eNetwork Communications Server
Version 6.0 für Windows NT

Handbuch für die Netzverwaltung

Version 6.0

SC12-2577-00

eNetwork Communications Server
Version 6.0 für Windows NT

Handbuch für die Netzverwaltung

Version 6.0

SC12-2577-00

Anmerkung: Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die allgemeinen Informationen unter Anhang B, „Bemerkungen“ auf Seite 241, gelesen werden.

Diese Ausgabe bezieht sich auf Version 6.0.

Diese Veröffentlichung ist eine Übersetzung des
IBM eNetwork Communications Server for Windows NT Network Administration Guide
IBM Form SC31-8656-00,
herausgegeben von International Business Machines Corporation, USA
© Copyright International Business Machines Corporation 1997, 1998

© Copyright IBM Deutschland Informationssysteme GmbH 1997, 1998

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
SW NLS
Kst. 2877
Juli 1998

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellen

Inhalt dieses Handbuchs

IBM eNetwork Communications Server für Windows NT (im vorliegenden Buch als *Communications Server* bezeichnet) ist eine Plattform für Übertragungsservices. Diese Plattform bietet eine Vielzahl von Services für Windows NT-Datenstationen, die mit Hosts und mit anderen Datenstationen kommunizieren. Communications Server-Benutzer können aus einer Vielfalt von Optionen für ferne Konnektivität auswählen.

Das *Handbuch für die Netzverwaltung* ist eine nützliche Quelle zur Planung und Verwaltung für Personen, die Communications Server verwenden oder die Verwendung planen. Dieses Handbuch enthält nützliche Informationen für Administratoren, den technischen Kundendienst, Service Coordinators und IBM Personal sowie für alle Personen, die an Entscheidungen über Informationssysteme mitwirken. Es enthält eine Übersicht über die Funktionen von Communications Server sowie die Schritte, die für die Erstellung von Communications Server-Konfigurationen für die unterstützten Datenstationen erforderlich sind.

Es wird davon ausgegangen, daß Windows NT 4.0 Server als Basisbetriebssystem verwendet wird.

Verwendung dieses Handbuchs

Das *Handbuch für die Netzverwaltung* enthält Informationen zur Planung der Installation und Konfiguration eines Netzes von Datenstationen. Dieses Handbuch unterstützt bei folgenden Aufgaben:

- Planung des Netzes
- Auswahl von Konfigurations- und Installationshilfsprogrammen
- Erstellung einer Schablonenkonfigurationsdatei
- Implementierung des Netzplans
- Verwaltung des Netzes

Die Definition eines Netzes von Datenstationen erfordert eine sorgfältige und gründliche Planung. Beim Aufbau eines Netzes müssen folgende Informationen vorliegen:

- Der Name der Datenstation, Profilnamen, Konfigurationsdateinamen und andere Namen im Netz
- Position des zentralen Alert-Verarbeitungssystems zum Senden von Alerts
- Die verfügbaren Datenstationen, die weiterhin verwendet werden können und die Anzahl der benötigten neuen Datenstationen
- Der Aufgabenbereich, den jede Datenstation im Netz haben soll
- Das auf jeder Datenstation zu installierende Paket, so daß diese den ihr zugeordneten Aufgabenbereich erfüllen kann
- Die bereits vorliegenden Hardware- und Softwareressourcen, die erhalten oder aktualisiert werden sollen

- Die neuen Hardware- und Softwareressourcen, die benötigt werden, bevor die Netzplanung implementiert werden kann
- Die Methode zur ständigen Verwaltung des Netzes und seiner Ressourcen
- Anzahl und Typ von Host-Verbindungen und Informationen, welche Datenstationen an die Hosts über Gateway und Gateway-Definition angeschlossen werden sollen

Die Schritte in „Communications Server-Konfigurationen implementieren“ auf Seite 199 enthalten eine Prozedur zur Bestimmung dieser Informationen für das Netz. Ist bereits eine funktionierende Prozedur vorhanden, kann diese verwendet werden; bevor eine diesbezügliche Entscheidung getroffen wird, sollte jedoch die Prozedur in dem angegebenen Kapitel gelesen werden.

In diesem Handbuch verwendete Konventionen

Folgende Konventionen werden in diesem Handbuch verwendet.

Textkonventionen

Fettdruck	Fettdruck kennzeichnet folgendes: • Verben, Funktionen, Schlüsselwörter und Parameter, die in einem Programm oder in der Befehlszeile verwendet werden können. Diese Werte sind von der Groß-/Kleinschreibung abhängig und müssen wie im Text dargestellt eingegeben werden. • Namen von Fensterelementen, wie z. B. Listen, Markierungsfelder, Eingabefelder, Druckknöpfe und Menüauswahlmöglichkeiten.
Kursivschrift	Kursivschrift kennzeichnet folgendes: • Eine Variable, für die ein Wert angegeben werden muß. • Buchtitel. • Ein Buchstabe oder ein Wort, der oder das genauso verwendet werden muß.
Fettdruck in Kombination mit Kursivschrift	Hervorhebung eines Worts.
GROSSSCHREIBUNG	Großschreibung kennzeichnet Konstanten, Dateinamen und Optionen, die in einem Programm oder in einer Befehlszeile verwendet werden können. Diese Werte können in Groß- oder Kleinschreibung eingegeben werden.
Anführungszeichen	Anführungszeichen kennzeichnen Nachrichten, die in einem Fenster angezeigt werden. Ein Beispiel hierfür sind Nachrichten, die in der Bedienerinformationszeile einer Emulationssitzung angezeigt werden.
`Beispiele`	Die Schrift für Beispiele kennzeichnet Informationen, die der Benutzer in die Befehlszeile oder in einem Fenster eingeben muß.

Zahlenkonventionen

Binärzahlen	Werden als B'xxxx xxxx' oder B'x' dargestellt. Eine Ausnahme bilden die Fälle, in denen zusätzlich Text angegeben ist („Ein Wert für die Binärzahl xxxx xxxx ist...“).
Bitpositionen	Ausgangspunkt ist 0 (Position ganz rechts - niedrigstwertiges Bit).
Dezimalzahlen	Dezimalzahlen mit mehr als 4 Ziffern werden in metrischer Darstellung angegeben. Gruppen von 3 Ziffern werden nicht durch einen Punkt, sondern durch eine Leerstelle voneinander getrennt. Beispiel: Die Zahl sechzehntausendeinhundertsiebenundvierzig wird wie folgt geschrieben: 16 147.
Hexadezimalzahlen	Werden im Text als hex xxxx oder X'xxxx' dargestellt. („Die Adresse des Nachbarknotens lautet hex 5D, was als X'5D' dargestellt wird.“)

Referenzliteratur

Weitere Informationen können der Dokumentation *Einstieg* entnommen werden, die eine vollständige Auflistung der Communications Server-Bibliothek und der Referenzliteratur enthält.

Die Communications Server-Homepage im Internet enthält allgemeine Produkt- und Serviceinformationen zu APARs und Berichtigungen. Es gibt zwei Möglichkeiten zum Aufrufen der Homepage:

1. Im Communications Server das Symbol **Home Page-Zugriff** auswählen oder
2. Mit einem Internet-Browser folgende URL aufrufen:

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

Überblick und Konzepte

Einführung in die Funktionen des Communications Server

Dieses Kapitel enthält eine Übersicht über die vom Communications Server unterstützten Übertragungsfunktionen und über die Methoden, mit denen das System so konfiguriert werden kann, daß es diese Funktionen ausführen kann. In späteren Kapiteln dieses Buches wird auf die Funktionen und Konfigurationsmethoden detaillierter eingegangen.

Unterstützte Funktionen

In diesem Abschnitt werden die folgenden Funktionen des Communications Server beschrieben:

- SNA-Übertragungsunterstützung
- Advanced Program-to-Program Communications (APPC) einschließlich Advanced Peer-to-Peer Networking (APPN)
- 32-Bit-Anwendungsprogrammierschnittstellen (APIs)
- High Performance Routing (HPR)
- SNA-Datenkomprimierung
- Erkennung der Servicegeber mit Discovery
- Konventionelle LU-Anwendung (LUA)
- Abhängiger LU-Requester (DLUR - Dependent Logical Unit Requester)
- SNA-Gateway
- AnyNet-Unterstützung
  - AnyNet SNA über TCP/IP (Zugriffsknoten und Gateway)
  - AnyNet Sockets über SNA (Zugriffsknoten und Gateway)
- TN3270E-Server
- TN5250-Server
- Zugriff auf Daten, die mit anderer Software erstellt wurden
  - AS/400 OLE DB Provider
  - Host Publisher
  - AS/400-Server für gemeinsam benutzte Ordner
- SNA-API-Client-Unterstützung
- Unterstützung für Novell IntranetWare für SAA-Client
- Konfigurations- und Verwaltungsunterstützung
- Lastausgleich
- Datensicherheit
- Adapterunterstützung
- DLC-Unterstützung
- APPN-MIB-Unterstützung
- Fehlertoleranter Modus
- Entry-Level-Emulationsfunktionen

SNA-Übertragungsunterstützung

Communications Server kann als SNA-Knoten vom Typ 2.0 und Typ 2.1 eingesetzt werden. Diese Unterstützung ermöglicht es, Programme für die Kommunikation mit vielen anderen SNA-Produkten von IBM zu schreiben.

APPC/APPN

Communications Server stellt Unterstützung für APPN-Endknoten und -Netzknoten für Datenstationen zur Verfügung, durch die die Kommunikation mit anderen Systemen im Netz erleichtert wird. Außerdem können mit der Erweiterungsfunktion für Zweigstellennetze Zweigstellen isoliert werden, um unnötigen CP-CP-Datenaustausch zu vermeiden.

Der Communications Server stellt APPC zur Unterstützung der Kommunikation zwischen Programmen mit verteilter Verarbeitung, den sogenannten Transaktionsprogrammen (TPs), zur Verfügung. Die TPs können sich auf jedem beliebigen Knoten im Netz befinden, der über APPC verfügt. APPC verwendet das LU 6.2-Protokoll für den Datenaustausch zwischen Programmen, die sich auf verschiedenen logischen Einheiten (LUs) befinden. Außerdem unterstützt APPC mehrere gleichzeitig bestehende Verbindungen und Parallelsitzungen. Dialogsicherheit bzw. Sitzungssicherheit zwischen kommunizierenden Programmen wird von APPC ebenfalls unterstützt.

Der Communications Server stellt APPC-Durchsatz in leistungskritischen LAN-Umgebungen zur Verfügung. Der Communications Server unterstützt die folgenden Konnektivitäten:

Tabelle 1. Unterstützte APPC-Verbindungen

Protokolle	Verbindung	Verbindungsart
Kanal	• CDLC (OEM) • MPC	
LAN (802.2)	• Token-Ring • Ethernet • Frame Relay • ATM-LAN-Emulation	
SDLC	• Synchron • Autosynchron • Modems	• Automatische Anwahl, Anwahl über DTR, permanent • Automatische Anwahl • Automatische Anwahl, permanent • Automatische Anwahl
X.25	• Synchron • Hayes AutoSync • X.25-Netz	• Automatische Anwahl, semipermanent • Automatische Anwahl, permanent • Automatische Anwahl
IP	SNA über IP	Von IP zur Verfügung gestellte Verbindungen
IP	HPR über IP	Von IP zur Verfügung gestellte Verbindungen

Anmerkung: APPC/APPN verfügt auch über eine Datenkomprimierungsfunktion. Weitere Informationen hierzu sind im Abschnitt „Datenkomprimierung“ auf Seite 66 enthalten. Weitere Informationen zur Verschlüsselung können dem Abschnitt „SNA-Verschlüsselung auf Sitzungsebene“ auf Seite 69 entnommen werden.

SNA-Unterstützung für LU 6.2

LU 6.2 ist eine Architektur für die Kommunikation zwischen Programmen. Der Communications Server unterstützt die folgenden wahlfreien SNA-Funktionen für LU 6.2:

- Austausch formatierter Daten und formatfreier Datenaustausch
- Synchronisationsebene der Bestätigung
- Sicherheitsunterstützung auf Sitzungs- und Dialogebene
- Mehrere LUs
- Parallelsitzungen, einschließlich der Möglichkeit, ein fernes System zu verwenden, um die Anzahl der Sitzungen zu ändern
- Transaktionen im Simultanmodus in eine oder in beide Richtungen
- Mehrere gleichzeitige Verbindungen mit SSCP-PU-Sitzungen, von denen jede mit einem Unterbereichsnetz verbunden werden kann

Eine Auflistung aller Funktionen kann der Dokumentation *Communications Server Programming Guide and Reference* entnommen werden.

APPC-Konfigurationserweiterungen

Zur Basiskonfiguration der Endknoten werden lediglich vier Parameter benötigt: die Netz-ID, der Name des lokalen Knotens, die Verbindungsart und die Zieladresse. Die Systemdefinition wird durch folgende Faktoren eingeschränkt:

- Die von IBM gelieferten Modi
- Implizite Erstellung einer Partner-LU und von Modusdefinitionen bei Zuordnung eines Dialogs
- Implizite Initialisierung von Sitzungsbegrenzungen (Funktion CNOS), wodurch eine explizite Initialisierung der Sitzungsbegrenzungen vor der Zuordnung von Dialogen nicht mehr erforderlich ist
- Entfernen von Sitzungsbegrenzungen für lokale LUs und Partner-LUs, wodurch ein größerer Freiraum für die Konfiguration und Initialisierung von Modussitzungsbegrenzungen möglich ist
- Standardwerte für Transaktionsprogrammnamen, -betrieb und -typ, wodurch die Notwendigkeit entfällt, Transaktionsprogrammdefinitionen für anwendbare Programme zu konfigurieren
- Dynamische Konfigurationsaktualisierungen
- Definitionen für implizite SNA-Gateway-Datenstationen
- Die Möglichkeit, eine Datei mit der Erweiterung ACG zu editieren, die Konfigurationsparameter enthält
- Die Möglichkeit, Systemdefinitionsinformationen mit Discovery zu finden

Da die SNA-Konfiguration als Textdatei gespeichert wird, läßt sich die Datei mit Hilfe eines Editors oder eines vom Benutzer geschriebenen Programms schnell und leicht ändern. Eine aktive Konfiguration kann dann überprüft und dynamisch aktualisiert werden (ohne den Communications Server zu stoppen).

Als nächstes können Verbindungen zu mehreren Hosts konfiguriert werden; es können mehrere Host-Verbindungen gleichzeitig aktiv sein. Verbindungen können so konfiguriert werden, daß sie auf Anforderung oder als Ergebnis eines im fehlertoleranten Modus aufgetretenen Fehlers gestartet werden.

Die Unterstützung von Discovery durch den Communications Server ermöglicht es einem Knoten, den Steuerpunktnamen, die MAC-Adresse und die SAP-Adresse eines anderen Communications Server-Netzknoten-Servers in einem Token-Ring- oder Ethernet-LAN dynamisch zu suchen. Dies bedeutet, daß der Benutzer den Steuerpunktnamen, die MAC- oder die SAP-Adresse einer Partnereinheit nicht kennen muß, bevor eine Verbindung zu dieser Einheit hergestellt werden kann. Derzeit können Client Access/400- und Personal Communications-Benutzer diese Funktion verwenden.

APPC-Basiskonzepte

Der folgende Abschnitt enthält eine Einführung in die APPC-Konzepte und -Terminologie.

Transaktionsprogramme: Ein *Transaktionsprogramm* (TP) ist ein Programm oder Teil eines Anwendungsprogramms, das APPC-DFV-Funktionen verwendet. Anwendungsprogramme benutzen diese Funktionen, um mit Anwendungsprogrammen auf anderen Systemen, die APPC unterstützen, zu kommunizieren.

Der Communications Server stellt die APPC-API zur Verfügung und unterstützt die IBM SAA-CPI-C-Aufrufe für Transaktionsprogramme.

Transaktionsprogramme geben APPC-Parameter aus, um APPC-Funktionen aufzurufen. Ein ***Parameter*** ist eine formatierte Anforderung, die ein Transaktionsprogramm ausgibt und die von APPC ausgeführt wird. Ein Programm verwendet APPC-Parameterfolgen, um mit einem anderen Programm zu kommunizieren. Zwei miteinander kommunizierende Programme können sich auf demselben oder auf verschiedenen Systemen befinden. Die APPC-API ist in beiden Fällen dieselbe.

Tauscht ein Transaktionsprogramm mit einem anderen Daten aus, wird das zweite Transaktionsprogramm als ***Partner***-Transaktionsprogramm bezeichnet.

Transaktionsprogramme können CPI-C-Aufrufe ausgeben. Durch diese Aufrufe profitieren die Anwendungsprogramme von der Konsistenz, die SAA bietet.

Logische Einheiten: Jedes Transaktionsprogramm kann über eine ***logische Einheit*** (LU) auf ein SNA-Netz zugreifen. Eine LU ist eine SNA-Software, die von Benutzerprogrammen Parameter erhält und diese verarbeitet. Ein Transaktionsprogramm gibt APPC-Parameter an seine LU aus. Diese Parameter bewirken, daß Befehle und Daten über das Netz an die Partner-LU weitergeleitet werden. Außerdem fungiert eine LU als Mittler zwischen den Transaktionsprogrammen und dem Netz, um den Austausch von Daten zwischen Transaktionsprogrammen durchzuführen. Eine einzelne LU kann Services für mehrere Transaktionsprogramme zur Verfügung stellen. Im Knoten können mehrere LUs gleichzeitig aktiv sein.

LU-Typen: Der Communications Server unterstützt die LUs vom Typ 0, 1, 2, 3 und 6.2. Die LU-Typen 0, 1, 2 und 3 unterstützen die Kommunikation zwischen den Host-Anwendungsprogrammen und verschiedenen Einheiten, wie z. B. nichtprogrammierbaren Datenstationen und Druckern.

Die LU 6.2 unterstützt die Kommunikation zwischen zwei Programmen, die sich auf Unterbereichsknoten des Typs 5 und/oder auf peripheren Knoten des Typs 2.1 befinden, sowie die Kommunikation zwischen Programmen und Einheiten. APPC ist eine Implementierung der LU-6.2-Architektur.

LU-Sitzungen: Bevor die Transaktionsprogramme miteinander kommunizieren können, müssen ihre LUs in einer ***Sitzung*** miteinander verbunden werden. Da eine Sitzung zwei LUs miteinander verbindet, wird sie als ***LU-LU***-Sitzung bezeichnet. Abb. 1 zeigt diese Kommunikationsbeziehung.

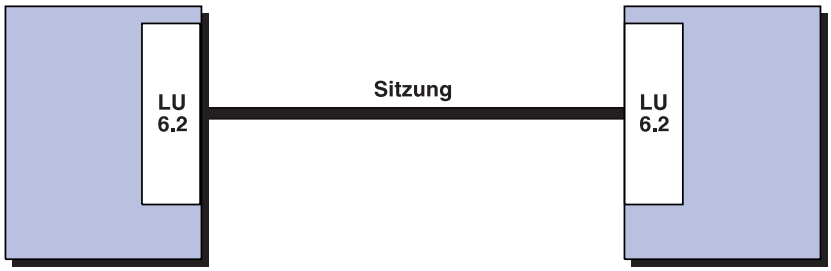


Abbildung 1. Sitzung zwischen zwei LUs (LU-LU)

Sitzungen haben die Funktion von Kanälen, die den Datenfluß zwischen zwei LUs in einem SNA-Netz steuern. Insbesondere sind Sitzungen für die Menge der übertragenen Daten, die Datensicherheit, die Weiterleitung von Daten im Netz und die Netzüberlastung zuständig.

Sitzungen werden von LUs verwaltet. Normalerweise arbeiten Transaktionsprogramme nicht mit Sitzungsmerkmalen. Sitzungsmerkmale werden folgendermaßen definiert:

- Bei der Konfiguration des Systems
- Bei der Verwendung der **SNA-Knotenoperationen**
- Bei der Verwendung der Verwaltungsparameter

Transaktionsprogrammdialoge: Die Kommunikation zwischen Transaktionsprogrammen wird ***Dialog*** genannt. Ähnlich wie beim Telefongespräch ruft ein Transaktionsprogramm das andere an, wobei sie einen „Dialog führen“, d. h., die beiden Transaktionsprogramme können miteinander kommunizieren, bis ein Transaktionsprogramm den Dialog beendet. Ein Dialog beginnt, wenn ein Transaktionsprogramm einen APPC-Parameter oder einen CPI-C-Aufruf ausgibt, durch den ein Dialog zugeordnet wird. Dialoge werden zwischen LU-LU-Sitzungen geführt.

Durch die Zuordnung eines Dialogs zu einer Sitzung wird eine Sende-Empfangsbeziehung zwischen den am Dialog beteiligten Transaktionsprogrammen hergestellt. Eines der beiden Transaktionsprogramme gibt Parameter zum Senden von Daten aus. Das andere Transaktionsprogramm gibt Parameter zum Empfangen von Daten aus.

Hat das sendende Transaktionsprogramm seine Datenübertragung beendet, kann es die Sendesteuerung des Dialogs an das empfangende Transaktionsprogramm übergeben. In Dialogen können Steuerinformationen und Daten ausgetauscht werden.

Abb. 2 zeigt einen Dialog zwischen zwei Transaktionsprogrammen in einer Sitzung.

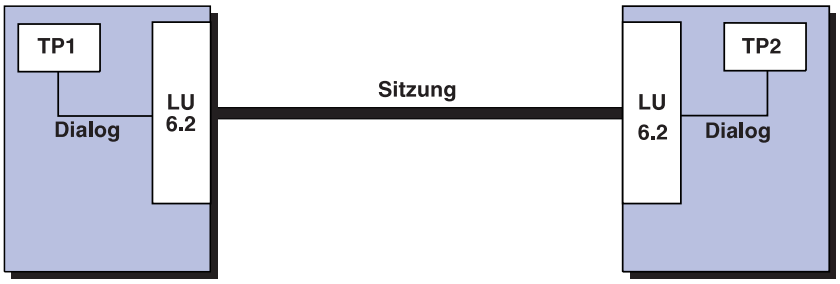


Abbildung 2. Dialog zwischen Transaktionsprogrammen in einer Sitzung

Eine Sitzung kann immer nur einen Dialog gleichzeitig unterstützen, nacheinander aber durchaus mehrere Dialoge. Da mehrere Dialoge Sitzungen erneut verwenden können, stellt eine Sitzung im Vergleich zum Dialog eine längerfristige Verbindung dar. Ordnet ein Programm einen Dialog zu und sind alle verfügbaren Sitzungen belegt, stellt die LU das ankommende Attach (Zuordnungsanforderung) zunächst in eine Warteschlange. Die Zuordnung wird durchgeführt, sobald eine Sitzung verfügbar wird.

Zwei LUs können auch Parallelsitzungen aufbauen, um mehrere Dialoge gleichzeitig zu unterstützen. Eine Parallelsitzung entsteht, wenn eines der Transaktionsprogramme einen Dialog zuordnet und eine Sitzung vorhanden ist, die aber durch einen anderen Dialog belegt ist. Die LU kann dann eine neue Sitzung anfordern, um die Zuordnung vorzunehmen.

Abb. 3 zeigt drei Parallelsitzungen zwischen zwei LUs; in jeder Sitzung wird ein Dialog ausgeführt.

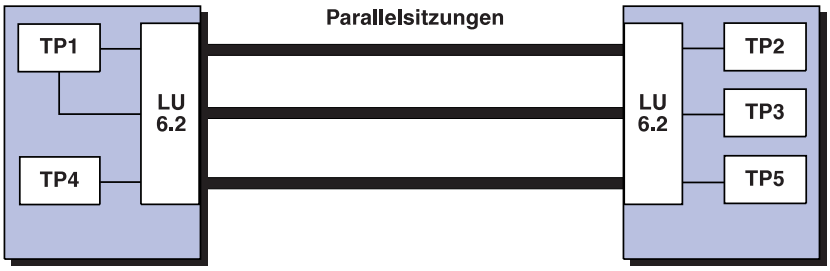


Abbildung 3. Parallelsitzungen zwischen LUs

Advanced Peer-to-Peer Networking (APPN)

Advanced Peer-to-Peer Networking (APPN) besteht aus einer Reihe von Funktionen, Formaten und Protokollen, die die Verwaltung eines SNA-Netzes erheblich erleichtern und die Benutzerfreundlichkeit einer APPC-Anwendung im Netz vergrößern. APPN erreicht dies durch Reduzierung der Konfigurationsanforderungen, dynamische Verzeichnissuche, Funktionen zur Berechnung des Leitwegs und der Weitervermittlung eines Sitzungsleitwegs.

Mit APPN lassen sich Programme erstellen, ohne daß die Einzeldaten des zugrundeliegenden Netzes bekannt sein müssen. Das einzige, was bekannt sein muß, ist der Name der Partner-LU, jedoch nicht, wo sie sich befindet. SNA ermittelt die Partner-LU-Lokation sowie den günstigsten Pfad zum Weiterleiten von Daten. Eine Änderung am zugrundeliegenden Netz, wie z. B. eine geänderte physische Adresse, das Hinzufügen eines neuen Adapters oder der Standortwechsel einer Einheit, hat keinen Einfluß auf die APPC-Programme.

Communications Server stellt Unterstützung für APPN-Endknoten und -Netzknoten für Datenstationen zur Verfügung, durch die die Kommunikation mit anderen Systemen im Netz erleichtert wird. Außerdem können mit der Erweiterungsfunktion für Zweigstellennetze Zweigstellen isoliert werden, um unnötigen CP-CP-Datenaustausch zu vermeiden.

- Die Endknotenfunktion umfaßt die folgenden Services:
  - Verbindung des lokalen Knotens mit einem Netzknoten, der Services zur Verfügung stellt, für Verzeichnis- und Weiterleitungsservices
  - Automatische erneute Aktivierung von CP-CP-Sitzungen, wenn die Verbindung eines Endknotens zu seinem Netzknoten-Server unterbrochen wird
- Die Netzknotenfunktion umfaßt die folgenden Services:
  - Services für die Weiterleitungsauswahl, die den besten Leitweg für eine Sitzung über ein APPN-Netz berechnen
  - Weitervermittlung eines Sitzungsleitwegs, die es zwei LUs an nicht benachbarten Knoten ermöglicht, an einer gemeinsamen Sitzung teilzunehmen, die über einen oder mehrere Zwischenknoten hinweg ausgeführt wird
  - Verzeichnisservices, die die Möglichkeit bieten, Partner-LU-Lokationen dynamisch zu ermitteln
  - Verbindungsnetzservices für das lokale Netz (LAN), die die Möglichkeit bieten, LAN-Zieladressen zu ermitteln, ohne sie konfigurieren zu müssen

    Diese Funktion ermöglicht es einem Knoten, eine direkte Verbindung zu einem anderen Knoten herzustellen, ohne daß eine LAN-Zieladresse konfiguriert sein muß.
  - Unterstützung für die Erweiterungsfunktion für Zweigstellennetze zur effizienten Verbindung einer Zweigstelle mit LANs, Endknoten und LEN-Knoten mit abhängigen und unabhängigen LUs, PUs (z. B. Schaltermaschinen) mit einem oder mehreren WANs. Dadurch können Netzknoten als Gateways für Zweigstellen fungieren. Ein LAN in jeder Zweigstelle kann als ein Verbindungsnetz konfiguriert werden.

Programmierschnittstellen

Communications Server unterstützt auf dem Server viele verschiedene 32-Bit-Anwendungsprogrammierschnittstellen (APIs) für Entwickler von Anwendungsprogrammen. Durch diese APIs können Anwendungsprogramme einfach auf Communications Server-Funktionen zugreifen und die DFV-Anforderungen von Verbindungen zu IBM Computern und zu Computern anderer Hersteller erfüllen. Außerdem unterstützen die mitgelieferten Schnittstellen SNA-Protokolle, d. h., die Standardisierung ist gewährleistet.

Zu den unterstützten APIs gehören die folgenden:

- Advanced Program-to-Program Communications (APPC)
- Common Programming Interface for Communications (CPI-C)
- Konventionelle LUA-RUI und -SLI
- Host Access Class Libraries (HACL)
- Java CPI-C (JCPI-C)
- WinSock (im Verbund mit AnyNet Sockets über SNA)
- Network Operator Facility (NOF)
- Verwaltungsservices
- Allgemeine Services

Auf den Clients wird außerdem die EHNAPPC-API (Enhanced APPC) bereitgestellt.

Für Anwendungsentwickler steht zudem das Communications Server Software Developers Tool Kit (das separat von der Communications Server-CD-ROM installiert werden kann) zur Verfügung. Es enthält Beispiele, Kopfdateien, Bibliotheksdateien und Online-Bücher zu den einzelnen APIs.

Weitere Informationen zu Communications Server-Programmierschnittstellen enthalten die Handbücher *Client/Server Communications Programming* und *System Management Programming*.

High Performance Routing (HPR)

High Performance Routing (HPR) ist eine Erweiterung zu APPN, die die Leistungsfähigkeit und Zuverlässigkeit der Datenweiterleitung erhöht und eine virtuelle Verbindung zwischen RTP-Knoten (RTP - Rapid Transport Protocol) herstellt. HPR ersetzt die Weitervermittlung eines Sitzungsleitwegs, die Weiterleitungsmethode, die in APPN verwendet wird.

HPR stellt schnellere Übertragungen an Zwischenknoten zur Verfügung, leitet Sitzungen an fehlerhaften Knoten und fehlgeschlagenen Verbindungen ohne Unterbrechung vorbei und reguliert den Datenfluß, indem es Netzüberlastungen vorhersieht und reduziert.

Communications Server unterstützt HPR-Verbindungen über Enterprise Extender (IP), SDLC (Synchronous Data Link Control, SDLC - synchrone Datenübertragungssteuerung), LAN, WAN, Kanal, MPC (Multi-Path Channel) und X.25-Verbindungen.

SNA-Datenkomprimierung

Die Datenkomprimierung auf Sitzungsebene erhöht den Durchsatz großer Datenmengen über DFV-Verbindungen und erzielt dadurch folgende Vorteile:

- Höherer Datendurchsatz auf langsamen Leitungen
- Kostensenkung bei teuren Verbindungen
- Kürzere Antwortzeiten und dadurch höhere Produktivität

Die SNA-Datenkomprimierung ist kompatibel mit den S/390- und AS/400-Implementierungen und kann mit allen LU-Typen verwendet werden.

Erkennung der Servicegeber mit Discovery

Discovery ist ein Protokoll für die LAN-Adreßauflösung, mit dem ein LAN-Knoten einen anderen LAN-Knoten lokalisieren kann, der den angegebenen Suchkriterien entspricht. Wenn die Suchparameter entsprechend angepaßt werden, kann ein Knoten nach APPN-Netzknoten, Knoten mit SNA-Grenzfunktion, AS/400-Systemen, SNA-Gateways oder benutzerdefinierten Server-Klassen suchen. Ein Server mit Communications Server für Windows NT kann auf Client-Anforderungen als Netzknoten-Server, als PU 2.0-Gateway oder als benutzerdefinierte Server-Klasse antworten. Außerdem kann ein Communications Server mit Hilfe von Discovery APPN-Knoten und SNA-Gateways lokalisieren.

Abhängiger LU-Requester (DLUR)

Der Communications Server bietet Unterstützung für DLUR-Endknoten und -Netzknoten für Datenstationen, damit diese die Vorteile der erweiterten SSCP-Unterstützung nutzen können, die ein abhängiger LU-Server (DLUS - Dependent LU Server) zur Verfügung stellt. Der DLUS wird von VTAM Version 4 Release 2 und höher unterstützt. Durch diese Unterstützung können traditionelle abhängige SNA-LUs, wie z. B. Emulationsprogramme und sogar Drucker, die zahlreichen Vorteile eines APPN-Netzes nutzen.

Einige dieser Vorteile sind:

- Abhängige LUs können sich an Knoten befinden, die keine Nachbarknoten des Hosts sind
- APPN-Suchlogik kann verwendet werden, um den besten Pfad für LU-LU-Sitzungen zu ermitteln

Weitere Informationen zum DLUR enthält der Abschnitt „Unterstützung für abhängigen LU-Requester (DLUR)“ auf Seite 61.

SNA-Gateway

Ein Gateway ermöglicht die Kommunikation zwischen Hosts, die PU 2.0-Datenstationen und Datenstationen unterstützen, die andere DLC-Arten verwenden. Ein SNA-Gateway kann die folgenden Funktionen übernehmen:

- Datenstationen die gemeinsame Benutzung derselben Host-Verbindung ermöglichen
- Datenstationen, die keine Funktion für mehrere PUs haben, Konnektivität zu mehreren Hosts zur Verfügung stellen
- Als PU-Pool für dedizierte untergeordnete PU-Datenstationen fungieren
- Als Protokollumsetzer zwischen Datenstationen fungieren, die für ihre Verbindungen DLCs verwenden, die sich von der DLC unterscheiden, die für die Host-Verbindung verwendet wird
- Systemdefinition auf dem Host und auf den Datenstationen reduzieren
- Dynamische Änderungen an den Netzdefinitionen und dynamisches Hinzufügen von Datenstationen ermöglichen
- Host-Ressourcen und die Anzahl der Host-Verbindungen reduzieren durch Verwendung eines LU-Pools und automatische Abmeldung der Sitzungen, die innerhalb eines vom Benutzer definierten Zeitraums nicht benutzt werden
- Zuverlässigkeit erhöhen durch Bereitstellung von Host-Ausweichverbindungen

Mit dem SNA-Gateway kann ein Host der Systemfamilie IBM System /390 Datenstationen unterstützen, die die LU-Typen 0, 1, 2, 3 oder die abhängige LU 6.2 (APPC) implementieren. Der SNA-Gateway unterstützt außerdem die LU-Typen 0, 1, 2 oder 3 für einen Host des Systems IBM AS/400. Der Host des Systems IBM AS/400 übergibt die Daten an einen Host der Systemfamilie IBM /390.

Jeder Host betrachtet den SNA-Gateway als einen SNA-PU-2.0-Knoten, der pro Datenstation eine oder mehrere LUs unterstützt. In bezug auf den Host gehören alle LUs zu der SNA-Gateway-PU. Der SNA-Gateway kann mehrere Host-Verbindungen gleichzeitig haben und verschiedene Datenstationssitzungen bestimmten Hosts zuordnen. Nur ein Host (und dieser muß sich an einer Verbindung mit der CP-PU befinden) kann als zentrales Alert-Verarbeitungssystem fungieren, und der Steuerpunktname wird an alle über den Gateway weitergeleiteten NMVTs angehängt.

