Communications Server (SDLC)

In Tabella 13 a pagina 167, i parametri host VTAM/NCP vengono confrontati con i parametri di Communications Server per i collegamenti SDLC.

Tabella 13 (Pagina 1 di 2). Riferimento incrociato parametri host/PC: SDLC

VTAM/NCP	Profilo/Parametri Communications Server	Osservazioni
NETID=	Configura nodo **Nome CP completo** (primo campo)	Questo parametro può essere utilizzato sia per le linee commutate che per quelle dedicate. Esso identifica la rete SNA con cui viene effettuato il collegamento mediante Communications Server.
NAME PU		Utilizzare sempre una NAME PU. Questo nome PU deve essere un nome non identico al nome CP locale in modo da poter definire una LU per il CP (control point).
IDBLK=	Configura nodo ID nodo locale **ID blocco**	L'IDBLK dell'host deve corrispondere ai primi 3 caratteri esadecimali dell'**ID nodo locale**, che viene impostato sul valore predefinito X'05D' per Communications Server. Specificare questo parametro quando si utilizzano linee commutate oppure ometterlo se si utilizza CPNAME=.
IDNUM=	Configura nodo ID nodo locale **ID unità fisica**	L'IDNUM dell'host deve corrispondere agli ultimi 5 caratteri esadecimali dell'**ID nodo locale**. Specificare questo parametro quando si utilizzano linee commutate oppure ometterlo se si utilizza CPNAME=.
CPNAME=	Definizione nodo Configura nodo **Nome CP completo** (secondo campo)	Specificare questo parametro quando si utilizzano linee commutate oppure ometterlo quando si utilizzano IDBLK= e IDNUM=.
LNCTL=SDLC	Tipo DLC: SDLC-WAC, SDLC-MPA, Porta COM (dipende dall'hardware utilizzato)	SDLC deve essere selezionato. Questo parametro viene utilizzato sia per le linee commutate che per quelle dedicate.
LOCADDR	Configura LU host **Indirizzo NAU**	Questi parametri devono avere lo stesso valore. Per le LU indipendenti, il VTAM consiglia la creazione di una definizione CDRSC oppure l'utilizzo dell'operando DYNLU invece della codifica LOCADDR=0. Per ulteriori informazioni sulla codifica delle definizioni CDRSC per le LU indipendenti, fare riferimento alla *VTAM Network Implementation Guide* Se viene utilizzata la SDDLU o la definizione dinamica per le LU indipendenti su VTAM 3.4 o versione successiva, non sono necessarie definizioni host per le LU dipendenti.

Tabella 13 (Pagina 2 di 2). Riferimento incrociato parametri host/PC: SDLC

VTAM/NCP	Profilo/Parametri Communications Server	Osservazioni
NRZI=YES/NO	Configura collegamenti SDLC-WAC, SDLC-MPA, Porta COM **Codifica NRZI**	Communications Server utilizza USE_NRZI_ENCODING=0 e USE_NRZI_ENCODING=1. Questo parametro si trova solo su PCM per Modem di tipo: commutato sincrono, non commutato sincrono e AutoSync. Lo schema di codifica, NRZI o NRZ, deve essere configurato nello stesso modo in entrambe le parti di un collegamento. Se gli schemi di codifica non corrispondono, i modem vengono collegati ma il trasferimento dati non viene eseguito correttamente ed il collegamento viene interrotto da Communications Server dopo un timeout del livello di collegamento (generalmente 40 secondi). Si consiglia l'utilizzo dello schema di codifica NRZ quando viene eseguito un collegamento ad una rete X.25 utilizzando un IBM Wide Area Connector.
DUPLEX= FULL/HALF	Configura collegamenti Solo SDLC-WAC e Porta COM **Comunicazione full-duplex**	I valori impostati su ciascuna parte devono essere compatibili con il tipo di modem e la relativa configurazione. Questo parametro viene utilizzato sia per le linee commutate che per quelle dedicate.
(TRANSFR * BFRS) –47	Configura periferiche SDLC-WAC, SDLC-MPA, Porta COM **Dimensione massima PIU** (265–4105)	Il valore della dimensione massima del campo di immissione deve essere inferiore o uguale al valore (TRANSFR * BFRS) - 47 indicato sull'host. Questo parametro viene utilizzato sia per le linee commutate che per quelle dedicate.
MAXDATA=	Configura periferiche SDLC-WAC, SDLC-MPA, Porta COM **Dimensione massima PIU** (265–4105)	Questi valori non devono corrispondere. Questo parametro viene utilizzato sia per le linee commutate che per quelle dedicate. Viene utilizzato il valore più basso.
MAXOUT=	Configura periferiche SDLC-WAC, SDLC-MPA, Porta COM **Numero finestre ricezione** (1–30)	Il **Numero finestre ricezione** in Communications Server deve essere uguale al parametro MAXOUT sull'host. Questo parametro viene utilizzato sia per le linee commutate che per quelle dedicate.
ADDR=	Configura periferiche SDLC-WAC, SDLC-MPA, Porta COM **Indirizzo stazione di collegamento** (01–FE)	Questi parametri devono avere lo stesso valore. Questo valore viene codificato come esadecimale sia per Communications Server che per VTAM/NCP. Questo parametro viene utilizzato sia per le linee commutate che per quelle dedicate.

VTAM e Communications Server (APPC)

In Tabella 14, i parametri host VTAM vengono confrontati con i parametri Communications Server per i collegamenti APPC.

Tabella 14. Riferimento incrociato parametri host/PC: APPC

VTAM	Profilo/Parametri Communications Server	Osservazioni
LU NAME	Configura LU host **Nome LU locale** oppure: Configura nodo **Nome CP completo** (secondo campo)	
LOCADDR	Configura LU host **Indirizzo NAU**	Questi parametri devono avere lo stesso valore. Per le LU indipendenti, il VTAM consiglia la creazione di una definizione CDRSC oppure l'utilizzo dell'operando DYNLU invece della codifica LOCADDR=0. Per ulteriori informazioni sulla codifica delle definizioni CDRSC per le LU indipendenti, fare riferimento alla *VTAM Network Implementation Guide* Se viene utilizzata la SDDLU o la definizione dinamica per le LU indipendenti su VTAM 3.4 o versione successiva, non sono necessarie definizioni host per le LU dipendenti.
NETID APPL	Configura LU partner 6.2 **Nome LU partner**	
Tabella interpretazione VTAM	Configura LU partner 6.2 **Nome LU partner**	Solo per le LU dipendenti.
Tabella LOGMODE LOGMODE=	Configura modo **Nome modo**	Questi parametri devono corrispondere.
Tabella LOGMODE RUSIZES=	Configura modo **Dimensione massima RU** (256–32767)	I valori finali vengono negoziati.

VTAM e Communications Server (MPC)

In Tabella 15 e in Tabella 16 a pagina 170 i parametri host IOCP/HCD e VTAM vengono confrontati con i parametri Communications Server per i collegamenti MPC (Multi-Path Channel).

Tabella 15. Riferimento incrociato parametri IOCP/HCD: MPC

IOCP/HCD	Profilo/Parametri Communications Server	Osservazioni
IOCP IODEVICE UNIT=SCTC	Tipo DLC: IBM-MPC	
HCD Tipo unità SCTC	Tipo DLC: IBM-MPC	

Tabella 16. Riferimento incrociato parametri VTAM: MPC

Istruzione definizione VTAM	Operando	Profilo/Parametri Communications Server	Osservazioni
VBUILD,TYPE=TRL	LNCTL=MPC	Tipo DLC: IBM-MPC	
	MPCLEVEL=HPDT		I collegamenti IBM-MPC Communications Server richiedono l'HPR/HPDT.
	MAXBFRU	Configura MPC DLC **Dimensione massima PIU**	Potrebbe influire sulle prestazioni e/o sull'utilizzo della memoria VTAM.
	MAXREADS	Configura MPC DLC **Numero buffer di ricezione**	Potrebbe influire sulle prestazioni e/o sull'utilizzo della memoria VTAM.
	READ	Configura MPC DLC	L'elenco degli indirizzi VTAM READ IODEVICE deve corrispondere all'elenco MPC DLC Communications Server dei sottocanali READ.
	WRITE	Configura MPC DLC	L'elenco degli indirizzi VTAM WRITE IODEVICE deve corrispondere all'elenco MPC DLC Communications Server dei sottocanali WRITE.
VBUILD,TYPE=LOCAL	CONNTYPE=APPN	Configura collegamenti IBM-MPC **Supporto APPN**	Il collegamento IBM-MPC Communications Server richiede l'APPN.
	XID=YES	Configura collegamenti IBM-MPC **Supporto APPN**	Il collegamento IBM-MPC Communications Server richiede la PU2.1.
	CPCP=YES	Configura collegamenti IBM-MPC **Supporto APPN**	Il collegamento IBM-MPC Communications Server richiede l'APPN.
	HPR=YES	Configura collegamenti IBM-MPC **Supporto HPR**	Il collegamento IBM-MPC Communications Server richiede l'HPR.
	NN	Configura nodo **Tipo nodo**	Il tipo di nodo PU VTAM deve corrispondere alla definizione Communications Server.
	DELAY		Potrebbe influire sulle prestazioni e/o sull'utilizzo della CPU VTAM.

ES/9000 e Communications Server (SDLC)

In Tabella 17, i parametri di 9370 Information System vengono confrontati con i parametri Communications Server per i collegamenti SDLC.

Tabella 17 (Pagina 1 di 2). Riferimento incrociato parametri host/PC: 9370 Information System via SDLC

9370/VTAM	Profilo/Parametri Communications Server	Osservazioni
QFI: invertito senza ritorno a zero (configurazione microcodice)	Configura collegamenti SDLC-WAC, SDLC-MPA, Porta COM **Codifica NRZI**	Questi parametri devono corrispondere. Questo parametro viene utilizzato sia per le linee commutate che per quelle dedicate. Communications Server utilizza USE_NRZI_ENCODING=0 e USE_NRZI_ENCODING=1. Il flusso dati sincroni.

Tabella 17 (Pagina 2 di 2). Riferimento incrociato parametri host/PC: 9370 Information System via SDLC

9370/VTAM	Profilo/Parametri Communications Server	Osservazioni
QFI: Protocollo (configurazione microcodice) VTAM: GROUP LNCTL = SDLC	Tipo DLC SDLC-WAC, SDLC-MPA Porta COM	I parametri microcodice e VTAM devono corrispondere. Questo parametro viene utilizzato sia per le linee commutate che per quelle dedicate.
MAXDATA	Configura periferiche SDLC-WAC, SDLC-MPA, Porta COM **Dimensione massima PIU** (265–4105)	Questi valori non devono corrispondere. Questo parametro viene utilizzato sia per le linee commutate che per quelle dedicate.
MAXBFRU * Dimensione IOBUF	Configura periferiche SDLC-WAC, SDLC-MPA, Porta COM **Dimensione massima PIU** (265–4105)	Il valore della dimensione massima del campo di immissione deve essere uguale o inferiore al valore di MAXBFRU per la dimensione IOBUF indicata sull'host. Questo parametro viene utilizzato sia per le linee commutate che per quelle dedicate.
MAXOUT=	Configura periferiche **Numero finestre ricezione** (1–30)	Il **Numero finestre ricezione** in Communications Server deve essere uguale al parametro MAXOUT sull'host. Questo parametro viene utilizzato sia per le linee commutate che per quelle dedicate.
ADDR=	Configura periferiche **Indirizzo stazione di collegamento** (01–FE)	I valori impostati per questi parametri devono corrispondere. Questo parametro viene utilizzato sia per le linee commutate che per quelle dedicate.
IDBLK=	Configura nodo ID nodo locale **ID blocco**	L'IDBLK dell'host deve corrispondere ai primi 3 caratteri esadecimali dell'**ID nodo locale**, che viene impostato sul valore predefinito X'05D' per Communications Server. Specificare questo parametro quando si utilizzano linee commutate oppure ometterlo se si utilizza CPNAME=.
IDNUM=	Configura nodo ID nodo locale **ID unità fisica**	L'IDNUM dell'host deve corrispondere agli ultimi 5 caratteri esadecimali dell'**ID nodo locale**. Specificare questo parametro quando si utilizzano linee commutate oppure ometterlo se si utilizza CPNAME=.
CPNAME=	Configura nodo **Nome CP completo** (secondo campo)	Specificare questo parametro quando si utilizzano linee commutate oppure ometterlo quando si utilizzano IDBLK= o IDNUM=.
LOCADDR	Configura LU host **Indirizzo NAU**	I parametri LOCADDR e NAU devono avere lo stesso valore. Per le LU indipendenti, il VTAM consiglia la creazione di una definizione CDRSC o l'utilizzo dell'operando DYNLU invece della codifica di LOCADDR=0. Per ulteriori informazioni sulla codifica delle definizioni CDRSC per le LU indipendenti, fare riferimento alla *VTAM Network Implementation Guide*. Questo parametro viene utilizzato sia per le linee commutate che per quelle dedicate.

Host e Communications Server (DLUR)

In Tabella 18, vengono confrontati i parametri host e Communications Server per i collegamenti VTAM su DLUR.

Tabella 18. Riferimento incrociato parametri VTAM Communications Server: Utilizzo del DLUR

VTAM	Communications Server	Osservazioni
IDBLK=	Configura PU DLUR **ID blocco**	L'IDBLK deve corrispondere ai primi 3 caratteri esadecimali dell'ID nodo, che viene impostato sul valore predefinito X'05D' per Communications Server Specificare questo parametro quando NON viene utilizzato CPNAME=.
IDNUM=	Configura PU DLUR **ID unità fisica**	L'IDBLK deve corrispondere agli ultimi 5 caratteri esadecimali dell'ID nodo. Specificare questo parametro quando NON viene utilizzato CPNAME=.
CPNAME=	Configura PU DLUR **Nome PU**	CPNAME deve corrispondere al nome della PU locale. Specificare questo parametro quando NON vengono utilizzati IDNUM= e IDBLK=.