Für die unterstützten Datenstationen sieht der SNA-Gateway wie eine SNA-PU-4-DFV-Steuereinheit aus; er leitet Host-Nachrichten wie z. B. BIND und UNBIND weiter. Die LUs des Netzes erkennen den SNA-Gateway nicht. Der SNA-Gateway erkennt jedoch alle LUs auf den Datenstationen.

AnyNet-Unterstützung

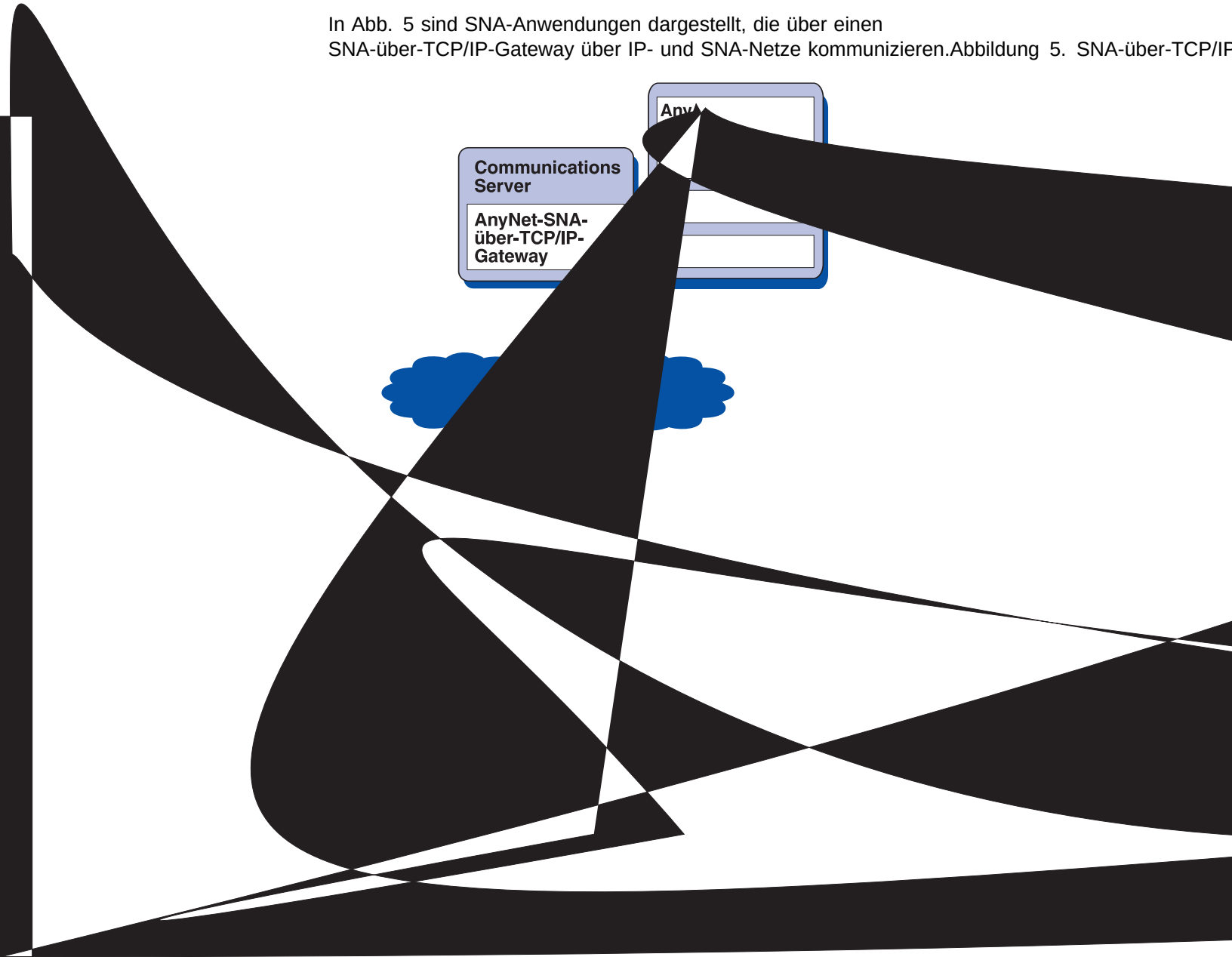
Der Communications Server vereinigt die Funktionen SNA über TCP/IP und Sockets über SNA der AnyNet-Produktfamilie. Durch diese Unterstützung kann ein vorhandenes Netz erweitert und vereinfacht werden, da SNA-Anwendungen über ein TCP/IP-Netz und Sockets-Anwendungen über ein SNA-Netz Daten ohne Änderungen der Anwendungen übertragen können.

SNA über TCP/IP

Die SNA-über-TCP/IP-Zugriffsknotenfunktion ermöglicht die Übertragung zwischen SNA-Anwendungen in einem IP-Netz. Diese Funktion unterstützt unabhängige LU 6.2 sowie abhängige LU 0, 1, 2, 3 oder 6.2 entweder mit oder ohne abhängigen LU-Requester (DLUR). Außerdem kann der SNA-über-TCP/IP-Zugriffsknoten in Kombination mit einem SNA-Gateway verwendet werden, um SNA-Gateway-Sitzungen über TCP/IP zu aktivieren.

Die SNA-über-TCP/IP-Gateway-Funktion erweitert den Einsatzbereich von SNA-Anwendungen, weil sie SNA-Anwendungen in einem SNA-Netz den Datenaustausch mit SNA-Anwendungen in einem IP-Netz ermöglicht. Der SNA-über-TCP/IP-Gateway unterstützt unabhängige LU 6.2-Sitzungen.

In Abb. 5 sind SNA-Anwendungen dargestellt, die über einen SNA-über-TCP/IP-Gateway über IP- und SNA-Netze kommunizieren.Abbildung 5. SNA-über-TCP/IP

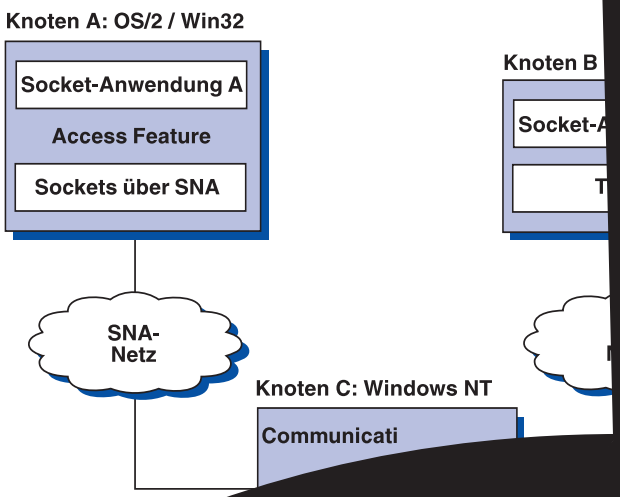


Sockets über SNA

Die Sockets über SNA-Zugriffsknotenfunktion erm
programmen, die die Socket-Schnittstelle WinSoc
wenden, die Übertragung über ein SNA-Netz.

Die Sockets-über-SNA-Gateway-Funktion ermögli
Socket-Anwendungen in SNA- und TCP/IP-Netzer
werden häufig dazu verwendet, unabhängige TCP
SNA-Netz zu verbinden.

In Abb. 6 sind Sockets-Anwendungen dargestellt,
Sockets-über-SNA-Gateway über IP- und SNA-Ne



TN3270E-Server

Mit der TN3270E-Server-Funktion können TCP/IP-Benutzer auf Anwendungen zugreifen, die sich auf einer Host-Maschine in einem SNA-Netz befinden. Alle TN3270- oder TN3270E-Client-Datenstationen, die dem Industriestandard entsprechen, können eine Verbindung zu TN3270E-Servern herstellen, um auf SNA-Netze zuzugreifen. Der TN3270E-Server unterstützt ATTN- und SYSREQ-Schlüsselverarbeitung und das Drucken von Host-Anwendungen aus auf an einer Datenstation angeschlossenen Druckern. Dabei kann es sich um lokale oder Netzdrucker handeln.

Communications Server unterstützt den Lastausgleich für Client-Verbindungen eines TN3270E-Servers, die zu denselben Host-Ressourcen führen, wenn der Client für den Lastausgleich konfiguriert ist.

TN3270E-Server unterstützt die IP- und Host-Namen-Filterung, die gesteuerten Zugriff auf LUs ohne Ändern von Client-Konfigurationen ermöglicht.

TN3270E-Server unterstützt außerdem die SSL-Identifikationsüberprüfung und -Verschlüsselung (SSL - Secure Sockets Layer) für sicheren Zugriff im TCP/IP-Netz. Wenn Sicherheit angegeben wird, muß der Server über ein von einer Zertifizierungsstelle (z. B. Verisign) ausgestelltes überprüftes Prüfdokument verfügen. Communications Server stellt ein Dienstprogramm zum Generieren und Verwalten von Schlüsseln und Prüfdokumenten zur Verfügung, die von SSL Version 3 verwendet werden.

In Abb. 7 ist ein Beispiel für TN3270E-Server-Verbindungen dargestellt.

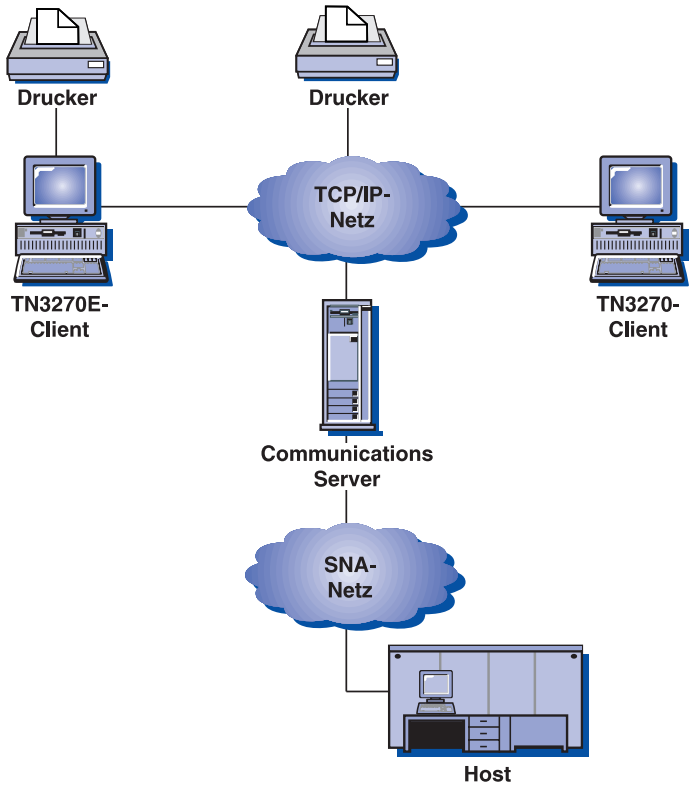


Abbildung 7. TN3270E-Server-Verbindungen

TN5250-Server

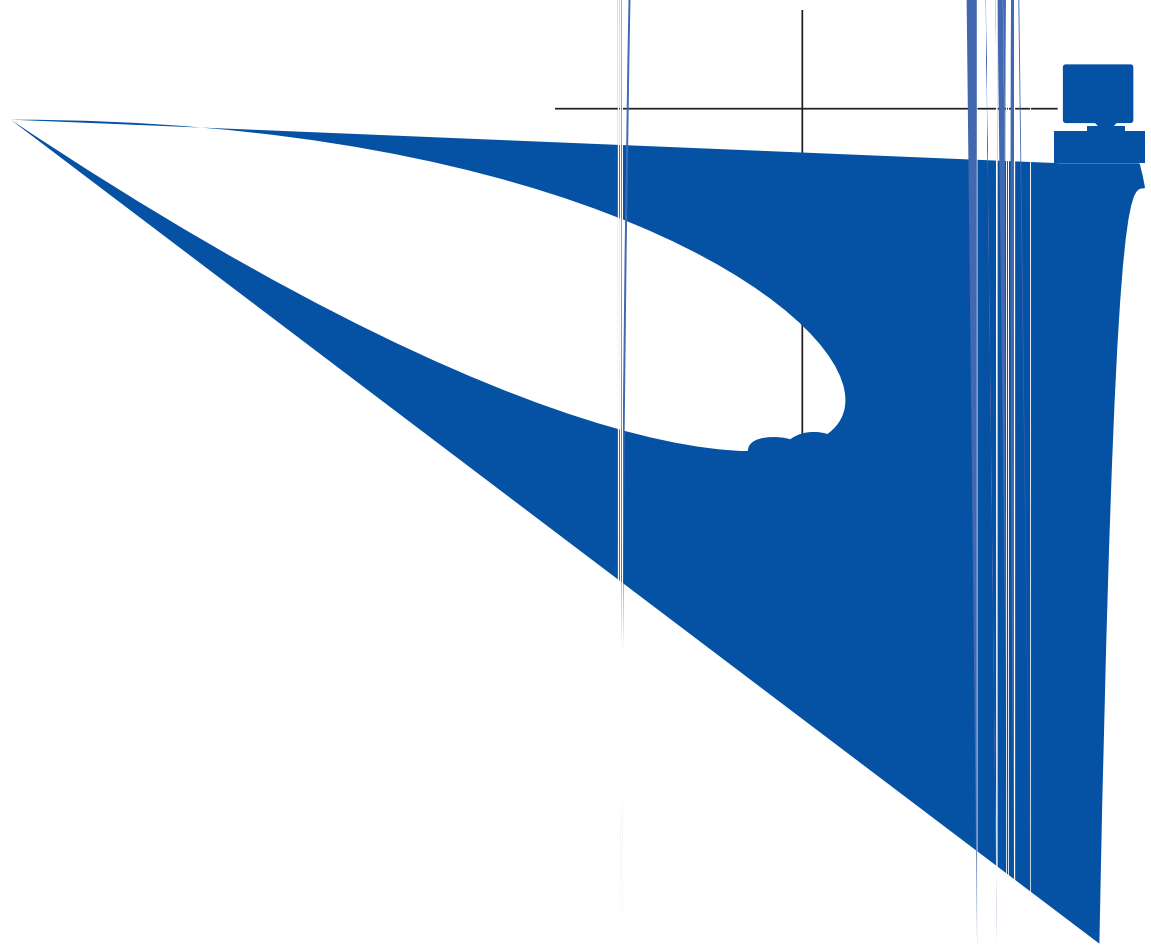
Mit der TN5250-Server-Funktion können TCP/IP-Benutzer auf Anwendungen zugreifen, die sich auf einer AS/400 in einem SNA-Netz befinden. Alle TN5250-Client-Datenstationen, die dem Industriestandard entsprechen, können eine Verbindung zu dem TN5250-Server herstellen, um auf SNA-Netze zuzugreifen.

Communications Server unterstützt den Lastausgleich für Client-Verbindungen von TN5250-Servern, die zu denselben AS/400-Systemen führen, wenn der Client für den Lastausgleich konfiguriert ist.

TN5250-Server unterstützt die IP- und Hostnamen-Filterung, die zentrales Verwalten des Client-Zugriffs auf den Server sowie die Client-Ausrichtung auf bestimmte AS/400-Systeme ermöglicht.

TN5250-Server unterstützt außerdem die SSL-Identifikationsüberprüfung und -Verschlüsselung (SSL - Secure Sockets Layer) für sicheren Zugriff im TCP/IP-Netz. Wenn Sicherheit angegeben wird, muß der Server über ein von einer Zertifizierungsstelle (z. B. Verisign) ausgestelltes überprüftes Prüfdokument verfügen. Communications Server stellt ein Dienstprogramm zum Generieren und Verwalten von Schlüsseln und Prüfdokumenten zur Verfügung, die von SSL Version 3 verwendet werden.

In Abb. 8 ist ein Beispiel für TN5250-Server-Verbindungen dargestellt.



Zugriff auf Daten, die mit anderer Software erstellt wurden

Communications Server unterstützt den Zugriff auf Daten, die sich auf Host-Maschinen, AS/400-Systemen und Datenstationen in SNA-Netzen befinden mit den folgenden Funktionen:

- AS/400 OLE DB Provider
- Host Publisher
- AS/400-Server für gemeinsam benutzte Ordner

AS/400 OLE DB Provider

Anwendungen, die OLE DB oder ActiveX verwenden, können über Communications Server auf Satzebene auf Dateien auf einem AS/400-System zugreifen. Dokumentation für diese Funktion sowie Informationen zum Entwickeln dieser Anwendungen mit Hilfe von Client Access enthält das Verzeichnis `csnt\sdk\as400_oledb`.

Host Publisher

Host Publisher ermöglicht den Web-Zugriff auf umfangreiche Web-Sites mit dynamischem Inhalt. Mit Host Publisher kann auf Daten auf S/390- oder AS/400-Hosts zugegriffen werden, um diese auf Web-Seiten zu veröffentlichen, die dynamisch nach dem Design des Benutzers erstellt wurden.

AS/400-Server für gemeinsam benutzte Ordner

Das AS/400-System verwendet Ordner zum Speichern und geordneten Ablegen von Dokumenten, elektronischer Post und anderen zugehörigen Objekten. Mit Communications Server können Platteneinheiten auf dem Server erstellt werden, die den Datenaustausch mit AS/400-Ordnern über AS/400 IFS (Integrated File System) ermöglichen. Wenn diese Platteneinheiten für gemeinsame Benutzung mit dem Server konfiguriert sind, können Clients mit NET USE eine Verbindung zu ihnen herstellen. Auf diese Weise können viele Clients die Verbindung zu Ordnern in dem AS/400-System so herstellen, als wären sie Laufwerke der lokalen Datenstation.

Mit gemeinsam benutzten Ordnern kann folgendes ausgeführt werden:

- Durch AS/400-Sicherheitsfunktionen den Zugriff auf Datenstationsdateien begrenzen
- Daten gleichzeitig mit vielen anderen Benutzern gemeinsam benutzen
- Datenstationsdateien in einem AS/400-Ordner sichern

Communications Server Client-Unterstützung

Communications Server stellt Unterstützung für SNA-API-Clients (auf der CD-ROM verfügbar) und für Novell IntranetWare für SAA-Clients zur Verfügung.

SNA-API-Client-Unterstützung

Die Communications Server-Unterstützung für SNA-API-Clients ermöglicht über TCP/IP und IPX verbundenen Clients den Zugriff auf SNA-APIs, ohne daß SNA-Protokolle zwischen den Clients und dem Server aktiv sein müssen. Dadurch kann die SNA-Konfiguration zum größten Teil auf dem zentralen Server erfolgen.

Communications Server unterstützt SNA-API-Clients unter Windows 95, Windows NT, Windows 3.1 und OS/2.

Die SNA-Clients bieten Unterstützung für CPI-C-, APPC-, EHNAPPC-, LUA-RUI-, JCPI-C- und HACL-API-Schnittstellen, wobei die eigentliche SNA-Verarbeitung auf dem Server stattfindet. Diese Clients werden zwar als Komponente des Servers bereitgestellt, installiert und konfiguriert werden sie jedoch auf dem Client.

Die 32-Bit-Windows- und -OS/2-Clients verfügen zusätzlich über die folgenden Verbesserungen:

- Verschlüsselung zwischen Client und Server
- Detailliertere Trace-Formatierung zur Erleichterung der Fehlerbehebung
- Starten und Stoppen des Trace-Vorgangs kann erfolgen, während der Client aktiv ist
- Client kann ohne Deinstallieren erneut installiert werden

Die Windows NT- und Windows 95-Clients werden über die gleiche ausführbare Datei ausgeführt. Diese Programmdatei kann auf einem gemeinsam benutzten Laufwerk installiert werden; Programmkorrekturen gelten für beide Clients. Der neue 32-Bit-Windows-Client kann mit Communications Servern sowie mit Novell IntranetWare- oder NetWare für SAA-Servern Daten austauschen.

Weitere Informationen zu den API-Clients von Communications Server enthält der Abschnitt „Planung für Client/Server-Kommunikation“ auf Seite 105.

Unterstützung für Novell IntranetWare für SAA-Client

Communications Server unterstützt über IPX oder TCP/IP verbundene Clients mit Emulationssoftwarepaketen, die die Novell Queue Element/Message Unit-Architektur (QEL/MU) für 3270-Emulation implementieren, wodurch die Clients Zugriff auf Großrechner-Host-Daten erhalten. Dazu gehört auch die Unterstützung häufig verwendeter Client-Funktionen, z. B. für LU-Kategorien wie dediziert, im Pool und PUBLIC (gelegentlich auch als Ressourcenarten bezeichnet).

Communications Server unterstützt Novell IntranetWare für SAA-Clients unter Windows 95, Windows NT, Windows 3.1 und OS/2.

Weitere Informationen zum Entwickeln dieser Clients enthält das Handbuch *Novell NetWare for SAA 3270 Client Interface Guide and Reference* mit der Teilenummer 100–002018–001.

Lastausgleich

Communications Server unterstützt jetzt den Lastausgleich für alle Client-Typen. Der Lastausgleich ermöglicht das Verteilen von LU 0 bis 3- und LU 6.2-Sitzungen auf Communications Server und IntranetWare für SAA-Server. Der Server gibt Services einschließlich Belastungsfaktoren an, die von Clients oder Servern gesammelt und verwaltet werden können, um einen Server auszuwählen.

Verzeichnisausnutzung

Zur Vereinfachung des Konfigurationsprozesses können mehrere Clients von einer zentralen Position aus mit dem Protokoll LDAP (Lightweight Directory Access Protocol) konfiguriert werden.

Informationen zur Verwendung der Verzeichnisausnutzung enthält der Abschnitt „Planung für Client/Server-Kommunikation“ auf Seite 105.

Konfigurations- und Verwaltungsunterstützung

Communications Server stellt Funktionen zum Konfigurieren und Verwalten von Ressourcen zur Verfügung.

Communications Server-Konfiguration

Dieser Abschnitt enthält eine Übersicht über die Komponenten der Communications Server-Konfiguration und die Verfahren zu ihrer Erstellung oder Änderung. Die Konfiguration besteht aus einer einzigen Datei (ACG) im Unterverzeichnis PRIVATE des Verzeichnisses, in dem das Produkt installiert ist (z. B. C:\IBMCS\PRIVATE). Die ACG-Datei kann mit der **Knotenkonfiguration** oder mit einem ASCII-Editor erstellt bzw. geändert werden. Mit einem ebenfalls bereitgestellten Prüfprogramm kann die ACG-Datei vor der Verwendung auf ihre Gültigkeit überprüft werden.

Zum Erstellen oder Ändern einer Communications Server-Konfiguration können folgende Methoden verwendet werden:

- **Knotenkonfiguration**
- Antwortdateikonfiguration

Knotenkonfiguration: Der Communications Server beinhaltet die Anwendung **Knotenkonfiguration** (PCSCFG), mit der die Communications Server-Funktionen über eine grafische Schnittstelle konfiguriert werden können; sie stellt Standardwerte zur Verfügung, so daß die Konfiguration mit einer minimalen Anzahl an Parametern ausgeführt werden kann. Wenn eine Konfiguration abgeschlossen ist, wird sie automatisch überprüft, und, sofern keine Konflikte auftreten, werden die erforderlichen Konfigurationsdateien erstellt. Beim Auftreten von Konflikten werden die Fehler gemeldet, so daß sie in der Konfiguration korrigiert werden können.
Die lokale Konfiguration wird auf Client- und Server-Ebene unterstützt. Die Fernkonfiguration des Servers wird von Windows NT- und Windows 95-Clients unterstützt.

Die meisten Konfigurationen können mit der **Knotenkonfiguration** erstellt werden. Einige Schlüsselwörter und Schlüsselwortparameter werden jedoch von der **Knotenkonfiguration** nicht unterstützt.

Antwortdateikonfiguration: Durch die Konfiguration mit Hilfe einer Antwortdatei kann eine Schablonenkonfigurationsdatei an die vom Benutzer gestellten Anforderungen angepaßt werden. Weitere Informationen zum Erstellen einer Konfiguration mit Hilfe von Antwortdateien enthält der Abschnitt „Konfiguration mit Schablonen- und Antwortdateien“ auf Seite 210.

SNA-Knotenoperationen: Die **SNA-Knotenoperationen** ermöglichen das Erstellen und Ändern ausgewählter Ressourcen.

Communications Server-Verwaltung

Communications Server stellt die folgenden Funktionen zum Verwalten von Ressourcen zur Verfügung.

- **SNA-Knotenoperationen**
- Befehlszeilendienstprogramme
- Verwaltung über das Web
- Tivoli Plus-Modul

Weitere Informationen zu den Möglichkeiten dieser Funktionen enthält der Abschnitt „Systemverwaltungseinrichtungen“ auf Seite 225.

Lastausgleich

Der Lastausgleich ist eine Communications Server-Funktion, die abhängige LU-Sitzungen (Host-zu-Datenstation) und unabhängige LU 6.2-Sitzungen dynamisch ausgleicht, indem diese auf den Datenfernverarbeitungs-Server mit der geringsten Auslastung verlegt werden. Communications Server ermöglicht den Lastausgleich für Communications Server-API-Programme und für 3270-Emulationen anderer Hersteller, die über TCP/IP-Protokolle verbunden werden, oder über TN3270- und TN5250-Emulationen anderer Hersteller. Welche Ressourcen in den Lastausgleich einbezogen werden, hängt von der Sitzungsart ab:

- Bei abhängigen LU-Sitzungen erfolgt der Lastausgleich zwischen den Servern innerhalb eines benannten LU-Pools und eines benannten Bereichs.
- Bei LU 6.2-Sitzungen erfolgt der Lastausgleich zwischen allen verfügbaren Servern in einem benannten Bereich oder zwischen den ausgewählten Servern in einer benannten Server-Liste.

Die Lastausgleichfunktionen von Communications Server sind in die SNA-Client-APIs integriert. Der Lastausgleich für die Clients wird über die **SNA-Client-Konfiguration** konfiguriert.

Bei abhängigen LU-Sitzungen können Emulationen, die SNA-Client-APIs verwenden, am Lastausgleich teilnehmen. Andernfalls ist der Kauf von 3270-, TN3270- oder TN5250-Emulationssoftware anderer Hersteller, die den Lastausgleich unterstützt, erforderlich.

Bei LU 6.2-Sitzungen entscheidet die vom SNA-API-Client hergestellte einleitende Verbindung darüber, welcher Server alle nachfolgenden LU 6.2-Sitzungen verwaltet.

Weitere Informationen zum Lastausgleich können dem Abschnitt „Planung für den Lastausgleich“ auf Seite 161 entnommen werden.

Datensicherheit

Communications Server stellt grundlegende und erweiterte Sicherheitsunterstützung auf Sitzungs- und Dialogebene zur Verfügung. Eine Sicherheitsfunktion besteht in der Begrenzung der Windows NT-Benutzer, die über die SNA-API-Clients auf SNA-Ressourcen Zugriff erhalten. Die Dialogsicherheit beinhaltet Unterstützung für die Kennwortsubstitution. Außerdem steht erweiterte LU-LU-Sicherheit zur Verfügung.

Communications Server bietet Unterstützung für SSL-Sicherheit (SSL - Secure Sockets Layer) für Verbindungen zwischen TN-Clients und dem TN3270E- oder dem TN5250-Server. Diese Sicherheitsfunktion verwendet SSL Version 3, um Datenverschlüsselung und Server-Identifikationsüberprüfung mit unterzeichneten Prüfdokumenten zur Verfügung zu stellen.

Adapterunterstützung

Communications Server stellt Adapterherstellern eine offene Schnittstelle zum Erstellen von Konnektivitätslösungen zur Verfügung. Eine nichtprogrammierbare Adapterschnittstelle steht für Adapterhersteller für die Communications Server-SDLC- und -X.25-Protokollgruppe zur Verfügung. Eine programmierbare Adapterschnittstelle für Adapterhersteller zum Erstellen von Konnektivitätslösungen mit vom Hersteller bereitgestellten Datenübertragungssteuerungen steht ebenfalls zur Verfügung.

DLC-Unterstützung

Communications Server ermöglicht die Datenfernverarbeitung über folgende DLCs:

- AnyNet (SNA über TCP/IP)
- Twinaxial (nur übergeordnet)
- LAN (alle mit NDIS übereinstimmenden Netzadapter)
- X.25 SDLC (synchron, asynchron und AutoSync)
- OEM (Unterstützung für Adapter von Fremdherstellern)
- Kanal (nur übergeordnet)
- MPC (nur HPR)
- Enterprise Extender

AnyNet-DLC (SNA über TCP/IP)

Weitere Informationen zur AnyNet-SNA-über-TCP/IP-DLC können in „SNA über TCP/IP“ auf Seite 14 nachgelesen werden.

IBM-MPC-DLC

Die MPC-DLC unterstützt Glasfaserverbindungen mit hoher Kapazität und Verfügbarkeit zu einem oder mehreren MPC-fähigen Hosts des IBM Systems /390 über die ESCON-Kanal-Adapterkarte (P/N 9663 001). MPC-Verbindungen bieten hohe Übertragungsgeschwindigkeiten mit transparenter Sicherung, falls physische Verbindungen unterbrochen werden oder vorübergehend nicht verfügbar sind. Über diese Kanal-zu-Kanal-Verbindung kann für LAN-Clients problemlos Zugriff auf S/390-Ressourcen und -Services bereitgestellt werden.

Enterprise Extender-DLC

Communications Server stellt jetzt auch HPR-Verbindungen in IP-Netzen unter Verwendung von UDP/IP-Paketen zur Verfügung. Vom HPR-Netz wird das zentrale IP-Netz als eine logische Verbindung angesehen. Vom IP-Netz werden die SNA-Übertragungen als UDP-Datagramme angesehen. Diese Datagramme werden unverändert an das zentrale IP-Netz weitergeleitet. Da keine Protokollumsetzung erfolgt und die Paketierung auf der Leitwegschicht ohne die Einbeziehung zusätzlicher Transportschichten stattfindet, führt dies zu einer effizienten Nutzung der Intranet-Infrastruktur für IP-Clients, die auf SNA-Daten zugreifen (z. B. TN3270-Clients oder Web-Browser mit IBM Host On-Demand) und für SNA-Clients.

APPN-MIB-Unterstützung

Communications Server unterstützt SNMP-Anforderungen (SNMP - Simple Network Management Protocol) für APPN-Verwaltungsinformationen von jedem SNMP-Verwaltungssystem aus.

Fehlertoleranter Modus

Beim Communications Server können bestimmte Host-Verbindungen so konfiguriert werden, daß sie automatisch aktiviert werden, wenn ein angegebener kritischer Server ausfällt. Dies bedeutet, daß konfigurierte Verbindungen zu einem Host durch Aktivierung alternativer Verbindungen auf einem Sicherungs-Server weiter benutzt werden können. Diese Funktion wird als fehlertoleranter Modus bezeichnet.

Die in einer kritischen Server-Konfiguration auf dem Sicherungs-Server benannten Verbindungen werden aktiviert, wenn der Sicherungs-Server eine Unterbrechung der Verbindung zum kritischen Server feststellt. Die Lizenz für den kritischen Server geht auf den Sicherungs-Server über.

Anmerkung: Der fehlertolerante Modus läßt nur die Aktivierung von Host-Verbindungen auf einem Sicherungs-Server zu und setzt Emulationssoftware voraus, die Ausweichpfade zum Sicherungs-Server unterstützt, wenn ein kritischer Server inaktiv wird.

Weitere Informationen zum fehlertoleranten Modus für Ausweichverbindungen können in „Planung für Sicherungs-Host-Verbindungen“ auf Seite 165 nachgelesen werden.

Entry-Level-Emulationsfunktionen

Communications Server beinhaltet eine Entry-Level-Version der häufig verwendeten Personal Communications 3270- und -5250-Emulation für Verwaltungszwecke. Diese Emulation bietet 5250- und 3270-Basisunterstützung auf dem Server, für einen Teil der Einrichtungen und Funktionen, die in der Vollversion der IBM Personal Communications-Produktfamilie der Emulationen enthalten sind.

Zu den verfügbaren Entry-Level-Emulationsfunktionen gehören die folgenden:

- Farbabgleich
- Befehlszeilenübertragung (nur 3270)
- Vollständiger Schriftartsatz
- Anzeigegrößen 2-5
- Zwei Sitzungen

Die grafische Tastaturneubelegung wird von der Entry-Level-Emulation zwar nicht unterstützt, aber der Benutzer kann die von der Vollversion der Emulation generierten Neubelegungsdateien verwenden.

Communications Server und SNA

In diesem Kapitel werden die vom Communications Server zur Verfügung gestellten SNA-Netzfunktionen vorgestellt. Das Kapitel enthält folgende Themen:

- Übersicht über SNA-Funktionen
- DLC-Definitionen
- Advanced Peer-to-Peer Networking (APPN)
- High Performance Routing (HPR)
- LU-Unterstützung
- Datenkomprimierung
- Verschlüsselung
- Verwaltungsservices (MS - Management Services)
- Flußsteuerung
- SNA-Gateway-Unterstützung

Überblick über SNA-Funktionen

Dieser Abschnitt enthält eine Übersicht, wie der Communications Server SNA auf einer Datenstation implementiert. Hier wird keine ausführliche Beschreibung der SNA-Funktionen gegeben. Genauere Informationen zu SNA können der folgenden Dokumentation entnommen werden:

- *Systems Network Architecture Concepts and Products*
- *Systems Network Architecture Technical Overview*
- *Systems Network Architecture Network Product Formats* (online in der Dokumentationsliste von Communications Server verfügbar)
- *Systems Network Architecture Format and Protocol Reference Manual: Architecture Logic for LU Type 6.2*

SNA definiert die Standardwerte, Protokolle und Funktionen, die von den Einheiten im Netz verwendet werden (vom Großrechner bis zu den Datenstationen), um mit einer anderen Einheit zu kommunizieren. Diese Kommunikation ermöglicht es den Einheiten, Informationen transparent gemeinsam zu benutzen und Ressourcen zu verarbeiten. Dies bedeutet, daß ein Benutzer an einer Datenstation nicht wissen muß, was im Hintergrund abläuft, um auf Informationen auf einem Host zuzugreifen oder um mit anderen Benutzern zu kommunizieren.