Nella Tabella 19 vengono elencati i seguenti parametri dell'istruzione PATH, utilizzati quando viene stabilito un collegamento tra l'host e la stazione di lavoro.

Tabella 19. Parametri VTAM Communications Server DLUR per collegamento da host a stazione di lavoro

VTAM	Communications Server	Osservazioni
DLURNAME=	Configura nodo **Nome CP completo** (secondo campo)	DLURNAME fornisce il nome del nodo DLUR che occupa la PU DLUR. Per Communications Server, rappresenta il nome CP completo.
DLCADDR= (1,C,INTPU)		Obbligatorio. Questo parametro comunica al DLUR che il collegamento è per una PU interna.
DLCADDR= (2,X,zzzzzzzz)	Configura PU DLUR **ID blocco e** **ID unità fisica**	zzzzzzzz in DLCADDR=(2,X,zzzzzzzzz) deve corrispondere all'ID nodo. Specificare questo parametro quando NON viene utilizzato DLCADDR=(3,C,puname).
DLCADDR= (3,C,puname)	Configura PU DLUR **Nome PU**	Il nome PU in DLCADDR=(3,C,puname) deve corrispondere al nome PU locale. Specificare questo parametro quando NON viene utilizzato DLCADDR=(2,X,zzzzzzzz).

NPSI e Communications Server (X.25)

Il supporto Communications Server X.25 abilita la trasmissione dei frame SNA in una rete X.25. X.25 considera i frame SNA come dati non codificati e li trasmette come pacchetti di dati nei dati. Invece di essere collegati direttamente, i due nodi di rete vengono collegati ad un intermediario chiamato PSDN (packet-switching data network). La rete X.25 può comprendere una qualsiasi delle connettività X.25.

Il software che interagisce con PSDN, dispone i dati SNA in pacchetti e li estrae integri è incluso in Communications Server. Sull'host S/370, le funzioni X.25 vengono gestite da un prodotto software separato chiamato NPSI (X.25 Network Control Program Packet Switching Interface). Le definizioni NPSI vengono generate con il NCP ed il software NPSI viene eseguito senza problemi di compatibilità con NCP nella stessa unità di controllo 3705, 3725, 3720 o 3745.

La maggior parte dei parametri X.25 specificati in Communications Server e nell'NPSI assume i valori accettati dall'utente e dal provider della rete X.25, invece che quelli specificati dai due nodi. Ad esempio, in presenza di un collegamento SDLC su una linea non commutata, l'unità di controllo host (NCP) viene configurata in modo da eseguire l'interrogazione ciclica di un particolare indirizzo secondario. Communications Server viene configurato in modo da rispondere a tale indirizzo su un collegamento fisico tra la stazione di lavoro Communications Server e l'host.

Collegamenti NPSI su X.25

In Tabella 20, vengono confrontati i parametri host e Communications Server per i collegamenti NPSI su X.25.

Tabella 20 (Pagina 1 di 2). Riferimento incrociato parametri host/PC: Collegamenti NPSI su X.25

NPSI	Profilo/Parametri Communications Server	Osservazioni
X25.LINE TYPE=	Tipo DLC Porta COM-X.25, X.25-WAC	Specificare **TYPE=P** per PVC e **TYPE=S** per SVC per la definizione della linea NPSI X.25.
CALL= (solo per tipo = S)	Configura periferiche Porta COM-X.25, X.25-WAC **Valori circuito virtuale**	I valori del circuito virtuale devono corrispondere alla descrizione della rete X.25.
MAXDATA=	Configura periferiche Porta COM-X.25, X.25-WAC **Dimensione massima PIU** (256–4105)	Questi valori non devono corrispondere.
VWINDOW	Configura periferiche Porta COM-X.25, X.25-WAC **Dimensioni finestra** (1–7)	Le **dimensioni della finestra SVC/PVC** devono corrispondere alle sottoscrizioni X.25.
MWINDOW	Configura periferiche Porta COM-X.25, X.25-WAC Valori frame **Dimensioni finestra** (1–7)	
FRMLGTH	Configura periferiche Porta COM-X.25, X.25-WAC Sequenza frame **Modulo**	Il valore **FRMLGTH** dell'host deve essere almeno MAXPKT +3 quando viene eseguito il Modulo 8 o MAXPKT +4 quando viene eseguito il Modulo 128. Le dimensioni del Modulo host e Communications Server e le dimensioni dei pacchetti devono corrispondere alla propria sottoscrizione X.25.

Tabella 20 (Pagina 2 di 2). Riferimento incrociato parametri host/PC: Collegamenti NPSI su X.25

NPSI	Profilo/Parametri Communications Server	Osservazioni
MAXPKTL	Configura periferiche Porta COM-X.25, X.25-WAC **Dimensioni pacchetto**	Le **dimensioni del pacchetto SVC/PVC** dell'host devono corrispondere al valore della sottoscrizione X.25.

VTAM/NCP e Communications Server (X.25)

In Tabella 21, vengono confrontati i parametri host e Communications Server per X.25 (VTAM/NCP).

Tabella 21 (Pagina 1 di 2). Riferimento incrociato parametri host/PC: X.25 (VTAM/NCP)

VTAM/NCP	Profilo/Parametri Communications Server	Osservazioni
NETID=	Configura nodo **Nome CP completo** (primo campo)	Questo parametro identifica la rete SNA con cui viene effettuato il collegamento mediante Communications Server.
PU NAME		Utilizzare sempre un nome PU. Questo nome PU non deve essere uguale al nome CP locale in modo da poter definire una LU per il CP (control point).
IDBLK=	Configura nodo ID nodo locale **ID blocco**	Le prime 3 cifre esadecimali dell'**ID nodo locale**, che viene impostato sul valore predefinito X'05D' per Communications Server. Specificare questo parametro quando si utilizzano linee commutate oppure ometterlo se si utilizza CPNAME=.
IDNUM=	Configura nodo ID nodo locale **ID unità fisica**	L'IDNUM dell'host deve corrispondere agli ultimi 5 caratteri esadecimali dell'**ID nodo locale**. Specificare questo parametro quando si utilizzano linee commutate oppure ometterlo se si utilizza CPNAME=.
CPNAME=	Configura nodo **Nome CP completo** (secondo campo)	Specificare questo parametro quando si utilizzano linee commutate oppure ometterlo quando si utilizzano IDBLK= e IDNUM=.
(TRANSFR * BFRS) - 47	Configura periferiche Porta COM-X.25, X.25-WAC **Dimensione massima PIU** (265–4105)	La **Dimensione massima PIU** deve essere uguale al valore impostato sull'host.
MAXDATA=	Configura periferiche Porta COM-X.25, X.25-WAC **Dimensione massima PIU** (265–4105)	Questi valori non devono corrispondere.

Tabella 21 (Pagina 2 di 2). Riferimento incrociato parametri host/PC: X.25 (VTAM/NCP)

VTAM/NCP	Profilo/Parametri Communications Server	Osservazioni
LOCADDR	Configura LU host **Indirizzo NAU**	Questi parametri devono avere lo stesso valore. Per le LU indipendenti, il VTAM consiglia la creazione di una definizione CDRSC oppure l'utilizzo dell'operando DYNLU invece della codifica LOCADDR=0. Per ulteriori informazioni sulla codifica delle definizioni CDRSC per le LU indipendenti, fare riferimento alla *VTAM Network Implementation Guide* Se viene utilizzata la SDDLU o la definizione dinamica per le LU indipendenti su VTAM 3.4 o versione successiva, non sono necessarie definizioni host per le LU dipendenti.

APPC su X.25

In Tabella 22 vengono confrontati i parametri relativi ad una stazione di lavoro Communications Server che esegue APPC (advanced program-to-program communications) collegate ad un host mediante X.25.

Tabella 22 (Pagina 1 di 2). Riferimento incrociato parametri host/PC: APPC su una rete Token-Ring IBM che utilizza la rete X.25 su un host

NCP	Profilo/Parametri Communications Server	Osservazioni
LU NAME	Configura LU locale 6.2 **Nome LU locale** oppure: Configura nodo **Nome CP completo** (secondo campo)	
LOCADDR	Configura LU host **Indirizzo NAU**	Questi parametri ***devono*** avere lo stesso valore. Per le LU indipendenti, il VTAM consiglia la creazione di una definizione CDRSC oppure l'utilizzo di un operando DYNLU invece della codifica di LOCADDR=0. Per ulteriori informazioni sulla codifica delle definizioni CDRSC per le LU indipendenti, fare riferimento alla *VTAM Network Implementation Guide* Se viene utilizzata la SDDLU o la definizione dinamica per le LU indipendenti su VTAM 3.4 o versione successiva, non sono necessarie definizioni host per le LU dipendenti.
NETID APPL	Configura LU partner 6.2 **Nome LU partner**	
Tabella interpretazione VTAM	Configura LU partner 6.2 **Nome LU partner**	Solo per le LU dipendenti.
Tabella LOGMODE LOGMODE=	Configura modo **Nome modo**	Questi parametri ***devono*** corrispondere.

Tabella 22 (Pagina 2 di 2). Riferimento incrociato parametri host/PC: APPC su una rete Token-Ring IBM che utilizza la rete X.25 su un host

NCP	Profilo/Parametri Communications Server	Osservazioni
Tabella LOGMODE RUSIZES=	Configura modo **Dimensione massima RU** (256–32767)	Questi valori devono corrispondere.

Definizioni linea host AS/400

Le definizioni della linea host AS/400 includono la corrispondenza dei parametri del programma host OS/400 con i parametri Communications Server. La Tabella 23 contiene i parametri della linea SDLC.

Tabella 23. Riferimento incrociato parametri AS/400 Communications Server: Definizione linea programma host OS/400

OS/400	Profilo/Parametri Communications Server	Osservazioni
NRZI= Codifica dati	Configura collegamenti SDLC-WAC, SDLC-MPA, Porta COM **Codifica NRZI**	Communications Server utilizza USE_NRZI_ENCODING=0 e USE_NRZI_ENCODING=1. Questo parametro si trova solo su PCM per Modem di tipo: commutato sincrono, non commutato sincrono e AutoSync.
Scelta velocità del modem	Configura periferiche Porta COM **Configura modem**	I parametri su entrambi i sistemi per i tipi di collegamento modem, commutato asincrono, devono corrispondere.
Ampiezza massima segmento (MAXFRAME)	Configura periferiche SDLC-WAC, SDLC-MPA, Porta COM **Numero finestre ricezione** (1–30)	I valori non commutati asincroni non devono corrispondere.
Numero max segmenti in attesa (MAXOUT)	Configura periferiche SDLC-WAC, SDLC-MPA, Porta COM **Numero finestre ricezione** (1–30)	Il **Numero finestre ricezione** in Communications Server deve essere uguale al parametro MAXOUT sull'host AS/400.

Definizioni unità di controllo host AS/400

La definizione dell'unità di controllo host AS/400 include la corrispondenza dei parametri del programma host OS/400 con i parametri Communications Server.

La Tabella 24 a pagina 177 mostra i parametri del programma host OS/400.

Tabella 24. Riferimento incrociato parametri AS/400 Communications Server: Parametri unità di controllo

OS/400	Profilo/Parametri Communications Server	Osservazioni
Tipo collegamento: *SDLC	Tipo DLC SDLC-WAC, SDLC-MPA Porta COM	Il tipo di collegamento su entrambi i sistemi deve corrispondere. Questo parametro si trova sulla descrizione della linea ma è necessario includerlo per completezza.
Linea non commutata collegata	Configura periferiche SDLC-WAC, SDLC-MPA, Porta COM **Linea commutata**	Questo parametro si riferisce ai collegamenti non commutati. Questo valore deve corrispondere ad una definizione di linea host definita in precedenza.
Elenco linee commutate	(nessuno)	Questo parametro può essere applicato ai collegamenti commutati. Questo valore deve corrispondere ad una definizione di linea host definita in precedenza.
Ampiezza massima segmento	Configura periferiche SDLC-WAC, SDLC-MPA, Porta COM **Dimensione massima PIU** (265–4105)	Questi valori non devono corrispondere.
Identificativo rete remota	Configura nodo **Nome CP completo** (primo campo)	Questi valori devono corrispondere.
Nome punto di controllo remoto	Configura nodo **Nome CP completo** (secondo campo)	Questi valori devono corrispondere.
Funzione collegamento dati:	Configura collegamenti SDLC-WAC, SDLC-MPA, Porta COM **Ruolo stazione di collegamento**	I parametri su entrambi i sistemi sono complementari. Se il ruolo host è primario, la stazione di lavoro Communications Server deve essere configurata come secondaria o negoziabile. Se non viene utilizzato *MP (multipoint), è consigliabile impostare il ruolo del collegamento dati su *NEG (negoziabile).
Indirizzo stazione	Configura periferiche SDLC-WAC, SDLC-MPA, Porta COM **Indirizzo stazione di collegamento** (01–FE)	Questi valori devono corrispondere.
Supporto sessione APPN CP: (Sì/No)	Configura collegamenti SDLC-WAC, SDLC-MPA, Porta COM **Supporto APPN**	Questi parametri devono corrispondere se si desidera utilizzare sessioni CP-CP.
Tipo nodo APPN:	Configura collegamenti SDLC-WAC, SDLC-MPA, Porta COM **Tipo CP adiacente**	Questi valori devono corrispondere.

Definizioni unità host AS/400

L'host AS/400 può creare una definizione di dispositivo quando la stazione di lavoro Communications Server si collega senza una definizione di dispositivo definita in precedenza.

In Tabella 25 sono contenuti i parametri dell'unità del programma host OS/400.