Ein SNA-Netz ist als System von Knoten und Verbindungen aufgebaut. Wichtig ist, daß dieser Aufbau nach logischen Gesichtspunkten gestaltet ist. SNA klassifiziert die Knoten nach ihren Funktionen und danach, in welchem Ausmaß sie andere Knoten im Netz steuern. Der Knotentyp ist nicht notwendigerweise mit einem speziellen Hardwaretyp verbunden. Die Funktionen eines Knotens können von verschiedenen Einheiten ausgeführt werden. Eine Datenstation, die als Gateway agiert, kann dieselben Funktionen ausführen wie eine DFV-Steuereinheit. Eine einzelne Einheit kann sogar mehr als einen Knoten enthalten.

Das SNA-Netz ist dafür verantwortlich, daß der Datentransport zwischen zwei Endbenutzern auf effiziente, ordentliche und zuverlässige Weise durchgeführt wird. Wenn z. B. ein Benutzer an einer Datenstation eine Nachricht an eine andere Datenstation sendet, führt SNA die folgenden Schritte aus:

- Packen der Nachricht in einem Format, das bei dieser Verbindungsart verwendet werden kann
- Adressieren des Pakets
- Auswählen eines Leitwegs für die Nachricht
- Überwachen der Übertragung, um zu gewährleisten, daß die Nachricht ihre Zieladresse erreicht
- Umwandeln der Nachricht in ein Format, das an der Zieladresse gelesen werden kann

Diese Aufgaben sind in SNA als separate Funktionsschichten definiert. Diese Schichten werden hier nicht erläutert; es ist jedoch wichtig, sich zu vergegenwärtigen, daß alle SNA-Schichten Teil einer logischen Verbindung sind.

Wie bereits erwähnt, werden die SNA-Knoten nach ihren DFV-Funktionen klassifiziert sowie nach dem Ausmaß der Steuerung, die der Knoten für andere Knoten im Netz übernimmt. Die SNA-Knoten werden grob in Unterbereichsknoten und periphere Knoten eingeteilt. Die Unterbereichsknoten sind wie Hubs und können mit den peripheren Knoten und anderen Unterbereichsknoten kommunizieren. Die Unterbereichsknoten aktivieren und steuern Ressourcen auf den peripheren Knoten. Unterbereichsknoten werden auch als Knoten des Typs 4 oder 5 eingestuft. Knoten des Typs 5 enthalten einen Steuerpunkt für Systemservice (SSCP - System Service Control Point), der einen zentralen Steuerpunkt für die an ihn angeschlossenen Knoten des Typs 4 zur Verfügung stellt. Ein Knoten des Typs 5 wird manchmal als Host-Knoten bezeichnet. Ein peripherer Knoten kann nur mit dem direkt an ihn angeschlossenen Unterbereichsknoten kommunizieren. Er kann jedoch Einheiten steuern, mit denen er verbunden ist. Eine Gruppensteuereinheit, die als peripherer Knoten agiert, kann z. B. die mit ihr verbundenen Datenstationen unterstützen. Periphere Knoten werden auch als Knoten des Typs 2 oder 2.1 bezeichnet.

Jeder Knoten enthält adressierbare Netzeinheiten (NAUs - Network Accessible Units), die Steuerungs- und Übertragungsfunktionen übernehmen. Eine dieser NAUs ist eine physische Einheit (PU - Physical Unit). Die PU verwaltet die physischen Ressourcen des Knotens. Andere NAUs, die sogenannten logischen Einheiten (LUs - Logical Units), stellen logische Zugriffspunkte zum Netz zur Verfügung, die eine Kommunikation zwischen Benutzern und Anwendungen auf den einzelnen Knoten ermöglichen. Die Kommunikation zwischen LUs wird als Sitzung bezeichnet. Sitzungen unterstützen nicht nur die Kommunikation zwischen Benutzern und Anwendungen, sondern auch die Kommunikation zwischen Anwendungen, damit diese die Verarbeitungsressourcen gemeinsam benutzen können. Die Kommunikation zwischen Anwendungen wird als APPC (Advanced Program-to-Program Communication) bezeichnet. APPC ist eine Gruppe von Programmierungskonventionen und Protokollen, die LU 6.2 implementieren. (APPC ist der Name für die LU 6.2.-Funktion bei Produkten, die diesen LU-Typ implementieren.)

DLC-Profile

Die Datenübertragungssteuerung (DLC - Data Link Control) ermöglicht den ordentlichen Austausch von Daten zwischen zwei Knoten über eine logische Verbindung. Die DLC stellt die erforderlichen Protokolle für die zuverlässige Weiterleitung von Basisübertragungseinheiten (BTUs - Basic Transmission Units) zwischen zwei Knoten im SNA-Netz zur Verfügung. Um Zugriff auf ein SNA-Netz zu erhalten, müssen für die Datenstation die entsprechenden DLC-Profile des Communications Server konfiguriert werden.

Weitere Informationen zur Konfiguration der entsprechenden DLC-Profile enthält der Online-*Lerntext*.

Advanced Peer-to-Peer Networking

Advanced Peer-to-Peer Networking ist eine Erweiterung von SNA, die zu den in den vorangegangenen Abschnitten beschriebenen Übertragungsfunktionen weitere hinzufügt. Es besteht aus den folgenden Basiskomponenten:

- APPN-Knotentypen
- Steuerpunkte
- Erweiterungsfunktion für Zweigstellennetze
- Datenübertragungssteuerung (DLC)
- Logische Verbindungen
- Verzeichnisservices
- Topologieservices und Services für die Weiterleitungsauswahl

APPN-Knotentypen

Dieser Abschnitt befaßt sich mit den drei von Communications Server implementierten Knotentypen, die an einem APPN-Netz teilnehmen können:

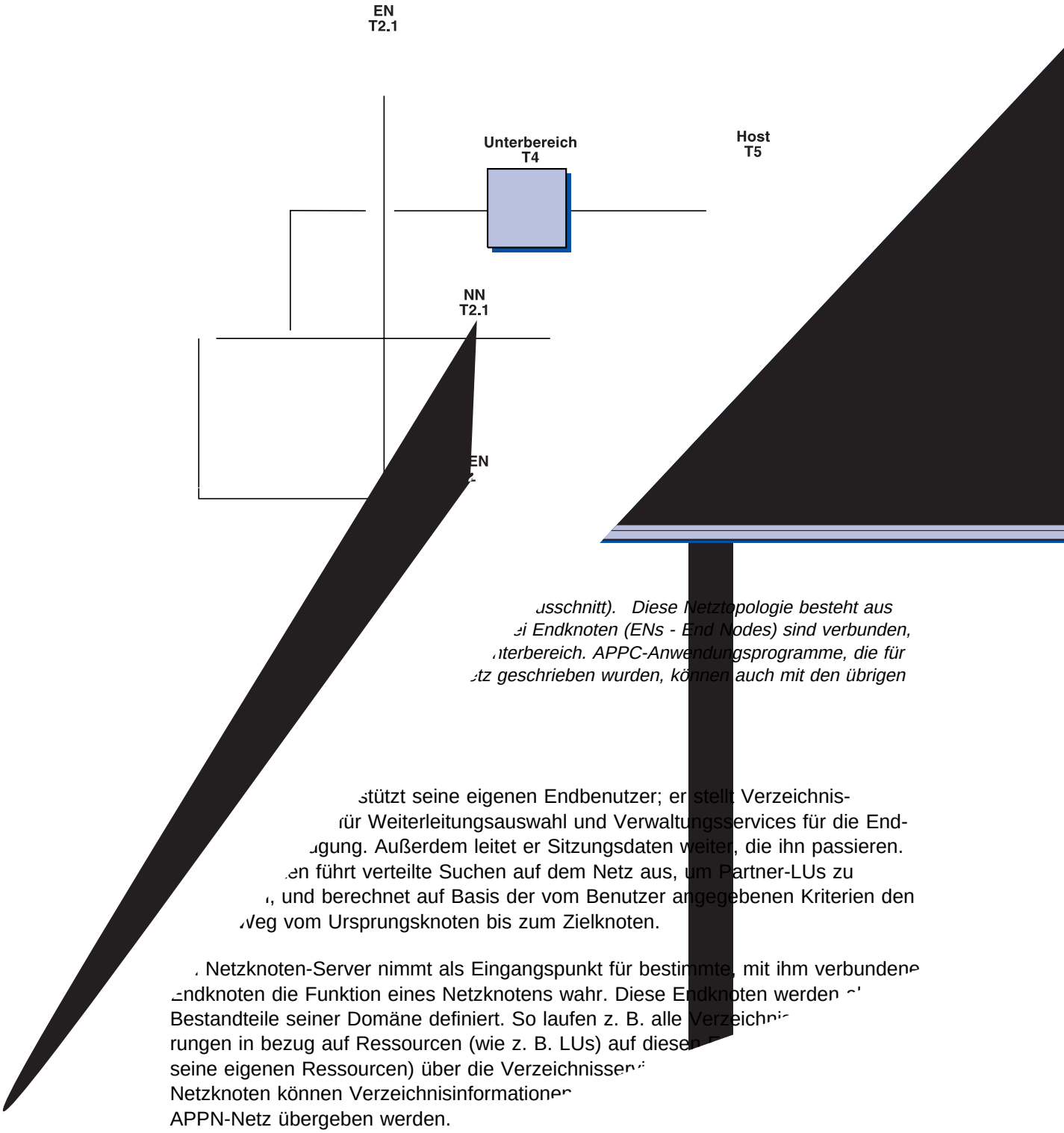
- Netzknoten
- Endknoten
- LEN-Knoten (LEN - Low Entry Networking)

Außerdem kann ein Netzknoten durch die Erweiterungsfunktion für Zweigstellennetze erweitert werden. Obwohl diese Komponente als Netzknoten Services für Endknoten bereitstellt, erscheint sie im Netz wie ein mit anderen Netzknoten verbundener Endknoten.

Jeder Knoten unterscheidet sich von den anderen im Netz durch einen eindeutigen Namen, der aus zwei Teilen besteht - einer Netz-ID und dem Namen des lokalen Knotens (auch als Name des Steuerpunkts bezeichnet). Der Name kennzeichnet jeden Knoten für alle übrigen Knoten im Netz. Dem Knoten können auch mehrere PU-Namen für gleichzeitigen Zugriff auf Hosts mit mehreren PUs T4/5 zugeordnet werden.

Knoten können als Endknoten oder Netzknoten konfiguriert werden; hat ein Endknoten jedoch keine CP-CP-Sitzungen (siehe „CP-CP-Sitzungen“ auf Seite 30) mit einem APPN-Netzknoten, agiert er als LEN-Knoten. Ein LEN-Knoten unterstützt keine APPN-Funktionen.

Eine detaillierte Beschreibung der Knotentypen folgt in den nächsten Abschnitten. Abb. 9 zeigt ein Beispiel eines APPN-Netzes, in dem all diese Knotentypen enthalten sind.



…usschnitt). Diese Netztopologie besteht aus …ei Endknoten (ENs - End Nodes) sind verbunden, …nterbereich. APPC-Anwendungsprogramme, die für …tz geschrieben wurden, können auch mit den übrigen

…stützt seine eigenen Endbenutzer; er stellt Verzeichnis- …für Weiterleitungsauswahl und Verwaltungsservices für die End- …gung. Außerdem leitet er Sitzungsdaten weiter, die ihn passieren. …en führt verteilte Suchen auf dem Netz aus, um Partner-LUs zu …, und berechnet auf Basis der vom Benutzer angegebenen Kriterien den …Weg vom Ursprungsknoten bis zum Zielknoten.

… Netzknoten-Server nimmt als Eingangspunkt für bestimmte, mit ihm verbundene …Endknoten die Funktion eines Netzknotens wahr. Diese Endknoten werden … Bestandteile seiner Domäne definiert. So laufen z. B. alle Verzeichnis… …rungen in bezug auf Ressourcen (wie z. B. LUs) auf diesen … seine eigenen Ressourcen) über die Verzeichnisserv… Netzknoten können Verzeichnisinformationen … APPN-Netz übergeben werden.

Ein Netzknoten stellt folgendes zur Verfügung:

- LU-LU-Sitzungsservices für seine lokalen LUs
- Weitervermittlung eines Sitzungsleitwegs
- Netz-Server-Funktionen (für Verzeichnissuchen im Netz und Weiterleitungsauswahl) für angeschlossene Endknoten oder LEN-Knoten (sowie für seine eigenen lokalen LUs)
- Leitwegfunktionen für Verwaltungsservices zum Weiterleiten von Verwaltungsservicedaten (wie z. B. Alerts) zwischen einem Services in Anspruch nehmenden Endknoten und einem Verwaltungsservice-ZAVS.

Endknoten

Ein Endknoten agiert in einer Peer-Umgebung für LU-LU-Sitzungen (unter Verwendung von LU 6.2-Protokollen) und stellt dabei zusätzliche APPN-Funktionen zur Verfügung. Ein Endknoten stellt den Endbenutzern an seinem eigenen Knoten APPN-Funktionen, wie z. B. Verzeichnisservices und Services für die Weiterleitungsauswahl, zur Verfügung. Er kann am APPN-Netz teilnehmen, indem er für Sitzungsanforderungen, die nicht direkt angeschlossene Knoten betreffen, die Services eines angeschlossenen Netzknoten-Servers nutzt; hierfür tauscht der Endknoten mit Hilfe von CP-CP-Sitzungen Verzeichnisserviceanforderungen und -antworten mit einem benachbarten Netzknoten (seinem Server) aus.

APPN-Endknoten können ihre lokalen LUs bei ihren Netzknoten-Server registrieren. Das Registrieren der Endknoten enthebt den Netzbediener am Netzknoten-Server von der Aufgabe, die Namen für die LUs an allen angeschlossenen Endknoten, für die der Netzknoten Services zur Verfügung stellt, im voraus zu definieren.

Ein APPN-Endknoten kann an mehrere Netzknoten angeschlossen werden; aktive CP-CP-Sitzungen sind jedoch immer nur mit einem Netzknoten möglich - seinem Netzknoten-Server. Die übrigen Netzknoten können verwendet werden, um Weitervermittlung eines Sitzungsleitwegs für den Endknoten zur Verfügung zu stellen oder als Ersatznetzknoten-Server, wenn der Hauptnetzknoten-Server nicht verfügbar ist. Zwischen zwei Endknoten werden keine CP-CP-Sitzungen hergestellt.

LEN-Knoten

Ein LEN-Knoten ist ein Knoten, der die T2.1-Basisprotokolle ohne APPN-Erweiterungen implementiert. In einem LEN-Knoten werden alle potentiellen Verbindungen mit Partner-LUs vordefiniert, bevor Sitzungen mit diesen eingeleitet werden. Ein LEN-Knoten, der mit einem APPN-Nachbarnetzknoten verbunden ist, benutzt die erweiterten APPN-Funktionen, indem er potentielle Verbindungen mit Partner-LUs vordefiniert, so als ob sie auf diesem Netzknoten vorhanden wären. Der Netzknoten kann seinerseits automatisch als Netzknoten-Server des LEN-Knotens fungieren, die aktuelle Zieladresse der Partner-LU lokalisieren und den besten Leitweg dorthin auswählen. Wenn er über einen Netzknoten führt, kann der LEN-Knoten an einem APPN-Netz teilnehmen, ohne mit allen Knoten eine direkte Verbindung haben zu müssen.

Steuerpunkte

Der Steuerpunkt (CP - Control Point) hat die Funktion, den Knoten und seine Ressourcen zu verwalten. Um APPN-Netzservices zu erhalten, muß der Steuerpunkt auf einem APPN-Endknoten mit dem Steuerpunkt eines Nachbarnetzknotens kommunizieren. Um das Netz zu verwalten, muß der Steuerpunkt auf einem APPN-Netzknoten außerdem mit den Steuerpunkten auf Nachbarnetzknoten kommunizieren. Der Steuerpunkt steuert Funktionen wie die Aktivierung und Inaktivierung von Adaptern und Verbindungen und unterstützt LUs bei der Initialisierung und der Beendigung einer Sitzung.

Beim Einrichten einer Datenstation muß der Name des Steuerpunkts definiert werden (auch bekannt als Name des lokalen Knotens). Der Steuerpunkt ist auch eine LU, die auch als einzige LU auf der Datenstation definiert sein kann.

CP-CP-Sitzungen

Zum Ausführen von Verzeichnisservices, Topologieservices und Services für Weiterleitungsauswahl verwenden Nachbarknoten im gesamten APPN-Netz zwei parallele CP-CP-Sitzungen, um Netzinformationen auszutauschen. Netzknoten verwenden CP-CP-Sitzungen zur Überwachung von Knoten in einer Netzverbindung sowie zur Protokollierung von Verzeichnis- und Sitzungsservices. Ein Netzknoten baut für jeden der Nachbarnetzknoten und jeden Services in Anspruch nehmenden Endknoten zwei Parallelsitzungen auf. Ein APPN-Endknoten baut für einen einzelnen Nachbarnetzknoten, der als aktueller Server fungiert, zwei Parallelsitzungen auf. Von LEN-Knoten werden CP-CP-Sitzungen nicht unterstützt.

Sobald eine Verbindung hergestellt wurde, tauschen die Knoten XIDs aus. Anschließend werden CP-CP-Sitzungen zwischen den Steuerpunkten in den direkt zugeordneten Knoten gestartet. Die CP-CP-Sitzungen verwenden LU 6.2-Protokolle, und damit zwei Steuerpunkte ihre Interaktionen starten und fortführen können, müssen beide Sitzungen einer gegebenen Verbindung aktiv sein. Alle CP-CP-Sitzungen werden zur Verzeichnissuche verwendet.

Nachdem CP-CP-Sitzungen aufgebaut sind, tauschen die beiden Knoten Nachrichten aus, die jeden Knoten über die Steuerpunktleistungen des anderen Knotens informieren. Sind beide Knoten Netzknoten, tauschen sie TDU-Nachrichten (TDU - Topology Database Update) aus. Die TDU-Nachrichten enthalten Kenndaten, Knoten- und Verbindungsmerkmale und die Ressourcenfolgenummer zur Identifizierung der neuesten Aktualisierungen jeder im TDU beschriebenen Ressource.

CP-CP-Verbindungsaktivierung

Communications Server versucht beim Starten zuerst die bevorzugte Server-Verbindung zu aktivieren. Communications Server versucht, alle anderen Verbindungen zu aktivieren, für die ***Beim Start aktivieren*** definiert wurde. Ist eine alternative parallele Verbindung zur bevorzugten NN-Server-Verbindung vorhanden, versucht Communications Server, die CP-CP-Sitzungen auf der alternativen Verbindung zu aktivieren, anstatt auf die Ergebnisse des Aktivierungsversuchs für die bevorzugte NN-Server-Verbindung zu warten.

Anmerkung: Wurde die Verbindung auf Anforderung des Operators vom lokalen Knoten inaktiviert, werden CP-CP-Sitzungen nicht neu aktiviert. Wurde die Verbindung auf Anforderung des Operators vom fernen Knoten inaktiviert, werden CP-CP-Sitzungen am lokalen Knoten neu aktiviert. Bei Verbindungen zwischen NN-Knoten werden nur auf Anforderung aktivierte Verbindungen (Verbindungen mit angegebenem Namen des benachbarten CP, für die nicht ***Beim Start aktivieren*** definiert ist) aktiviert.

Reaktivierung von CP-CP-Verbindungen

Der Communications Server stellt Unterstützung zur Reaktivierung von CP-CP-Verbindungen bereit. Der Verlust von CP-CP-Sitzungen zwischen einem Endknoten und seinem Netzknoten-Server und zwischen Nachbarnetzknoten kann Auswirkungen auf den Betrieb eines APPN-Netzes haben. Die Unterstützung für die Reaktivierung von CP-CP-Verbindungen erhöht die Zuverlässigkeit eines APPN-Netzes, indem diese wichtigen Sitzungen wieder gestartet werden, wenn sie aufgrund eines Fehlers oder der Inaktivierung der Verbindung beendet wurden.

Ein Reaktivierungsversuch der CP-CP-Verbindung wird durch eine CP-CP-Verbindungsaktivierung, einen CP-CP-Sitzungsfehler oder Ablaufen eines CP-CP-Wiederholungszeitgebers initialisiert. CP-CP-Sitzungen werden durch Communications Server mit dem ersten der folgenden Elemente aktiviert:

1. Der bevorzugten Server-CP-CP (wenn diese nicht bereits vorher versucht wurde).
2. Wurde DLUR konfiguriert, einen benachbarten CP verwenden, der DLUR-Registrierung unterstützt.
3. Dem letzten (zuletzt aktivierten) NN, mit dem noch kein Versuch gemacht wurde und zu dem eine aktive Verbindung besteht.
4. Dem ersten eines beliebigen übergeordneten NNs für die Erweiterungsfunktion für Zweigstellennetze.

Anmerkung: Wenn die CP-CP-Verbindungen aufgrund eines Verbindungsfehlers beendet wurden, aktiviert der Communications Server die Verbindung nicht erneut. Für eine Verbindung kann ***Automatisch reaktivieren*** (unbegrenzte Wiederholung) konfiguriert werden, um wichtige Verbindungen aktiviert zu halten.

Erweiterungsfunktion für Zweigstellennetze

Die Erweiterungsfunktion für Zweigstellennetze besteht aus einer Untergruppe von Grenzknoten, die dafür konzipiert wurde, eine Zweigstelle mit einem zentralen APPN-WAN-Netz zu verbinden. Die miteinander verbundenen Netze können Basisnetze (d. h., sie haben dieselbe Netz-ID) oder Nicht-Basisnetze sein. Ein Knoten, der die Erweiterungsfunktion für Zweigstellennetze unterstützt, ist ein Zweigstellennetzknoten, der normalerweise über LAN- und WAN-Schnittstellen verfügt und außerdem DLUR und HPR umfassen kann.

Verbindungen an einem Knoten, die die Erweiterungsfunktion für Zweigstellennetze unterstützen, werden als ***übergeordnete Zweigstellenverbindungen*** oder ***untergeordnete Zweigstellenverbindungen*** definiert. Abb. 10 zeigt ein Beispiel für die Arbeitsweise eines Zweigstellennetzknotens in einem Netz. In dieser Abbildung ist der Knoten in der Mitte ein Zweigstellennetzknoten. Normalerweise ist der benachbarte CP (übergeordneter Zweigstellenknoten) der Netzknoten-Server (NNS) für den Zweigstellennetzknoten, der für den übergeordneten Zweigstellenknoten als ein Endknoten erscheint.

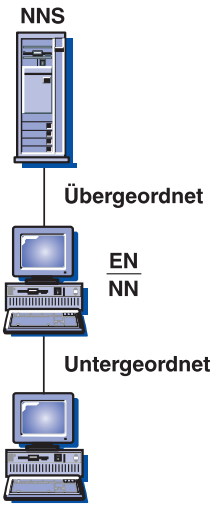


Abbildung 10. Konzeptioneller Überblick über übergeordnete und untergeordnete Zweigstellenverbindungen

Übergeordnete Zweigstellenverbindungen werden im Zweigstellennetzknoten für das zentrale Netz als übergeordnet definiert. Ein Knoten mit einer übergeordneten Verbindung kann als ein peripherer Knoten betrachtet werden, der an das zentrale Netz angeschlossen ist.

Untergeordnete Zweigstellenverbindungen werden im Zweigstellennetzknoten entsprechend definiert. Der Knoten betrachtet untergeordnete Verbindungen als Verbindungen mit Endknoten (Steuerpunkten) in der Domäne. Untergeordnete Zweigstellenverbindungen sind normalerweise LAN-Verbindungen (müssen dies jedoch nicht sein). Endknoten, die über untergeordnete Zweigstellenverbindungen angeschlossen sind, können als lokale Ressourcen betrachtet werden. Der Zweigstellennetzknoten ist der Netzknoten-Server für diese Endknoten. An untergeordneten Zweigstellenverbindungen stellt dieser Netzknotenservices für Domänenendknoten, LEN-Endknoten, abhängige T2.0-Knoten und T2.1-Knoten sowie lokale LUs und PUs bereit.

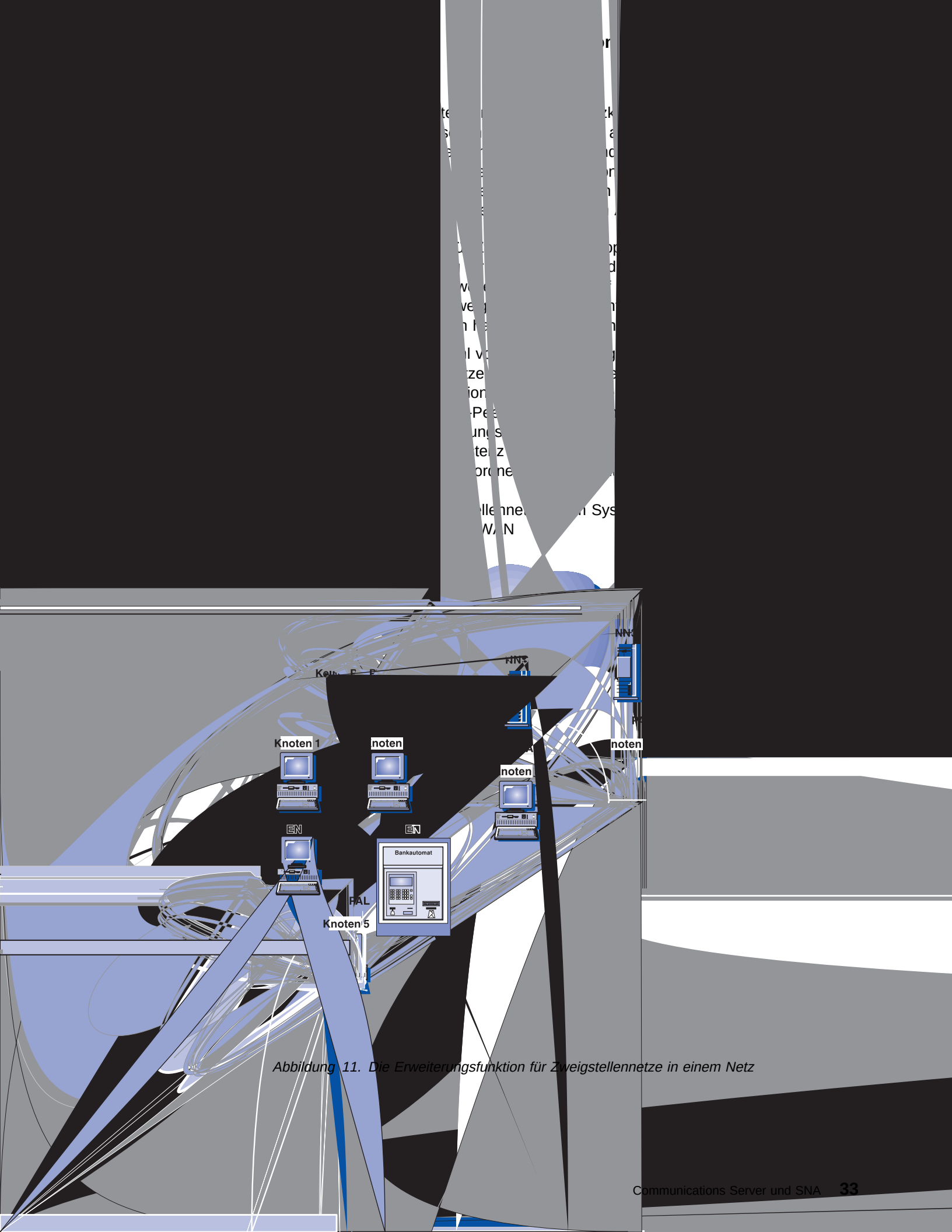


Abbildung 11. Die Erweiterungsfunktion für Zweigstellennetze in einem Netz

Abb. 11 auf Seite 33 zeigt, wie Knoten eines Zweigstellennetzes in einem Netz arbeiten. Gestrichelte Linien stellen logische Verbindungen dar. In der Abbildung werden die Knoten 1, 2, 3 und 4 für die Erweiterungsfunktion für Zweigstellennetze konfiguriert und fungieren sowohl als Endknoten als auch als Netzknoten. Sie verbergen ihre untergeordnete Topologie vor dem WAN-Netz (d. h., sie erscheinen den übergeordneten Netzknoten-Servern als Endknoten). Für die Knoten in den untergeordneten LANs fungieren die Knoten als Netzknoten-Server. Knoten 5 erscheint als ein Endknoten für Knoten 2, ist jedoch ein Netzknoten-Server (NNS) für andere Endknoten in dem LAN. Für NNS erscheint Knoten 5 als LU auf Knoten 2.

Versucht ein Endnoten, dem Knoten 1 seine Services zur Verfügung stellt, eine Sitzung mit einem Endknoten über das WAN aufzubauen, kann Knoten 1 eine Lokalisierungsanforderung (Sendeanforderung) auf seiner Verbindung der Erweiterungsfunktion für Zweigstellennetze an seinen Netzknoten-Server senden. Wurde der Ziel-CP gefunden, bestimmt der Netzknoten-Server einen Leitweg von Knoten 1 zum Ziel-CP. Knoten 1 modifiziert den Leitweg, bevor er an den Quellenendknoten zurückgegeben wird. Der Quellenendknoten verwendet diesen Leitweg für seine Sitzung.

Einschränkungen für die Erweiterungsfunktion für Zweigstellennetze

Die folgenden Einschränkungen gelten für Netze, die für die Verwendung der Erweiterungsfunktion für Zweigstellennetze konfiguriert wurden:

- Ein Zweigstellennetzknoten kann nur über eine übergeordnete Zweigstellenverbindung mit einem Netzknoten verbunden werden.
- Um eine Suchschleife zu verhindern, müssen untergeordnete Endknoten tatsächliche Endknoten sein und keine Knoten, die ein Endknotenabbild darstellen.
- Ein Knoten kann keine CP-CP-Sitzungen mit dem Zweigstellennetzknoten über über- und untergeordnete Zweigstellenverbindungen gleichzeitig haben.
- Der Zweigstellennetzknoten kann CP-CP-Sitzungen immer nur über eine übergeordnete Zweigstellenverbindung ausführen; d. h., er kann CP-CP-Sitzungen mit maximal einem Netzknoten-Server ausführen.
- Die Erweiterungsfunktion für Zweigstellennetze stellt keine Twinaxialunterstützung bereit.
- Ein Knoten der Erweiterungsfunktion für Zweigstellennetze kann nicht über untergeordnete DLUR-Sitzungen verfügen.

Konfiguration der Erweiterungsfunktion für Zweigstellennetze

Zum Konfigurieren der Erweiterungsfunktion für Zweigstellennetze muß zunächst ein Zweigstellennetzknoten konfiguriert werden. Anschließend muß entweder eine DLC (für eine implizite Verbindung) oder ein Zweigstellennetzknoten konfiguriert werden. Eine Verbindung, die für die Erweiterungsfunktion für Zweigstellennetze konfiguriert wurde, ist eine übergeordnete Zweigstellenverbindung. Bei einem Zweigstellennetzknoten sind alle Verbindungen, die nicht für die Unterstützung der Funktion konfiguriert wurden, untergeordnete Zweigstellenverbindungen.

Sind Verbindungen zwischen den Zweigstellennetzknoten definiert, müssen diese als ***Peer***-Verbindungen definiert werden, so daß sie in der .ACG-Datei die Verbindungsart **LEARN** haben. Alternativ dazu kann für die Verbindung **ACTIVATE_AT_STARTUP=1** definiert werden, so daß die Verbindung immer aktiv ist. Wenn Zweigstellenknoten miteinander verbunden werden, treten Schleifen in der Topologie auf. Dies kann akzeptiert werden, solange die Verbindungen immer aktiv sind, oder wenn die Verbindungen beim Aktivieren als LEARN eingestuft werden. Werden Verbindungen zwischen Zweigstellennetzknoten als **END_NODE**- oder **NETWORK_NODE**-Verbindungen definiert, interpretiert die an den übergeordneten Knoten gemeldete Topologie die Verbindungen möglicherweise falsch, was zu Zuordnungsfehlern führen kann.

Für die Konfiguration der Erweiterungsfunktion für Zweigstellennetze kann auch eine ACG-Datei verwendet werden.

Verwaltung der Erweiterungsfunktion für Zweigstellennetze

In den folgenden Abschnitten wird beschrieben, wie eine Konfiguration geprüft wird und welche Einschränkungen bei der Netzkonfiguration gelten.

Die Konfiguration prüfen: Mit den **SNA-Knotenoperationen** an einem Knoten, der die Erweiterungsfunktion für Zweigstellennetze unterstützt, kann ermittelt werden, ob eine lokale Zweigstelle erfolgreich konfiguriert wurde. Während der Laufzeit darf eine Anzeige der Topologie von dem Knoten nie mehr als zwei Netzknoten enthalten: sich selbst und den übergeordneten Netzknoten-Server.

Anmerkung: Für CP-CP ist nur eine übergeordnete Verbindung verfügbar. Jede Datenstation muß als Endknoten konfiguriert werden, und der Netzknoten-Server muß dabei als bevorzugter Netzknoten-Server definiert werden.

Die **SNA-Knotenoperationen** können verwendet werden, um zu prüfen, ob die DLC oder die Verbindung so konfiguriert wurde, daß die Erweiterungsfunktion für Zweigstellennetze korrekt unterstützt wird. Die **SNA-Knotenoperationen** können auch verwendet werden, um zu ermitteln, ob eine aktive Verbindung eine übergeordnete oder untergeordnete Zweigstellenverbindung ist. Untergeordnete Endknoten, die mit AnyNet registriert wurden, registrieren ihre Ressourcen nicht.