Tabella 25. Riferimento incrociato parametri AS/400 Communications Server: Parametri dispositivo

OS/400	Profilo/Parametri Communications Server	Osservazioni
Nome ubicazione remota	Configura LU locale 6.2 **Nome LU locale** oppure: Configura nodo **Nome CP completo** (secondo campo)	Questi valori devono corrispondere.
Unità di controllo collegata	(nessuno)	Questo parametro si riferisce ai collegamenti non commutati. Questo valore deve corrispondere ad una definizione di linea host definita in precedenza.
Nome ubicazione locale		Utilizzare il valore predefinito fornito.
Identificativo rete remota	Configura nodo **Nome CP completo** (primo campo)	Utilizzare il valore predefinito fornito.
Modo	Configura modo **Nome modo**	Utilizzare il valore predefinito fornito.

Descrizione linea host AS/400 e Communications Server

La Tabella 26 contiene la descrizione della linea di programma host AS/400.

Tabella 26. Riferimento incrociato parametri host/PC: Descrizione linea

OS/400	Profilo/Parametri Communications Server	Osservazioni
Indirizzo adattatore locale:	Configura collegamenti **Indirizzo destinazione LAN**	I due indirizzi devono corrispondere per stabilire una comunicazione.

Descrizione unità di controllo host AS/400 e Communications Server

La Tabella 27 a pagina 179 contiene la descrizione dell'unità di controllo del programma host OS/400.

Tabella 27. Riferimento incrociato host/PC: Descrizione unità di controllo

OS/400	Profilo/Parametri Communications Server	Osservazioni
Linea commutata attiva	(nessuno)	Questo parametro si riferisce ai collegamenti non commutati. Questo valore deve corrispondere ad una definizione di linea host definita in precedenza.
Punto di controllo remoto	Configura nodo **Nome CP completo** (secondo campo)	I nomi devono corrispondere.
Identificativo rete remota	Configura nodo **Nome CP completo** (primo campo)	Utilizzare il valore predefinito oppure mettere in corrispondenza i parametri se differenti dall'ID della rete locale AS/400.
Descrizione unità di controllo modello		Questo parametro deve essere SI' se AS/400 utilizza una rete di collegamento.
ID rete di collegamento e nome CP rete di collegamento	Configura reti di collegamento **Nome rete di collegamento**	Questi valori devono corrispondere per tutti i nodi inclusi in una rete di collegamento.

Descrizioni dei biassiali AS/400

La Tabella 28 contiene la descrizione dei biassiali AS/400.

Tabella 28. Riferimento incrociato host/PC: Descrizione unità di controllo

AS/400	Profilo/Parametri Communications Server	Osservazioni
Linea non commutata collegata	(nessuno)	Questo parametro si riferisce ai collegamenti non commutati. Questo valore deve corrispondere ad una definizione di linea host definita in precedenza.
Punto di controllo remoto	Configura nodo **Nome CP completo** (secondo campo)	I nomi devono corrispondere.
Identificativo rete remota	Configura nodo **Nome CP completo** (primo campo)	Utilizzare il valore predefinito oppure mettere in corrispondenza i parametri se differenti dall'ID della rete locale AS/400.
Funzione collegamento dati=*SEC:	Configura collegamenti SDLC-WAC, SDLC-MPA Porta COM **Ruolo stazione di collegamento**	I parametri su entrambi i sistemi sono complementari. Se il ruolo host è primario, la stazione di lavoro Communications Server deve essere configurata come secondaria o negoziabile. Se non viene utilizzato *MP (multipoint), è consigliabile impostare il ruolo del collegamento dati su *NEG (negoziabile).

Definizioni linea host AS/400 (X.25)

Le definizioni della linea host AS/400 includono la corrispondenza dei parametri del programma host OS/400 con i parametri Communications Server. La Tabella 29 contiene i parametri della linea X.25.

Tabella 29. Riferimento incrociato parametri AS/400 Communications Server: Definizione linea programma host OS/400 (X.25)

OS/400	Profilo/Parametri Communications Server	Osservazioni
Indirizzo di rete locale	Configura periferiche **Indirizzo locale**	Entrambi gli indirizzi vengono generalmente stabiliti dal fornitore della rete.
Tipo di collegamento	Configura periferiche Porta X.25-COM X.25-WAC **Linea commutata**	Il tipo di collegamento su entrambi i sistemi deve corrispondere.
Supporto DCE X.25	N/A	Deve essere impostato su SI', se il collegamento tra i due sistemi è point-to-point e non passa attraverso una rete X.25.
Ampiezza massima segmento	Configura periferiche Porta X.25-COM X.25-WAC **Dimensione massima PIU**	Le dimensioni massime del frame su entrambi i sistemi devono corrispondere.
Dimensioni pacchetto assunte	Configura periferiche Porta X.25-COM X.25-WAC **Dimensioni pacchetto**	Questo valore viene stabilito dal fornitore della rete ed è identico per la trasmissione e la ricezione.
Dimensioni massime pacchetto	N/A	Questo valore viene stabilito dal fornitore della rete.
Modulo	Configura periferiche Porta X.25-COM X.25-WAC **Sequenza**	Questo valore viene stabilito dal fornitore della rete.
Dimensioni finestra assunte	Configura periferiche Porta X.25-COM X.25-WAC **Dimensioni finestra**	Questo valore viene stabilito dal fornitore della rete ed è identico per la trasmissione e la ricezione.
Inserimento indirizzo di rete	Configura periferiche Porta X.25-COM X.25-WAC	Questo valore viene stabilito dal fornitore della rete e deve essere identico per entrambi i sistemi.
Voci canale logico	Configura periferiche Porta X.25-COM X.25-WAC **Valori circuito virtuale**	Questi valori vengono stabiliti dal fornitore della rete e dal tipo di circuito virtuale X.25.

Definizioni unità di controllo host AS/400 (X.25 PVC)

La definizione dell'unità di controllo host AS/400 include la corrispondenza dei parametri del programma host OS/400 con i parametri Communications Server.

La Tabella 30 a pagina 181 mostra i parametri del programma host OS/400 per X.25 PVC.

Tabella 30. Riferimento incrociato parametri AS/400 Communications Server X.25 PVC: Parametri unità di controllo

OS/400	Profilo/Parametri Communications Server	Osservazioni
ID canale logico X.25	Configura collegamenti Porta COM-X.25, X.25-WAC **Numero canale logico**	Questi valori vengono stabiliti dal fornitore della rete.
Tipo collegamento: *X25	Configura collegamenti	I tipi di collegamento su entrambi i sistemi devono corrispondere.
Collegamento commutato: *NO		Tutti i PVC non sono commutati.
Ampiezza massima segmento	Configura periferiche Porta X.25-COM X.25-WAC **Dimensione massima PIU**	Non è necessario che i valori relativi alla dimensione massima del frame corrispondano.
Ruolo collegamento dati	Configura periferiche Porta X.25-COM X.25-WAC **Ruolo stazione di collegamento**	I parametri su entrambi i sistemi sono complementari. Se il ruolo host è primario la stazione di lavoro Communications Server deve essere configurata come secondaria o negoziabile.
Livello di rete X.25	Configura periferiche Porta X.25-COM X.25-WAC **Conformità CCITT**	Questi valori vengono stabiliti dal fornitore della rete.
Protocollo livello di collegamento X.25: *QLLC		Questo valore deve essere QLLC.

Definizioni unità di controllo host AS/400 (X.25 SVC)

La definizione dell'unità di controllo host AS/400 include la corrispondenza dei parametri del programma host OS/400 con i parametri Communications Server.

La Tabella 31 mostra i parametri del programma host OS/400 per X.25 SVC.

Tabella 31 (Pagina 1 di 2). Riferimento incrociato parametri AS/400 Communications Server X.25 SVC: Parametri unità di controllo

OS/400	Profilo/Parametri Communications Server	Osservazioni
Tipo collegamento: *X25	Configura collegamenti	I tipi di collegamento su entrambi i sistemi devono corrispondere.
Collegamento commutato: *SI'		Tutti gli SVC sono commutati.
Ampiezza massima segmento	Configura periferiche Porta X.25-COM X.25-WAC **Dimensione massima PIU**	Non è necessario che i valori relativi alla dimensione massima del frame corrispondano.
Numero collegamento	Configura periferiche Porta X.25-COM X.25-WAC **Indirizzo DTE locale**	Questo valore viene stabilito dal fornitore della rete.
Ruolo collegamento dati	Configura periferiche Porta X.25-COM X.25-WAC **Ruolo stazione di collegamento**	I parametri su entrambi i sistemi sono complementari. Se il ruolo host è primario la stazione di lavoro Communications Server deve essere configurata come secondaria o negoziabile.

Tabella 31 (Pagina 2 di 2). Riferimento incrociato parametri AS/400 Communications Server X.25 SVC: Parametri unità di controllo

OS/400	Profilo/Parametri Communications Server	Osservazioni
Livello di rete X.25	Configura periferiche Porta X.25-COM X.25-WAC **Conformità CCITT**	Questi valori vengono stabiliti dal fornitore della rete.
Protocollo livello di collegamento X.25: *QLLC		Questo valore deve essere QLLC.

AS/400 e Communications Server (X.25 PVC)

La Tabella 32 contiene i parametri della linea X.25.

Tabella 32. Riferimento incrociato AS/400 Communications Server: Collegamento PVC X.25

AS/400	Profilo/Parametri Communications Server	Osservazioni
ID canale logico X.25	Configura collegamenti Porta COM-X.25, X.25-WAC **Tipo collegamento**	I due parametri devono corrispondere alla sottoscrizione X.25. Questo campo AS/400 può essere trovato nella descrizione dell'unità di controllo. E' stata inclusa per una maggiore completezza.

Tabella 33. Riferimento incrociato parametri AS/400 Communications Manager: Descrizione unità di controllo

AS/400	Profilo Communications Manager/Parametri	Osservazioni
Nome punto di controllo remoto	Configura nodo **Nome CP completo** (secondo campo)	Questi valori devono corrispondere.
Tipo collegamento commutato		AS/400 non avvia il collegamento senza *DIAL.
Identificativo rete remota	Configura nodo **Nome CP completo** (primo campo)	Utilizzare il valore predefinito o mettere in corrispondenza i parametri se differenti dall'ID della rete locale AS/400.

Implementazione delle configurazioni Communicati

REFID='POST406'.

Di seguito è riportata una procedura suggerita per l'installazione e la configurazione del software per la rete:

1. Pianificazione dell'hardware.
2. Pianificazione delle applicazioni software.
3. Definizione delle convenzioni per la creazione dei nomi.
4. Definizione degli indirizzi di rete.
5. Selezione degli strumenti di configurazione ed installazione.
6. Definizione della configurazione maschera.
7. Creazione delle configurazioni ed installazione.
8. Creazione dei materiali per l'utente.
9. Gestione della rete.

In questo capitolo vengono fornite le informazioni necessarie per il completamento della procedura suggerita.

Introduzione

Una configurazione maschera definisce le informazioni sulla configurazione comuni ad un gruppo di server. E' possibile creare una o più configurazioni maschera. Ciascun file di configurazione del server viene avviato con la configurazione maschera e può contenere i pochi parametri necessari per la personalizzazione della configurazione in base al server. Ciò consente di eseguire una configurazione del server semplificata.

La configurazione maschera può essere utilizzata anche per specificare le opzioni di configurazione che non è possibile specificare utilizzando i file di risposta.

Per le informazioni sull'utilizzo dei file di risposta e dei file maschera per le operazioni di configurazione ed installazione, fare riferimento alla sezione “Configurazione con i file maschera e di risposta” a pagina 194.

Mentre si raccolgono informazioni nei passi riportati di seguito è necessario accumulare i totali per i requisiti RAM e di spazio su disco fisso per ciascuna stazione di lavoro. In questo modo, è possibile accertarsi di disporre dell'hardware necessario per consentire l'utilizzo del software scelto per gli utenti.

Passo 1. Pianificazione dell'hardware

Una volta stabilito che è possibile utilizzare i server esistenti, è necessario verificare che l'hardware esistente disponga di memoria e di spazio su disco fisso sufficienti. L'hardware esistente deve anche includere le unità di sistema e video, le stampanti, gli adattatori, i modem ed i cavi corretti per il software che si desidera installare.

Se si intende acquistare nuovi server, registrare l'hardware a disposizione sui fogli di lavoro preparati per gli utenti.

Memoria

Per i requisiti di memoria per Communications Server, fare riferimento alla *Guida operativa*.

Capacità di memoria

Durante la pianificazione dell'hardware per l'esecuzione di Communications Server, è importante stabilire come verrà utilizzato il server in termini di capacità ed i tipi di sessione che Communications Server supporterà. Tra queste sono incluse le sessioni TN3270E, le sessioni client API SNA e le sessioni SNA tradizionali per un host ed altre sessioni ancora. In base a questo numero, è possibile calcolare il carico medio sul server e stabilire la quantità di memoria corretta per il server.

Nota: Queste stime vanno aggiunte ai requisiti del sistema operativo di base (Windows NT Server) e a tutte le altre applicazioni simultaneamente in esecuzione sullo stesso sistema.

Utilizzare la seguente tabella per stabilire quale sarà il carico medio sul server:

Tabella 34. Capacità di memoria

Tipo di sessione client	Utilizzo della memoria per sessione
Gateway SNA (tradizionale)	29.9 KB
Client API SNA	25.2 KB
TN3270E	15.8 KB

Il consumo di memoria stimato per un Communications Server attivo in assenza di sessioni o collegamenti attivi è pari a 21 MB. Per ridurre al minimo la perdita di prestazioni, è consigliabile ridurre la quantità di paginazione eseguita (scambio dei segmenti di memoria con il disco). Provare a rendere disponibile nel sistema la quantità di memoria richiesta dal software in esecuzione, con ulteriori 5 - 10 MB come buffer. Ad esempio, un'installazione di Communications Server che supporta 1000 sessioni del client TN3270E richiede le seguenti quantità di memoria (basate sui valori indicati nella Tabella 34).

Sistema operativo Microsoft Windows NT Server	19.0 MB (valore stimato)
Communications Server per Windows NT	21.0 MB
Sessioni TN3270E (1 000 X 15.8 KB)	15.8 MB
Contingenza	10.0 MB
Memoria totale consigliata	65.8 MB

Nota: 65.8 MB non è una quantità di memoria obbligatoria per 1000 sessioni TN3270E. Questo valore è consigliato se si desidera ottenere le prestazioni migliori.

Velocità della CPU

Quando viene stabilita la velocità minima richiesta per il processore, è necessario conoscere il numero medio di transazioni che verranno elaborate dal server ogni minuto. Una transazione è costituita da qualsiasi scambio di informazioni tra il client e l'host mediante il server, sia che si tratti di aggiornamento del video che di una voce del database richiesta.

Quando viene calcolato il carico CPU medio, moltiplicare il numero medio di sessioni con il numero medio di transazioni al minuto per sessione ed il fattore di scala facendo riferimento alla seguente tabella (basata sul tipo di sessione).

Tipo di sessione client	Fattore di carico CPU (100 Mhz)	Fattore di carico CPU (166 Mhz)
Gateway SNA (tradizionale)	.004	.002
Client API SNA	.021	.011
TN3270E	.011	.006

Ad esempio, per supportare 1000 sessioni TN3270E simultanee, con una media di 6.7 transazioni al minuto, il carico medio della CPU a 166 Mhz è pari a 1000 X 6.7 X .006 oppure 40.2%. Le prestazioni si riducono rapidamente quando l'utilizzo della CPU è superiore all'80%. Una CPU più veloce migliora le prestazioni di Communications Server e del sistema e consente ad un numero maggiore di utenti e transazioni di utilizzare il server simultaneamente. Se Communications Server non supporta le velocità di CPU più elevate, si consiglia l'utilizzo di CPU a 100 Mhz.

Passo 2. Pianificazione delle applicazioni software

Le applicazioni software prevedono requisiti in aggiunta a quelli per Communications Server. Per ulteriori informazioni, fare riferimento alla documentazione relativa all'applicazione software.

Passo 3. Definizione delle convenzioni per la creazione dei nomi

Le reti create con Communications Server richiedono la creazione e l'utilizzo di numerosi nomi per i diversi oggetti presenti nella rete. Alcuni di questi nomi possono essere gli stessi da server a server, ma altri nomi devono essere univoci sulla rete per evitare conflitti tra i server che provano ad accedere alle risorse della rete.

Ad esempio, in due LAN possono essere definiti alcuni nomi di dominio identici. Finché queste LAN non vengono collegate, non si verifica nessun conflitto. Tuttavia, se esse vengono collegate successivamente ad una LAN backbone, si verifica un conflitto tra i nomi nella LAN.

Ciò significa che è necessario definire delle convenzioni per la creazione dei nomi. Tali convenzioni sono rappresentata da regole e standard utilizzati per l'assegnazione dei nomi alle diverse risorse di rete.

Le seguenti sezioni elencano le convenzioni per la creazione dei nomi che è necessario pianificare. Se si conoscono già le convenzioni per la creazione dei

nomi che verranno utilizzate nella pianificazione, registrarle durante la pianificazione della rete.

Criteri per la creazione dei nomi

Durante la definizione delle convenzioni per la creazione dei nomi, è necessario stabilire:

- I criteri da utilizzare per la creazione dei nomi e degli indirizzi per la rete
- Come si intende preservare la coerenza di questi nomi ed indirizzi e, laddove necessario, la loro univocità nella rete

Se si desidera collegare un server ad una rete del computer host, ad esempio, è possibile che la maggior parte dei nomi che è necessario utilizzare nella rete vengano scelti per l'utente dal personale host. In questo caso, per le unità fisiche e logiche richieste dall'host, è necessario registrare questi nomi per i file di configurazione del server.

Come altro esempio, è possibile scegliere di assegnare ai server della rete i nomi degli utenti che li utilizzano. Per una rete di piccole dimensioni, questa operazione può funzionare finché la quantità di nomi è limitata e si è in grado di preservarne l'univocità. Tuttavia, ciò non è possibile con le reti di grosse dimensioni in quanto i nomi degli utenti generalmente non sono univoci. E' necessario creare un'altra convenzione per la creazione dei nomi delle stazioni di lavoro di una rete di grosse dimensioni.

Qualsiasi criterio venga scelto per l'assegnazione dei nomi, accertarsi di registrarlo in modo da poter fare riferimento alle informazioni appropriate ogni volta che vengono aggiunte nuove risorse alla rete.

Tipi di nomi e restrizioni

La maggior parte dei nomi devono essere univoci all'interno della rete in cui essi vengono utilizzati. Nelle seguenti sezioni vengono elencati i tipi di nomi che potrebbero essere rilevati durante le pianificazione dell'installazione e della configurazione di una rete. E' necessario esaminare questi nomi prima di iniziare la pianificazione della rete in modo da acquisire familiarità con essi.

Per ciascun nome vengono fornite le seguenti informazioni:

- Una definizione
- La necessità o meno di preservare l'univocità del nome nella rete
- Restrizioni sulla creazione dei nomi

Nomi utilizzati da più di un componente

I nomi utilizzati da più di un componente sono:

- Id di rete
- Password
- ID utente
- Nomi NAU (Network addressable unit)

Id i rete: Gli ID di rete sono nomi assegnati alle reti e vengono utilizzati da tutti i server e da tutte le stazioni di lavoro (nodi) nella rete specifica per conservare un'identità univoca in tutte le reti collegate. L'ID di rete viene utilizzato anche nelle registrazioni degli errori e nelle segnalazioni della gestione rete associate agli errori del sistema di rete.

E' possibile considerare la rete in due modi differenti. Il primo è quello di considerarla come una rete fisica costituita da un “ring” in un ambiente token-ring o da una “stringa” in un ambiente di rete PC o Ethernet. Il secondo è quello di considerarla come una rete logica che potrebbe non essere identica alla rete fisica. Due o più reti fisiche (ad esempio, due token ring ed una stringa Ethernet) possono essere collegate allo scopo di mantenerle nella stessa rete logica.

Gli ID di rete sono univoci tra le reti logiche; in caso contrario, le reti sarebbero logicamente la stessa rete. In una rete logica, i nomi LU devono essere univoci per evitare conflitti tra i nomi. Tra reti logiche, l'ID di rete garantisce nomi univoci. Un nome LU può essere identico su due reti logiche; tuttavia, l'ID di rete per ciascuna rete logica rende univoci i nomi LU completi. Anche se le reti non sono correntemente collegate, gli ID di rete devono essere univoci se si pianifica di collegare le reti successivamente.

E' necessario registrare gli ID di rete presso l'IBM. In questo modo ci si accerta che le reti SNA possano essere interconnesse successivamente senza provocare alcun conflitto di indirizzi. Per ulteriori informazioni sulla registrazione degli ID di rete, rivolgersi ad un rivenditore IBM.

Di seguito sono riportate le restrizioni relative agli ID di rete:

- **Lunghezza**: Da 1 a 8 caratteri
- **Caratteri consentiti**: Da A a Z, da 0 a 9, $, @, #

Password: Le password sono funzioni di sicurezza richieste da applicazioni e servizi configurati in modo appropriato che consentono di proteggere i dati e limitare l'accesso alle risorse.

Le password non devono essere univoche all'interno delle rete. Esse sono specifiche per l'utente.

Di seguito sono riportate le restrizioni relative alle password LU-LU:

- **Lunghezza**: Da 1 a 8 caratteri
- **Caratteri consentiti**: Qualsiasi stringa esadecimale

Di seguito sono riportate le restrizioni relative alle altre password, come quelle per i collegamenti CPI-C ed AS/400:

- **Lunghezza**: Da 1 a 10 caratteri
- **Caratteri consentiti**: Qualsiasi stringa ASCII

ID utente: Gli ID utente sono nomi di identificazione univoci che vengono assegnati agli utenti delle risorse di rete in modo da fornire loro accesso al database, alla LAN o alle risorse host che dispongono di emulazione.

Gli ID utente devono essere univoci nella rete.

Di seguito sono riportate le restrizioni relative agli ID utente:

- **Lunghezza**: Da 1 a 8 caratteri
- **Caratteri consentiti**: A - Z, a - z, 0 - 9, $, @, #

Nomi NEU (Network Addressable Unit)

I tipi di nome che è necessario specificare in Communications Server sono:

- Nomi CP (nomi di nodo locale)
- Nomi LU

Nomi CP (nomi di nodo locale): Il CP (control point) è responsabile della gestione del nodo e delle relative risorse. In un nodo finale APPN il CP deve comunicare con il CP presente in un nodo di rete adiacente per ottenere i servizi di rete APPN. In un nodo di rete APPN, il CP deve comunicare con i CP presenti nei nodi di rete adiacenti per gestire la rete. Il CP gestisce funzioni come attivazione e disattivazione dell'adattatore, attivazione e disattivazione del collegamento ed assiste le LU nelle fasi di avvio e chiusura delle sessioni.

Il nome CP rappresenta la seconda metà del nome CP completo nella definizione NODO di Communications Server.

I nomi CP devono essere univoci all'interno di una rete. Tuttavia, un nodo può avere più nomi PU che vengono definiti nella definizione di collegamento (**LINK_STATION**) e scambiati su XID3 con host differenti. Questi nomi PU multipli devono essere univoci all'interno del nodo e nell'host in fase di collegamento.

PU e CP non sono identici nella subarea VTAM. Un nome PU per ciascun nodo periferico in un dominio VTAM viene definito nel VTAM e rappresenta il modo in cui VTAM considera i nodi periferici. I nodi periferici non riconoscono i nomi PU nel VTAM ovvero, il VTAM non inoltra i nomi PU ai nodi periferici. Se si desidera che il nome PU in un nodo periferico sia identico a quello definito nel VTAM, è necessario coordinare questa operazione. Si consiglia di eseguirla anche se non è necessaria per l'SNA.

Per il VTAM, il CP è una LU utilizzata per l'attivazione delle sessioni LU 6.2 tra il CP ed una LU VTAM (ad esempio, CICS). Il nome CP definito nel nodo periferico deve corrispondere ad una definizione LU nel VTAM se il VTAM avvia le sessioni LU 6.2 nel CP. In caso contrario, il VTAM apprende il nome CP quando il nome periferico avvia una sessione in una LU VTAM.

Per Communications Server, il nome CP (senza includere l'ID di rete) viene considerato come nome CP del nodo locale e nome PU. Il solo flusso che contiene il nome PU del nodo periferico è una segnalazione. Tuttavia, quando Communications Server (APPC/APPN) invia una segnalazione, esso include il nome CP (il tipo di risorsa è CP) nella segnalazione e non un nome PU. Se i programmi di emulazione inviano un nome PU nelle segnalazioni, il nome è identico al nome CP (perché Communications Server utilizza il nome CP come nome PU del nodo). Il focal point host può essere definito solo su un collegamento in cui il nome PU è identico al nome CP. Inoltre, i collegamenti host con un nome PU diverso dal nome CP non possono disporre di sessioni CP-CP con l'host oppure instradare il traffico APPN sul collegamento. Tutte le segnalazioni includono il nome CP anche se la segnalazione è provocata da una condizione verificatasi in un collegamento che utilizza un altro PU.

Di seguito sono riportate le restrizioni relative ai nomi di nodo locale:

- **Lunghezza**: Da 1 a 8 caratteri
- **Caratteri consentiti**: A - Z, 0 - 9, $, @, #
- **Primo carattere**: A - Z, $, @, #

Nomi LU (Logical Unit): I nomi LU (logical unit) sono nomi assegnati ad entità logiche SNA in un nodo, che forniscono funzioni di supporto per l'elaborazione delle transazioni. Questa consente loro di comunicare con altre LU nella rete, incluse le applicazioni host.

Di seguito sono riportate le restrizioni relative ai nomi LU:

- **Lunghezza**: Da 1 a 8 caratteri
- **Caratteri consentiti**: A - Z, 0 - 9, $, @, #

Nomi LU Socket su SNA: Per una corretta inizializzazione, è necessario che il gateway Socket su SNA disponga di un nome LU configurato per il gateway. Il gateway Socket su SNA definisce dinamicamente il nome LU configurato in Communications Server all'inizializzazione.

Utilizzando una convenzione predefinita per la creazione dei nomi per la LU Socket su SNA, i nomi consentono di:

- Controllare quali nomi rappresentano LU del gateway Socket su SNA e quali nomi rappresentano altre LU nella rete.
- Analizzare e risolvere tutti gli errori di mappatura e di instradamento nel caso in cui questi si verifichino.
- Abilitare la mappatura algoritmica da utilizzare durante la mappatura degli indirizzi IP con i nomi LU Socket su SNA.

Per ulteriori informazioni sulla mappatura degli indirizzi IP con i nomi LU, consultare la sezione “Configurazione di Socket AnyNet su SNA” a pagina 86.

Passo 4. Definizione degli indirizzi di rete

Verificare la coerenza ed univocità degli indirizzi presenti nella rete. Ciascun indirizzo deve essere univoco. Gli indirizzi che vengono definiti dipendono da come viene configurata la rete. Le seguenti sezioni descrivono gli indirizzi per:

- LAN
- SDLC
- X.25

Registrare gli indirizzi utilizzati per accertarsi, laddove necessario, che gli indirizzi non entrino in conflitto e che rispettino le convenzioni scelte per la creazione dei nomi.