Unterstützte Funktionen

Der Communications Server unterstützt die Basisfunktionen von APPN Version 2 (sowohl Endknoten als auch Netzknoten). Zusätzlich werden die folgenden Funktionen unterstützt:

- Endknoten

Funktionssatz	Funktion
162	MS_CAPS als Steuerbereichsendknoten (SOC - Sphere Of Control)
171	Fehlerdiagnosedaten im Alert
177	LAN-Alert
178	SDLC/LAN-LLC-Alert
181	X.25-Alert
182	Angehaltener Alert für CPMS
1002	Name der angrenzenden Verbindungsstation
1007	Parallele TGs
1011	Mehrere lokale unabhängige LUs
1012	CP=LU
1018	EN-Ressourcen vor dem Registrieren löschen
1067	Abhängiger LU-Requester
1070	Sitzungsverschlüsselung
1107	Zentrale Ressourcenregistrierung (für LUs)
1116	Registrierung von LUs, denen ein DLUS Services zur Verfügung stellt
1200	Baumstruktur- und TG-Caching
1400	HPR-Basis (ANR)
1401	RTP (Rapid Transport Protocol)
1402	Steuerungsfluß über RTP
1520	Allgemeine Betriebsservices

- Netzknoten

Funktionssatz	Funktion
164	MS_CAPS mit Unterbereichs-ZAVS
171	Fehlerdiagnosedaten im Alert
177	LAN-Alert
178	SDLC/LAN-LLC-Alert
181	X.25-Alert
182	Angehaltener Alert für CPMS
1002	Name der angrenzenden Verbindungsstation
1007	Parallele TGs
1011	Mehrere lokale unabhängige LUs
1012	CP=LU
1018	EN-Ressourcen vor dem Registrieren löschen
1067	Abhängiger LU-Requester
1070	Sitzungsverschlüsselung
1100	Sicheres Speichern des Verzeichnis-Caches
1101	Vorheriges Laden des Verzeichnis-Caches
1107	Zentrale Ressourcenregistrierung (für LUs)
1116	Registrierung von LUs, denen ein DLUS Services zur Verfügung stellt
1118	EN-TG-Vektorregistrierung
1121	Erweiterungsfunktion für Zweigstellennetze
1200	Baumstruktur- und TG-Caching
1203	Erkennen und Eliminieren von TDU-Konflikten
1301	Datenaustausch für Zwischensitzungen ohne Nachrichtendosierung
1400	HPR-Basis (ANR)
1401	RTP (Rapid Transport Protocol)
1402	Steuerungsfluß über RTP
1520	Allgemeine Betriebsservices

Datenübertragungssteuerung

Die Datenübertragungssteuerung (DLC - Data Link Control) stellt die erforderlichen Protokolle für die zuverlässige Übertragung von Basisübertragungseinheiten (BTUs - Basic Transmission Units) zwischen zwei Knoten im APPN-Netz und die Verwaltung der logischen Verbindungen zwischen Knoten zur Verfügung.

Verbindungen

Eine Verbindung verbindet Nachbarknoten über eine zugrundeliegende DLC miteinander.

Parallelverbindungen

Der lokale Knoten kann mehrere Verbindungen zu einem Nachbarknoten haben. Diese Zuordnungen werden als ***Parallelverbindungen*** bezeichnet. Jede Parallelverbindung erhält eine eindeutige Nummer (Übertragungsgruppennummer), und es können ihnen unterschiedliche Verbindungsmerkmale zugewiesen werden. Um zwei Parallelverbindungen zwischen zwei Knoten herzustellen, dürfen sich zwar die Verbindungsstationen für die Verbindungen auf demselben Adapter auf einem Knoten befinden, auf dem anderen Knoten müssen sie sich jedoch auf verschiedenen Adaptern befinden; dies bedeutet, daß die Kombination von Adapternummer und Adresse der Nachbar- oder Zielverbindungsstation für jede Verbindung eindeutig sein muß.

Verbindungsaktivierung

Die Nachrichteneinheit, die zur Übertragung von Knoten- und Verbindungsmerkmalen an Nachbarknoten verwendet wird, nennt sich ***Austausch-ID*** (XID - Exchange Identification). Bei Angabe von **USE_PU_NAME_IN_XID=1** wird der Name der PU im CP-Namensfeld der XID verwendet. Andernfalls wird der Name des Steuerpunkts in diesem Feld verwendet. XIDs werden vor und während der Verbindungsaktivierung zwischen den Knoten ausgetauscht, um Verbindungs- und Knotenmerkmale festzulegen und auszuhandeln, und nach der Verbindungsaktivierung, um Änderungen an diesen Merkmalen weiterzuleiten.

APPN-Knoten benutzen beim Austausch mit anderen T2.1- oder Grenzknoten das Format XID3, um die Funktionen festzulegen. Bei PU 2.0-Verbindungen wird das Schlüsselwort **LINK_STATION** zur Angabe des Namens der PU und der Knoten-ID verwendet, die mit XID3 ausgetauscht werden.

Bei Angabe von **USE_PU_NAME_IN_XID=1** wird der Name der PU im Namensfeld der XID verwendet. Andernfalls wird der Name des Steuerpunkts in diesem Feld verwendet. Informationen zu den Merkmalen des Sendeknotens sind in XID3 enthalten. Dazu gehören die Funktion der Verbindungsstation (primär, sekundär oder aushandelbar), TG-Nummer, Knotentyp, die Nummer der logischen Verbindung, die maximale Größe der Basisübertragungseinheit, die empfangen werden kann, die Knoten-ID und der PU-Name. Der Name der PU ist normalerweise der Name des Steuerpunkts; mit dem Schlüsselwort **LINK_STATION** können jedoch auch andere PU-Namen und Knoten-IDs definiert werden, um simultane PU 2.0-Anschlüsse zu unterstützen.

Verbindungsarten

Die folgenden sechs Verbindungsarten werden normalerweise in Communications Server-Knoten definiert:

- Primärer Netzzugriff, ursprünglich aktiviert (APPN oder Host)
- Primärer Netzzugriff, Host-Verbindung
- Primärer Netzzugriff, ständig in Gebrauch (Gebrauch, wenn erforderlich)
- Sekundärer Netzzugriff, ankommende Verbindung (vordefinierte Verbindungsmerkmale)
- Sekundärer Netzzugriff, beschränkte Verwendung (auch als begrenzte Ressource bezeichnet)

Communications Server-Konfiguration stellt eine Methode bereit, um die Verwendung dieser Verbindungsarten zu definieren und zu steuern. In diesem Abschnitt werden die verwendeten Knoten-, DLC- und Verbindungskonfigurationsparameter sowie die Beziehungen und Abhängigkeiten zwischen diesen Parametern beschrieben. Folgende Kategorien werden beschrieben:

- Verbindungsdefinitions- und Aktivierungsparameter
- Verbindungsinaktivierungsparameter
- Andere Verbindungsparameter

Die folgenden Parameter werden beschrieben:

- **Definitions- und Aktivierungsparameter**
  - Beim Start aktivieren
  - Auf Anforderung aktivieren
  - Automatische Verbindungswiederholung
  - Maximale Anzahl Aktivierungsversuche
  - Reaktivierung auf Anforderung des Benutzers
- **Inaktivierungsparameter**
  - Inaktivitätszeitlimit
  - Begrenzte Ressource
- **Andere Verbindungsparameter**
  - Verbindungsnetz
  - Unterstützung für CP-CP-Sitzung
  - Unterstützung für High Performance Routing (HPR)
  - Typ des Nachbarknotens
  - Bevorzugter Netzknoten-Server
  - SSCP-Sitzungsanforderung
  - PU-Name (wenn der Parameter für die SSCP-Sitzungsanforderung auf **1** gesetzt wurde)

Anmerkung: Diese Parameter sind in der ACG-Datei enthalten und sind möglicherweise in den Anzeigen nicht verfügbar (über **Knotenkonfiguration**).

Verbindungsdefinitions- und -aktivierungsparameter

In diesem Abschnitt werden Definitions- und Aktivierungsparameter beschrieben.

Beim Start aktivieren

Eine ***beim Start aktivierte Verbindung*** wird normalerweise für primäre Netzzugriffsverbindungen verwendet, die beim Start von Communications Server zuerst aktiviert werden. Die Verbindung wird aktiviert, wenn Communications Server auf der Maschine gestartet wird und bleibt während der gesamten Ausführung von Communications Server aktiv.

Um eine Verbindung als beim Start zu aktivieren zu definieren, **ACTIVATE_AT_STARTUP=1** im Schlüsselwort **LINK_STATION** der ACG-Datei angeben. Verbindungen werden in der Regel als beim Start zu aktivieren konfiguriert, wenn sie für die Netzkonnektivität wichtig sind. Wichtige Verbindungen können auch für automatische Verbindungswiederholung definiert werden (siehe „Automatische Verbindungswiederholung“ auf Seite 42).

Die Verbindung von einem APPN-Endknoten (EN) zu seinem bevorzugten Netzknoten-Server (NN-Server) ist ein Beispiel für diese Art von Verbindung.

Eine nicht beim Start zu aktivierende Verbindung, die als **ACTIVATE_AT_STARTUP=0** codiert ist, kann beispielsweise eine Host-Verbindung sein, die beim Starten von Communications Server nicht sofort benötigt wird, eine ankommende Verbindung, deren Verbindungsmerkmale ein Knoten steuern möchte, oder eine Verbindung, deren ständige Aufrechterhaltung zu teuer ist. Diese Verbindungen werden als beim Start nicht zu aktivierende Verbindungen definiert und werden aktiviert, wenn die Verbindungsressourcen durch eine Anwendung (siehe „Auf Anforderung aktivieren“) oder den Partner angefordert werden.

Auf Anforderung aktivieren

Eine ***auf Anforderung zu aktivierende*** Verbindung (auch als „automatisch aktiviert“ bezeichnet) wird normalerweise für den Zugriff auf eine Partner-LU verwendet, für die eine dynamische Aktivierung der Verbindung erforderlich ist. Beim Starten von Communications Server bleibt die Verbindung inaktiviert. Sie wird jedoch als verfügbare Verbindung in die Topologie eingefügt, wenn ein benachbarter CP-Name angegeben wird. Die Verbindung wird aktiviert, wenn ein Transaktionsprogramm (TP) eine Verbindung zu einer fernen LU anfordert, die voraussetzt, daß die Verbindung aktiv ist. Communications Server verwendet die vollständig qualifizierte Partner-LU, die für die Aktivierung der Verbindung definiert wurde.

Um eine Verbindung als eine auf Anforderung zu aktivierende Verbindung zu definieren, müssen **ACTIVATE_AT_STARTUP=0** und **FQ_ADJACENT_CP_NAME**=(netid.cpname) im Schlüsselwort **LINK_STATION** in der ACG-Datei des ursprünglichen Knotens konfiguriert werden. Ist der Partner nicht der **FQ_ADJACENT_CP_NAME**, muß das Schlüsselwort **PARTNER_LU** konfiguriert werden.

Häufig wird eine auf Anforderung zu aktivierende Verbindung entweder als eine begrenzte Ressource konfiguriert (siehe „Begrenzte Ressource“ auf Seite 45) oder mit einem Inaktivitätszeitlimit (siehe „Inaktivitätszeitlimit“ auf Seite 44), so daß die Verbindung inaktiviert wird, wenn sie nicht mehr benötigt wird.

Ein Beispiel für eine auf Anforderung zu aktivierende Verbindung ist eine Verbindung mit einem Partner, die für eine begrenzte Zeit aktiv sein muß. Eine Verbindung kann so teuer sein, daß es möglicherweise nicht sinnvoll ist, sie ständig aufrechtzuerhalten. Dies kann beispielsweise bei einem oder mehreren Computern der Fall sein, die regelmäßig miteinander kommunizieren. Am Ende jedes Tages muß eine der Maschinen eine Verbindung mit einer fernen Maschine aktivieren, um die täglichen Ergebnisse zu senden oder die Daten zu sichern.

Ein anderes Beispiel liegt vor, wenn Verbindungen zu einem Daten- oder einem Druck-Server bestehen. Die Verbindung benötigt Ressourcen am Server. Um Beschränkungen der maximalen Anzahl von Verbindungsstationen und Sitzungen am Server zu vermeiden, eine auf Anforderung zu aktivierende Verbindung so konfigurieren, daß die Ressourcen am Daten-Server freigegeben werden, nachdem die Anforderungen über die auf Anforderung zu aktivierende Verbindung ausgeführt wurden.

Eine auf Anforderung zu aktivierende Verbindung ist nicht unbedingt eine begrenzte Ressource, kann jedoch als eine solche definiert werden, indem der Parameter **LIMITED_RESOURCE=1** zu dem Schlüsselwort **LINK_STATION** hinzugefügt wird (siehe „Begrenzte Ressource“ auf Seite 45).

Automatische Verbindungswiederholung

Dies ist eine Fehlerbehebungsfunktion, die die Verfügbarkeit einer fehlerhaften Verbindung erhöht. Muß eine Verbindung nach einem Fehler reaktiviert werden (ohne Benutzereingriff), kann die automatische Verbindungswiederholung verwendet werden. Diese Funktion bewirkt die automatische Ausführung von Reaktivierungsversuchen für die Verbindung, wenn die folgenden Parameter im Schlüsselwort **LINK_STATION** oder **PORT** angegeben sind:

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

Wurde einer dieser Parameter im Schlüsselwort **PORT** angegeben, werden die Werte vom Schlüsselwort **LINK_STATION** verwendet, wenn der Parameter **INHERIT_PORT_RETRY_PARMS** angegeben wurde.

Nach einer erfolgreichen Aktivierung wird der Intervallzeitgeber auf 0 zurückgesetzt.

Es kann von Vorteil sein, die automatische Verbindungswiederholung bei jeder der folgenden Verbindungsarten zu verwenden:

- Eine Verbindung mit einem NN, die beim Start aktiviert wird. Fällt die Verbindung aus, wird nur eine Verbindung zu einem Netzknoten-Server (NN) reaktiviert.
- Host-Verbindung
- Eine primäre Verbindung, die über eine Ausweichverbindung verfügt (normalerweise auch als eine beim Start zu aktivierende Verbindung definiert)
- Jede Verbindung, die ständig aktiviert bleiben muß.

Maximale Anzahl Aktivierungsversuche

Maximale Anzahl Aktivierungsversuche ist ein Parameter zur Aktivierung der Verbindung, der einen Mechanismus bereitstellt, mit dem verhindert wird, daß abhängiger LU-Host-Datenaustausch (z. B. LUA-, 3270-, ein LU 2-Gateway-

Reaktivierung auf Anforderung des Benutzers

Eine ***vom Benutzer angeforderte Reaktivierung*** ist eine Reaktivierung einer Verbindung, die vom Benutzer über die **SNA-Knotenoperationen** oder über die Befehlszeile, beispielsweise mit Communications Server, angefordert wird.

Verbindungsinaktivierungsparameter

Im folgenden Abschnitt werden die Inaktivierungsparameter beschrieben.

Inaktivitätszeitlimit

Das ***Inaktivitätszeitlimit*** ist ein SDLC-Verbindungsinaktivierungsparameter, der das Inaktivieren von Verbindungen steuert. Das Inaktivitätszeitlimit gibt den Zeitraum (in Sekunden) an, während dem eine Verbindung ohne Aktivität bleiben kann, bevor sie inaktiviert wird. Dies entspricht ungefähr dem Parameter **LINK_DEACT_TIMER** im Schlüsselwort **LINK_STATION**. Der Unterschied besteht darin, daß der Parameter **LINK_DEACT_TIMER** wartet, bis alle Sitzungen beendet sind (der Sitzungszähler 0 erreicht), bevor die Verbindungsinaktivierung in Gang gesetzt wird. Der **INACTIVITY_TIMER** ignoriert den Sitzungszähler und setzt die Inaktivierung in Gang, nachdem auf der Verbindung während des angegebenen Zeitraums keine Aktivität stattfand.

Die Funktion des Inaktivitätszeitlimits wurde für Situationen implementiert, in denen eine Emulationssitzungs-, LUA-, 3270- oder eine LEN-Verbindung versehentlich für einen längeren Zeitraum aktiv bleibt. Stellt der Knoten für die Dauer des **INACTIVITY_TIMER** keine Aktivität über diese Verbindungsart fest, wird die Verbindung automatisch inaktiviert, unabhängig davon, ob Sitzungen und Dialoge in dieser Verbindung vorhanden sind. Laut Definition wird mit **LINK_DEACT_TIMER** keine Unterbrechung herbeigeführt, während **INACTIVITY_TIMER** zu einer Unterbrechung führt.

Anmerkungen:

1. Das Inaktivitätszeitlimit kann bei Verbindungen, die als begrenzte Ressource oder nicht als begrenzte Ressource definiert sind, verwendet werden. Ist eine Verbindung als begrenzte Ressource definiert und bleiben Dialoge aktiv, läuft das Zeitlimit für begrenzte Ressource nicht ab, und die Verbindung wird inaktiviert, wenn das Inaktivitätszeitlimit abläuft. Ist eine Verbindung als nicht begrenzte Ressource definiert, wird das Inaktivitätszeitlimit verwendet, um die Verbindung zu inaktivieren, um Ressourcen am fernen Ende freizugeben.
2. Bei Verwendung von HPR wird das Inaktivitätszeitlimit ignoriert. Dies hat folgenden Grund: HPR kann nicht erkennen, welche Art von Datenaustausch über die Verbindung erfolgt, und das HPR-Keepalive-Protokoll generiert genügend Datenaustausch, so daß die Verbindung nie ohne Aktivität bleibt.

Um das Inaktivitätszeitlimit für eine SDLC-Verbindung zu konfigurieren, wird der Parameter **INACTIVITY_TIMER**= n im Parameter **LINK_STATION_SDLC_SPECIFIC_DATA** des Schlüsselworts **LINK_STATION** der ACG-Datei codiert; dabei ist n 40-160. Um das Inaktivitätszeitlimit für eine Verbindung zu konfigurieren, wird der Parameter **LINK_DEACT_TIMER**= n im Schlüsselwort **LINK_STATION** der ACG-Datei codiert; dabei ist n 0-1000. 0 gibt kein Zeitlimit an, d. h. (die Verbindung bleibt aktiv). Der SDLC-Standardwert ist 80 und der Standardwert für die Verbindung ist 10.

Begrenzte Ressource

Eine als begrenzte Ressource definierte Verbindung wird normalerweise für primäre Netzzugriffsverbindungen mit begrenzter Verwendung und für sekundäre Netzzugriffsverbindungen verwendet. Eine als begrenzte Ressource definierte Verbindung ist eine Verbindung, die automatisch inaktiviert wird, wenn ihr Sitzungszähler 0 erreicht. Sie kann als **ACTIVATE_AT_STARTUP=1** oder **ACTIVATE_AT_STARTUP=0** definiert werden. Ist für die Verbindung **ACTIVATE_AT_STARTUP=1** definiert, wird sie beim Starten von Communications Server gestartet. Ist für die Verbindung **ACTIVATE_AT_STARTUP=0** definiert, wird sie beim Start von Communications Server in die Topologie eingefügt, wenn der benachbarte CP-Name angegeben wird, und wird beim Anfordern der Services aktiviert.

Anmerkung: Beim Start zu aktivierende Verbindungen werden nur in die Topologie eingefügt, wenn sie aktiv sind.

Um eine als begrenzte Ressource definierte Verbindung zu konfigurieren, **LIMITED_RESOURCE=1** im Schlüsselwort **LINK_STATION** der ACG-Datei angeben. Der Parameter **LINK_DEACT_TIMER**= n wird im Schlüsselwort **LINK_STATION** angegeben, und der Parameter **ADJACENT_NODE_TYPE=LEARN** muß angegeben werden.

Anmerkung: Bei **CP_CP_SESSION_SUPPORT=1** ist die Verbindung keine begrenzte Ressource. Bei der Konfigurationsprüfung wird dies als Warnung markiert. Aktive CP-CP-Sitzungen sorgen dafür, daß die Verbindung nicht inaktiviert wird.

Verbindungsnetze

Verbindungsnetze ermöglichen es APPN-Knoten in einem LAN, direkte Verbindungen miteinander herzustellen, ohne daß auf jedem Knoten eine logische Verbindung definiert sein muß. Durch diese Funktion werden Systemdefinitionen wesentlich reduziert, ohne daß alle Sitzungen über einen Netzknoten geleitet werden müssen, was sich auf die Leistung auswirken würde. Außerdem ermöglicht sie es neuen Knoten, die zum LAN hinzugefügt werden, im vollen Umfang an APPC-Dialogen teilzunehmen, ohne daß an allen übrigen Knoten Definitionsänderungen erforderlich sind.

Ein Netzknoten im Verbindungsnetz geht davon aus, daß alle Knoten in einem Verbindungsnetz direkte Verbindungen zueinander aufbauen können. Bei der Berechnung des Leitwegs für eine Sitzung berücksichtigt der Knoten die direkte Verbindung und wählt normalerweise die direkte Verbindung als optimalen Leitweg aus. Ist der direkte Leitweg berechnet, sendet der Netzknoten die zur Aktivierung der Verbindung zu verwendende Adresse des Partners an den Endknoten.

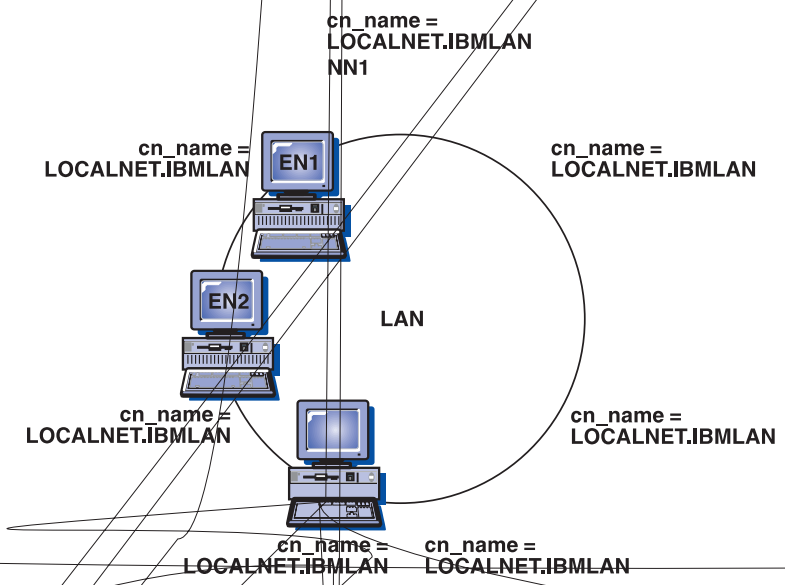
Der Verbindungsnetzleitweg wird möglicherweise nicht verwendet, wenn die Sicherheit des Verbindungsnetzes nicht den Anforderungen entspricht. Ist die DLC des Verbindungsnetzes nicht sicher und wird im Parameter **MODE_NAME** ein Modus wie z. B. #BATCHSC verwendet, versucht der Netzknoten, einen sicheren Leitweg zu finden, wobei das Verbindungsnetz nicht berücksichtigt wird.

Werden [illegible]en verwendet, betrachtet APPN das gesamte über Brücken angesc[illegible]kale Netz als ein einziges logisches Netz. Da Verbindungen zwischen [illegible]igen Systemen im LAN hergestellt werden können, wird nur ein Verbi[illegible] benötigt. Dieses Verbindungsnetz sollte in allen APPN-Systemen auf d[illegible]efiniert sein.

Ein [illegible]en erhält während der Registrierung der Endknoten und bei APP[illegible]ichnissuchen Informationen vom Verbindungsnetz. Der Netzknoten-Ser[illegible]lt damit genügend Informationen, um eine direkte Verbindung zwischen de[illegible]gsendpunktknoten ohne Weiterleitung über Zwischenknoten zu be[illegible]n.

D[illegible]rbindungsnetz kann nur von Endknoten und Netzknoten genutzt werden; V[illegible]dungen zu LEN-Knoten müssen immer noch explizit definiert werden.

A[illegible]. 12 zeigt ein Beispiel für ein Verbindungsnetz. Diese Darstellung eines LAN zeigt das Verbindungsnetz mit dem Namen LOCALNET.IBMLAN. Durch diese Definition kann jeder Endknoten eine direkte Verbindung mit jedem anderen Endknoten herstellen, solange für alle Endknoten NN1 als Netzknoten-Server aktiv ist.



Andere Verbindungsparameter

Andere **LINK_STATION**-Schlüsselwortparameter, die in den vorherigen Abschnitten erwähnt wurden, aber möglicherweise nicht klar sind oder implizit definiert wurden, sind:

- Typ des Nachbarknotens
- Bevorzugter Netzknoten-Server
- SSCP-Sitzungsanforderung

Dieser Abschnitt enthält eine Kurzbeschreibung dieser Parameter.

Typ des Nachbarknotens

Dieser Parameter gibt den Typ des Knotens an, der ein Nachbarknoten des Knotens ist, der die Verbindung definiert. Zu den gültigen Typen gehören:

- DSPU_NOXID
- DSPU_XID
- END_NODE
- HOST_DEP_LU_ONLY
- HOST_XID0
- LEARN
- NETWORK_NODE
- SUBAREA_LEN

Weitere Einzelheiten können der *Configuration File Reference* entnommen werden.

Bevorzugter Netzknoten-Server

Dieser Parameter gibt an, ob der Nachbarnetzknoten als Netzknoten-Server über die definierte Verbindung verwendet werden soll.

SSCP-Sitzungsanforderung

Dieser Parameter gibt an, ob SSCP-PU-Sitzungen vom Host über die definierte Verbindung angefordert werden.

-CP-Sitzungen Services zur Verfügung stellt, muß der LEN-Knoten den Steuerpunkt des Netzknotens für alle LUs, einschließlich der LUs auf den Endknoten (ENs), als „Eignersteuerpunkt“ definieren.

Abbildung 13. LEN-Knoten-Verzeichnis. Im Verzeichnis des LEN-Knotens müssen alle LUs aufgeführt sein, mit denen der Knoten kommuniziert. Da der benachbarte Netzknoten (NN) dem LEN-Knoten auch ohne CP

Ist eine LU nicht im Verzeichnis eines Endknotens eingetragen, startet der Endknoten eine Suche (Locate), um die gewünschte LU zu finden. Um die Suche einzuleiten, ruft der Endknoten die Services seines Netzknoten-Servers auf. Abb. 14 zeigt ein Beispiel eines Endknotenverzeichnisses.

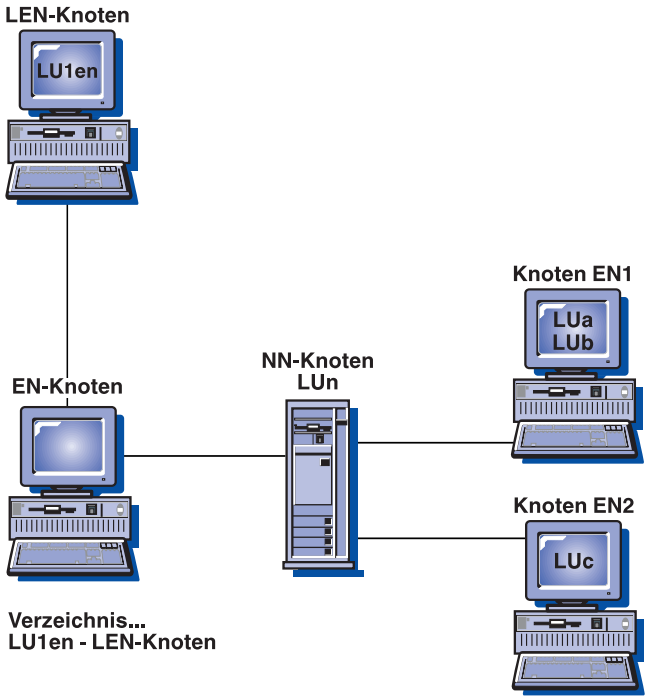


Abbildung 14. Endknotenverzeichnis. Der Endknoten (EN) benutzt die Services seines Netzknoten-Servers, um die Position der LUs zu ermitteln. Keine der LUs im APPN-Netz muß auf dem Endknoten definiert sein. Die LU des Nachbar-LEN-Knotens muß dagegen definiert sein, da sie weder mit dem Netzknoten verbunden, noch Teil des APPN-Netzes ist.

Ein Netzknoten stellt den Endknoten, die ihm zugeordnet sind, zusammen mit allen anderen Netzknoten im APPN-Netz verteilte Verzeichnisservices zur Verfügung. Der Ursprungsnetzknoten empfängt den Namen einer Ziel-LU von einem Endknoten, der seine Services in Anspruch nimmt, in einer Suchanforderung (Locate) oder den Namen einer sekundären LU in einer BIND-Anforderung von einem LEN-Knoten. Der Netzknoten prüft die aktuelle Position der LU, wenn sie im Verzeichnis des Endknotens enthalten ist (sich jedoch nicht auf den Netzknoten selbst befindet). Diese Überprüfung wird vorgenommen, indem eine gesteuerte Suche an den Zielnetzknoten-Server gesendet wird.

Abbildung 15. Netzknotenverzeichnis. I

Topologieservices und Services für Weiterleitungsauswahl

Ein Netzknoten stellt sich und den Endknoten, die ihm zugeordnet sind, Services zur Weiterleitungsauswahl zur Verfügung. Er verwaltet eine interne Netztopologiedatenbank, die die vollständigen und aktuellen Topologiedaten über das Netz enthält. Diese Topologiedaten setzen sich aus den Merkmalen aller Netzknoten im Netz und aller Verbindungen zwischen den Netzknoten zusammen. Alle Netzknoten enthalten eine Kopie der Topologiedatenbank.

Ein Netzknoten benutzt die Netztopologiedatenbank, um Leitwege für Sitzungen zu berechnen, die ihren Ursprung in den LUs auf dem Netzknoten oder auf den Endknoten haben, denen er Services zur Verfügung stellt. Jeder vom Netzknoten berechnete Leitweg ist der Leitweg mit der zur Zeit niedrigsten Gewichtung vom Knoten, auf dem sich die Ursprungs-LU befindet, zu dem Knoten, auf dem sich die Ziel-LU befindet. Zur Ermittlung eines günstigen Pfads durch das Netz weist der Algorithmus zur Auswahl des Leitwegs zunächst Knoten und Verbindungen eine bestimmte Gewichtung zu. Je nach relativer Wichtigkeit der Merkmale für die angeforderte Serviceklasse errechnet der Algorithmus für die Gewichtung einen skalaren Wert für jeden Knoten und jede logische Verbindung.

Topologiedatenbank

Die Netztopologiedatenbank auf einem Netzknoten enthält Informationen zu allen Netzknoten und zu allen Übertragungsgruppen, die die Knoten miteinander verbinden. Sie ist eine vollständig vervielfältigte Datenbank, die von allen Netzknoten im Netz zur Weiterleitungsauswahl gemeinsam benutzt wird. Zur Verwaltung der Datenbank ist es erforderlich, daß Aktualisierungen im Rundsendebetrieb an alle Netzknoten gesendet werden. Die Aktualisierungen werden mittels TDU-Nachrichten durchgeführt, die für jede der in einer TDU beschriebenen Ressourcen Knotenidentifikationsinformationen, Knoten- und Verbindungsmerkmale sowie Aktualisierungsfolgenummern zur Kennzeichnung der jüngsten Änderungen enthalten.

Eine lokale Topologiedatenbank auf einem Endknoten enthält nur Informationen über sich und direkt angeschlossene Knoten.

Die Komponente mit den Topologieservices und den Services für die Weiterleitungsauswahl verwendet CP-CP-Sitzungen zwischen Netzknoten, um Informationen zur Erstellung und Verwaltung einer Topologiedatenbank auszutauschen. Diese Topologiedatenbank auf den Netzknoten wird mit Hilfe von Aktualisierungen stets auf dem neuesten Stand gehalten; diese werden an alle Netzknoten übertragen, sobald eine Ressource (ein Knoten oder eine Verbindung) aktiviert oder inaktiviert wird oder sich die Merkmale einer bestehenden Ressource ändern.

Jeder Netzknoten verwaltet eine lokale Konfigurationsdatenbank und eine Netztopologiedatenbank, wie in Abb. 16 auf Seite 53 gezeigt. Die lokale Konfigurationsdatenbank befindet sich nur auf dem jeweiligen Knoten, während die Netztopologiedatenbank auf allen Netzknoten vervielfältigt wird.

Tabelle 2 zeigt die in der Konfigurationsdatenbank auf dem lokalen Netzknoten enthaltenen Informationen.

Tabelle 2. Lokale Netzknoten-Konfigurationsdatenbank

Knoten	Verbindung	zwischen
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
NN8	c	NN8—NN6
	d	NN8—NN7
	j	NN8—EN3
	h	NN8—EN4

Tabelle 3 zeigt die in der Netztopologiedatenbank auf dem lokalen Netzknoten enthaltenen Informationen.

Tabelle 3. Netztopologiedatenbank auf dem lokalen Netzknoten

Knoten	Verbindung	zwischen
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

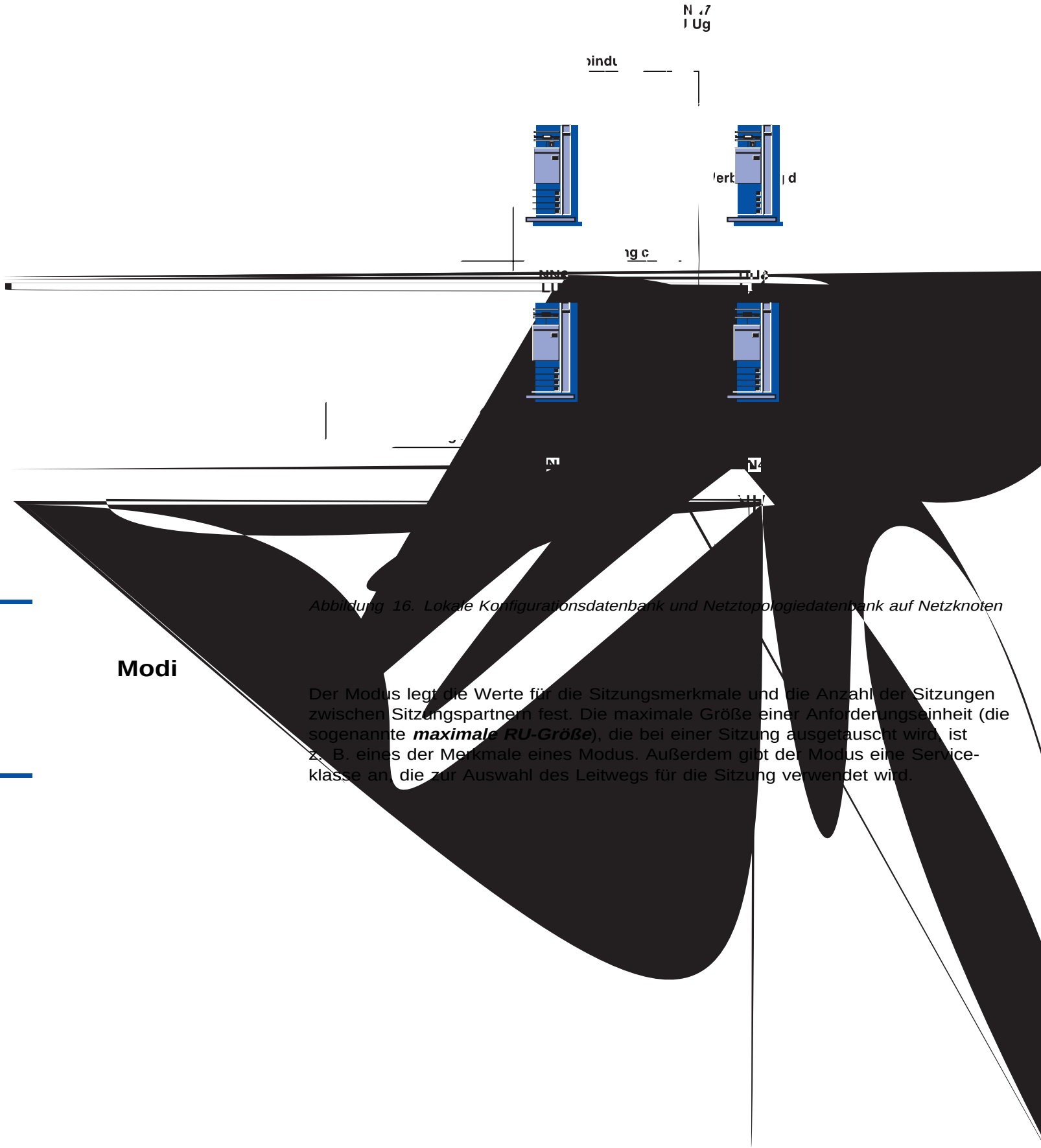


Abbildung 16. Lokale Konfigurationsdatenbank und Netztopologiedatenbank auf Netzknoten

Modi

Der Modus legt die Werte für die Sitzungsmerkmale und die Anzahl der Sitzungen zwischen Sitzungspartnern fest. Die maximale Größe einer Anforderungseinheit (die sogenannte ***maximale RU-Größe***), die bei einer Sitzung ausgetauscht wird, ist z. B. eines der Merkmale eines Modus. Außerdem gibt der Modus eine Serviceklasse an, die zur Auswahl des Leitwegs für die Sitzung verwendet wird.