Indirizzi dell'adattatore LAN

Gli indirizzi dell'adattatore LAN sono numeri esadecimali a 12 caratteri codificati nell'adattatore dal produttore (indirizzo gestito a livello universale) oppure assegnati dal responsabile di rete (indirizzo gestito a livello locale). Ciascun adattatore di rete nella stazione di lavoro che si sta configurando per le comunicazioni LAN deve disporre di un indirizzo univoco.

E' possibile utilizzare gli indirizzi gestiti a livello universale, anche definiti “indirizzi cablati”, per gli adattatori di rete oppure assegnare gli indirizzi gestiti a livello locale. Gli indirizzi dell'adattatore LAN devono essere univoci all'interno della rete. Se vengono utilizzati indirizzi gestiti a livello locale, verificare che gli indirizzi siano univoci nella rete.

Gli indirizzi gestiti a livello locale sono piuttosto vantaggiosi nel caso in cui si verifichi un malfunzionamento dell'adattatore che richiede la sostituzione di quest'ultimo. E' possibile trasferire l'indirizzo esistente nell'adattatore sostitutivo ed evitare di modificare le configurazioni che fanno riferimento a questo indirizzo. Se vengono utilizzati indirizzi gestiti a livello universale, è necessario modificare l'indirizzo dell'adattatore di rete per tutte le stazioni di lavoro che accedono all'adattatore malfunzionante.

Di seguito sono riportate le restrizioni relative alla configurazione degli indirizzi dell'adattatore LAN:

- **Lunghezza**: 12 caratteri
- **Caratteri consentiti**: A, B, C, D, E, F, 0-9
- **Intervallo**: da X'400000000000' a X'7FFF FFFF FFFF'

Sulla LAN, è possibile scegliere di utilizzare gli indirizzi dell'adattatore LAN gestiti a livello locale. In questo modo, vengono assegnati numeri esadecimali come gli indirizzi dell'adattatore LAN a ciascun adattatore LAN invece di utilizzare gli indirizzi universali dell'adattatore LAN creati negli adattatori LAN. E' possibile decidere di utilizzare una convenzione con i seguenti criteri:

- Le prime 4 cifre sono sempre X'4000'
- Le 3 cifre successive sono sempre X'268' per rappresentare il proprio reparto
- Le cifre finali sono comprese nell'intervallo da X'01000' a X'FFFFF' per rappresentare le stazioni di lavoro individuali della rete

Gli indirizzi gestiti a livello universale su Ethernet sono nel formato Ethernet. E' possibile specificare il tipo di formato (Ethernet o Token-ring) quando vengono utilizzati indirizzi gestiti a livello locale. Durante la configurazione dell'indirizzo di destinazione nei collegamenti SNA, verificare che il formato dell'indirizzo sia identico a quello specificato nella stazione remota. Con il bridge, è possibile essere su un token-ring a livello locale e avere la stazione remota su un Ethernet ed utilizzare un indirizzo di formato Ethernet (con scambio di byte).

Indirizzi di stazione secondaria SDLC

Gli indirizzi di stazione vengono utilizzati per identificare una stazione secondaria nella rete.

Gli indirizzi della stazione secondaria devono essere univoci nella rete. La stazione primaria comunica con una stazione secondaria utilizzando l'indirizzo della stazione secondaria. La stazione secondaria comunica con quella primaria utilizzando il proprio indirizzo.

Per i collegamenti tra punti, se la stazione secondaria supporta l'indirizzo di trasmissione X'FF', la stazione primaria riconoscerà l'indirizzo secondario remoto. La stazione secondaria può specificare qualsiasi valore compreso tra X'01' e X'FE'.

Per le stazioni primarie che non supportano l'indirizzo di trasmissione, la stazione secondaria deve essere impostata sullo stesso valore definito nella stazione primaria. Il valore deve essere compreso tra X'01' e X'FE'.

Nota: La maggior parte delle stazioni supportano l'indirizzo di trasmissione, per cui l'indirizzo della stazione secondaria nella stazione primaria deve utilizzare il valore X'FF'.

Le stazioni negoziabili dispongono di indirizzi di stazione secondaria locale configurati tra X'01' e X'FE'. Viene utilizzato l'indirizzo secondario della stazione negoziata con quella secondaria.

Per le stazioni secondarie su un collegamento a più punti, l'indirizzo deve corrispondere al valore specificato nel nodo che fornisce la funzione del server primario a più punti. L'indirizzo sarà compreso nell'intervallo tra X'01' e X'FE'.

Indirizzi X.25

Gli indirizzi X.25 vengono utilizzati per identificare le risorse che comunicano con le reti X.25. Le reti X.25 implementano la raccomandazione CCITT che definisce l'interfaccia tra DTE (data terminal equipment) e PSDN (packet-switching data network). Gli indirizzi X.25 devono essere univoci all'interno di una rete. Questi indirizzi sono disponibili presso il fornitore della rete X.25.

Indirizzi Internet

Gli indirizzi IP (Internet Protocol) vengono utilizzati per instradare i dati nella rete. A ciascun host TCP/IP viene assegnato almeno un indirizzi IP univoco. L'indirizzo IP assegnato all'host non definisce un host nella rete ma piuttosto un'interfaccia per una rete.

Un nodo Communications Server deve disporre di un indirizzo IP univoco per ciascuna interfaccia di rete che instrada dati TCP/IP nel nodo. Ad esempio, un nodo Communications Server che instrada il traffico TCP/IP su una rete SNA (utilizzando la funzione del gateway Socket su SNA) necessita di indirizzi IP univoci sia per la rete SNA che per la rete TCP/IP. L'indirizzo IP dell'interfaccia TCP/IP identifica il collegamento del gateway Socket su SNA alla rete IP, mentre l'indirizzo IP identifica il collegamento alla rete SNA, che appare al sistema come una rete TCP/IP "virtuale".

Un indirizzo IP è costituito da un campo a 32 bit distinto in 2 parti:

- La prima parte del campo indirizzo contiene l'indirizzo di rete; la seconda parte contiene l'indirizzo host.
- Il numero di bit utilizzati per le porzioni rete e host di un indirizzo IP è variabile e dipende dalla classe di indirizzi dell'indirizzo IP.
- Una maschera di rete consente l'utilizzo di una parte della porzione host dell'indirizzo IP come indirizzo di sottorete.

La classe degli indirizzi IP viene stabilita dalla lettura dei primi 3 bit superiori dell'indirizzo. Come mostrato nella Tabella 35, Communications Server supporta le classi di indirizzi A, B e C. Per ulteriori informazioni, fare riferimento alla *Guide to Sockets over SNA*.

Tabella 35. Classi di indirizzi IP supportate da Communications Server

Classe di indir.	Maschera di rete predefinita	Distribuzione di bit per indirizzi di rete e host	Per un indirizzi IP decimale con punti nel formato *a.b.c.d*, l'intervallo dei valori per *a* è:
A	255.0.0.0	indirizzo di rete a 8 bit; indirizzo host a 24 bit	1–127 Ad esempio, 9.0.0.0 è un indirizzo di rete IP di Classe A.
B	255.255.0.0	indirizzo di rete a 16 bit; indirizzo host a 16 bit	128–191 Ad esempio, 132.11.0.0 è un indirizzo di rete IP di Classe B.
C	255.255.255.0	indirizzo di rete a 24 bit; indirizzo host a 8 bit	192–223 Ad esempio, 220.11.44.0 è un indirizzo di rete IP di Classe C.

Passo 5. Selezione degli strumenti di configurazione e di installazione

Communications Server utilizza gli strumenti di configurazione illustrati nelle seguenti sezioni. Per ulteriori informazioni sull'utilizzo di questi strumenti, fare riferimento al manuale *Guida operativa*.

Applicazione Configurazione nodo

L'applicazione **Configurazione nodo** è un'applicazione grafica che consente di gestire le informazioni sulla configurazione SNA. Tale applicazione utilizza una vista ad albero per organizzare i dati di configurazione SNA in modo da mostrare le relazioni tra le definizioni. L'utente viene assistito durante la creazione di una configurazione mediante un elenco di attività integrate, il *Supporto didattico* in linea e la guida contestuale. L'applicazione è responsabile della creazione dei file di configurazione per l'utente e della verifica dei dati forniti.

Configurazione remota

L'applicazione **Configurazione nodo** può essere utilizzata anche per collegarsi ad un Communications Server remoto e configurare direttamente le risorse. L'utente può gestire in remoto la configurazione di un Communications Server da qualsiasi parte della rete.

Un client per la gestione remota installa solo le applicazioni di gestione su un client, inclusa l'applicazione **Configurazione nodo**. Da questo client, un utente può eseguire operazioni complete di gestione e configurazione di qualsiasi Communications Server presente nella rete.

I client per la gestione remota di Windows 95 e Windows NT utilizzano la sicurezza del dominio Windows NT per l'autenticazione del collegamento client al server senza immettere nuovamente l'ID utente e la password. Il client deve appartenere ad un dominio Windows NT, partecipando ad un dominio Communications Server oppure eseguendo il collegamento in locale con una password ed un ID utente sincronizzati.

Agli utenti del client per la gestione remota, esterni al dominio Windows NT, viene richiesto di fornire l'ID utente e la password, mediante una richiesta oppure memorizzando questi valori nel file di configurazione del client.

Gli utenti autorizzati all'utilizzo dei client di gestione remota vengono memorizzati nel gruppo locale IBMCSADMIN, che si trova in Communications Server o nell'unità di controllo del dominio a cui appartiene Communications Server. Tale gruppo di utenti viene creato durante l'installazione e può essere gestito utilizzando l'applicazione User Manager di Windows NT. Per eseguire il collegamento in locale al server, è necessario assegnare diritti di utente agli utenti del client per la gestione remota nel gruppo IBMCSADMIN.

File di configurazione ASCII

L'applicazione **Configurazione nodo** di Communications Server memorizza i dati di configurazione in un file di configurazione ASCII che l'utente può leggere. Ciò consente all'utente di modificare i file di configurazione senza utilizzare **Configurazione nodo**. Per ulteriori informazioni su questo file e sulla relativa sintassi, fare riferimento a *Configuration File Reference*. Utilizzando questo file, un responsabile di rete può apportare rapidamente delle modifiche alla configurazione utilizzando attività automatiche come l'esecuzione di script o i servizi di

Gestione Web

La gestione Web consente ad un utente di modificare un file di configurazione di Communications Server caricandolo in una finestra di editazione. Le modifiche vengono inviate al server, verificate e salvate per un uso immediato. L'utente può arrestare e riavviare il server utilizzando le modifiche apportate oppure applicare le modifiche apportate alla configurazione ad un sistema in esecuzione.

Configurazione con i file maschera e di risposta

I file maschera e di risposta di Communications Server consentono la creazione o la modifica di una configurazione mediante un editor. E' possibile configurare tutte le parole chiave ed i parametri di configurazione di Communications Server con i file di risposta. I file maschera e di risposta hanno lo stesso formato dei file di configurazione di Communication Server (.ACG).

Nota: Il formato dei file .ACG è documentato nel file OCDNTS50.DAT contenuto nella directory di installazione di Communications Server (ad esempio, C:\IBMCS). Per ulteriori informazioni sulle parole chiave e sui parametri utilizzati nei file .ACG, fare riferimento a *Configuration File Reference*.

I file maschera possono semplificare la distribuzione di massa delle configurazioni ai server remoti. Un file maschera può specificare le parole chiave comuni a diversi server. Ad esempio, se è necessario configurare più server come gateway SNA con un supporto client implicito, molte parole chiave saranno identiche. E' possibile creare un file maschera di configurazione in cui sono riportate queste parole chiave comuni.You can create template files for each configuration with a set of common keywords.

Inoltre, è possibile utilizzare i file di risposta per aggiungere, modificare o cancellare le parole chiave in un file maschera. Il file maschera di configurazione originale rimane invariato. Un file di risposta viene unito ad un file maschera specificando la parola chiave INCLUDE alla fine del file maschera. Ad esempio, se un file di risposta viene chiamato *myconfig.rsp*, l'ultima riga del file maschera che utilizzerà il file di risposta sarà `INCLUDE = myconfig.rsp`. Quando il file maschera ed il file di risposta vengono uniti, è possibile assegnare al file di configurazione ottenuto un nome con l'estensione .ACG in modo da distinguerlo dagli altri file .ACG.

Quando delle configurazioni vengono create mediante l'utilizzo dei file maschera e di risposta, il programma di utilità per la verifica ricerca le directory secondo il seguente ordine:

1. La directory locale da cui si sta richiamando il programma di utilità per la verifica
2. La sottodirectory PRIVATE nella directory di installazione di Communications Server.

Per accertarsi che il programma di utilità per la verifica possa individuare i file maschera e di risposta, è necessario memorizzarli nella sottodirectory PRIVATE. La sottodirectory PRIVATE si trova anche dove sono memorizzati i file di configurazione (.ACG).

Campi chiave

Il campo chiave è il parametro in una parola chiave che denomina la parola chiave e la distingue in modo univoco da altre parole chiave dello stesso tipo. Il parametro @KEY_NAME specifica il campo chiave per la parola chiave.

Il campo chiave è sempre il primo parametro in una parola chiave che contiene un campo chiave (ad esempio, **MODE_NAME** nella parola chiave **MODE**).

Alcune parole chiave non dispongono di campi chiave perché possono essere specificate una sola volta in un file di configurazione. Un esempio di parola chiave che è possibile specificare una sola volta è la parola chiave **TN3270E_DEF**.

Aggiunta di parole chiave ad un file maschera

Quando il file di risposta viene utilizzato per aggiungere una nuova definizione di parola chiave, è necessario fornire tutta la parola chiave. Il campo chiave deve essere fornito con un valore univoco. Se dalla parola chiave vengono omessi dei sottocampi, vengono utilizzati i valori predefiniti relativi a questi campi. Ad esempio, per aggiungere una parola chiave **MODE** alla configurazione, il file di risposta può contenere la seguente parola chiave:

```
MODE=(
     MODE_NAME=MYMODE
     COS_NAME=#INTER
     CRYPTOGRAPHY=NONE
     DEFAULT_RU_SIZE=1
     MAX_NEGOTIABLE_SESSION_LIMIT=8192
     MAX_RU_SIZE_UPPER_BOUND=4096
     MIN_CONWINNERS_SOURCE=4096
)
```

Il base al contenuto del file di risposta si assume che nella maschera non esiste una parola chiave **MODE** con il parametro `MODE_NAME=MYMODE`. Se tale parola chiave esiste, i parametri vengono aggiornati con i valori forniti nel file di risposta.

Se il parametro `MODE_NAME` è stato omesso dal file di risposta, viene generato un errore durante la verifica della configurazione poiché non è stato possibile identificare in modo univoco il parametro `MODE_NAME`. Nel file di risposta non sono stati specificati tutti i parametri disponibili per la parola chiave **MODE**. I restanti parametri utilizzano i valori predefiniti assegnati dal file OCDSNT50.DAT. Tale aggiunta alla configurazione assumerebbe il seguente aspetto:

```
MODE=(
     MODE_NAME=MYMODE
     AUTO_ACT=0
     COMPRESSION=PROHIBITED
     COS_NAME=#INTER
     CRYPTOGRAPHY=NONE
     DEFAULT_RU_SIZE=1
     MAX_NEGOTIABLE_SESSION_LIMIT=8192
     MAX_RU_SIZE_UPPER_BOUND=4096
     MIN_CONWINNERS_SOURCE=4096
     PLU_MODE_SESSION_LIMIT=8192
     RECEIVE_PACING_WINDOW=20
)
```

Modifica di una parola chiave in un file maschera

Quando il file di risposta viene utilizzato per modificare la definizione di una parola chiave esistente, la parola chiave di origin5e deve essere presente nel file maschera. Se non è presente nel file maschera, il file di risposta aggiunge una voce alla nuova configurazione. Il parametro chiave deve essere specificato nel file di risposta per identificare la parola chiave di destinazione. Nella parola chiave del file maschera vengono aggiornati solo i parametri specificati nella parola chiave del file di risposta. I parametri non specificati nel file di risposta restano invariati. Ad esempio, se nel file maschera è presente la seguente parola chiave **MODE**:

```
MODE=(
     MODE_NAME=#INTER
     AUTO_ACT=0
     COMPRESSION=PROHIBITED
     COS_NAME=#INTER
     CRYPTOGRAPHY=NONE
     DEFAULT_RU_SIZE=1
     MAX_NEGOTIABLE_SESSION_LIMIT=8192
     MAX_RU_SIZE_UPPER_BOUND=4096
     MIN_CONWINNERS_SOURCE=4096
     PLU_MODE_SESSION_LIMIT=8192
     RECEIVE_PACING_WINDOW=20 )
```

e la seguente parola chiave è specificata nel file di risposta:

```
MODE=(
     MODE_NAME=#INTER
     AUTO_ACT=10
)
```

la configurazione ottenuta avrebbe la seguente definizione per la parola chiave **MODE**:

```
MODE=(
     MODE_NAME=#INTER
     AUTO_ACT=10
     COMPRESSION=PROHIBITED
     COS_NAME=#INTER
     CRYPTOGRAPHY=NONE
     DEFAULT_RU_SIZE=1
     MAX_NEGOTIABLE_SESSION_LIMIT=8192
     MAX_RU_SIZE_UPPER_BOUND=4096
     MIN_CONWINNERS_SOURCE=4096
     PLU_MODE_SESSION_LIMIT=8192
     RECEIVE_PACING_WINDOW=20
)
```

Cancellazione di una parola chiave da un file maschera

Quando il file di risposta viene utilizzato per cancellare una parola chiave dalla maschera, è necessario specificare il parametro ed il valore che identificano la parola chiave, insieme con la parola chiave `DELETE`. Ad esempio, se il file maschera specifica la seguente parola chiave:

```
MODE=(
     MODE_NAME=#INTER
     AUTO_ACT=0
     COMPRESSION=PROHIBITED
     COS_NAME=#INTER
     CRYPTOGRAPHY=NONE
     DEFAULT_RU_SIZE=1
     MAX_NEGOTIABLE_SESSION_LIMIT=8192
     MAX_RU_SIZE_UPPER_BOUND=4096
     MIN_CONWINNERS_SOURCE=4096
     PLU_MODE_SESSION_LIMIT=8192
     RECEIVE_PACING_WINDOW=20
)
```

ed il file di risposta contiene la seguente parola chiave:

```
MODE=(
     MODE_NAME=#INTER
            DELETE
)
```

la configurazione ottenuta non contiene la definizione del modo `#INTER`.

La parola chiave **DELETE** può trovarsi dopo una specifica *parameter=value* o su una riga, prima o dopo del parametro. Ad esempio, sono validi i seguenti utilizzi della parola chiave **DELETE**:

```
MODE=(
     MODE_NAME=#INTER
            DELETE
)
MODE=(
            DELETE
     MODE_NAME=#INTER
)
MODE=(
     MODE_NAME=#INTER DELETE
)
```

La parola chiave **DELETE non** può trovarsi davanti ad una specifica *parameter=value* sulla stessa riga. Ad esempio, non è valido il seguente utilizzo della parola chiave **DELETE**:

```
MODE=(
     DELETE MODE_NAME=#INTER
)
```

Per cancellare tutte le parole chiave di un particolare tipo oppure per cancellare una parola chiave che non dispone di un campo chiave, sono necessari solo la parola chiave e la parola chiave **DELETE**. Ad esempio,

```
TN3270E_DEF=(
            DELETE
)
```

Passo 6. Scelta delle funzioni di Communications Server

Di seguito vengono descritte le funzioni supportate per Communications Server. E' possibile che alcune o tutte queste funzioni siano supportate per il tipo di collegamento in uso:

Configurazione gateway SNA Configurando un gateway SNA, è possibile scambiare dati tra stazioni di lavoro client downstream ed un computer host mainframe SNA (Systems Network Architecture). Il gateway esegue una funzione di concentratore, che rende disponibili le risorse LU di uno o più host e le PU host alle stazioni di lavoro client SNA downstream, su qualsiasi supporto di comunicazione supportato da Communications Server.

Configurazione server TN3270E Configurando un server TN3270E, è possibile scambiare dati tra stazioni di lavoro client TCP/IP downstream che eseguono applicazioni TN3270E (o TN3270) ed un computer host mainframe SNA (Systems Network Architecture). Il server esegue una funzione di concentratore che rende disponibili le risorse LU di uno o più host e le PU host alle sessioni TN3270E (o TN3270) downstream, su qualsiasi supporto di comunicazione supportato da Communications Server.

Configurazione server TN5250 Configurando un server TN5250, è possibile scambiare dati tra stazioni di lavoro client downstream su una rete TCP/IP che esegue applicazioni TN5250 ed una stazione AS/400 su una rete SNA. Il server esegue la funzione di gateway che rende disponibili le sessioni video AS/400 ai client TN5250 downstream, su qualsiasi supporto di comunicazione supportato da Communications Server.

Configurazione nodo di rete APPN I nodi di rete sono responsabili della gestione e dell'instradamento delle informazioni in una rete APPN. Essi gestiscono una directory contenente tutte le risorse (LU) disponibili su nodi finali collegati direttamente e gestisce una topologia di tutti i nodi di rete presenti nella rete APPN. Quando un nodo presente nella rete richiede una sessione LU 6.2 indipendente, il nodo di rete è responsabile dell'individuazione della risorsa remota richiesta dalla sessione e dell'apertura e dell'instradamento della sessione tra i due nodi.

Configurazione DLUR/DLUS Communications Server supporta le sessioni LU dipendente sulle reti APPN. Per questo motivo è necessario che Communications Server funzioni come un DLUR (dependent LU requester), che richiede i servizi di instradamento di un DLUS (dependent LU server) che risiede su un host.

Communications Server supporta il DLUR per i dispositivi e le sessioni locali e per i dispositivi e le sessioni downstream. In entrambi i casi, il nodo locale deve essere configurato in modo da essere collegato in una rete APPN.

Configurazione gateway SNA AnyNet su TCP/IP Il gateway SNA su TCP/IP instrada il traffico SNA (LU 6.2 indipendente) tra reti TCP/IP ed SNA. Il gateway SNA su TCP/IP, ad esempio, consente alle applicazioni APPC o CPI-C in esecuzione su un altro nodo di accesso SNA AnyNet su TCP/IP di comunicare con nodi peer SNA su una rete SNA.

Il gateway SNA AnyNet su TCP/IP deve essere configurato come nodo di rete APPN. Ciò consente l'instradamento delle sessioni APPC nei nodi peer SNA appropriati.

Configurazione Socket AnyNet su SNA Sono disponibili due tipi di nodi Socket AnyNet su SNA: nodi di accesso e nodi gateway. I nodi di accesso consentono l'esecuzione in locale delle applicazioni socket TCP/IP e la relativa comunicazione con altri gateway o nodi di accesso presenti in qualche posto nella rete SNA. Il gateway Socket AnyNet su SNA ha le funzioni di un programma di conversione dei protocolli, che consente la comunicazione delle applicazioni di una rete TCP/IP con le applicazioni socket in esecuzione su un nodo di accesso presente nella rete SNA. Utilizzando due gateway, è possibile collegare reti TCP/IP separate su una rete SNA.

Configurazione client API SNA I client API SNA sono macchine separate da Communications Server che possono eseguire applicazioni SNA durante l'utilizzo del codice SNA su un nodo di Communications Server per la gestione effettiva della sessione. Communications Server semplicemente stabilisce e gestisce una sessione come se l'origine fosse il nodo locale, ma inoltra i dati applicativi al client API SNA invece che alle proprie API applicative.

I client API SNA consentono di eseguire le applicazioni SNA senza dover installare uno stack per le comunicazioni SNA, come Communications Server per Windows NT, sulla stessa macchina. In questo modo è possibile utilizzare macchine meno potenti per l'esecuzione delle applicazioni SNA mentre una macchina centrale più potente può essere utilizzato come server SNA per questi client API SNA.

I client API SNA supportano due tipi di applicazioni: applicazioni APPC (LU 6.2 indipendente) ed applicazioni API LUA, come i programmi di emulazione 3270.

Configurazione CPI-C o APPC Communications Server supporta applicazioni CPI-C o APPC (ad esempio, programma di emulazione APPC3270 o 5250 per un sistema AS/400). La rete APPC è molto flessibile e versatile e può essere complicata. La complessità della configurazione dipende da come verrà utilizzato Communications Server e da quanto lavoro dovrà essere svolto dall'applicazione.

Sessioni LU 6.2 dipendente per un host Communications Server supporta le sessioni LU 6.2 dipendente con una PU host.

Configurazione 3270 Communications Server supporta le sessioni 3270 con un host.

Configurazione focal point Communications Server supporta ubicazioni focal point remote per l'instradamento delle informazioni relative alle segnalazioni per specifiche applicazioni di servizi di gestione. Il nodo locale individua i focal point remoti in una rete APPN.

Configurazione cartelle condivise AS/400 Communications Server consente di creare sul server delle unità disco che comunicano con le cartelle AS/400 mediante l'IFS (Integrated File System) AS/400. Se il server condivide queste unità disco, i client possono utilizzare il comando NET USE per il collegamento. Più client possono collegarsi alle cartelle presenti nel sistema AS/400 come se fossero unità di stazioni di lavoro.

Passo 6.1 Pianificazione dei programmi applicativi

Controllare le proprie applicazioni per accertarsi di soddisfarne i requisiti. In particolare, controllare i requisiti per:

- Modi
- TP (transaction program)
- Definizioni LU (host, LU 6.2)
- LU partner

Passo 7. Creazione configurazioni ed installazione

E' necessario stabilire come verrà configurato ed installato Communications Server sui server dell'utente. E' possibile:

- Fornire agli utenti delle istruzioni per l'installazione e la configurazione di Communications Server. E' possibile preparare le istruzioni oppure stampare le copie della *Guida operativa*. Inoltre, è necessario fornire informazioni specifiche per cia come l'ID di rete, il nome CP (control point) e l'indirizzo di rete.
- E' necessario fornire agli utenti le istruzioni per l'installazione di Communications Server con una configurazione esistente o un file maschera. E' anche necessario fornire un file di risposta specifico per ciascun server, insieme con i CD Communications Server o l'accesso alle immagini CD.
- Configurare ed installare Communications Server sui server utente. A meno che non si disponga di un gruppo limitato di utenti, potrebbe risultare utile l'utilizzo di un prodotto che assiste l'utente durante la configurazione, l'installazione e la distribuzione del software per più stazioni di lavoro. Esempi di questo tipo di prodotto includono IBM NVDM/2 (NetView Distribution Manager/2), Tivoli TME-10 e Microsoft SMS (System Management Server).

Utilizzo della configurazione e dell'installazione del file di risposta

Se si sceglie di utilizzare la configurazione e l'installazione del file di risposta, fare riferimento alla sezione “Configurazione con i file maschera e di risposta” a pagina 194.

Passo 8. Creazione dei materiali per l'utente

Dopo aver pianificato la rete e stabilito come procedere all'implementazione della pianificazione, è necessario creare i materiali per l'utente finale. Ciò significa che è necessario preparare la documentazione relativa all'installazione, alla configurazione ed all'utilizzo quotidiano oltre alle procedure di backup.

Preparazione della documentazione

Preparare una serie di documenti personalizzati in modo da assistere gli utenti durante l'installazione, la configurazione e l'utilizzo di Communications Server e delle applicazioni locali in base alle proprie esigenze particolari. Le sezioni che seguono contengono suggerimenti per il tipo di informazioni che è necessario includere.