Serviceklasse

Bei der Initialisierung einer Sitzung wird mit BIND ein Modusname festgelegt. Dieser Modusname wird der Definition einer Serviceklasse (COS - Class Of Service) zugeordnet, die zur Ermittlung des günstigsten Leitwegs zwischen Ursprungs- und Zielknoten der Sitzung verwendet wird. Die Serviceklassendefinitionen geben die Merkmale an, die Knoten und Verbindungen besitzen müssen, um bei der Wahl des Sitzungsleitwegs berücksichtigt zu werden. Durch diese Angabe kann der Algorithmus zur Weiterleitungsauswahl bestimmen, ob ein Knoten oder eine Verbindung akzeptabel ist. Aus der Menge, die akzeptabel ist, berechnet der Algorithmus den besten Leitweg für die Sitzung.

Da Serviceklassendefinitionen variieren können, kann es, je nach dem angegebenen Modusnamen, für verschiedene Sitzungen unterschiedliche Leitwege zwischen denselben Ursprungs- und Zielknoten geben. Jeder Netzknoten kann den Leitweg mit der niedrigsten Gewichtung (den wünschenswertesten) zu einer beliebigen Zieladresse berechnen.

Wird eine Sitzung sowohl über ein APPN-Netz als auch über ein Unterbereichsnetz aufgebaut, verwendet sie zwei Serviceklassen:

- Im APPN-Netz benutzt die Sitzung die Serviceklasse, die für den vom Transaktionsprogramm benutzten Modus definiert ist. Diese Definition steht in der aktiven Konfiguration der Datenstation. Die Serviceklasse wird verwendet, um die Sitzung im APPN-Netz weiterzuleiten.

  Wird als Standardmodusname BLANK (DEFAULT_MODE_NAME(BLANK) angegeben, ist die zugeordnete Serviceklasse #CONNECT.

- Im Unterbereichsnetz kann der Name der Serviceklasse in die Anmeldemodustabelle geschrieben werden, und zwar in das Eintragsfeld für den von der Sitzung verwendeten Modusnamen. Diese Serviceklasse wird vom Programm VTAM benutzt, um die Sitzung über das Unterbereichsnetz weiterzuleiten.

  Wird als Standardmodusname BLANK (DEFAULT_MODE_NAME(BLANK) angegeben oder ist in den Eintragsfeldern der Anmeldemodustabelle gar keine Serviceklasse definiert, verwendet die Serviceklasse standardmäßig den Eintrag BLANK in der ISTSDCOS-Tabelle.

In beiden Fällen benutzen beide Netze den Modusnamen, um den Namen der Serviceklasse zu ermitteln, die beiden Serviceklassennamen müssen jedoch nicht unbedingt identisch sein.

SNA-Übertragungspriorität

Die Übertragungspriorität ist ein Wert, der in der Serviceklasse angegeben wird. Sie wird im BIND des COS/TPF-Steuervektors gesendet. Sobald die Sitzung eingeleitet ist, erhalten die Daten nachfolgender Sitzungen die im COS/TPF-Steuervektor angegebene Übertragungspriorität.

Eine Sitzung, die eine Serviceklasse mit hoher Priorität benutzt, kann Daten an Sitzungen mit niedriger Priorität weitergeben. Sitzungen mit interaktivem Datenaustausch, bei denen die Antwortzeit von Bedeutung ist, wie z. B. Emulationssitzungen, sollten eine hohe Priorität erhalten. Sitzungen, die große Datenmengen übertragen, wie z. B. Dateiübertragungen für NetView Distribution Manager, sollten eine niedrigere Priorität erhalten.

Wird die Übertragungspriorität unterstützt, dann wird nach Möglichkeit verhindert, daß Sitzungen, bei denen große Datenmengen übertragen werden, den Datenfluß zwischen interaktiven Sitzungen behindern.

Die vier Übertragungsprioritäten heißen Netz, hoch, mittel und niedrig. Die Netzpriorität wird für Netzsteuerungsdaten, wie z. B. Topologie- und Verzeichnisservices verwendet. Die übrigen Prioritäten werden für Benutzerdaten verwendet.

Der Communications Server unterstützt Übertragungsprioritäten für LAN-, SDLC- und X.25-Verbindungen. Der Vorteil dieser Funktion tritt besonders zutage, wenn das Netz überlastete langsame Verbindungen enthält.

Weiterleitungsauswahl

Wenn der Netzknoten-Server eine Antwort auf seine Suche (Locate) erhalten hat, berechnet die Komponente mit den Topologieservices und den Services für die Weiterleitungsauswahl den für die angeforderte Serviceklasse günstigsten Leitweg vom Ursprungsknoten zum Zielknoten.

Da die Komponente mit den Topologieservices und den Services für Weiterleitungsauswahl Topologiedatenbankaktualisierungen als Merkmale für beliebige Ressourcenänderungen sendet und empfängt, wird jeder Leitweg anhand der neuesten Informationen berechnet.

Weiterleitungsauswahl für VTAM-Benutzer

Zur Weiterleitung des APPC-Verkehrs über einen Unterbereich müssen die Datenstationen, die mit dem Unterbereich verbunden sind, im Communications Server als Netzknoten definiert sein. Auf jedem Netzknoten ist eine Verbindung definiert, die den Knoten mit dem Unterbereich verbindet. Aus der Sicht des Netzknotens sind Partner-LUs am anderen Ende des Unterbereichs als auf dem Host befindlich definiert (ein LEN-Knoten). Aus der Sicht des Hosts muß jeder Netzknoten, der mit dem Unterbereich verbunden ist, mit einem PU-Makro für das Programm VTAM definiert werden. Alle logischen Zieleinheiten des Typs LU 6.2 innerhalb des APPN-Netzes, die für eine spezielle Verbindung vorgesehen sind, werden unter der PU (Netzknoten) so definiert, als befänden sie sich tatsächlich auf der PU. Die LUs können sich aber durchaus auf anderen Knoten innerhalb des APPN-Netzes befinden, die mit dem Netzknoten verbunden sind. Der Host sieht nur die Netzknoten-PU. Die Netzknoten-PU kann auch eine Gateway-PU sein. Ist der Parameter bei dem NCP auf YES gesetzt, und es sind keine PU- oder Steuerpunkt-Sitzungen aktiv, ist SETN-Verkehr (**CP_CP_SESS_SUPPORT=NO**) nicht zulässig. Wenn der Name der PU in der VTAM-Definition mit dem im Communications Server definierten Namen des Steuerpunkts identisch ist, kann der Steuerpunkt in den VTAM-Definitionen nicht als LU definiert werden. Im Programm VTAM müssen sowohl PU- als auch LU-Namen eindeutig sein.

Das PU-Makro muß die Anweisung **XID=YES** enthalten, damit bei der Aktivierung der PU ein XID-Austausch stattfinden kann. Dieser Parameter wird im Hauptknoten des NCP codiert. Er darf nicht in der PU-Anweisung eines Hauptknotens mit Wählleitung stehen.

Für SNA-Einheiten mit Wählleitung kann ein neuer Parameter im PU-Makro verwendet werden: **CPNAME**=cccccccc. Er gibt den Steuerpunktnamen des mit dem Unterbereich verbundenen Netzknotens an. In der Definitionsanweisung für die PU mit Wählleitung muß entweder **CPNAME** oder **IDBLK** und **IDNUM** angegeben werden. Beides kann angegeben werden. Der Netzknoten stellt dem VTAM-Programm seinen Steuerpunktnamen im XID-Austausch während der Verbindungssequenz zur Verfügung. Das Programm VTAM benutzt den Namen des Steuerpunkts, um das entsprechende PU-Makro zu lokalisieren. Wenn kein PU-Makro mit dem entsprechenden Steuerpunktnamen existiert, verwendet das VTAM-Programm zur Lokalisierung des PU-Makros die Parameter **IDNUM** und **IDBLK**.

Um den APPC-Datenfluß von einem APPN-Netz über den Unterbereich zu einem anderen Teil des APPN-Netzes weiterzuleiten, muß der Name des Netzes (**NETID**) des VTAM-Eignerprogramms mit der Netz-ID des APPN-Netzes übereinstimmen. Im Communications Server kann die Netz-ID (des mit dem Unterbereich verbundenen Netzknotens) mit Hilfe des Profils für Merkmale des lokalen SNA-Knotens ermittelt werden.

Weitervermittlung eines Sitzungsleitwegs

Die Weitervermittlung eines Sitzungsleitwegs ist eine Funktion, die von einem Netzknoten ausgeführt wird. Sie ermöglicht es einem Netzknoten, Daten, die für einen anderen Knoten bestimmt sind, zu empfangen und weiterzuleiten. Die Ursprungs- und Zieladresse der Daten kann ein Endknoten, ein Netzknoten oder ein LEN-Knoten sein. Der Teil einer Sitzung zwischen zwei Nachbarknoten wird als Sitzungsabschnitt bezeichnet.

Unterstützung für High Performance Routing (HPR)

Communications Server unterstützt HPR über Enterprise Extender- (IP), SDLC- (Synchronous Data Link Control- synchrone Datenübertragungssteuerung), LAN-, WAN-, Kanal-, MPC- (Multi-Path Channel) und X.25-Verbindungen.

Automatic Network Routing (ANR) von HPR reduziert die Speicher- und Verarbeitungsanforderungen in Zwischenknoten auf ein Minimum. Dies ist für Hochgeschwindigkeitsnetze mit niedrigen Fehlerraten eine bessere Lösung als die Weitervermittlung eines Sitzungsleitwegs von APPN.

HPR verbessert die SNA-Weiterleitung mit den folgenden Funktionen:

- Protokollunabhängige Zwischenknoten

  Protokollunabhängige Zwischenknoten registrieren die Verbindungen, die über sie laufen, nicht.

  Ein HPR-Zwischenknoten benötigt keine Steuerblöcke oder Pufferpools, um die über ihn laufenden Verbindungen zu unterstützen. Er benötigt auch keine Leitwegtabellen, da die Leitweginformationen in jedem Paket enthalten sind. Mit Automatic Network Routing (ANR) empfängt ein HPR-Zwischenknoten einfach ein Paket, untersucht die Paketkopfzeile, um eine Kennung für die logische Verbindung mit dem nächsten Knoten zu finden, und sendet das Paket über diese Verbindung.

- Für einen HPR-Zwischenknoten gilt folgendes:
  - Er stellt Pakete nicht wieder her, da die HPR-Verbindungsendpunkte verlorengegangene Pakete mit RTP (Rapid Transport Protocol) ermitteln und wiederherstellen. Hat das LAN hohe Fehlerraten, kann auch eine ERP-Unterstützung (ERP - Error Recovery Protocol) auf Verbindungsebene gewählt werden. Dies sollte jedoch bei Verbindungen mit niedrigen Fehlerraten nicht erforderlich sein.
  - Er fügt segmentierte Pakete nicht erneut zusammen, um sie wieder zu segmentieren, da die HPR-Verbindungsendpunkte automatisch eine Paketgröße wählen, die von allen Zwischenknoten im Leitweg unterstützt wird.
  - Puffer werden nicht aktiv verwaltet und eine Überlastung wird nicht verhindert, da die HPR-Verbindungsendpunkte mit Flußsteuerungsalgorithmen eine Überlastung an Zwischenknoten verhindern.
  - Der Leitweg eines Pakets wird nicht anhand einer Tabellensuche festgelegt, da die HPR-Verbindungsendpunkte eine Quellenweiterleitung durchführen und die Paketweiterleitungsinformationen anhand von Kennungen erstellen, die von den einzelnen Zwischenknoten für eine optimale Leistung ausgewählt wurden.

  Folgendermaßen vorgehen, um protokollunabhängige Zwischenknoten zu erzielen:

  - Die Pufferkapazität der Endpunkte des Leitwegs muß für die Leitwegverzögerung und den Anwendungsdurchsatz ausreichen. Dieser Wert hängt von der jeweiligen Netzkonfiguration ab.
  - Die Datenübertragungsverbindungen müssen I-Feldgrößen unterstützen, die groß genug sind, um die HPR-Kopfzeilen zu enthalten und alle Anwendungsdaten effizient zu übertragen.
  - Die Datenübertragungsverbindungen müssen sehr zuverlässig sein, da sich eine hohe Fehlerrate negativ auf den HPR-Durchsatz auswirkt.

  Bei Konfigurationen, die diese Bedingungen nicht erfüllen, ist APPN ohne HPR immer noch eine gültige Implementierungsmöglichkeit. Die HPR-Technik ist eine APPN-Option; APPN ohne HPR ist weiterhin verfügbar und wird unterstützt.

- Vermeidung von Überlastung

  Ein HPR-Netz kann eine sehr hohe Verbindungsauslastung erreichen. Mit der sogenannten ARB-Flußsteuerung (ARB - Automatic Rate Based) stellen die HPR-Verbindungsendpunkte Netzüberlastungen automatisch fest und verringern die Übertragungsbelastung. Dadurch wird verhindert, daß Pakete verlorengehen, was bei anderen Leitwegalgorithmen aufgrund mangelnder Puffer in Zwischenknoten vorkommen kann.

- Automatische Rufweiterleitung ohne Unterbrechung

  Stellt ein HPR-Verbindungsendpunkt fest, daß ein Leitweg fehlschlug, errechnet er automatisch einen neuen Leitweg, baut die Verbindung wieder auf und stellt alle aufgrund des Fehlers verlorengegangenen Pakete wieder her. Da HPR-Zwischenknoten protokollunabhängig sind (d. h., sie registrieren die Verbindungen nicht, die über sie laufen), sind sie an diesem Wiederherstellungsprotokoll nicht beteiligt. Da bei erfolgreicher Umschaltung des Leitwegs keine Pakete verlorengehen, werden Anwendungen, die den Leitweg verwenden, durch den Fehler nicht unterbrochen.

- Software mit bestehender Hardware kompatibel
  HPR ist eine Softwareerweiterung von APPN; d. h., HPR kann auf den vorhandenen LAN- oder WAN-Adaptern und Frame Relay-Verbindungen verwendet werden. Da HPR nicht versucht, dedizierte Bandbreite und garantierten Echtzeittransport zur Verfügung zu stellen (diese Funktionsebene wird den Breitbandnetzservices überlassen), entsprechen die Leistungseinschränkungen bei Paketweiterleitungsverzögerungen den Einschränkungen bei APPN ohne HPR. Die von HPR verwendeten Steuerpunktprotokolle entsprechen bis auf wenige Zusätze den Protokollen von Basis-APPN, so daß HPR-Knoten zusätzlich in einem bestehenden APPN-Netz ohne Vorplanung oder Koordination installiert werden können.

RTP (Rapid Transport Protocol)

RTP ist eine Gruppe von Nachrichtenformaten und -protokollen, die konzipiert wurden, um moderne Datenübertragungsmedien zu verwenden, den Systemaufwand in Zwischenknoten auf ein Minimum zu reduzieren und Pfade automatisch umzuschalten, wenn eine Verbindung im Pfad ausfällt.

RTP-Verbindungen werden in einem ***HPR-Teilnetz*** aufgebaut und zum Transport von Sitzungsdaten verwendet. Ein HPR-Teilnetz ist der Teil eines APPN-Netzes, das RTP-Verbindungen aufbauen und HPR-Sitzungsdaten übertragen kann. RTP-Verbindungen sind quasi ***Transportleitungen***, über die Sitzungen ausgeführt werden. Diese Verbindungen können sehr schnell Daten weiterleiten, indem sie eine Weitervermittlung eines Sitzungsleitwegs der unteren Ebene verwenden und die Datenübertragung über die Verbindungen für Fehlerbehebung und Flußsteuerung minimieren. Diese Datenflüsse werden von RTP-Verbindungsendpunkten verwaltet. Der physische Pfad einer RTP-Verbindung kann automatisch geändert werden, um Daten an einem fehlerhaften Knoten oder einer fehlgeschlagenen Verbindung vorbeizuleiten, ohne daß die Sitzungen unterbrochen werden müssen. Daten, die sich zum Zeitpunkt der Störung im Netz befanden, werden automatisch wiederhergestellt.

RTP führt die Fehlerbehebung an den Endpunkten aus und nicht auf der Verbindungsebene. Die Leistung wird verbessert, indem die Anzahl der für die Fehlerbehebung erforderlichen Datenflüsse reduziert wird. Außerdem wird ERP (Error Recovery Protocol) auf Verbindungsebene für alle Verbindungen unterstützt. Mit ERP kann ein verlorengegangenes Paket an einem Ende einer Verbindung ermittelt und wiederhergestellt werden, indem am anderen Ende der Verbindung eine Übertragungswiederholung des Pakets angefordert wird. Wird ERP verwendet, werden HPR-Pakete als numerierte Informationsrahmen (I-RAHMEN) gesendet. Bei Verlust eines Rahmens ermittelt die DLC den Verlust, und der Rahmen wird erneut gesendet. Wird ERP nicht verwendet, werden HPR-Pakete als Rahmen mit nicht numerierten Daten (UI-RAHMEN) gesendet. Bei Verlust eines Rahmens kann die DLC den Verlust nicht ermitteln, und das RTP (Rapid Transport Protocol) von HPR muß die verlorengegangenen Pakete an den Endpunkten einer Verbindung ermitteln und wiederherstellen. In beiden Fällen werden verlorengegangene Pakete an den Endpunkten einer Verbindung von RTP ermittelt und wiederhergestellt. Für jeden vorhandenen Anschluß kann eine beliebige Anzahl von Verbindungen vorhanden sein, die ERP verwenden oder ERP nicht verwenden.

ERP kann für jede einzelne Verbindung aktiviert oder inaktiviert werden. Da RTP verlorengegangene Pakete an den Endpunkten einer Verbindung ermittelt und wiederherstellt, können beim Aufbau des Netzes entweder ERP-Verbindungen oder

Nicht-ERP-Verbindungen verwendet werden. Dadurch kann bei Verbindungen mit einer hohen Paketverlustrate ERP auf Verbindungsebene angegeben werden, und der Durchsatz bei anderen Verbindungen kann maximiert werden, indem angegeben wird, daß diese nicht ERP auf Verbindungsebene verwenden. In der Regel ist die Verwendung von ERP in LANs nicht zu empfehlen.

Anmerkung: ERP ist in einer WAN-Umgebung immer aktiviert.

Fluß- und Überlastungssteuerung erfolgen ebenfalls durch RTP an den Endpunkten. RTP verwendet eine Technik, die als ARB-Flußsteuerung (ARB - Automatic Rate Based) bezeichnet wird, um - wenn möglich - die volle Bandbreite des Netzes zu verwenden. RTP erhöht die Geschwindigkeit, mit der Pakete gesendet werden, wenn das Netz diese erhöhte Geschwindigkeit unterstützt. Eine Überlastung wird automatisch erkannt, und die Sendegeschwindigkeit wird bei Auftreten einer Überlastung entsprechend reduziert. Die konfigurierte effektive Kapazität von Verbindungen im Verbindungspfad wird verwendet, um sowohl die ursprüngliche Sendegeschwindigkeit als auch die Erhöhung dieser Geschwindigkeit zu ermitteln.

Unterstützung für Steuerungsflüsse (CF - Control Flow) über RTP-Verbindungen ist nun mit HPR in Communications Server verfügbar. Früher haben Steuerungsflüsse einschließlich CP-CP-Sitzungen und Nachrichten zur Leitwegkonfiguration APPN-Verbindungen verwendet, während die Datenflüsse HPR-Verbindungen verwendet haben. Nun können sowohl Steuerungsflüsse als auch Datenflüsse RTP-Verbindungen verwenden. Zu den Vorteilen dieser Unterstützung gehört die automatische Pfadumschaltung für CP-CP-Sitzungen. Steuerungsflüsse laufen automatisch über RTP, wenn beide Endpunkte der Verbindung diese Funktion unterstützen.

Automatic Network Routing (ANR)

Automatic Network Routing (ANR) ist eine protokollunabhängige Weiterleitungstechnik, die von RTP ermöglicht wird, wobei eine Nachricht mit einem Kennsatz ankommt, der den nächsten Zwischenschritt im Pfad eindeutig kennzeichnet. Wegen seines einfachen Aufbaus kann ANR auf einer sehr niedrigen Ebene ohne Kenntnis der Verbindungen, die diesen Pfad verwenden, ausgeführt werden. ANR reduziert Zyklen und Speicheranforderungen zum Weiterleiten von Paketen über Zwischenknoten. Die schnelle Paketvermittlungsfunktion von ANR erhöht die Leistung in Zwischenknoten durch Weiterleitung auf einer niedrigeren Ebene als APPN sowie Ausführung von Fehlerbehebung, Segmentierung, Flußsteuerung und Überlastungs-
steuerung am Endknoten statt am Zwischenknoten.

ANR-Zwischenknoten können die SNA-Sitzungen oder RTP-Verbindungen nicht erkennen. Die Leitweginformationen für jedes Paket werden mit dem Paket in einer Netzkopfzeile übertragen. Jeder Knoten entfernt die Informationen, die er in der Kopfzeile gelesen hat, bevor er das Paket weiterleitet, so daß der nächste Knoten seine Leitweginformationen an einer festen Position in der Kopfzeile findet. Anders als bei Basis-APPN müssen keine Leitwegtabellen für Sitzungsanschlüsse beibehalten werden, wodurch die Vermittlung von Paketen über Knoten schneller durchgeführt werden kann.

LU-Unterstützung

SNA definiert die LU-Typen 0, 1, 2, 3, 4, 6.0, 6.1 und 7. Die LU-Typen 0,1, 2, 3, 4 und 7 unterstützen die Kommunikation zwischen Anwendungsprogrammen und verschiedenen Datenstationstypen. Die LU-Typen 6.0 und 6.1 ermöglichen die Kommunikation zwischen Programmen, die sich auf Unterbereichsknoten des Typs 5 befinden. LU-Typ 6.2 unterstützt die Kommunikation zwischen zwei Programmen, die sich auf Unterbereichsknoten des Typs 5 und/oder auf peripheren Knoten des Typs 2.1 befinden, sowie die Kommunikation zwischen Programmen und Einheiten.

Der Communications Server unterstützt die LU-Typen 0, 1, 2 und 3, die die Kommunikation mit Host-Anwendungen unterstützen, die Einheiten wie z. B. die folgenden unterstützen:

LU-Typ 0 3650 und 4700 Bankendatenstationen

LU-Typ 1 3270-Drucker

LU-Typ 2 interaktive 3270-Bildschirme

LU-Typ 3 3270-Drucker

Die Kommunikation wird nur zwischen LUs desselben LU-Typs geführt. Eine LU 2 kommuniziert zum Beispiel mit einer anderen LU 2, aber nicht mit einer LU 3. Der Communications Server unterstützt außerdem die LU 6.2 oder APPC.

Durch die SNA-Funktionen des Communications Server können Anwendungen die APPC-API benutzen, um eine Funktion für verteilte Transaktionsverarbeitung zur Verfügung zu stellen, bei der zwei oder mehr Programme eine Verarbeitungsfunktion gemeinsam ausführen. Diese Funktion beinhaltet, daß die beiden Programme miteinander kommunizieren, damit sie lokale Ressourcen, wie z. B. Prozessorzyklen, Datenbanken, Warteschlangen für die Vorgangsbearbeitung und physische Schnittstellen wie Tastatur und Bildschirm gemeinsam benutzen können.

Der Communications Server unterstützt APPC über die APPC-APIs. Weitere Informationen sind den folgenden Veröffentlichungen zu entnehmen:

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

Die folgenden Funktionen des Communications Server unterstützen eine Reihe von LU-Typen:

- SNA-Gateway
  Der SNA-Gateway ermöglicht es Hosts des IBM Systems /370 und/oder Hosts der Architektur des IBM Systems /390, mit dem LAN verbundene Datenstationen zu unterstützen, die die LU-Typen 0, 1, 2, 3 oder 6.2 benutzen, um über eine SNA-Gateway-Datenstation zu kommunizieren.

  Der SNA-Gateway unterstützt außerdem die LU-Typen 1, 2 oder 3 für AS/400-Hosts, die die Daten verarbeiten oder an Hosts der Architektur des IBM Systems /370 oder /390 weiterleiten können.

- Konventionelle LU-Anwendung (LUA)
  Die LUA besteht aus Systemsoftware, die Serviceroutinen zur Unterstützung von LUs 0, 1, 2 und 3 zur Verfügung stellt.

SDDLU-Unterstützung

Durch die Unterstützung für selbstdefinierende abhängige logische Einheiten (SDDLU - Self-Defining Dependent Logical Unit) kann eine abhängige LU auf dem Host (VTAM) dynamisch definiert und aktiviert werden. In VTAM wird dies als dynamische Definition abhängiger LUs (DDDLU) bezeichnet. SDDLU wird im Communications Server aktiviert, indem in einer LU-Definition eine LU_MODEL-Anweisung codiert wird.

Zur Aktivierung der DDDLU-Funktion in VTAM den Operanden LUGROUP in der PU-Definitionsanweisung für die PU sowie einen Hauptknoten der LU-Gruppe codieren. Um die von IBM gelieferte SDDLU-Ausgangsroutine zu verwenden, die LU-Namen erstellt, sollte zusätzlich der Operand LUSEED in der PU-Anweisung codiert werden.

Der Operand LUGROUP gibt den Namen der Modell-LU-Definitionsgruppe an, die VTAM verwendet, wenn es für diese PU dynamisch LUs definiert. Der Hauptknoten der LU-Gruppe enthält die Modelldefinitionsanweisungen. Dynamische Definitionen für LUs werden mit Hilfe der in diesem Hauptknoten enthaltenen Modell-LU-Definitionen erstellt.

Der Operand LUSEED stellt einen Musternamen zur Verfügung, den die SDDLU-Ausgangsroutine verwendet, um für die dynamisch erstellte LU einen Namen zu generieren. Wenn die richtigen Anweisungen in der PU-Anweisung hinzugefügt und der Hauptknoten der LU-Gruppe codiert wurden, müssen die Hauptknoten aktiv sein, damit die SDDLU-Funktion aktiviert werden kann.

Unterstützung für abhängigen LU-Requester (DLUR)

Der abhängige LU-Requester (DLUR) ist eine Architektur, die dazu dient, abhängige LU-Unterstützung in einem APPN-Netz bereitzustellen. Der Communications Server unterstützt Basis-DLUR-Funktionen sowie die folgenden wahlfreien Funktionen:

- SDDLU-Unterstützung

  Durch Verwendung der SDDLU-Unterstützung können die von DLUR unterstützten LUs für VTAM dynamisch definiert werden, dadurch entfällt die Notwendigkeit, diese LUs vorzudefinieren.

- TakeOver/GiveBack-Unterstützung

  Durch diese Unterstützung können LU-LU-Sitzungen aktiv bleiben, selbst wenn die Verbindung zwischen den DLUR- und DLUS-Knoten fehlgeschlagen ist. Die Verbindung kann mit demselben oder einem anderen DLUS wiederhergestellt werden, ohne daß die LU-LU-Sitzungen unterbrochen wurden.

- Unterstützung für mehrere Teilnetze

  Durch diese Unterstützung können sich der DLUR-Knoten, DLUS-Knoten und der Knoten, der die Anwendung enthält, jeweils in verschiedenen Teilnetzen befinden.

- Registrierung von LUs, denen ein DLUS Services zur Verfügung stellt

  Ein Endknoten-DLUR registriert seine LUs so, daß der Netzknoten diese LUs lokalisieren kann, ohne Suchanforderungen an den DLUR stellen zu müssen.

- Unterstützung für Sicherungs-DLUS

  Ist die Verbindung zum primären DLUS fehlgeschlagen oder kann sie nicht aktiviert werden, versucht der Communications Server automatisch, eine Verbindung mit dem Sicherungs-DLUS aufzubauen.

DLUR verwenden

Zur Verwendung der DLUR-Funktion eine Definition **DLUR_DEFAULTS** konfigurieren und den Verbindungsnamen aus dieser Definition als Host-Verbindung für die LUA-, abhängige LU 6.2- oder Gateway-Definitionen verwenden. Communications Server sendet den PUNAME, CPNAME und die NODEID an den DLUS. Der PUNAME wird als Teil der Signalinformationen (CV X'0E') gesendet.

- Ist der DLUS eine höhere Version (unterstützt die Prüfung von CV X'0E' in REQACTPU), wird der PUNAME im Suchalgorithmus verwendet. Dies ist bei VTAM 4.3 mit PTF oder höher verfügbar.
- Ist der DLUS eine niedrigere Version, wird CV X'0E' ignoriert.
- Gibt es keine Übereinstimmung bei PUNAME oder ist der DLUS eine niedrigere Version, versucht der DLUS eine PU mit übereinstimmendem CP-Namen oder NODEID (IDBLK/IDNUM) zu lokalisieren, entweder vordefiniert in einem VTAM-Hauptknoten für Wählleitungen oder dynamisch erstellt mit dem Ausgang ISTEXCCS.

Verbindungen zum Netz mit der ausgewählten Konnektivität (Token-Ring, SDLC, AnyNet usw.) müssen vor dem Herstellen der DLUR-zu-DLUS-Verbindung konfiguriert und aktiviert werden. Wurde eine APPN-Verbindung zwischen dem DLUR und dem DLUS aufgebaut, werden zwischen dem DLUR und dem DLUS zwei Steuersitzungen mit dem Spezialmodus CPSVRMGR zwei Steuersitzungen eingerichtet. Diese beiden Steuersitzungen werden auch als CP-SVR-Pipe bezeichnet und erscheinen als eine Verbindung zum Communications Server. Diese kann daher mit Hilfe von **SNA-Knotenoperationen** aktiviert, inaktiviert und angezeigt werden.

Ist die Pipe aktiviert, können PUs und LUs, die die Pipe als ihre Host-Verbindung definiert haben, SSCP-zu-PU- und SSCP-zu-LU-Unterstützung erhalten. LU-LU-Sitzungen verwenden nicht die Pipe, sondern den besten zur Verfügung stehenden Pfad durch das Netz.

In der DLUR-Umgebung kann in den LU-6.2-Sitzungen eine beliebige Anzahl dedizierter PUs definiert werden. Über die dedizierte PU kann der Gateway dadurch untergeordneten Datenstationen Zugriff für die Netzverwaltung bieten, ohne daß dafür viele physische Verbindungen zu den Hosts erforderlich sind.

Abb. 17 zeigt eine Communications Server-Datenstation, die als DLUR-Gateway für eine Datenstation und eine 4702-Steuereinheit fungiert.

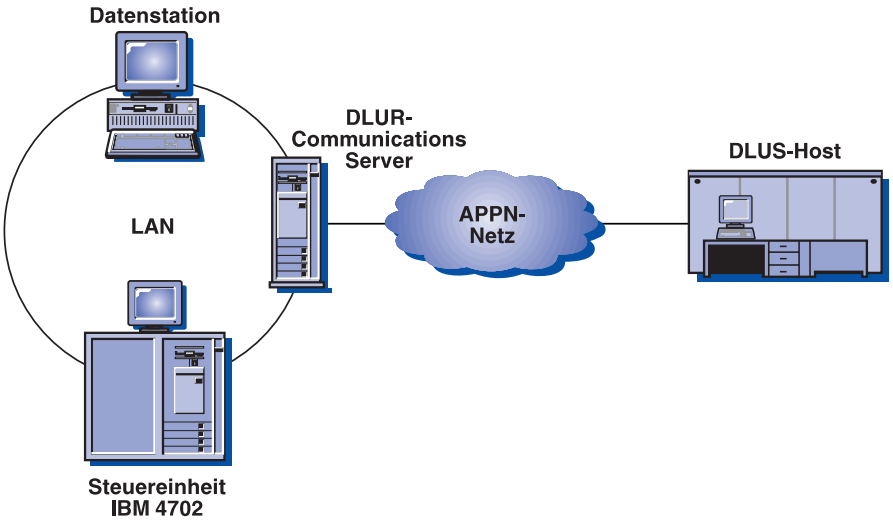


Abbildung 17. DLUR-Verbindung zu einem Host über einen Communications Server-Gateway

LU-LU-Sitzungen

Die LUs des Communications Server können sowohl Sitzungen einleiten als auch auf Anforderungen nach Einleitung einer Sitzung antworten. Wie eine LU Anforderungen einleitet und darauf antwortet, wird dadurch festgelegt, ob es sich um eine unabhängige oder abhängige LU handelt.