Configurazione ed installazione dei materiali e delle procedure

La *Guida operativa* e la Guida in linea per l'installazione sono disponibili per guidare gli utenti durante l'installazione di Communications Server. Le istruzioni devono suggerire all'utente quale dei seguenti passi eseguire durante l'installazione del software:

- Quando eseguire il back up dei file di configurazione
- Se accettare i valori predefiniti per la creazione di un file di configurazione Communications Server

  Potrebbero essere necessarie informazioni sulla rete, come indirizzi dell'adattatore LAN, nomi di rete e così via.
- Quando procedere all'installazione con un file di risposta fornito
- Quando procedere all'installazione con un file di configurazione personalizzato fornito

Se necessario, fornire la documentazione appropriata agli utenti.

Materiali e procedure di Communications Server

Per utilizzare le funzioni e le API di Communications Server, si consiglia di consultare i seguenti materiali:

- *Guida operativa*
- Programmi scritti dall'utente per le API Communications Server selezionate

Avvio e arresto di Communications Server

Per la procedura relativa all'avvio o all'arresto di Communications Server, fare riferimento alla *Guida operativa*.

Se si dispone di istruzioni differenti per l'avvio o l'arresto, fornirle agli utenti.

- Numeri di telefono per l'individuazione dei problemi relativi all'host (rivolgersi all'assistenza per l'host)
- Procedure di logon per sistemi o applicazioni host
- Procedura per l'arresto dell'applicazione host

  Rivolgersi all'assistenza per l'host.
- Procedure di scollegamento

  Le istruzioni devono includere requisiti speciali per lo scollegamento dei sistemi o delle applicazioni. E' possibile richiedere queste informazioni all'assistenza per l'host.

Materiali e procedure per i programmi applicativi

E' necessario fornire agli utenti procedure ed altre informazioni per i programmi applicativi, che è possibile utilizzare sulla rete. In generale, è necessario fornire:

- Procedure per l'avvio dei programmi applicativi
- Procedure per l'esecuzione dei programmi applicativi
- Procedure per la risposta ai messaggi generati dal programma applicativo
- Procedure per l'individuazione dei problemi
- Se necessario, le procedure per l'arresto del programma applicativo

Rivolgersi al programmatore dell'applicazione per le precedenti informazioni.

Materiali e procedure per l'individuazione dei problemi

Per le procedure sull'individuazione e la segnalazione dei fare riferimento alla *Guida operativa*.

Preparazione delle procedure di backup

E' possibile che talvolta gli utenti cancellino o modifichino i file di configurazione, il registro, il file system, i programmi applicativi ed altri programmi o file creati in locale. Inoltre, nei server potrebbero essere effettuate cancellazioni o modifiche non accettabili, specialmente quando diversi utenti accedono alle stazioni di lavoro del server durante le ore di lavoro.

Per questo motivo, è necessario preparare e documentare le procedure di backup per la rete. Potrebbe anche risultare necessario modificare gli attributi dei file selezionati sui server ed impostarli per la sola lettura in modo che gli utenti non possano modificarli.

Passo 9. Gestione della rete

Dopo aver completato la pianificazione, l'installazione e la configurazione della rete e una volta che questa è in esecuzione su base quotidiana, l'attività che resta da svolgere è la gestione. E' necessario pianificare l'aggiunta, la modifica o la cancellazione delle risorse e degli utenti della rete e pianificare la risoluzione dei problemi.

Lo stesso livello di passi di pianificazione ed implementazione deve essere eseguito per le modifiche apportate alla rete durante l'impostazione iniziale. Per queste modifiche apportate alla rete, è necessario seguire gli stessi passi utilizzati per la pianificazione, l'installazione e la configurazione iniziali.

Communications Server fornisce i seguenti strumenti che consentono di controllare quotidianamente le prestazioni della rete:

- **Operazioni nodo SNA**
- Programmi di utilità della riga comandi
- Gestione Web
- Client di gestione remota
-

Controllo e gestione di una rete

Programmi per la gestione del sistema

Questo capitolo fornisce una panoramica dei programmi per la gestione del sistema Communications Server e descrive le funzioni che sono comuni a ciascun programma. Ogni programma dispone anche di funzioni univoche che vengono descritte per ciascuno di essi.

I programmi per la gestione del sistema consentono di controllare le risorse di comunicazione di Communications Server. Essi inoltre consentono di modificare queste risorse per migliorare l'efficienza dei servizi di comunicazione SNA oppure per controllare e provare questi servizi durante l'individuazione dei problemi.

Per un elenco delle risorse che è possibile gestire, fare riferimento alla *Guida operativa*.

Communications Server può essere gestito con i seguenti programmi di utilità:

- **Operazioni nodo SNA**
- Gestione remota
- Programmi di utilità della riga comandi
- Gestione basata sul Web
- Controllo ActiveX Operazioni nodo SNA
- Modulo Tivoli Plus
- Supporto APPN MIB
- ROPS (Remote Operations Support) S/390

E' possibile utilizzare qualsiasi combinazione di questi programmi per la gestione di Communications Server.

Funzioni comuni dei programmi per la gestione del sistema

Ciascun programma per la gestione del sistema può effettuare le seguenti operazioni relative alle risorse:

- Visualizzazione delle informazioni sulle risorse
- Avvio delle risorse
- Arresto delle risorse
- Eliminazione delle risorse
- Avvio delle commutazioni di percorso

E' possibile eseguire un sottoinsieme di queste operazioni per ciascuna risorsa, come illustrato in Tabella 36 a pagina 206.

Tabella 36. Operazioni di gestione per le risorse di Communications Server

Risorsa	Visualizzazione	Avvio	Arresto	Eliminazione	Commutazione percorso
Connessioni	X	X	X	X	
Informazioni su ubicazione CPI-C	X			X	
Periferiche	X	X	X	X	
PU DLUR	X	X	X		
LU locale da 0 a 3	X			X	
LU locale 6.2	X			X	
Sessioni LU 6.2	X		X		
Gateway DLUR / PU 2.0	X			X	
Connessioni RTP	X				X
Sessioni TN3270E	X		X		
Sessioni TN5250	X		X		

Operazioni nodo SNA

Operazioni nodo SNA è un'applicazione in linea che consente di controllare le risorse per le comunicazioni gestite da Communications Server.Questa applicazione consente di arrestare, avviare e controllare le risorse presenti nella rete.

Questa applicazione consente di arrestare, avviare e controllare le risorse presenti nella rete. **Operazioni nodo SNA** è supportata anche dai client remoti Windows 95 e Windows NT. Questo supporto consente ad **Operazioni nodo SNA** di collegarsi ai Communications Server remoti e gestirli.

Operazioni nodo SNA può essere utilizzato per la gestione delle risorse nella rete. Le funzioni di programmazione per la gestione del sistema di Communications Server consentono di configurare e gestire i nodi presenti nella rete SNA. **Operazioni nodo SNA** fornisce un diagramma con vista ad albero della configurazione che consente di selezionare e modificare le risorse in un'interfaccia grafica gerarchica.

Nella finestra principale di **Operazioni nodo SNA** è possibile gestire più finestre.

L'utente può definire più di una configurazione Communications Server ed alternare le configurazioni in base alle proprie esigenze. Quando viene avviato Communications Server, la configurazione predefinita viene fornita come prima scelta per la configurazione ed il funzionamento del nodo a meno che non venga specificata un'altra configurazione. Una volta completata una nuova configurazione, è possibile sostituire la configurazione predefinita con quella nuova. Utilizzare **Operazioni nodo SNA** per applicare la nuova configurazione e verificare che la porzione rilevante del prodotto venga eseguita in base alla configurazione fornita.

Mediante **Operazioni nodo SNA** è possibile avviare altri programmi Communications Server, come **Log Viewer**, **Trace Facility** o **Configurazione nodo**.

Gestione remota

L'applicazione **Operazioni nodo SNA** può essere utilizzata anche per eseguire il collegamento ad un Communications Server remoto e gestirne direttamente le risorse. L'utente può gestire in remoto le risorse per un Communications Server da qualsiasi parte della rete.

Un client per la gestione remota installa solo le applicazioni di gestione su un client, inclusa l'applicazione **Operazioni nodo SNA**. Da questo client, un utente può gestire in modo completo qualsiasi Communications Server presente nella rete.

I client per la gestione remota di Windows 95 e Windows NT utilizzano la sicurezza del dominio Windows NT per autenticare il collegamento client al server senza immettere nuovamente l'ID utente e la password. Il client deve appartenere ad un dominio Windows NT, partecipando ad un dominio Communications Server oppure eseguendo il collegamento in locale con una password ed un ID utente sincronizzati.

Agli utenti del client per la gestione remota, esterni al dominio Windows NT, viene richiesto di fornire l'ID utente e la password, mediante un prompt oppure memorizzando questi valori nel file di configurazione del client.

Gli utenti autorizzati all'utilizzo dei client di gestione remota vengono memorizzati nel gruppo locale IBMCSADMIN, che si trova in Communications Server o nell'unità di controllo del dominio a cui appartiene Communications Server. Tale gruppo di utenti viene creato durante l'installazione e può essere gestito utilizzando

IBMCSADMIN nella macchina Windows NT su cui è in esecuzione Communications Server.

Questa funzione può essere installata dal CD-ROM di Communications Server. La maggior parte delle funzioni dell'applicazione **Operazioni nodo SNA** sono disponibili mediante un browser Web. E' possibile interrogare lo stato del nodo, ottenere informazioni sulle risorse, modificare le risorse, visualizzare ed editare i file di configurazione, visualizzare le registrazioni dei messaggi ed eseguire altre attività di gestione. La funzione di gestione Web consente anche di editare i file di configurazione e visualizzare il file di registrazione. I passi necessari per l'utilizzo di queste funzioni sono documentati nella pagina **Welcome to Communications Server Web Administration** sul Web.

Controllo ActiveX Operazioni nodo SNA

E' disponibile una versione di controllo ActiveX di **Operazioni nodo SNA**. Questo controllo consente di integrare **Operazioni nodo SNA** in qualsiasi applicazione che supporti i controlli integrati, come MMC (Microsoft Management Console). Il nome del controllo, ubicato nella directory di installazione del prodotto, è CSNTACTX. Esso dispone di tutte le funzioni di **Operazioni nodo SNA** ed offre il vantaggio di incorporare **Operazioni nodo SNA** in altre applicazioni, consentendo la gestione incrociata del prodotto.

Modulo Tivoli Plus

Se viene utilizzato TMS (Tivoli Management Environment) per eseguire la gestione centrale delle periferiche e delle applicazioni presenti nella rete, il modulo Tivoli Plus di Communications Server consente di gestire Communications Server anche da TME. Tale modulo può essere installato sul server TME. Nella directory TME del CD-ROM di Communications Server è disponibile un'immagine installabile TME. Per accedere alle funzioni TME Plus installate, fare doppio clic sull'icona TivoliPlus aggiunta al pannello **Desktop for Administrator** di TME. Facendo doppio clic sull'icona IBM CSPlus, è possibile utilizzare le icone presenti nel pannello per effettuare le seguenti azioni:

- Distribuire, installare e disinstallare Communications Server
- Avviare, arrestare ed interrogare il server
- Visualizzare e modificare le risorse del server
- Elencare i file di configurazione
- Instradare i messaggi di errore da Communications Server in una Tivoli Enterprise Console
- Stabilire i controlli e le soglie per gli attributi principali di Communications Server

Quando si fa doppio clic su un'icona presente nel pannello IBM CSPlus, immettere le informazioni nei campi della finestra di dialogo che viene visualizzata. Nella finestra di dialogo è disponibile una guida relativa ai campi.

Supporto MIB APPN

Communications Server supporta le richieste SNMP (simple network management protocol) per le informazioni sulla gestione APPN del sistema di gestione SNMP.

SNMP Service viene installato dal separatore **Servizi** nel menu a discesa **Rete** del pannello di controllo di Windows NT. Una volta installato il software SNMP Service sul computer, è necessario configurarlo con informazioni valide per rendere operativo SNMP.

Per configurare SNMP, l'utente deve essere collegato come membro del gruppo di responsabili del computer locale.

Le informazioni relative alla configurazione SNMP identificano le destinazioni delle comunità e dei trap.

ROPS (Remote Operations Support) S/390 per il programma NetView

Appendici

Appendice A. Pianificazione di Communications Server

Questa appendice fornisce le informazioni necessarie per la pianificazione dell'ambiente Communications Server.

Hardware compatibile

Questa sezione descrive l'hardware IBM che supporta Communications Server. Queste descrizioni includono informazioni su:

- Adattatori per comunicazioni
- Modem
- Adattatori per crittografia a livello sessione

Adattatori per comunicazioni

Per un elenco degli adattatori per comunicazioni supportati da Communications Server, consultare il seguente URL su Internet:

http://www.software.ibm.com/enetwork/commserver/about/comp_products/comp_csnt.html

Modem

Il Communications Server supporta i seguenti tipi di modem:

- Modem asincroni:
  - Modem compatibili con la serie di comandi Hayes** AT
  - Modem IBM conformi agli standard di interfaccia ITU-T (CCITT) V.24/V.28 (EIA RS-232-D) e V.35
  - Sono supportati anche i modem non-IBM asincroni, insieme con la funzione di base dell'interfaccia standard tra DTE (data terminal equipment) e DCE (data circuit-terminating equipment) ITU-T (CCITT) V.24 (EIA RS-232-D) per le comunicazioni asincrone
  - Modem conformi all'interfaccia standard tra DTE e DCE RS-232-D
- Modem sincroni ed unità CSU/DSU che supportano la serie di comandi V.24bis
- Modem compatibili con il protocollo Hayes AutoSync

Gli utenti X.25 richiedono un modem sincrono ed unità CSU/DSU che supportano la serie di comandi V.24bis o un modem compatibile con il protocollo Hayes AutoSync. Per il tipo di collegamento e di modem consigliati, rivolgersi al fornitore della rete.