Unabhängige LU

Eine unabhängige LU kann ohne Unterstützung des SSCP eine LU-LU-Sitzung aktivieren (das heißt, eine BIND-Anforderung senden) und hat daher keine SSCP-LU-Sitzung. Eine unabhängige LU kann BINDs senden und empfangen. Der Sender des BIND wird als primäre LU (PLU - Primary Logical Unit) bezeichnet, der Empfänger des BIND als sekundäre LU (SLU - Secondary Logical Unit).

Nur eine LU 6.2 kann eine unabhängige LU sein. Communications Server unterstützt sowohl die Protokolle der unabhängigen LU für andere Knoten des Typs 2.1 als auch für LEN-Unterbereichsknoten des Typs 5.

Bei unabhängigen LUs sind Parallelsitzungen zwischen denselben zwei LUs und Mehrfachsitzungen zwischen einer LU und mehreren anderen LUs möglich. Ihre Sitzungslimits hängen vom Modusnamen ab und können von 1 bis 32767 gehen.

Abb. 18 auf Seite 64 zeigt, wie Mehrfach- und Parallelsitzungen von einer unabhängigen LU hergestellt werden können. LUx unterstützt Parallelsitzungen mit LUy und eine Einzelsitzung mit LUz. Die Pfeilrichtung gibt die Beziehung zwischen PLU und SLU bei der Sitzung an. LUx fungiert für die Sitzung mit LUz und für eine der Sitzungen mit LUy als die PLU. Für eine der Parallelsitzungen mit LUy fungiert LUx außerdem als die SLU.

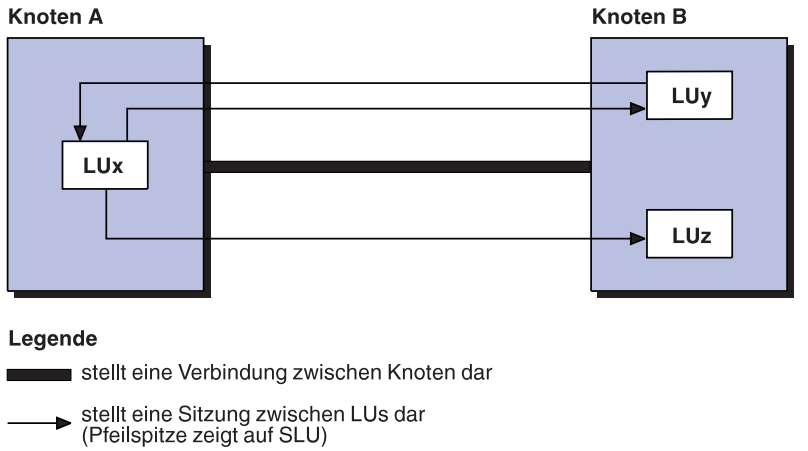


Abbildung 18. Mehrfach- und Parallelsitzungen

Abhängige LU

Eine abhängige LU ist eine LU, die von einem SNA-Host-System gesteuert wird. Um eine LU-LU-Sitzung zu aktivieren, benötigt eine abhängige LU Unterstützung von einem SSCP. Sie benötigt eine SSCP-LU-Sitzung, um ein BIND zu senden. Die Protokolle abhängiger LUs erhalten Unterstützung vom Communications Server, jedoch nur für Unterbereichsknoten des Typs 5, die Protokolle des Typs 2.0 verwenden, nicht jedoch für andere periphere Knoten des Typs 2.1. Abhängige LUs dienen nur als SLUs und verfügen über ein LU-LU-Sitzungslimit von 1. Durch die Unterstützung mehrerer PUs in Communications Server können jedoch mehrere gleichzeitige SSCP-PU-Sitzungen mit abhängigen LU-Sitzungen aufgebaut werden.

Der abhängige LU-Requester (DLUR) ermöglicht Communications Server, die von einem abhängigen LU-Server (DLUS) zur Verfügung gestellte erweiterte SSCP-Unterstützung zu nutzen. Einige der Vorteile dieser Funktion sind:

- Die abhängigen LUs können sich auf Knoten befinden, die keine Nachbarknoten des Hosts sind.
- Die APPN-Suchlogik ermittelt den besten Pfad für LU-LU-Sitzungen.
- Von SNA abhängige LUs können die Vorteile eines APPN-Netzes nutzen.

Zur Verwendung des DLUR einen Parameter **DEFINE_DEPENDENT_LU_SERVER** konfigurieren und den Verbindungsnamen aus dieser Definition für die Definitionen für die LUA, abhängige LU 6.2 oder den Gateway verwenden.

LU 6.2

Unabhängige LUs werden für das Programm VTAM durch die Codierung LOCADDR=0 definiert. Es können beliebig viele LUs mit LOCADDR=0 definiert werden. Zu beachten ist jedoch, daß nicht alle LUs des Typs 6.2 unabhängige LUs sind.

Wenn die LUs eines Teils des APPN-Netzes für das Programm VTAM definiert werden, müssen diese als auf jenem Netzknoten befindlich definiert werden, der diesen Teil des APPN-Netzes mit dem Unterbereichsnetz verbindet. Je nach der Definition der PU auf diesem Netzknoten muß jede LU definiert werden, die von dem anderen Teil des APPN-Netzes erreicht werden soll. Zu beachten ist, daß Steuerpunkte LUs sind.

Eine LU muß in VTAM definiert werden, um eine Sitzung mit einer anderen LU aufzubauen, wenn diese Sitzung über das Unterbereichsnetz ausgeführt werden soll. Es gibt keine effektive Methode, dieses Verfahren zu umgehen (wie z. B. Platzhalterzeichen von APPN); VTAM muß der Name jeder Ziel-LU explizit mitgeteilt werden.

Da ein APPN-Netz häufig Änderungen unterworfen ist, sollten die LUs des APPN-Netzes nach Möglichkeit stets auf einem besonderen Hauptknoten definiert werden. In VTAM können auch LUs definiert werden, die noch gar nicht existieren.

Sonstige LUs

Wenn der Netzknoten seine Verbindung zum Unterbereichsnetz für eine 3270-Emulation verwendet, werden die LUs des Typs 2 der 3270-Emulation in demselben PU-Makro definiert wie die LUs des Typs 6.2 des APPN-Netzes. Die Verbindung wird auch für Verbindungen zwischen der 3270-Emulation und dem Host verwendet.

APPN-Netzknoten und T2.1-Unterstützung

APPN ist eine Erweiterung der IBM SNA- und T2.1-Knotenarchitektur. APPN ermöglicht die Verbindung zweier Systeme sehr unterschiedlicher Größe zu Netzen mit dynamischer Topologie. Ein APPN-Netz ist einfacher zu benutzen, zuverlässiger und bietet mehr Flexibilität als traditionelle SNA-Netze.

Weitere Informationen zu APPN-Netzknoten können dem *3174 APPN Implementation Guide* entnommen werden.

Datenkomprimierung

Als Datenkomprimierung wird der Vorgang bezeichnet, bei dem sich wiederholende Byte oder Zeichenfolgen komprimiert werden, um Datensätze oder Blöcke zu kürzen. Dies reduziert die erforderliche Übertragungszeit. Durch Verringerung der Datenmenge, die zwischen Host- und Datenstationssitzungen übertragen werden, können auf langsamen Leitungen der Durchsatz erhöht und auf teuren Leitungen die Kosten pro Bit gesenkt werden.

Die gemessen an der Anzahl übertragener Byte durch die Datenkomprimierung zu erwartende Leistungssteigerung steht zur normalen Übertragungsart häufig im Verhältnis 2:1. Dies bedeutet, daß bei aktiver Datenkomprimierung etwa jedes zweite Byte in den Puffern, die für Protokollumsetzung der untergeordneten Ebene benötigt werden, eingespart werden kann.

Datenkomprimierung empfiehlt sich in den folgenden Fällen:

- Es sind kürzere Antwortzeiten, besonders auf Leitungen mit niedriger Übertragungsgeschwindigkeit gewünscht.
- Die Kosten auf Leitungen, bei denen sich die Gebühr nach dem Datenvolumen richtet, sollen reduziert werden.
- Es sollen weniger Mietleitungen verwendet werden.

Datenkomprimierung sollte nicht bei jeder aktiven Sitzung angewendet werden, da es ein paar Nachteile gibt, die zu beachten sind:

- Komprimierung und Dekomprimierung erfordern zusätzliche CPU-Zyklen.
- Es wird mehr Speicherplatz (32 Byte bis 9 KB) benötigt.
- Datenkomprimierung erfordert eine sichere Verbindung (definiert in der Tabelle für APPN-Serviceklassen [COS]).
- Optimierung der RU-Größe kann erforderlich sein, um die beste Leistung zu erhalten. Jede RU wird komprimiert und anschließend gesendet. Beim Senden von Paketen können durch eine größere RU-Größe im Modus mehr vollständige Pakete gesendet werden.

  Anmerkung: Wieviel mehr Speicher benötigt wird, hängt vom verwendeten Komprimierungsalgorithmus ab. Der Mehrbedarf bezieht sich auf den Speicher, der zusätzlich zu dem Speicherplatz für die Nachricht benötigt wird.

Ausführlichere und technische Beschreibungen verschiedener Komprimierungsalgorithmen können den folgenden Veröffentlichungen entnommen werden:

- *SNA Formats*
- *Better OPM/L Text Compression IEEE Transactions on Communications, Band COM-34, Nr. 12, SS. 1176-1182,1986*
- *IBM ITSC VTAM V3R4 and V3R4.1 Planning Guide*
- *A Technical Guide to ESA/390 Compression*

Die folgenden Abschnitte beschreiben die SNA-Komprimierung auf Sitzungsebene und die Implementierung im Communications Server.

SNA-Komprimierung auf Sitzungsebene

Bei der SNA-Komprimierung auf Sitzungsebene wird die Datenkomprimierung in der LU-LU-Halbsitzung implementiert. Mit dem Communications Server ist sie für alle unterstützten LU-Typen verfügbar, d. h. LU-Typen 0, 1, 2, 3 und 6.2. Datenkomprimierung auf Sitzungsebene bietet die folgenden Vorteile:

- Es ist effizienter, Daten vor der Verschlüsselung zu komprimieren.
- Für unterschiedliche Datentypen können jeweils unterschiedliche Algorithmen am effizientesten sein.
- Anwendungsprogramme müssen nicht über eine eigene Komprimierungslogik verfügen.

Für SNA-Komprimierung auf Sitzungsebene sind normalerweise zwei Algorithmen definiert, Verschlüsselung für Ausführungshäufigkeit (RLE - Run Length Encoding) und eine Form von Lempel-Ziv (LZ). Der Communications Server unterstützt die SNA-Komprimierung auf Sitzungsebene durch Verwendung der folgenden Algorithmen:

- KEINE Komprimierung.
- RLE-Komprimierung: RLE ist der einfachste und bekannteste Algorithmus, bei dem Zeichenfolgen oder identische Byte durch kürzere codierte Zeichenfolgen ersetzt werden.
- LZ9-Komprimierung - LZ9 ist ein dynamischer Komprimierungsalgorithmus, der zuvor aufgetretene Zeichenfolgen (in der aktuellen oder in vorangegangenen RUs) zu einem 9-Bit-Code komprimiert, der den Nullursprungsindex eines Eintrags in der Komprimierungs-/Dekomprimierungstabelle darstellt. In den Tabelleneinträgen werden zuvor aufgetretene Zeichenfolgen gespeichert.
- LZ10-Komprimierung - LZ10 ist ein dynamischer Komprimierungsalgorithmus, der zuvor aufgetretene Zeichenfolgen (in der aktuellen oder in vorangegangenen RUs) zu einem 10 Bit-Code komprimiert, der den Nullursprungsindex eines Eintrags in der Komprimierungs-/Dekomprimierungstabelle darstellt. In den Tabelleneinträgen werden zuvor aufgetretene Zeichenfolgen gespeichert.

In der Regel werden die Daten mit LZ stärker komprimiert als mit RLE, jedoch auf Kosten eines höheren Bedarfs an Speicherplatz und höherer CPU-Auslastung.

Die SNA-Komprimierung auf Sitzungsebene betrachtet die Sitzung aus zwei Richtungen, PLU-SLU und SLU-PLU. Die primäre logische Einheit (PLU - Primary Logical Unit) ist diejenige LU, die für die Einleitung der Sitzung verantwortlich ist. Die sekundäre logische Einheit (SLU - Secondary Logical Unit) ist die antwortende LU. Die PLU aktiviert eine Sitzung durch Senden einer Anforderung zum Binden einer Sitzung (BIND) an die SLU, die mit einem BIND antwortet. Dies bedeutet, daß verschiedene Komprimierungsalgorithmen in der Richtung PLU-SLU und SLU-PLU verwendet werden können. Ermöglicht wird dies durch die BIND-Vereinbarung der Komprimierungsstufen. Die LU 6.2 kann für eine Sitzung jede Kombination von Komprimierungsstufen verwenden (z. B. kann die PLU RLE verwenden und die SLU-PLU LZ9). Bei allen anderen LU-Typen ist die Komprimierung aktiviert oder inaktiviert. Ist sie aktiviert, dann ist die Komprimierungsstufe für PLU-SLU LZ9 und die für SLU-PLU RLE.

Datenkomprimierung des Communications Server

Der Communications Server unterstützt SNA-Datenkomprimierung auf Sitzungsebene mit den Komprimierungsalgorithmen RLE, LZ9 und LZ10. Mit dem Communications Server kann die Datenkomprimierung für die Kommunikation über CPI-C-Sitzungen (über APPC-Sitzung), APPC-Sitzungen (LU 6.2) und LUA-Sitzungen (LU 0, LU 1, LU 2 und LU 3) gewählt werden.

Zum Aktivieren der Datenkomprimierung wird eine zweiteilige Konfiguration verwendet. Der Communications Server-Knoten muß für Datenkomprimierung aktiviert sein, und zunächst muß die LU (APPC und LUA) aktiviert sein. Die beiden Komprimierungsfelder des Knotens (Stufe und Token) befinden sich im Fenster mit den Merkmalen des lokalen Knotens (Schlüsselwort **NODE** in der .ACG-Datei).

Das Komprimierungsstufenfeld wird auf die höchste Stufe gesetzt, mit der eine Sitzung gestartet werden kann: NONE, RLE, LZ9 oder LZ10. Dieses Feld hat Vorrang vor allen konfigurierten oder angenommenen Komprimierungsstufen (die einzige Ausnahme bildet die eigenständige Datenstation mit verteilter Funktion, die die Knotendefinition nicht benötigt). Wird für die Unterstützung einer 3270-Emulation oder von 3270-Druckern eine Sitzung mit LUA (LU 0, LU 1, LU 2 und LU 3) konfiguriert, wird für die Datenkomprimierung LZ9 benötigt. Die übrigen Komprimierungsstufen lassen für diese LU-Typen keine Datenkomprimierung zu.

Die Standardgröße der Anforderungseinheiten für komprimierte Modi ist doppelt so groß wie die BTU-Größe der Verbindung. Bei Paketvermittlung soll diese Standardgröße vielleicht nicht benutzt werden; statt dessen eine größere Größe und Paketsegmentierung verwenden.

Die LU 6.2-Komprimierung kann durch folgendes aktiviert werden:

- Verwendung der vom Communications Server gelieferten Modi
  - #INTERC
  - #BATCHC
  - #BATCHCS
  - #INTERCS
- Ändern oder Hinzufügen von Modi mit aktivierter Komprimierung

Drei Moduskomprimierungsfelder, gewünschte Komprimierung, Komprimierungsstufe PLU->SLU und Komprimierungsstufe SLU->PLU erscheinen in der Anzeige für die Modusdefinition (Schlüsselwort **MODE** in der .ACG-Datei).

Die gewünschte Komprimierung kann zwei Werte annehmen:

Prohibited (Verhindert) Keine Komprimierung.

Requested (Angefordert) Dieser Wert wird verwendet, um Datenkomprimierung mit den in der Komprimierungsstufen PLU->SLU und SLU->PLU definierten Werten anzufordern. Die angeforderte Stufe ist eventuell nicht verfügbar; dies kann die folgenden Gründe haben:

- Die Knoteneinstellungen enthalten eine Begrenzung für die zulässige Stufe.
- Die SLU hat niedrigere Stufen vereinbart.

Die SLU berücksichtigt die von der PLU angeforderten Komprimierungsstufen, sofern sie nicht durch ihre Knotenkomprimierungseinstellungen eingeschränkt ist.

Weitere Informationen zur Communications Server-Komprimierung enthält der Online-Hilfetext des Programms oder die *Configuration File Reference*.

SNA-Verschlüsselung auf Sitzungsebene

Durch SNA-Verschlüsselung auf Sitzungsebene können entweder alle oder ausgewählte Daten, die zwischen der Datenstation und dem Host übertragen werden, verschlüsselt werden. Sollen beliebige Daten einer Datenstation durch Verschlüsselung geschützt werden, muß auch für den Host Verschlüsselung konfiguriert werden.

Um Datenvertraulichkeit zu ermöglichen, muß auf dem Server ein IBM SecureWay 4758 PCI Cryptographic Coprocessor (als IBM 4758 bezeichnet) installiert sein. Dieser Adapter muß anhand der mitgelieferten Anweisungen initialisiert werden.

Im Communications Server richtet sich die Verschlüsselung auf LU-6.2-Sitzungsebene nach der Modusbeschreibung, die für ein bestimmtes Transaktionsprogramm verwendet wird. Es gibt zwei Verschlüsselungsstufen:

- APPC-Sitzungsebene

  Nur zwischen zwei LUs; kein Steuerpunkt ist an der Umsetzung der Schlüssel beteiligt.

- Umsetzung des APPN-Sitzungsschlüssels

  Zusätzlich zur Ursprungs-LU setzen der Steuerpunkt der Ursprungs-LU (Endknoten oder Netzknoten) und eventuell sein Netzknoten-Server die Schlüssel um.

Um einen Modus zur Verschlüsselung zu konfigurieren, das Fenster "SNA-Einrichtungen" öffnen und **MODI** auswählen. Im Fenster "Modusdefinition" muß **Konfigurationsdefinition...** ausgewählt werden. Das Fenster "Unterstützung von Komprimierung und Verschlüsselung auf Sitzungsebene" erscheint. Die Parameter für die Verschlüsselungskonfiguration teilen sich in zwei Hälften:

- Bei der Verschlüsselung auf Sitzungsebene kann angegeben werden, ob die Verschlüsselung wahlfrei (die LUs verhandeln) oder verbindlich (Verschlüsselung muß verwendet werden) ist.

  Anmerkung: Die Verschlüsselung von Communications Server zu einem Host ist immer als verbindlich konfiguriert.

- Bei der Umsetzung des APPN-Sitzungsschlüssels kann angegeben werden, daß nur die LU den Schlüssel umsetzt, daß nur der Endknoten den Sitzungsschlüssel umsetzt oder daß der Endknoten und sein Netzknoten den Schlüssel umsetzen.

Zum Speichern und Umsetzen von Schlüsseln benötigt der Communications Server weitere Programme. Für die Schlüsselspeicherung ist ein CGA-Produkt (CGA - Common Cryptographic Architecture) erforderlich, das von den im IBM Adapter 4758 enthaltenen Dienstprogrammen verwaltet wird. Der Communications Server ruft ein CGA-Produkt auf, das mit dem IBM Adapter 4758 zusammenarbeitet, um die Schlüssel zu erhalten und die Daten zu verschlüsseln.

VTAM-Benutzer:

Der Communications Server verschlüsselt nicht die SNASVCMG-Sitzung. In der APPL-Anweisung der Definition der VTAM-Anwendung muß der Parameter ENCR=OPT angegeben werden. Bei der Verwendung von VTAM muß die Verschlüsselung in der Anweisung MODEENT angegeben werden. Beispiel:

```
ENCR=B'0011' FÜR VERBINDLICHE VERSCHLÜSSELUNG
```

Um die VTAM-Verschlüsselungsfunktionen zu benutzen, muß IBM PCF (PCF - Programmed Cryptographic Facility) vor dem Starten von VTAM initialisiert werden.

Ab VTAM Version 3, Release 4.1 verwendet VTAM für Verschlüsselungsservices, wie z. B. Verschlüsselung auf Sitzungsebene, eine neue Schnittstelle für die Funktion ICSF/MVS (Integrated Cryptographic Service Facility/MVS). Diese Schnittstelle stimmt mit CCA (Common Cryptographic Architecture), wie von ICSF/MVS implementiert, überein. Mit dieser Unterstützung kann der Verschlüsselungsservice nach dem Start von VTAM gestartet und gestoppt werden, wobei der Hauptschlüssel geändert werden kann, ohne daß VTAM oder aktive LU-LU-Sitzungen unterbrochen werden müssen.

Weitere Informationen zur Definition der Datenverschlüsselung können der Dokumentation *OS/390 eNetwork Communications Server: SNA Network Implementation* entnommen werden.

Verwaltungsservices

Die Verwaltungsservices (MS - Management Services) des Communications Server sind auf Netzkomponenten aufgeteilte Funktionen zum Bedienen, Verwalten und Steuern eines Netzes. Diese Funktionen basieren auf der SNA-Verwaltungsservicearchitektur, die in der *Systems Network Architecture Management Services Reference* beschrieben wird.

ZAVS, Servicepunkte und Eingangspunkte

Der Communications Server bietet eine Programmierunterstützung, die eine Installation von ZAVS-, Servicepunkt- und Eingangspunktanwendungen der Verwaltungsservices ermöglicht. MS-Servicepunktanwendungen sind nur eine Variante der MS-Eingangspunktanwendungen und unterscheiden sich von diesen nur in der Art der Funktionen, die sie zur Verfügung stellen; ansonsten kommunizieren sie mit einem MS-ZAVS genauso wie MS-Eingangspunktanwendungen.

Zentrales Alert-Verarbeitungssystem (ZAVS) Ein MS-ZAVS ist ein zentraler Steuerpunkt zur Verwaltung eines Netzes. Von einer MS-Servicepunktanwendung oder einer MS-Eingangspunktanwendung kann das MS-ZAVS bestimmte Daten anfordern, die den Betrieb des Netzes betreffen, wie z. B. Fehler- und Leistungsdaten oder die Programmkennung.

Das MS-ZAVS kann außerdem bestimmte nicht angeforderte MS-Daten von den Knoten empfangen, die es auf der Basis der Kategorie der MS-Daten verwaltet. Eine MS-Kategorie sind beispielsweise MS-Alerts. Ein MS-ZAVS kann eine oder mehre Kategorien von MS-Daten verwalten; dabei können ein oder mehrere MS-ZAVS in einem Netz vorhanden sein. Der IBM Communications Server, das Programm IBM NetView und das Betriebssystem IBM OS/400 sind Beispiele für Programme, die MS-ZAVS-Funktionen zur Verfügung stellen.

Servicepunkt Ein MS-Servicepunkt ist die Funktion in einem Knoten, die Daten von Einheiten anfordern und erfassen kann, die selbst nicht als MS-Eingangspunkte fungieren können, wie z. B. Einheiten, die über LAN-Protokolle (jedoch nicht SNA-Protokolle der höheren Ebene) mit dem Knoten des MS-Servicepunkts verbunden sind. Abgesehen vom Erfassen nicht lokaler Daten funktioniert ein MS-Servicepunkt in bezug auf das MS-ZAVS wie ein MS-Eingangspunkt. Die Programme IBM NetView/PC und IBM LAN Netzwerk-Manager sind Beispiele für MS-Eingangspunktanwendungen, die MS-Servicepunktfunktionen und MS-Eingangspunktfunktionen zur Verfügung stellen.

Eingangspunkt Ein MS-Eingangspunkt ist die Funktion in einem Knoten, die lokale MS-Daten erfaßt und sie auf Anforderung oder unaufgefordert an ein MS-ZAVS zur Verarbeitung sendet. Der Communications Server stellt die MS-Eingangspunktfunktion zum Senden von Alerts an das Alert-MS-ZAVS zur Verfügung. Diese Alerts können vom Communications Server oder den DLCs kommen, die dieser verwendet. Der Communications Server bietet außerdem Programmierunterstützung für Anwendungen, wie z. B. die Programme IBM NetView/PC und IBM LAN Netzwerk-Manager, indem er die an das MS-ZAVS zu sendenden Alerts liefert.

Ebenen der SNA-MS-Architektur

Ein SNA-Programm implementiert eine bestimmte Ebene (oder Generation) der SNA-MS-Architektur; einige Programme unterstützen mehrere Ebenen der Architektur. Der Communications Server kann MS-Daten an SNA-Programme, die eine der drei Ebenen der MS-Architektur implementieren, senden und MS-Datendaten von diesen empfangen. Diese Ebenen lauten:

Ebene der Mehrdomänenunterstützung (MDS - Multiple Domain Support)
Ein SNA-Programm, das die MDS-Ebene der MS-Architektur implementiert, wie z. B. Communications Server und IBM NetView Version 2 Release 2 (oder später). Es kann MDS-Nachrichteneinheiten (MDS/MUs - Multiple Domain Support Message Units) senden und empfangen. Das Programm IBM NetView Version 2 Release 2 stellt die MDS-Ebene nicht als Steuerpunkt, sondern als Unterbereichs-LU zur Verfügung und benutzt zum Transport von MDS-MUs SNASVCMG-Modussitzungen. Als ZAVS unterstützt es explizite, implizite (primäre) und implizite (Ausweich-) ZAVS-Eingangspunktbeziehungen. Das Programm IBM NetView Version 2 Release 2 unterstützt auch weiterhin die Beziehung zwischen Host-ZAVS und Eingangspunkt für Eingangspunktprogramme, die die MDS-Ebene nicht unterstützen.

Migrationsebene
Ein SNA-Programm, das die vorherige Ebene der Verwaltungsservicearchitektur implementiert, wie z. B. IBM OS/400 Version 1 Release 3 Modifikationsstufe 0 (oder früher). Ein Programm der Migrationsebene kann explizite, Standard- und Domänen-ZAVS-Eingangspunktbeziehungen unterstützen. Die Domänen-ZAVS-Eingangspunktbeziehung wird hergeleitet, wenn CP-CP-Sitzungen mit einem Knoten der Migrationsebene aktiviert werden. Ein Netzknoten der Migrationsebene, der Services zur Verfügung stellt, sendet keine MS-Funktionen für ZAVS-Benachrichtigung an die Endknoten, die seine Services in Anspruch nehmen, und ein Endknoten, der auf Migrationsebene Services in Anspruch nimmt, akzeptiert keine MS-Funktionen für ZAVS-Benachrichtigung von dem Netzknoten, der ihm seine Services zur Verfügung stellt. Er kann CP-MSUs senden und empfangen, aber keine MDS-MUs. Als ZAVS unterstützt er nur die MS-Kategorie für Alerts.

Ebene des Vektortransports für Netzverwaltung (NMVT)
Ein SNA-Produkt, das die NMVT-Ebene der SNA-MS-Architektur implementiert, wie z. B. IBM NetView Version 2 Release 1 (oder später). NMVT ist eine Verwaltungsserviceanforderungseinheit (RU - Request Unit), die über eine aktive Sitzung zwischen PU-Verwaltungsservices und Steuerpunkt-Verwaltungsservices übertragen wird. Wird NMVT von einer Datenstation über einen Gateway weitergeleitet, dann fügt der Gateway NMVT seinen Steuerpunktnamen hinzu.

Flußsteuerung

Zur Verwaltung des Datenflusses im Netz verwendet der Communications Server angepaßte Nachrichtendosierung auf Sitzungsebene. Die Nachrichtendosierung wird bei jedem Nachbarknotenpaar vorgenommen, das am Sitzungsleitweg teilnimmt. Die Nachrichtendosierung zwischen zwei Nachbarknoten ist unabhängig von der Nachrichtendosierung, die zwischen anderen Nachbarknoten desselben Leitwegs vorgenommen wird.

Nachrichtendosierung auf Sitzungsebene

Angepaßte Nachrichtendosierung auf Sitzungsebene verwendet ein auf Fenstern basierendes Schema, in dem ein Sender nur eine begrenzte Anzahl, oder ein ***Fenster***, von Anforderungseinheiten nach expliziter Sendeerlaubnis senden kann. Die Fenstergröße kann, je nach den Rahmenbedingungen beim Empfänger, geändert werden. Durch diese Funktion kann ein Knoten die Datenmenge steuern, die während des normalen Sitzungsbetriebs gesendet und empfangen wird. Die Fenstersteuerung ermöglicht dem empfangenden Knoten, die Geschwindigkeit zu steuern, mit der die ankommenden Daten in den Sitzungspuffern empfangen werden. Angepaßte Nachrichtendosierung auf Sitzungsebene bietet einem Knoten, der viele Sitzungen unterstützt, ein dynamisches Mittel, um Ressourcen zu einer Sitzung zuzuordnen, auf der viele Aktivitäten stattfinden, und um nicht verwendete Ressourcen von Sitzungen zurückzufordern, auf denen keine Aktivitäten stattfinden. Durch angepaßte Nachrichtendosierung auf Sitzungsebene kann der empfangende Knoten seine verfügbaren Pufferressourcen effizient nutzen.

Da die Nachrichten in jedem Sitzungsabschnitt zwischen den Endpunkten unabhängig dosiert werden, können sowohl Endpunktknoten als auch Zwischenknoten die Nachrichtendosierung für die Sitzungen, die sie ausführen, je nach ihrer eigenen lokalen Belastung anpassen. Diese Aktion ist die Basis für globale Flußsteuerung und die Verwaltung bei Überlastung in APPN-Netzen.

Wenn jedoch eine interaktive Sitzung und eine Sitzung, die eine große Datei überträgt, eine Verbindung gemeinsam benutzen, sollten die Daten der interaktiven Sitzung so schnell wie möglich übertragen werden. Hierfür gibt es zwei Methoden:

1. Der Dateiübertragungssitzung wird eine niedrigere Priorität zugewiesen. #BATCH verwendet niedrige Priorität.
2. Feste Nachrichtendosierung mit einer kleinen Fenstergröße für die Dateiübertragungssitzung verwenden, so daß interaktive Sitzungsdaten die Verbindung verwenden können, wenn die Dateiübertragungssitzung auf eine Antwort auf Nachrichtendosierung wartet. Besteht eine direkte Verbindung zu einem NCP-Host, kann ein Fenster für feste Nachrichtendosierung für abgehende und ankommende Daten verwendet werden, um Nachrichtendosierung in beide Richtungen auf das Empfangsfenster im definierten Modus zu setzen.

Angepaßte BIND-Nachrichtendosierung

BIND-Übertragungen können bei hohen Datenaufkommen vorkommen, insbesondere beim Start von Knoten oder des Netzes. Angepaßte BIND-Nachrichtendosierung wird benutzt, um den Fluß von BINDs zwischen zwei Nachbarknoten zu steuern. Hierfür wird derselbe Fensteralgorithmus benutzt, der auch für Nachrichtendosierung auf Sitzungsebene verwendet wird.

Segmentierung und erneutes Zusammenfügen

Zur Übertragung von RUs, die länger sind als die von einer bestimmten Verbindung zugelassenen größten Basisübertragungseinheit, unterstützt der Communications Server die Segmentierung und das erneute Zusammenfügen von Daten. Diese Segmente werden auf dem Partnerknoten wieder zu ganzen RUs zusammengefügt. Durch diesen Vorgang kann die für eine Sitzung definierte RU-Größe von der Verbindung unabhängig sein, die für die Weiterleitung verwendet wird.

HPR-Nachrichtendosierung

High Performance Routing (HPR) verfügt über ARB (Adaptive Rate-Based Congestion Control) als neue Methode zur Flußsteuerung. ARB reguliert den Datenfluß durch Vorhersage von Überlastungen im Netz und Reduzierung der Übertragungsgeschwindigkeit des Knotens im Netz, so daß Überlastungen verhindert werden und nicht erst im Nachhinein darauf reagiert wird.

Feste Nachrichtendosierung

Feste Nachrichtendosierung ermöglicht es zwei Sitzungen, eine physische Verbindung gemeinsam zu benutzen. Ohne feste Nachrichtendosierung werden die zu übertragenden Daten in eine gemeinsame DLC-Warteschlange gestellt, wobei interaktive Daten auf die bis bereits in der Warteschlange befindlichen Daten folgen. Feste Nachrichtendosierung reduziert außerdem den Speicherplatz, der zum Einreihen der Daten in die DLC-Warteschlange verwendet werden kann. Mit dem NCP kann feste Nachrichtendosierung für abgehende und ankommende Daten verwendet werden, um eine Definition der festen Nachrichtendosierung für den Host zu vermeiden. Im allgemeinen stellt die angepaßte Nachrichtendosierung die effizienteste Methode der Datenübertragung zwischen Knoten dar.

Übertragungspriorität ermöglicht genauso wie die feste Nachrichtendosierung die gemeinsame Benutzung einer physischen Verbindung zwischen Sitzungen. Sie blockiert zwar Speicherplatz, da Daten in die DLC-Warteschlangen gestellt werden, sie benötigt aber nicht die zusätzlichen Nachrichtendosierungsantworten, die bei der festen Nachrichtendosierung erforderlich sind.

LUs zu Hosts zuordnen

Werden mehrere Unterbereichs-Host-Verbindungen definiert, darf der Datenverkehr von der Domäne eines bestimmten Hosts nur eine logische Verbindung verwenden. Zu beachten ist, daß manuell angewählte Verbindungen eine einzige Verbindung darstellen. Zur Unterstützung jedes weiteren Hosts muß jeweils eine weitere PU definiert werden. Nur über die auf dem Steuerpunkt definierten Host-Verbindungen können CP-CP-Sitzungen ausgeführt werden, und nur diese können am APPN-Netz teilnehmen. Verbindungen mit der Einstellung **USE_PU_NAME_IN_XID=1** dürfen keine CP-CP-Sitzungen ausführen. Andernfalls können über die Host-Verbindungen CP-CP-Sitzungen ausgeführt werden, und diese können auch an der APPN-Kommunikation teilnehmen. Das Schlüsselwort **LINK_STATION** gibt den Namen der PU und die für die PU zu verwendende logische Verbindung an. Werden Parallelverbindungen benötigt (in Situationen, in denen mehr als 254 abhängige LUs vorhanden sind), muß für eine der Verbindungen die CP-CP-Sitzungsunterstützung auf NO gesetzt sein.

Jede abhängige LU kann als nur einer PU zugeordnet definiert werden. Das Schlüsselwort **LOCAL_LU** gibt den Namen der Host-Verbindung an, der für eine abhängige LU des Typs 6.2 verwendet wird. Das Schlüsselwort **LU_0_TO_3** gibt den Namen der Host-Verbindung für LUA an, das 3270-Profil gibt die Host-Verbindung für jede 3270-Emulationssitzung an.

Der Steuerpunkt definiert eine PU automatisch mit dem Steuerpunktnamen. Abhängige LUs, die auf einem Unterbereichs-SSCP definiert sind, können der Steuerpunkt-PU zugeordnet werden. (Tatsächlich kann die automatisch definierte LU für den Steuerpunkt auch als abhängige LU definiert werden.) Jede zusätzliche PU 2.0 für einen anderen Unterbereichs-Host erfordert eine separate Verbindung und PU-Definition. Eine PU wird definiert, indem in einem Schlüsselwort **LINK_STATION** PU angegeben wird. Dies ist nicht notwendig, wenn alle LUs unabhängig sind.

Wenn die SSCP-PU-Sitzung Alerts an den Host senden soll, muß die ZAVS-Verbindung mit dem Schlüsselwort **NODE** in der .ACG-Datei definiert werden. Wenn ein Host die Alerts empfangen soll, muß eine logische Verbindung für den Steuerpunkt zum Host angegeben werden. Ist die Verbindung zu diesem Host nicht verfügbar, zeichnet der Communications Server die Alerts auf. Die einzigen Netzverwaltungsanforderungen, die von einem PU 2.0-Host akzeptiert werden, sind diejenigen für die Steuerpunkt-PU. Mit der Steuerpunkt-PU werden Antworten an denselben Host zurückgesendet.

Jede abhängige LU muß eine konfigurierte lokale Adresse haben, die mit der auf dem Host konfigurierten identisch ist. Die Verwendung des SNA-Gateways ermöglicht jedoch eine Gateway-Adreßumsetzung. Eine abhängige LU 6.2 kann als eine unabhängige LU für einen Peer-Knoten fungieren; dies bedeutet, daß sie nur für den Unterbereich abhängig ist. Solch eine LU sollte Teil eines APPN-Netzes sein, bei dem andere Verbindungen zu demselben Unterbereich bestehen, also zu dem Unterbereich, der den steuernden SSCP enthält. Nur eine Unterbereichsverbindung ist für das APPN-Netz zugelassen, außer wenn die Unterbereiche unabhängig sind. Ein Gateway kann zwar Parallelverbindungen zu demselben Unterbereich haben, aber nur über eine Verbindung können CP-CP-Sitzungen und der APPN-Datenaustausch ausgeführt werden.

Ein SSCP im Unterbereichsnetz aktiviert die abhängigen LUs, die er steuert, nachdem die Verbindung zu ihm hergestellt ist. Solange die LU nicht aktiviert wurde, kann sie keine Sitzung einleiten. Wird APPC inaktiviert, dann werden alle Hosts, die sich in einer aktiven Sitzung mit einer PU auf dem Knoten befinden, aufgefordert, die Verbindung zu trennen. Die Hosts geben die Verbindung frei, nachdem zunächst die LUs inaktiviert wurden und anschließend die PU in der SSCP-PU-Sitzung.

SNA-Gateway-Unterstützung

Communications Server stellt einen SNA-Gateway mit vollem Funktionsumfang zur Verfügung. Dieser Gateway ermöglicht mehreren, mit dem LAN verbundenen Datenstationen über eine oder mehrere physische Verbindungen zu einem oder mehreren Hosts auf Hosts des IBM Systems /370 oder /390 zuzugreifen. Dies ermöglicht eine Senkung der pro Datenstation anfallenden Kosten für Host-Verbindungen.

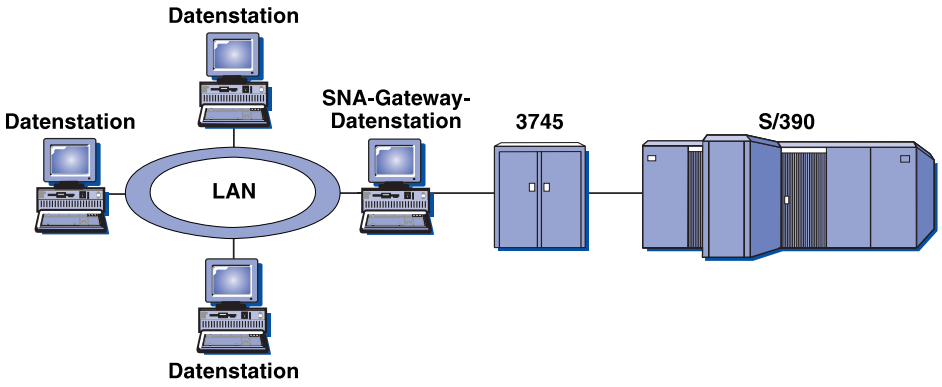


Abbildung 19. Beispiel für SNA-Gateway-Konfiguration

Der Communications Server-Gateway unterstützt die SNA-Protokolle LU 0, 1, 2, 3 und abhängige LU 6.2 (APPC). Mit der AnyNet-SNA über TCP/IP-Funktion können untergeordnete Datenstationen nun über ein IP-Netz mit dem SNA-Gateway kommunizieren. Der Gateway unterstützt außerdem LU 0, 1, 2 oder 3 zu einem Host des Systems IBM AS/400 im SNA-Durchgriff. Der AS/400-Host übergibt die Datei an einen IBM System /390-Host.

Ein Gateway kann auch als Protokollumsetzer zwischen Datenstationen dienen, die mit einem LAN und einer WAN-Host-Leitung verbunden sind.

Die in dem Gateway definierten LUs können einer bestimmten Datenstation fest zugeordnet werden oder zum Pool für mehrere Datenstationen zusammengeschlossen werden. Durch das Zusammenschließen zu Pools können Datenstationen allgemeine LUs gemeinsam benutzen; dies erhöht die Effizienz der LUs und reduziert die Konfigurations- und Startvoraussetzungen auf dem Host. Außerdem können mehrere LU-Pools definiert werden, die jeweils einer bestimmten Anwendung zugeordnet sind. Andererseits sind auch allgemeine Pools möglich, die mehreren Hosts zugeordnet sind. Wenn ein Client die Verbindung zu dem Gateway herstellt, ruft der Gateway eine LU aus dem Pool ab, um eine Sitzung aufzubauen. Die LU wird im Pool wieder für den Zugriff durch andere Datenstationen freigegeben, sobald die Sitzung beendet ist.

Außerdem kann ein SNA-Gateway die Weiterleitung von NMVTs (Network Management Vector Transports) zwischen den Datenstationen und dem Host unterstützen.

Jeder Host betrachtet den SNA-Gateway als einen SNA-PU-2.0-Knoten, der pro Datenstation eine oder mehrere LUs unterstützt. In bezug auf den Host gehören alle LUs zu der SNA-Gateway-PU. Der SNA-Gateway kann mehrere Host-Verbindungen gleichzeitig haben und verschiedene Datenstationssitzungen bestimmten Hosts zuordnen.

Für die unterstützten Datenstationen sieht der SNA-Gateway wie eine SNA-PU-4-DFV-Steuereinheit aus; er leitet Host-Anforderungen wie z. B. BIND und UNBIND weiter. Die Datenstations-LUs erkennen den SNA-Gateway nicht. Der SNA-Gateway erkennt jedoch alle LUs auf den Datenstationen.

Untergeordnete Anwendungen, die Standard-SNA-Konnektivitätsprotokolle für LU 0, 1, 2 und 3 sowie abhängige LU 6.2 verwenden und über einen SNA-Gateway mit einem Host kommunizieren, werden von Communications Server unterstützt. In Tabelle 4 sind die SNA-Gateway-Funktionen zusammengefaßt.

Tabelle 4. SNA-Gateway - Zusammenfassung

Funktion	**Beschreibung**
Aktive Datenstationen	254 (LAN) pro Adapter 128 (X.25)
DLCs	AnyNet (SNA über TCP/IP) Twinaxial (nur übergeordnet) LAN (alle mit NDIS übereinstimmenden Netzadapter) X.25 SDLC (synchron, asynchron und AutoSync) OEM-Kanal (nur übergeordnet) MPC-Kanal (nur übergeordnet, DLUR erforderlich) Enterprise Extender
Untergeordnete Datenstationen	Jedes Produkt, das die Standard-SNA-Konnektivitätsprotokolle für LU 0, 1, 2, 3 und LU 6.2 unterstützt.
Dynamische Hinzufügungen und Änderungen	Ja
Unterstützung impliziter Datenstationen	Ja
LUs im Pool	Ja
Maximale Anzahl LUs	254 pro PU; keine Begrenzung der Anzahl PUs
Betriebsart	Mehrere untergeordnete PUs (nicht erkennbar für den Host) PUs nicht sichtbar für den Host (außer über DLUR)
Unterstützung mehrerer PUs	Ja
Segmentierungsunterstützung	Ja
Unterstützte LU-Typen	LU 0, 1, 2, 3 und abhängige LU 6.2

Planung und Installation

Planung für AnyNet-Unterstützung

Communications Server ermöglicht folgende zwei Arten von AnyNet-Unterstützung:

- AnyNet-SNA-über-TCP/IP-Zugriffsknoten und -Gateway
- AnyNet-Sockets-über-SNA-Zugriffsknoten und -Gateway

Die AnyNet-SNA-über-TCP/IP-Funktion von Communications Server ermöglicht SNA-Anwendungen die Kommunikation über verbundene IP- und SNA-Netze.

Die SNA-über-TCP/IP-Zugriffsknotenfunktion ermöglicht die Kommunikation zwischen SNA-Anwendungen in einem IP-Netz. Diese Funktion unterstützt unabhängige LU 6.2 sowie abhängige LU 0, 1, 2, 3 oder 6.2 entweder mit oder ohne abhängigen LU-Requester (DLUR). Außerdem kann der SNA-über-TCP/IP-Zugriffsknoten in Kombination mit einem SNA-Gateway verwendet werden, um SNA-Gateway-Sitzungen über TCP/IP auszuführen.

Die SNA-über-TCP/IP-Gateway-Funktion erweitert den Einsatzbereich von SNA-Anwendungen, weil sie SNA-Anwendungen in einem SNA-Netz den Datenaustausch mit SNA-Anwendungen in einem IP-Netz ermöglicht. Der SNA-über-TCP/IP-Gateway unterstützt unabhängige LU 6.2-Sitzungen.

Weitere Informationen zum Konfigurieren von AnyNet SNA über TCP/IP enthält der Abschnitt „AnyNet SNA über TCP/IP konfigurieren“.

Die Sockets-über-SNA-Zugriffsknotenfunktion ermöglicht TCP/IP-Anwendungsprogrammen, die die Socket-Schnittstelle WinSock 1.1 und WinSock 2.0 verwenden, die Kommunikation über ein SNA-Netz.

Die Sockets-über-SNA-Gateway-Funktion ermöglicht die Kommunikation zwischen Socket-Anwendungen in SNA- und TCP/IP-Netzen. Sockets-über-SNA-Gateways werden häufig dazu verwendet, unabhängige TCP/IP-Netze über ein zentrales SNA-Netz zu verbinden.

Weitere Informationen zum Konfigurieren von Sockets über SNA enthält der Abschnitt „AnyNet Sockets über SNA konfigurieren“ auf Seite 96.

AnyNet SNA über TCP/IP konfigurieren

Dieser Abschnitt enthält ausführliche Informationen zum Konfigurieren von AnyNet SNA über TCP/IP.

SNA-Ressourcen zu IP-Adressen zuordnen

Einer der entscheidenden Schritte zum Ermöglichen der SNA-über-TCP/IP-Kommunikation wird nicht in den Anzeigen von Communications Server ausgeführt. Bevor SNA-Sitzungen oder -Verbindungen eingerichtet werden können, muß SNA über TCP/IP die IP-Adresse des Partners feststellen. Dazu wird die SNA-Kennung des Partners mit Hilfe der folgenden Arbeitsschritte einer IP-Adresse zugeordnet.

1. SNA über TCP/IP empfängt die SNA-Kennung von Communications Server in einem der folgenden Formate:
   - Für LU-Namen - `netz-id.lu-name`
   - Für CP-Namen - `netz-id.cp-name`
   - Für IDBLK- und IDNUM-Werte, konfiguriert als `Nachbarknoten-ID`, mit den beiden Feldern `Block-ID` und `ID der physischen Einheit`
2. SNA über TCP/IP generiert mit Hilfe der Kennung wie folgt einen Domänennamen:
   - Für LU-Namen - `lu-name.netz-id.sna-suffix`
   - Für CP-Namen - `cp-name.netz-id.sna-suffix`
   - Für IDBLK- und IDNUM-Werte - `bbbnnnnn.sna-suffix`

   Anmerkung: Der Standardwert für `sna-suffix` ist **SNA.IBM.COM**. Zusätzliche Informationen zum Suffix des SNA-Domänennamens enthält die Online-Hilfefunktion.

Abb. 20 zeigt Beispiele für Domänennamen, die von SNA über TCP/IP generiert wurden.

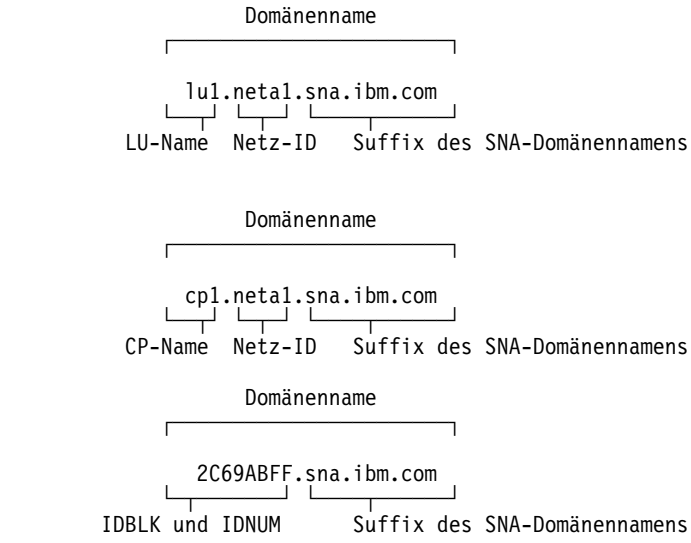


Abbildung 20. Formate der von SNA über TCP/IP erstellten Domänennamen

3. SNA über TCP/IP fordert, daß der Domänenname in eine IP-Adresse umgesetzt wird.
4. TCP/IP verwendet die Datei HOSTS oder den Domänennamens-Server, um den Domänennamen in eine IP-Adresse umzusetzen (zum Beispiel `9.67.192.28`).

Wenn das IP-Netz SNA-über-TCP/IP-Gateways enthält, sind bei der Adreßzuordnung außerdem folgende Punkte zu beachten:

- Wenn die Partner-LU über einen Gateway erreicht werden kann, muß der Domänenname des Partners der IP-Adresse des Gateways zugeordnet werden. Wenn parallele Gateways vorhanden sind, sollte der Domänenname jeder Gateway-IP-Adresse zugeordnet werden.

- Zur Minimierung der für AnyNet benötigten Adreßzuordnungsinformationen empfiehlt sich die Verwendung einer Namenskonvention, bei der der lokale LU-Name mit dem TCP/IP-Host-Namen übereinstimmt. Beispiel: Angenommen, der Host-Name des lokalen Computers lautet PATR.ANYNET.OURCORP.COM. Bei Verwendung des LU-Namens PATR und der Netz-ID ANYNET und Festlegung des SNA-Domänennamensuffixes auf OURCORP.COM, wird TCP/IP von AnyNet dazu aufgefordert, den Namen PATR.ANYNET.OURCORP.COM aufzulösen. Dieser Name sollte im Domänennamens-Server bereits vorhanden sein.

Domänennamen und IP-Adressen definieren

In diesem Abschnitt wird die TCP/IP-Funktion für Namensauflösung beschrieben, die von AnyNet zum Zuordnen von SNA-Ressourcen zu IP-Adressen verwendet wird. Diese Funktion fragt sowohl die Datei HOSTS als auch die Domänennamens-Server ab, um einen Domänennamen (z. B. `lu1.neta1.sna.ibm.com`) in eine IP-Adresse (z. B. 10.1.1.1) umzuwandeln.

Datei HOSTS Mit den HOSTS-Dateien von TCP/IP können dem Netz IP-Adressen zugeordnet werden. Durch das Anwachsen des Netzes kann das Verwalten der Datei HOSTS auf jeder Endbenutzerdatenstation jedoch zu zeitaufwendig werden; in diesem Fall empfiehlt es sich, einen Domänennamens-Server zu verwenden.

In der Datei HOSTS (im Unterverzeichnis drivers\etc des Windows NT-Systemverzeichnisses) ist folgendes aufgelistet:

- IP-Adresse
- Domänenname
- Weitere Aliasnamen für den Domänennamen

Beispiel: Wenn die IP-Adresse 10.1.1.1, die Netz-ID NETA1, der SNA-Ressourcenname LUA1 und das Standardsuffix für den SNA-Domänennamen (`sna.ibm.com`) verwendet werden, ist folgendes in die Datei HOSTS einzutragen:

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

Domänennamens-Server Domänennamen und IP-Adressen können auch in der Domänennamens-Server-Datenbank definiert werden.

Jeder SNA-Kennung wird von einem Domänennamens-Server eine entsprechende IP-Adresse zugeordnet. Die Position dieser Server wird unter "Netzwerk" in der Systemsteuerung konfiguriert.

Weitere Informationen zu HOSTS-Dateien und Domänennamens-Servern enthält die TCP/IP-Dokumentation. Wenn die lokale Datenstation die TCP/IP-Unterstützung von Windows NT verwendet, enthält die im Lieferumfang des Windows NT-Produkts enthaltene TCP/IP-Dokumentation nähere Informationen.

Überlegungen zum SNA-über-TCP/IP-Gateway

Die folgenden Informationen beziehen sich auf Gateways und nicht auf Zugriffsknotenfunktionen.

Eindeutige CP-Namen und Verbindungsnetznamen definieren

Für Konfigurationen mit zwei oder mehr SNA-über-TCP/IP-Gateways, die ein SNA-Netz mit zwei oder mehr IP-Netzen verbinden, muß für jedes IP-Netz ein eindeutiger SNA-Steuerpunktname (CP-Name) und ein eindeutiger SNA-Verbindungsnetzname definiert werden.

Dadurch entsteht der Eindruck, als würden sich alle LUs, die sich auf Zugriffsknoten im IP-Netz befinden, auf einem Knoten mit diesem CP-Namen befinden.

Mit der Adreßumkehrdatei des Domänennamens-Servers oder der Datei HOSTS den CP-Namen und den Verbindungsnetznamen für ein bestimmtes IP-Netz definieren. Die IP-Adresse 127.0.0.3 dem CP-Namen zuordnen und die IP-Adresse 127.0.0.4 dem Verbindungsnetznamen zuordnen.

Das folgende Beispiel zeigt Einträge in der Umkehrdatendatei. Für ein IP-Netz mit der SNA-Netz-ID NETA, dem CP-Namen MYCPNAME und dem Verbindungsnetznamen MYCNET wären folgende Einträge zu definieren:

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

Anmerkungen:

1. Ein Punkt muß am Ende des Namens nur angegeben werden, wenn sich die Definition in der DNS-Adreßumkehrdatei befindet. Für Definitionen in der Datei HOSTS ist kein Punkt erforderlich.
2. Das Suffix des SNA-Domänennamens darf nicht angegeben werden.

Die AnyNet-SNA-über-TCP/IP-Funktion von Communications Server stellt einen Standard-CP-Namen ($ANYNET.$GWCP) und einen standardmäßigen Verbindungsnetznamen ($ANYNET.$GWCNET) zur Verfügung. In Konfigurationen mit einem IP-Netz wird die Standardvorgabe verwendet, wenn kein CP-Name und kein Verbindungsnetzname definiert wird. In Konfigurationen mit mehreren Gateways, die mehrere IP-Netze verbinden, kann ein IP-Netz die Standardvorgabe verwenden. Für alle anderen IP-Netze müssen jedoch eindeutige CP-Namen und Verbindungsnetznamen definiert werden.

Abb. 21 auf Seite 85 zeigt das Definieren von CP-Name und Verbindungsnetzname für eine Konfiguration mit zwei IP-Netzen.

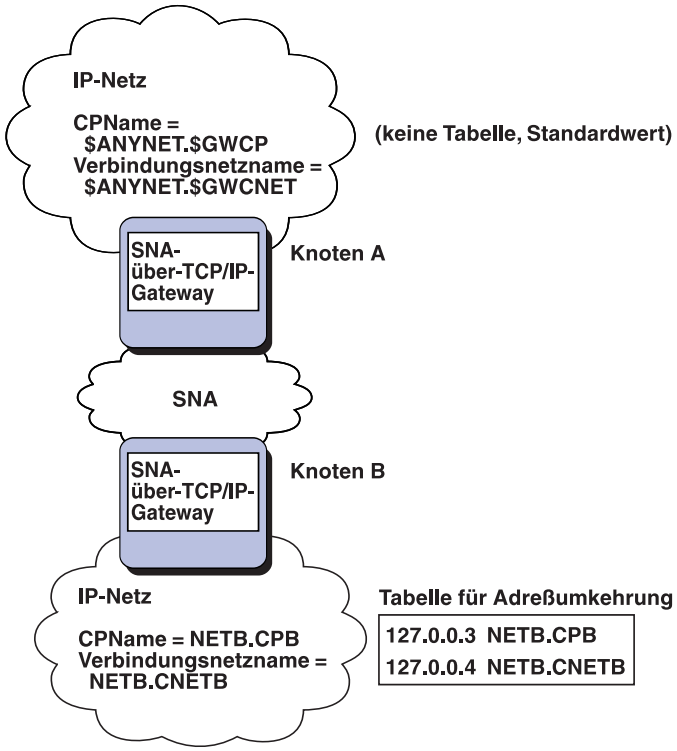


Abbildung 21. Einen CP-Namen und einen Verbindungsnetznamen definieren

Mit dem Platzhaltereintrag die Domänennamens-Server-Definitionen reduzieren

Wenn der SNA-über-TCP/IP-Gateway verwendet wird und die Konfiguration die folgenden Benennungsbedingungen einhält, kann die Anzahl der Domänennamens-Server-Einträgen reduziert werden, indem ein Domänennamenseintrag für jede SNA-Netz-ID definiert wird, auf die über einen oder mehrere SNA-über-TCP/IP-Gateways zugegriffen werden kann.

- Jedes SNA-Netz muß über eine SNA-Netz-ID verfügen, die unter allen vorhandenen SNA-Netzen eindeutig ist.
- Jedes IP-Netz muß über eine SNA-Netz-ID verfügen, die unter allen vorhandenen IP-Netzen eindeutig ist.
- Ein SNA-Netz und ein IP-Netz dürfen dieselbe SNA-Netz-ID verwenden.

Wenn für jede SNA-Netz-ID ein einziger Domänennamenseintrag festgelegt wird, braucht nicht für jede LU im SNA-Netz, mit der über das IP-Netz kommuniziert werden soll, ein Domänennamenseintrag definiert zu werden. Durch einen Platzhaltereintrag (*) können die LU-Namen aller LUs angegeben werden, die über dieselbe SNA-Netz-ID verfügen. Durch Angeben eines Platzhalters anstelle von *luname* in dem Eintrag kann ein einzelner Domänennamens-Server-Eintrag definiert werden, der alle LUs in dem betreffenden Netz darstellt.

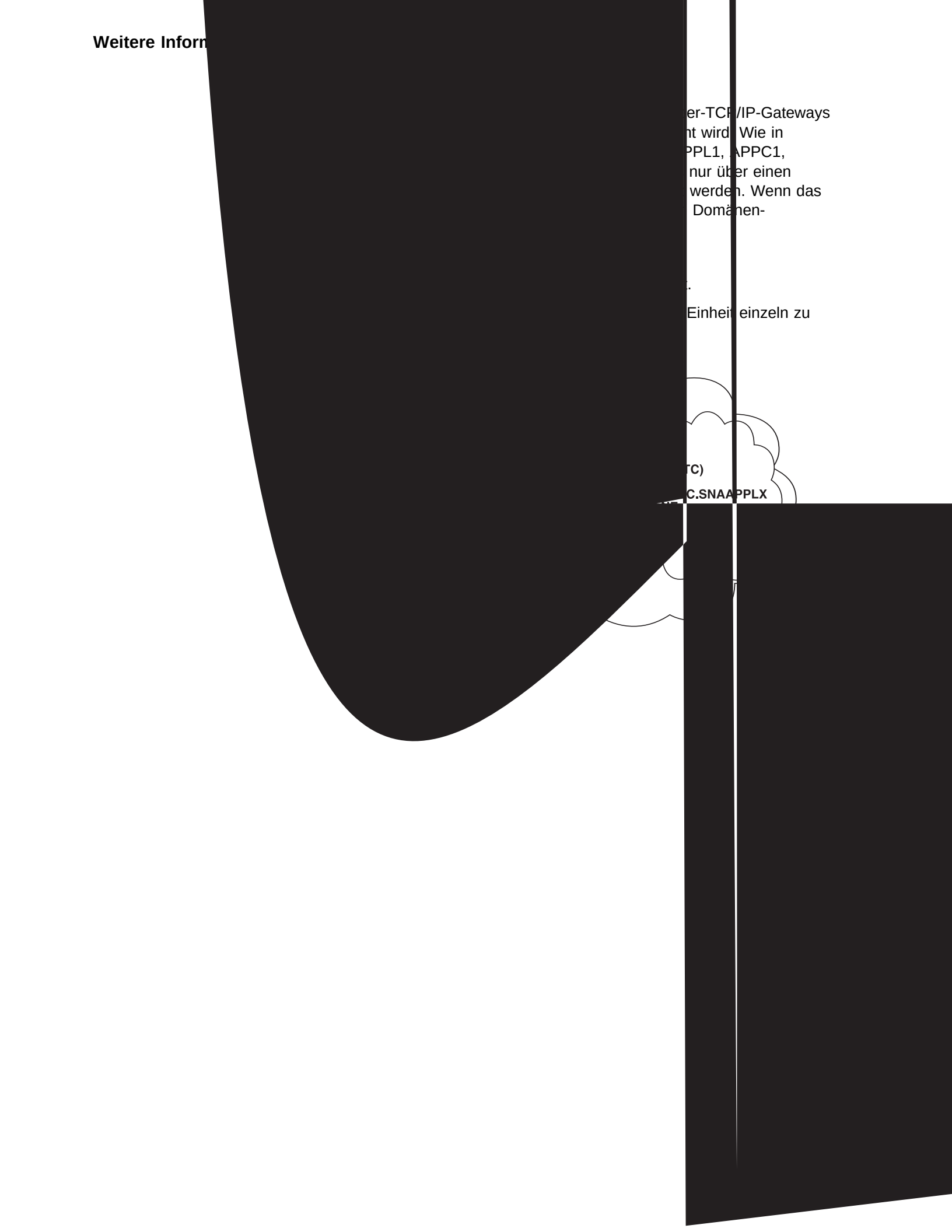
Anmerkung: Bei Verwendung des Platzhaltereintrags muß der vollständige Platzhalter angegeben werden. Teilweise Platzhalter wie z. B. LUA* sind nicht zulässig.

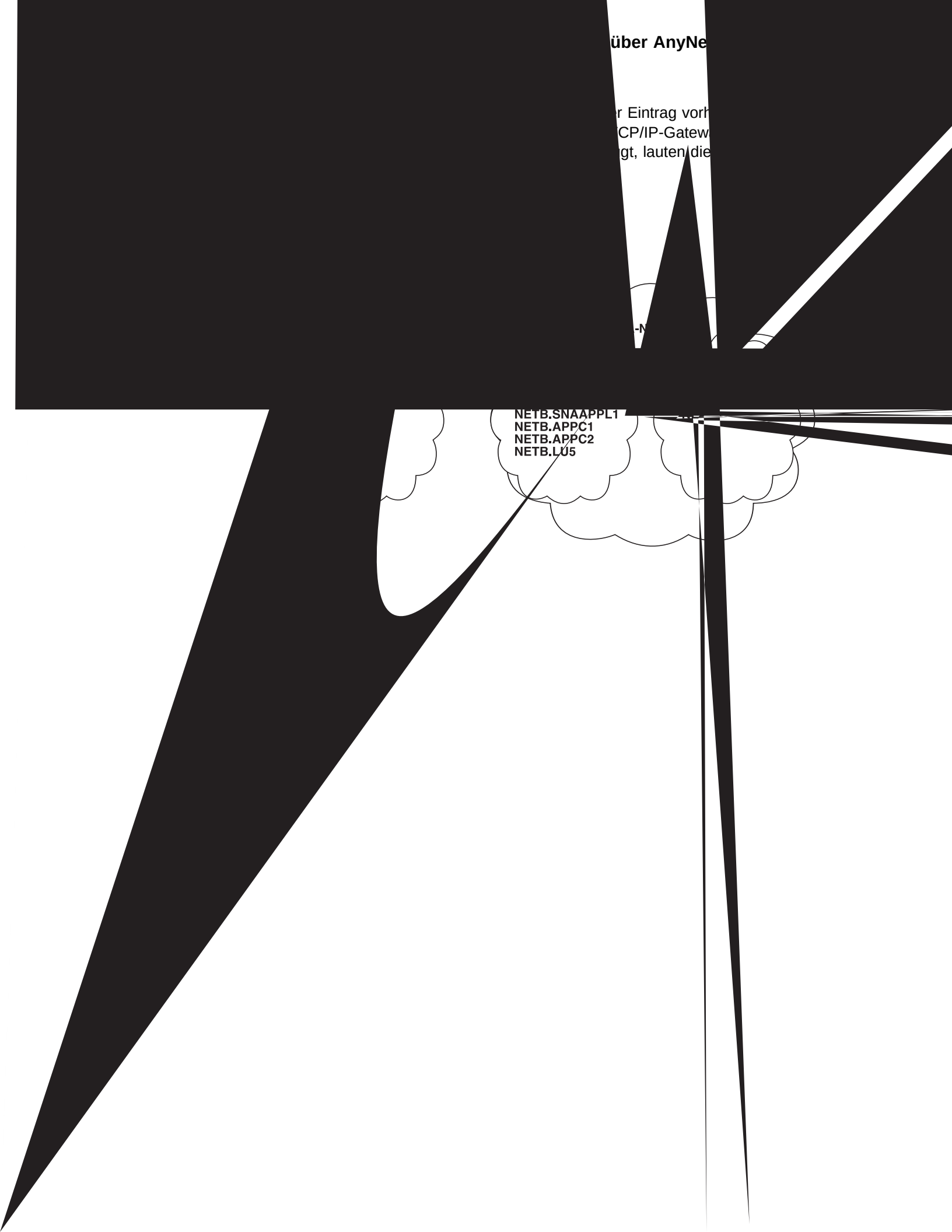
Weitere Inform

er-TCP/IP-Gateways
nt wird. Wie in
PPL1, APPC1,
nur über einen
werden. Wenn das
Domänen-

.

Einheit einzeln zu




über AnyNe
r Eintrag vorh
CP/IP-Gatew
gt, lauten die
NETB.SNAAPPL1
NETB.APPC1
NETB.APPC2
NETB.LU5

Überlegungen zur SNA-über-TCP/IP-Zugriffsknotenfunktion

Die folgenden Informationen beziehen sich nur auf Zugriffsknoten und nicht auf Gateways.

Weiterleitung von SNA-Sitzungen über AnyNet SNA über TCP/IP

Wenn eine SNA-Anwendung eine Sitzung einleitet, muß Communications Server zunächst festlegen, welcher Transporttyp zu verwenden ist (SNA, IP oder eine Kombination von beiden).

Der Benutzer kann seinen bevorzugten Transporttyp durch Festlegen der Routing-Vorgabe konfigurieren. Die Routing-Vorgabe kann über die Standard-Routing-Vorgabe der AnyNet-über-TCP/IP-Einheit für den gesamten Knoten oder beim Definieren der Partner-LUs einzeln für jede LU festgelegt werden.

Die Tabelle der Routing-Vorgaben wird nur für neue Sitzungen verwendet. Bereits vorher vorhandene Sitzungen verwenden denselben Transport, sie werden nicht beendet und anschließend über neue Leitwege geführt, wenn die Tabelle der Routing-Vorgaben geändert wird.

Anmerkung: Die Routing-Vorgabe für einen Knoten wird nur für Sitzungen verwendet, die von dem Knoten aus eingeleitet werden (Zugriffsknotensitzungen). Die Routing-Vorgabe gilt nicht für Sitzungen, die über einen Knoten weitergeleitet werden.

Der Benutzer kann die Standard-Routing-Vorgabe auf einen der folgenden Werte einstellen:

Zuerst Basisanschluß
: Anforderungen werden über SNA geleitet. Ist kein SNA-Leitweg verfügbar, werden die Anforderungen über TCP/IP geleitet.

Zuerst Nicht-Basisanschluß
: Anforderungen werden über TCP/IP geleitet. Ist kein TCP/IP-Leitweg verfügbar, werden die Anforderungen über SNA geleitet.

Nur Basisanschluß
: Anforderungen werden ausschließlich über SNA geleitet. Ist kein SNA-Leitweg verfügbar, schlägt die Verbindung fehl.

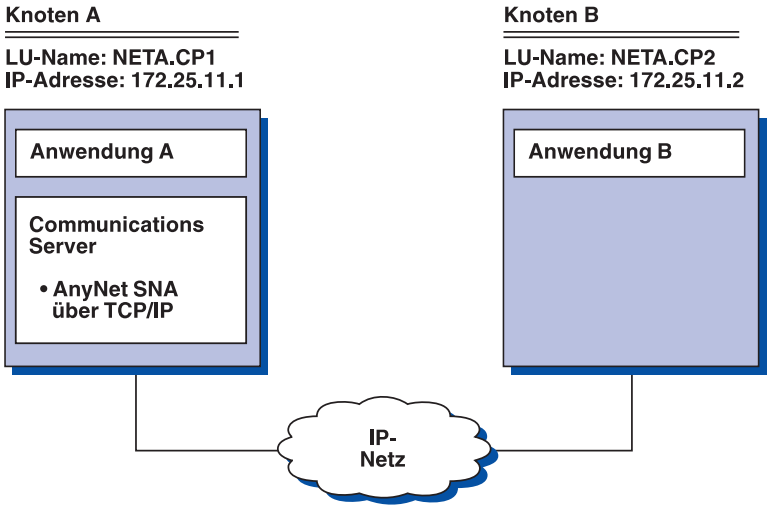
Nur Nicht-Basisanschluß
: Anforderungen werden ausschließlich über TCP/IP geleitet. Ist kein TCP/IP-Leitweg verfügbar, schlägt die Verbindung fehl.