Per un elenco di modem supportati da Communications Server, consultare il seguente URL su Internet:

http://www.software.ibm.com/enetwork/commserver/about/comp_products/comp_csnt.html

Adattatori per crittografia a livello sessione

Per utilizzare la crittografia a livello sessione, è necessario disporre del programma Programmed Cryptographic Facility e di uno dei seguenti adattatori:

- IBM SecureWay 4758 PCI Cryptographic Coprocessor Adapter
- Altri adattatori conformi all'IBM Common Cryptographic Architecture

Nota: Se viene utilizzato un adattatore diverso dall'IBM 4758, è necessario utilizzare i verb di crittografia API. Per ulteriori informazioni, fare riferimento a *Communications Server Programming Guide and Reference*.

Software di emulazione

Per un elenco dei software di emulazione supportati da Communications Server, consultare il seguente URL su:

http://www.software.ibm.com/enetwork/commserver/about/comp_products/comp_csnt.html

Considerazioni sulla compressione dati

Prima di utilizzare la compressione dati SNA è necessario eseguire diversi passi di configurazione sui sistemi in uso. La compressione dati SNA è supportata su:

- VTAM V3R4.1 o versione successiva
- OS/400 V2R3 o versione successiva

Quando viene eseguita la compressione, ciascuna RU viene compressa indipendentemente e ad essa viene aggiunta un'intestazione di compressione. TH e RH non vengono compresse. La compressione non viene eseguita quando la RU è inferiore a 20 byte o superiore a 64K byte oppure, solo in caso di RLE, se le dimensioni dei dati compressi, inclusa l'intestazione di compressione, sono superiori a quelle dei dati originali.

Prima di iniziare la configurazione delle funzioni appropriate di Communications Server per la compressione dati, verificare che il sistema partner sia in grado di supportare tale funzione.

Pianificazione del collegamento host/VTAM

Prima di richiedere la compressione dati in una sessione per un host S/370 o S/390* con emulazione 3270 o comunicazioni di tipo LU 6.2, è necessario installare e configurare il VTAM Versione 3 Rilascio 4.1 (VTAM V3R4.1) per negoziare tali richieste.

Il programmatore del sistema host VTAM deve fornire le definizioni VTAM appropriate necessarie per la compressione dati. Di seguito è riportato un elenco riepilogativo delle definizioni necessarie. Degli esempi sono riportati subito dopo l'elenco.

- Le opzioni di avvio VTAM devono contenere il parametro **CMPVTAM**=x
- E' necessaria una voce LOGMODE con il parametro **COMPRES=**
- Questa voce LOGMODE deve essere contenuta nella tabella dei modi in uso

- E' necessario includere un'istruzione APPL VTAM con i parametri **CMPAPPLI=** e **CMPAPPLO=** relativi all'applicazione che verrà utilizzata
- La definizione della LU VTAM per la sessione deve specificare la tabella dei modi e la tabella LOGMODE definite per la compressione.

CMPVTAM Rappresenta il parametro delle opzioni di avvio VTAM che indica il livello massimo di compressione consentito per qualsiasi sessione collegata a questo host. La sintassi di questo parametro è la seguente:

```
CMPVTAM=n
```

dove n è il livello di compressione consentito per una richiesta, compreso nell'intervallo da 0 a 4. Il valore consigliato è 4, che consente l'utilizzo di tutti i livelli di compressione dati.

COMPRES Rappresenta la voce della tabella VTAM MODEENT nella definizione LOGMODE che viene utilizzata dalla LU. La sintassi è la seguente:

```
COMPRES=value
```

dove "value" rappresenta SYSTEM, REQUESTED o PROHIBITED. SYSTEM deve essere codificato per tutti i tipi di LU supportati.

CMPAPPLO Rappresenta il parametro della definizione APPL (application) VTAM che imposta il livello di compressione richiesto per i dati RU (Request/Response Unit) in uscita. La sintassi è la seguente:

```
CMPAPPLO=n
```

dove "n" è il livello di compressione dati richiesto per la direzione del flusso dei dati PLU -> SLU, chiamati anche dati in uscita. Per tutte le sessioni di tipo LU supportate da Communications Server, il valore "n" può essere uguale a 0, 1 o 2 per indicare la compressione dati di livello 0, 1 e 2. Tuttavia, per le LU di tipo 0, 1, 2 e 3, Communications Server riserva sempre le risorse di compressione di livello 2.

CMPAPPLI Rappresenta il parametro della definizione APPL (application) VTAM che imposta il livello di compressione richiesto per i dati RU (Request/Response Unit) in uscita. La sintassi è la seguente:

```
CMPAPPLI=m
```

dove "m" è il livello di compressione dati richiesto per il flusso dei dati SLU -> PLU, chiamati anche dati in arrivo. Il valore per m dipende dal tipo di LU utilizzato per la sessione:

- Per le sessioni LU 3270, "m" può avere un valore pari a 0 o 1.
- Per le sessioni LU 6.2, "m" può avere un valore pari a 0, 1 o 2.

Nota: VTAM rappresenta sempre la LU primaria (PLU) e Communications Server rappresenta la LU secondaria (SLU) per le LU di tipo 0, 1, 2 e 3.

Di seguito sono riportati esempi codificati, estratti dagli elenchi VTAM originali, che indicano l'utilizzo e la collocazione dei parametri descritti in precedenza. Osservare con attenzione le righe evidenziate.

```
************************************************************
SSCPID=20,HOSTSA=20,XNETALS=YES,                              X
GWSSCP=YES,                                                   X
NODELST=NODES1,                                               X
CMPVTAM=4,                                                   X
CONFIG=K0,SUPP=NOSUP,                                         X
NETID=USIBMRA,HOSTPU=ISTPUS20,HOSTSA=20,SSCPNAME=RAK,         X
SSCPDYN=YES,SSCPORD=PRIORITY,                                 X
ASYDE=TERM,                                                   X
NOTRACE,TYPE=VTAM,IOINT=0,                                    X
NOTRACE,TYPE=SMS,ID=VTAMBUF,                                  X
PPOLOG=YES,                                                   X
NODETYPE=NN,                                                  X
CPCP=YES,                                                     X
CSALIMIT=0,                                                   X
NOTNSTAT,DYNLU=YES,                                           X
IOBUF=(3500,256,3,,1,58),                                     X
LPBUF=(1100,,2,,1,4),                                         X
LFBUF=(100,,,,1,1),                                           X
CRPLBUF=(2400,,,,1,4),                                        X
SFBUF=(60,,,,1,1)
************************************************************
```

Figura 41. Parametro di avvio VTAM. In questo VTAM è consentito il livello di compressione fino a 4.

```
*****************************************************************
* LOGMODE PER PROVA DI COMPRESSIONE - BASATO SU D4C32XX3
*
*****************************************************************
*                                                               *
*              3274 MODEL 1C (SNA REMOTA)                @OY02946*
*              SCHERMO PRIMARIO 24 X 80 (1920)
*
*              SCHERMO ALTERNATIVO STABILITO DALL'APPLICAZIONE     *
*****************************************************************
D4C3COMP MODEENT LOGMODE=D4C3COMP,                             *
                 FMPROF=X'03',                                 *
                 TSPROF=X'03',                                 *
                 PRIPROT=X'B1',                                *
                 SECPROT=X'90',                                *
                 COMPROT=X'3080',                              *
                 RUSIZES=X'87F8',                              *
                 PSERVIC=X'028000000000000000000300',          *
                 APPNCOS=#CONNECT,                             *
                 COMPRES=REQD                                 *
```

Figura 42. Tabella Logmode VTAM. La macro MODEENT configurata con la compressione dati richiesta.

```
   VBUILD TYPE=APPL
*********************************************************************
* ISTRUZIONI APPL VTAM PER CICS/MVS* 3.3                             *
*********************************************************************
RAKAC001 APPL ACBNAME=RAKAC001,                                      *
              MODETAB=MTAPPC,                                        *
              EAS=20,                                                *
              SONSCIP=YES,                                           *
              AUTH=(ACQ,VPACE,PASS),                                 *
              PARSESS=YES,                                           *
              VPACING=5,                                             *
              CMPAPPLI=1                                  *
              CMPAPPLO=2
```

INDTACPR Questo valore rappresenta il livello massimo di compressione utilizzato per i dati in arrivo.

OUTDTACPR Questo valore rappresenta il livello massimo di compressione utilizzato per i dati in uscita.

Per le sessioni LU 6.2, i livelli di compressione dati 0, 1 e 2 sono supportati in entrambe le direzioni, ovvero per entrambi i flussi di dati in uscita ed in arrivo.

Per le informazioni sull'abilitazione di Communications Server per la compressione dati, fare riferimento al manuale *Guida operativa*.

Considerazioni sulle prestazioni

Le prestazioni relative alle comunicazioni del computer in generale e a quelle del Communications Server in particolare, sono soggette ad un grande numero di variabili. L'intento delle seguenti informazioni è quello di introdurre alcuni dei fattori che influiscono sulle prestazioni delle comunicazioni in un ambiente Communications Server.

La velocità della linea di comunicazione influisce sulle prestazioni relative alle comunicazioni. Questa velocità viene generalmente espressa come numero di bps (bits per second) che è possibile trasmettere sulla linea. Generalmente, quanto più alto è il numero di bps tanto più elevate saranno le prestazioni ottenute sulla linea.

Oltre alla velocità dei bit, altri fattori collegati alla linea possono influire sulle prestazioni relative alle comunicazioni. Ad esempio, alcune linee possono trasmettere i dati solo in una direzione alla volta. Per modificare la direzione delle comunicazioni (che possono eseguire un inoltro), la stazione invia una ***RTS*** (request to send) ed attende l'emissione ***CTS*** (clear to send). L'esecuzione di questo ***scambio*** (dipendente dal tipo di modem) richiede ulteriore tempo. Un altro fattore è rappresentato dalla qualità della trasmissione della linea di comunicazione. Quando si verifica un errore relativo alla linea, la maggior parte dei protocolli lo rilevano ed inviano nuovamente i dati. Una linea che presenta un numero di errori di trasmissione più basso fornirà prestazioni migliori.

E' possibile ottenere prestazioni più elevate se i protocolli vengono eseguiti in un modo di trasmissione dati ***duplex***, in cui il protocollo può ricevere e trasmettere dati simultaneamente. LAN e X.25 sono protocolli duplex. SDLC può essere eseguito nel modo duplex o half-duplex.

Per utilizzare il modo duplex per SDLC, è necessario utilizzare un adattatore appropriato (l'adattatore MPA non supporta il modo duplex) ed una stazione remota che supporti il modo duplex.

Con l'aumentare della velocità della linea, la velocità dei bit rappresenta un vincolo minore per le prestazioni. Tale vincolo è collegato invece ai ritardi relativi ai dispositivi che utilizzano la linea di comunicazione (modem, unità di controllo o vincoli interni al computer). Alle alte velocità, questi ritardi possono influire sulle prestazioni delle comunicazioni più della velocità dei bit della linea.

L'analisi delle seguenti situazioni richiede un certo impegno. Ad esempio, ritardi nelle comunicazioni maggiori di quelli previsti possono essere causati da uno dei seguenti motivi:

- Una linea di comunicazione sovraccarica
- Un sistema host sovraccarico
- Un'unità di controllo 3X74 sovraccarica
- Un'unità di controllo di rete 37*xx* sovraccarica
- Una definizione VTAM o NCP non ottimale
- Un progetto di rete o una gestione di rete non corretto
- Swap ed utilizzo eccessivo della memoria del sistema operativo

In un ambiente di comunicazioni ad alta velocità, come una LAN, la velocità dei bit della linea di comunicazione è meno significativa poiché la capacità di comunicazione è determinata principalmente dalla velocità dei dispositivi di comunicazione. Spesso è possibile ottenere migliori prestazioni nelle comunicazioni aumentando le capacità di elaborazione della stazione di lavoro, dell'host o degli altri componenti della rete. Ciò non significa che la velocità dei bit di una rete LAN non rappresenti mai un vincolo; piuttosto, prima che le prestazioni della LAN vengano ridotte in maniera significativa, potrebbe essere necessario eseguire diversi computer alla rispettiva velocità di comunicazione.

Per riassumere, in molti casi le prestazioni di Communications Server sono determinate principalmente da fattori collegati alla rete di comunicazione in uso. Per ottenere buone prestazioni a costi ragionevoli è necessario conoscere l'intera rete ed effettuare un'analisi dei singoli componenti.

Indice analitico

Numerico

A

D

E

F

G

H

I

L

M

N

T

U

V

W

X

Riservato ai commenti del lettore

eNetwork Communications Server
per Windows NT
Guida per il responsabile di rete **SC13-2794-00**

Commenti relativi alla pubblicazione in oggetto potranno contribuire a migliorarla.
Si invita il lettore ad usare lo spazio sottostante citando, ove possibile, i riferimenti alla pagina ed al paragrafo; i suggerimenti ed i commenti inviati potranno essere usati liberamente dall'IBM e dalla Selfin e diventeranno proprietà esclusiva delle stesse.
Si prega di non utilizzare questo foglio per richiedere informazioni tecniche su sistemi, programmi o pubblicazioni; per tali esigenze si consiglia di rivolgersi al punto di vendita o alla filiale IBM interessata.

Commenti:

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

Nome . . . . . .

Mansione/Titolo . . . . . .

Indirizzo . . . . . .

. . . . . Piegare . . . . . Piegare . . . . . .

. . . . . Piegare . . . . . Piegare . . . . . .

SELFIN S.p.A.

Translation Assurance

via F. Giordani, 7

80122 - N A P O L I

Printed in the European Union

SC13-2794-00