Konfigurationsbeispiele für AnyNet SNA über TCP/IP

Dieser Abschnitt enthält Beispiele zum Ermöglichen der SNA-über-IP-Kommunikation über AnyNet. Die folgenden Konfigurationsanweisungen sind nur für das Betriebssystem Windows NT vollständig. In allen Beispielen ist das SNA-Domänennamenssuffix SNA.IBM.COM.

Weitere Informationen zum Konfigurieren von AnyNet für andere in diesem Abschnitt genannte Plattformen (z. B. VTAM oder AS/400) enthält die dazugehörige Produktdokumentation.

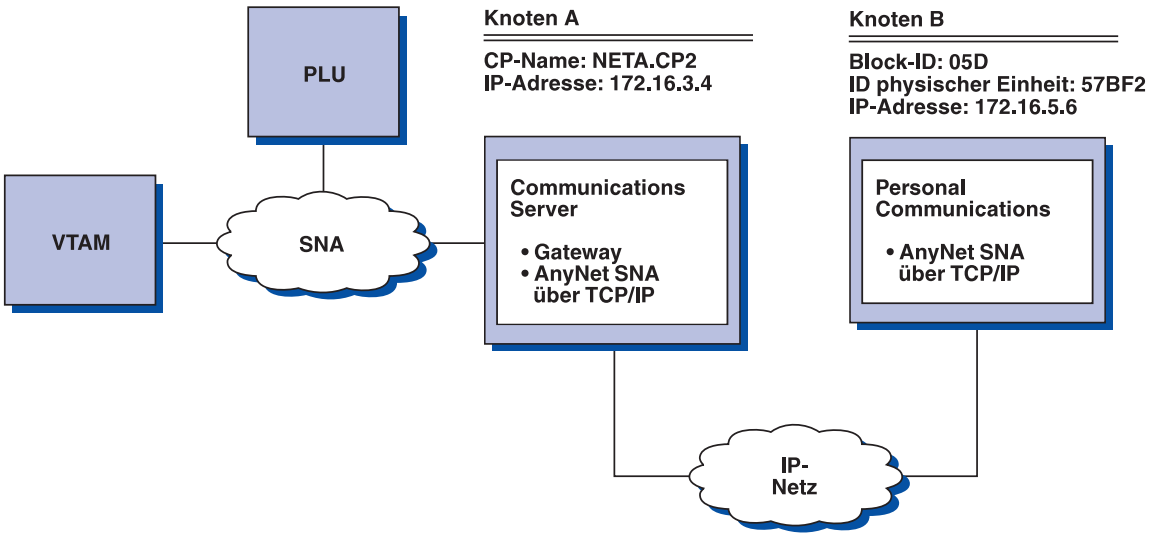
Beispiel 1: APPC- oder CPI-C-Anwendungen über ein TCP/IP-Netz ausführen



Weitere Informati

Beispiel 2: 327 **Schritte**ÕÅãÁKÃ×òÕÅãÁ

Beispiel 3: SNA-Gateway verwenden, um 3270-Emulation zwischen SNA- und TCP/IP-Netzen zu ermöglichen



Schritte

Mit den folgenden Schritten kann die Kommunikation zwischen Knoten B und dem VTAM-Host eingerichtet werden.

Für Knoten A folgendes ausführen:

1. Den folgenden Eintrag zur lokalen Datei HOSTS hinzufügen:

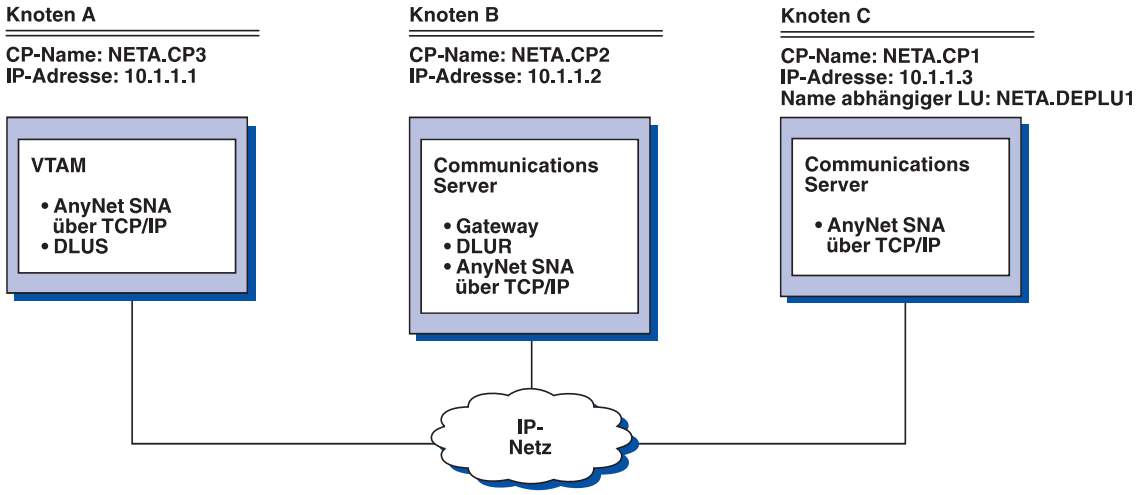
   ```
   172.16.5.6 05D57BF2.SNA.IBM.COM
   ```

2. Bei der Knotendefinition **NETA.CP2** als Steuerpunktnamen verwenden und beim Definieren von Clients die Einheit ANYNET verwenden, um implizite Schablonen zuzuordnen. Weitere Informationen enthalten die Hilfetextanzeigen der **Knotenkonfiguration**.

Für Knoten B folgendes zur lokalen Datei HOSTS hinzufügen:

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

Beispiel 4: Einen SNA-Gateway für 3270-Emulation über ein TCP/IP-Netz verwenden



Schritte

Mit den folgenden Schritten kann die Kommunikation zwischen Knoten C und Knoten A eingerichtet werden.

Für Knoten B folgendes ausführen:

1. Den folgenden Eintrag zur lokalen Datei HOSTS hinzufügen:

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

2. Bei der Knotendefinition **NETA.CP2** als Steuerpunktnamen verwenden, beim Festlegen der AnyNet-SNA-über-TCP/IP-Verbindungsdefinition **NETA.CP1** als Namen des Nachbarsteuerpunkts verwenden und bei der DLUS-Zuordnung für eine Client-Schablone **NETA.CP3** als DLUS-Namen verwenden. Dabei sicherstellen, daß die Routing-Vorgabe für NETA.CP3 auf Nicht-Basisanschluß gesetzt ist. Weitere Informationen enthalten die Hilfetextanzeigen der **Knotenkonfiguration**.

Für Knoten C folgendes ausführen:

1. Den folgenden Eintrag zur Datei HOSTS hinzufügen:

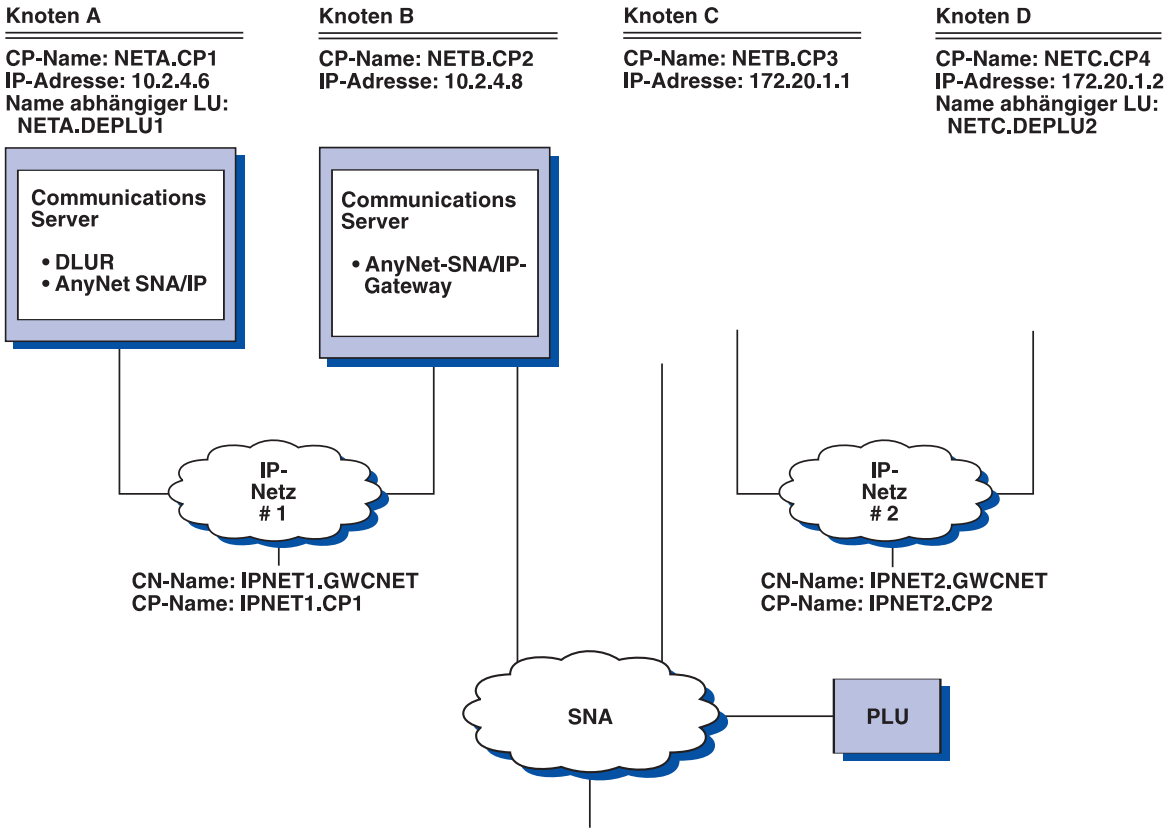
   ```
   10.1.1.2    CP2.NETA.SNA.IBM.COM
   ```

2. Bei der Knotendefinition **NETA.CP1** als Steuerpunktnamen verwenden und beim Festlegen der AnyNet-SNA-über-TCP/IP-Verbindungsdefinition **NETA.CP2** als den Namen des Nachbarsteuerpunkts verwenden. Weitere Informationen enthalten die Hilfetextanzeigen der **Knotenkonfiguration**.

Für Knoten A den folgenden Eintrag zur Datei HOSTS hinzufügen:

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

Beispiel 5: 3270-Emulation auf zwei Windows NT-Datenstationen in verschiedenen IP-NetzenPlanung für AnyNet-Unterstützung



CP-Name: NETB.C

Schritte

Mit den folgenden Schritten kann die Kommunikation von den Knoten A und D zum Knoten E eingerichtet werden.

Für Knoten A folgendes ausführen:

1. Die folgenden Einträge zur lokalen Datei HOSTS hinzufügen:

```
10.2.4.8    CP5.NETB.SNA.IBM.COM
127.0.0.4   IPNET1.GWCNET
127.0.0.3   IPNET1.CP1
```

2. Bei der Knotendefinition **NETA.CP1** als Steuerpunktnamen verwenden und beim Konfigurieren von DLUR-PUs **NETB.CP5** als DLUS-Namen verwenden. Dabei sicherstellen, daß die Routing-Vorgabe für NETB.CP5 auf Nicht-Basisanschluß gesetzt ist. Weitere Informationen enthalten die Hilfetextanzeigen der **Knotenkonfiguration**.

Für Knoten B die folgenden Einträge zur Datei HOSTS hinzufügen:

```
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
```

Für Knoten C die folgenden Einträge zur Datei HOSTS hinzufügen:

```
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
```

Für Knoten D folgendes ausführen:

1. Den folgenden Eintrag zur lokalen Datei HOSTS hinzufügen:

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

2. Bei der Knotendefinition **NETC.CP4** als Steuerpunktnamen verwenden und beim Konfigurieren der DLUR-PUs **NETB.CP5** als DLUS-Namen verwenden. Dabei sicherstellen, daß die Routing-Vorgabe für NETB.CP5 auf Nicht-Basisanschluß gesetzt ist. Weitere Informationen enthalten die Hilfetextanzeigen der **Knotenkonfiguration**.

Hilfreiche Hinweise

Dieser Abschnitt enthält hilfreiche Hinweise zur Optimierung, zur TCP/IP-Konnektivität über SLIP oder PPP und zu dynamischen IP-Adressen.

Optimierung

Wenn auf eine LU über mehrere SNA-über-TCP/IP-Gateways zugegriffen werden kann und der Name dieser LU mehreren IP-Adressen zugeordnet wurde, müssen beim Konfigurieren der AnyNet-Basisparameter die Parameter **CONN_RETRY_SECS** und **CONNWAIT_SECS** des Schlüsselworts **ANYNET_COMMOM_PARAMETERS** erhöht werden. Dadurch wird sichergestellt, daß versucht wird, TCP-Verbindungen zu allen möglichen Adaptern und Gateways herzustellen. Es kann bis zu 90 Sekunden dauern, bis eine TCP-Verbindung zu einer inaktiven IP-Adresse fehlschlägt.

Dynamische IP-Adressen

Im allgemeinen ist AnyNet SNA über TCP/IP davon abhängig, daß eine statische Zuordnung von SNA-Ressourcen (z. B. LU-Namen, CP-Namen oder idblk/num) zu IP-Adressen erfolgt. Je nach aktueller Konfiguration und Art der Verbindungseinleitung kann es jedoch möglich sein, AnyNet SNA über TCP/IP in Umgebungen mit dynamischer Zuordnung von IP-Adressen (z. B. DHCP) zu verwenden.

APPC- oder CPIC-Anwendungen: Ein SNA-über-TCP/IP-Zugriffsknoten mit dynamisch zugeordneter IP-Adresse kann jederzeit Sitzungen mit einem anderen SNA-über-TCP/IP-Zugriffsknoten oder -Gateway einleiten, der über eine statische IP-Adresse verfügt.

Ein SNA-über-TCP/IP-Zugriffsknoten oder -Gateway mit statischer IP-Adresse (Knoten A) kann jedoch nur auf folgende Weise eine Sitzung mit einem Partner einleiten, der über eine dynamische IP-Adresse verfügt (Knoten B):

1. Wenn Knoten B zuerst eine Sitzung mit oder über Knoten A eingeleitet hat.
2. Wenn die in Schritt 1 eingeleitete Sitzung noch aktiv ist.

Abhängige LU-Anwendungen

Anmerkung: Die Informationen in diesem Abschnitt gelten für LU 0, 1, 2, 3 oder für abhängige LU 6.2-Anwendungen.

SNA-über-TCP/IP-Zugriffsknoten mit dynamisch zugeordneten IP-Adressen können abhängige LU-Kommunikation unterstützen, wenn folgende Kriterien erfüllt sind:

- Die abhängige LU-Kommunikation erfolgt über einen SNA-Gateway mittels eines der folgenden Produkte:
  - Communications Server/2 4.1 mit APAR JR10461
  - Communications Server/2 Version 5
  - Communications Server für Windows NT 5.01 oder höher
- Der SNA-über-TCP/IP-Zugriffsknoten mit dynamisch zugeordneter IP-Adresse leitet Verbindungen zu einem SNA-Gateway mit statischer IP-Adresse ein.

Abhängige LU-Kommunikation über DLUS/DLUR mit AnyNet SNA über TCP/IP wird nicht unterstützt, wenn der DLUR-Knoten über eine dynamisch zugeordnete IP-Adresse verfügt.

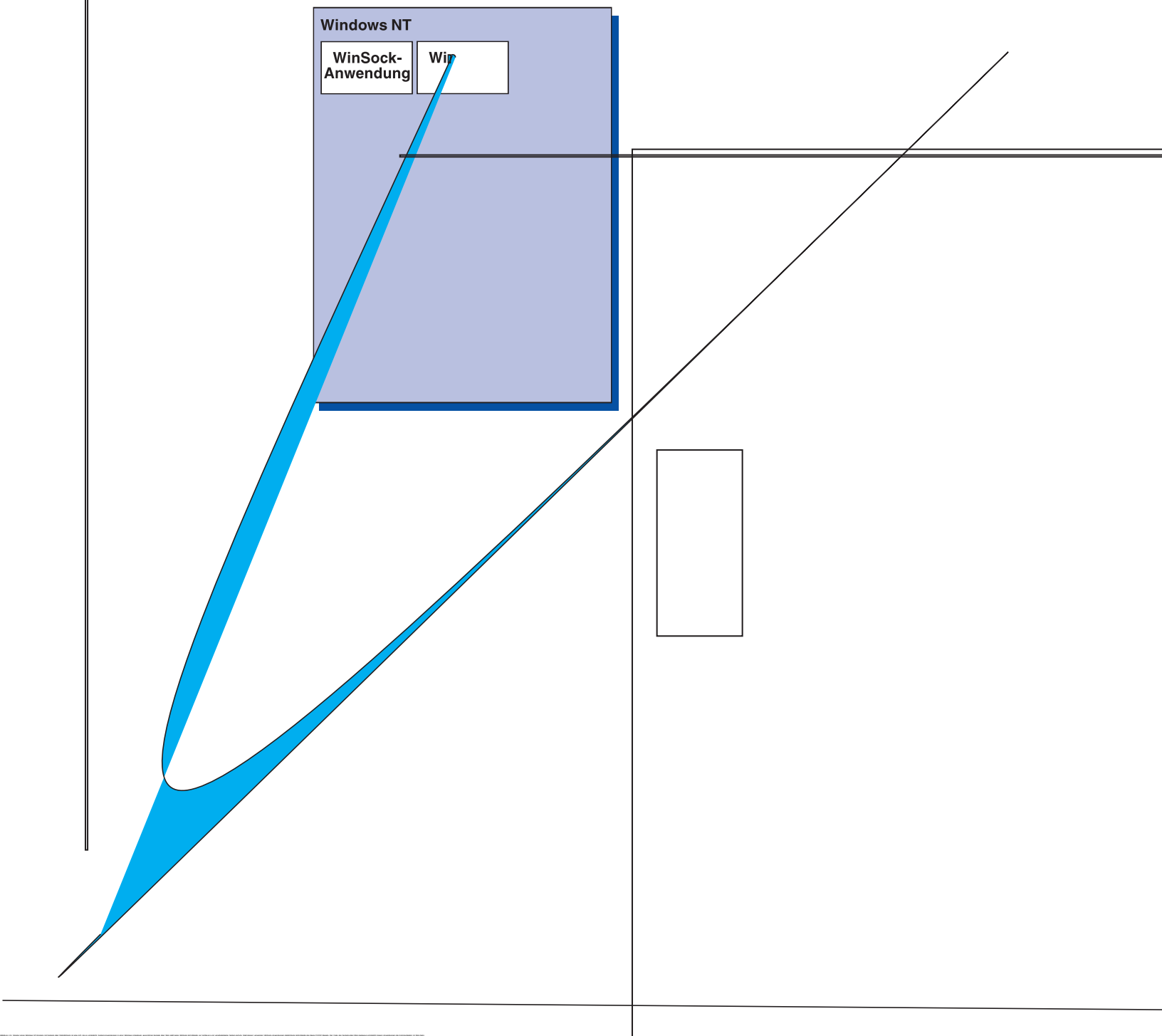
AnyNet Sockets über SNA konfigurieren

Dieser Abschnitt enthält Informationen zum Konfigurieren von Sockets über SNA.

Die Sockets-über-SNA-Zugriffsknotenfunktion von Communications Server ermöglicht WinSock-kompatiblen Anwendungen die Kommunikation über SNA-Netze. Die Sockets-über-SNA-Gateway-Funktion ermöglicht die Kommunikation zwischen Socket-Anwendungen in SNA- und TCP/IP-Netzen.

Funktionsweise von Sockets über SNA

Abb. 24 zeigt die Struktur eines Windows NT-Knotens, auf dem Sockets über SNA ausgeführt wird, und illustriert, wie Socket-Anwendungsprogramme und Sockets über SNA auf einem Windows NT-Knoten funktionieren.



Sockets-über-SNA-Gateway ermöglicht in einem IP-Netz ausgeführten Socket-Anwendungen die Kommunikation mit Socket-Anwendungen, die auf Sockets-über-SNA-Knoten ausgeführt werden. Dazu werden Pakete zwischen SNA- und IP-Netzen weitergeleitet und zwischen SNA- und IP-Protokollen umgewandelt. Der AnyNet-Gateway-Einheitentreiber unterstützt die Weiterleitung von Paketen zwischen TCP/IP- und SNA-Netzen, und der Sockets-über-SNA-Code ermöglicht die Umwandlung zwischen beiden Protokollen.

LU 6.2-Aufruf aus einem Socket-Aufruf generieren

Damit Informationen im TCP/IP-Format über SNA weitergeleitet werden können, ordnet Sockets über SNA den IP-Adressen im SNA-Netz qualifizierte LU-Namen zu. Wenn ein Anwendungsprogramm Sockets über SNA aufruft, um eine Datenstromverbindung mit einem anderen Anwendungsprogramm aufzubauen, richtet Sockets über SNA zwei Halbduplex-LU 6.2-Dialoge für die Datenstromverbindung ein.

Für alle an ein einziges Ziel gesendeten Datagramme richtet Sockets über SNA einen LU 6.2-Dialog ein. Für die Datagrammübertragung dedizierte Dialoge werden freigegeben, wenn sie innerhalb eines angegebenen Zeitraums nicht verwendet werden.

IP-Adresse einem im SNA-Netz qualifizierten Namen zuordnen

Wenn ein Anwendungsprogramm Sockets über SNA aufruft, um mit einem anderen Anwendungsprogramm Daten auszutauschen, gibt es die IP-Adresse des Zielknotens an. Sockets über SNA muß die IP-Adresse einer SNA-Adresse zuordnen, um einen entsprechenden LU 6.2-Aufruf abzusetzen. Für jede IP-Adresse, die einen Knoten darstellt, gibt es einen entsprechenden im SNA-Netz qualifizierten Namen.

Im Abschnitt „Übersicht über Weiterleitung und Zuordnung“ auf Seite 98 wird erläutert, wie die Adreßzuordnung funktioniert, und es werden Richtlinien und Anforderungen zum Einrichten der IP-LU-Adreßzuordnung beschrieben.

Daten über SNA- und IP-Netze weiterleiten und zuordnen

Sockets-über-SNA-Gateways ermöglichen die Kommunikation zwischen Socket-Anwendungsprogrammen in IP- und SNA-Netzen durch Kombinieren der Weiterleitungsfunktion von TCP/IP mit der Protokollumsetzung und den Adreßzuordnungsfunktionen von Sockets über SNA.

Protokollumsetzung und Adreßzuordnung sind erforderlich, wenn Daten über Knoten weitergeleitet werden, die unterschiedliche Transportprotokolle verwenden. Der Sockets-über-SNA-Gateway führt die Protokollumsetzung automatisch durch, sobald festgestellt wurde, welcher Transporttyp der Ziel-IP-Adresse zugeordnet ist. Eine Zusammenfassung der Leitwegwahl und der Zuordnung enthält der Abschnitt „Weiterleitung und Zuordnung von Daten durch den Sockets-über-SNA-Gateway“ auf Seite 101.

Von Sockets über SNA bereitgestellte Unterstützung für Anwendungsprogramme

Sockets über SNA unterstützt Anwendungen unter WinSock 1.1 und WinSock 2.0 (nur Windows NT 4.0), die AF_INET-Sockets verwenden.

Sockets über SNA unterstützt keine Anwendungen, die Rundsendebetrieb verwenden.

Wenn Sockets-über-SNA-Gateway zur Weiterleitung von Informationen von und zu einem mit der Sockets-über-SNA-Funktion von VTAM Version 3 Release 4 konfigurierten MVS/ESA-Knoten verwendet werden soll, muß auf dem MVS/ESA-Knoten zunächst die Funktion `route` installiert werden. Zum Installieren der Funktion `route` unter MVS/ESA die vorläufige Programmkorrektur (Program Temporary Fix) PTF UW03567 installieren. PTFs sind über die folgenden Quellen zu beziehen:

- Information Access
- SoftwareXcel Extended
- IBMLink (ServiceLink)

Zugriff auf diese Quellen kann bei der IBM Kundenunterstützung angefordert werden.

Planung für Sockets über SNA

In diesem Abschnitt wird beschrieben, was der Netzplaner bei der Konfiguration eines Netzes mit Sockets über SNA berücksichtigen sollte.

Übersicht über Weiterleitung und Zuordnung

Dieser Abschnitt beschreibt die Grundkonzepte der Internet-Adressierung und ihren Bezug zu Weiterleitung und Zuordnung. Dazu gehören die folgenden Informationen:

- „Internet-Adressierung“
- „IP-Leitwegtabelle“ auf Seite 100
- „Von Sockets über SNA verwendete SNA-Netz-ID“ auf Seite 100
- „IP-Adresse einem LU-Namen zuordnen“ auf Seite 100
- „Weiterleitung und Zuordnung von Daten durch den Sockets-über-SNA-Gateway“ auf Seite 101

Internet-Adressierung

Jedem Host wird mindestens eine eindeutige Internet Protocol-Adresse (IP-Adresse) zur Weiterleitung von Daten im Netz zugeordnet.

Anmerkung: In der Gruppe der IP-Protokolle bezeichnet ***Host*** ein Endsystem. Dieses Endsystem kann jede beliebige Datenstation sein; es muß nicht unbedingt ein Großrechner sein.

Die dem Host zugeordnete IP-Adresse definiert keinen Host im Netz; sie definiert eine Netzschnittstelle auf diesem Host zu einem Netz. Beispiel: Die Adresse der SNA-Netzschnittstelle kennzeichnet die Verbindung eines Knotens zum SNA-Netz.

Ein Gateway-Host verfügt über eine eindeutige IP-Adresse für jede Netzschnittstelle. Da der Sockets-über-SNA-Gateway SNA- und TCP/IP-Daten weiterleitet, müssen für die TCP/IP- und SNA-Schnittstellen eindeutige IP-Adressen definiert werden.

Im folgenden Abschnitt werden IP-Adreßformat, Adreßklassen und Netzmasken beschrieben. Ausführliche Informationen enthält die TCP/IP-Dokumentation.

IP-Adreßformat und Adreßklassen: Eine IP-Adresse besteht aus einem zweiteiligen 32-Bit-Adreßfeld:

- Der erste Teil des Adreßfelds enthält die Netzadresse; der zweite Teil enthält die Host-Adresse.
- Die Anzahl der für die Netz- und Host-Abschnitte verwendeten Bit einer IP-Adresse sind variabel und hängen von der Adreßkategorie der IP-Adresse ab.
- Mit Hilfe einer Netzmaske kann ein Teil des Host-Abschnitts der IP-Adresse als eine Teilnetzadresse verwendet werden.

Die Standardnetzmasken sind in Tabelle 5 aufgeführt.

Tabelle 5. Von Sockets über SNA unterstützte IP-Adreßmasken

Für eine IP-Adresse in der Schreibweise mit Trennzeichen im Format *a.b.c.d* gilt für *a* der folgende Wertebereich:	**Standardnetzmaske**
1–127	255.0.0.0
128–191	255.255.0.0
192–223	255.255.255.0

Von Sockets über SNA verwendete Masken: Sockets über SNA verwendet die beiden folgenden Maskenarten:

- **Teilnetzmaske**

  Die Teilnetzmaske wird für die Weiterleitung verwendet. Sie wird beim Konfigurieren des lokalen Knotens und der Leitwege angegeben. Der Benutzer kann die Standardteilnetzmaske übernehmen oder einen anderen als den Standardwert angeben, um Teilnetzadressen zu definieren.

- **Adreßmaske**

  Die Adreßmaske wird für die Zuordnung generierter IP-LU-Adressen verwendet und beim Konfigurieren festgelegt.

IP-Leitwegtabelle

Jeder Host verfügt über eine IP-Leitwegtabelle mit Informationen über mögliche Ziele und wie sie erreicht werden können. Leitwegeinträge werden in folgenden Fällen hinzugefügt:

- Beim Definieren der lokalen IP-Adresse. Weitere Informationen enthält die Online-Hilfe.
- Beim Definieren von Leitweganweisungen im Fenster **Knotenkonfiguration**. **AnyNet Sockets konfigurieren** und danach **Leitwege** anklicken. Weitere Informationen enthält die Online-Hilfe.
- Wenn ein Leitweg mit weniger Zwischenschritten gefunden wird. Dies ist der Fall, wenn der Sockets-über-SNA-Gateway eine ICMP-Umleitung oder RIP-Nachricht erhält. Weitere Informationen enthält der Abschnitt „Leitwegerkennungsfunktion Discovery“ auf Seite 102.

Ein Beispiel für eine Leitwegtabelle enthält Abb. 25 auf Seite 101.

Von Sockets über SNA verwendete SNA-Netz-ID

Für jeden Leitweg, der über die SNA-Schnittstelle (sna0) definiert w ã èÃne e

Weiterleitung und Zuordnung von Daten durch den Sockets-über-SNA-Gateway

Die folgenden Schritte zeigen in Kurzform, wie der Sockets-über-SNA-Gateway feststellt, ob Daten über SNA oder TCP/IP weitergeleitet werden sollen, und wie die Adreßzuordnung erfolgt:

1. Sockets über SNA durchsucht seine Leitwegtabelle nach einem Leitweg, auf dem die Daten zur Ziel-IP-Adresse gelangen können. Wenn Sockets über SNA keine geeigneten Leitwege findet, wird die Verbindungsanforderung an den Basis-TCP/IP-Stapel weitergeleitet.
2. Wenn Sockets über SNA einen geeigneten Leitweg findet, gibt der Leitwegeintrag an, wie das Ziel erreicht werden kann:
   a. Wenn die Router-Adresse die Adresse einer lokalen Netzschnittstelle (z. B. sna0) ist, sind Zielnetz-, Teilnetz- oder Host-Adresse direkt erreichbar.
   b. Ist die Router-Adresse die Adresse eines Gateways oder eines Routers, kann das Ziel nur über diesen Gateway oder Router erreicht werden.

   Abb. 25 zeigt ein Beispiel für eine IP-Leitwegtabelle.

```
Ziel-IP-Adresse    Zielmaske            Gateway-IP-Adresse   Verwendungszähler
-------------------------------------------------------------------------------
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
```

Abbildung 25. Beispiel für eine IP-Leitwegtabelle

3. Wird in der Sockets-über-SNA-Leitwegtabelle kein Leitweg gefunden, geht Sockets über SNA davon aus, daß das TCP/IP-Ziel über ein IP-Basisnetz erreicht werden kann. Weitere Informationen zur Weiterleitung von Daten in TCP/IP enthält die TCP/IP-Dokumentation.
4. Wenn der ausgewählte Leitweg darauf hindeutet, daß die Daten über die SNA-Schnittstelle (sna0) geleitet werden sollten, sucht Sockets über SNA in der IP-LU-Zuordnungstabelle nach der nächsten Zwischenschrittadresse:
   a. Wenn Sockets über SNA einen geeigneten Eintrag findet, wird eine LU 6.2-Verbindung hergestellt.
   b. Wenn Sockets über SNA keinen geeigneten Eintrag findet, schlägt der Verbindungsversuch fehl.
   c. Sockets über SNA übergibt die Zieladresse und die Daten an Communications Server.
5. Alle für Sockets über SNA definierten Leitwege werden im Basis-TCP/IP-Stapel gespiegelt, so daß Pakete von IP über SNA weitergeleitet werden können.

Leitwegerkennungsfunktion Discovery: Die Leitwegerkennungsfunktion Discovery von Sockets-über-SNA-Gateway ermöglicht die effizientere Weiterleitung von TCP/IP-Datenverkehr und reduziert die erforderliche Anzahl explizit definierter Leitweganweisungen im Netz. Diese Funktion muß nicht ausgewählt oder konfiguriert werden.

Ein Problem bei großen Netzen besteht darin, das Hinzufügen neuer Netze oder Teilnetze zu erkennen und festzustellen, welches der richtige Router zum Erreichen des neuen Netzes oder Teilnetzes ist. Sockets über SNA löst dieses Problem dadurch, daß alle Knoten zunächst einen Standard-Router verwenden, der andere Knoten informiert, wenn ein kürzerer Direktweg gefunden wird. Dieses Verfahren ist effizienter als die für TCP/IP typische Übermittlung von Leitweginformationen im Rundsendebetrieb.

Anmerkung: Um diese Funktion möglichst effektiv zu nutzen, sollte die algorithmische Zuordnung von IP-Adressen zu LU-Namen und ein zentrales APPN-Netz verwendet werden. Andernfalls müssen die Knoten für alle fernen Knoten, mit denen sie kommunizieren, LU-Namen und IP-Adressen explizit definieren.

Abb. 26 zeigt ein Konfigurationsbeispiel.

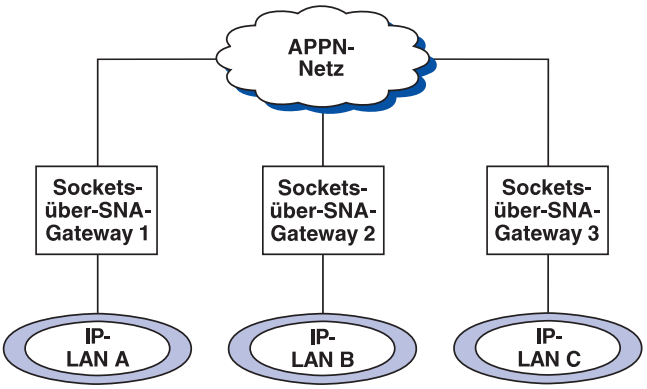


Abbildung 26. Beispiel für ein Netz, das die Sockets-über-SNA-Leitwegerkennungsfunktion Discovery verwendet

Für dieses Szenario gilt folgendes:

- Die Gateways 1, 2 und 3 sind Sockets-über-SNA-Gateways, die mit IP-LAN-Netzen verbunden sind. Diese Gateways verbinden die IP-LAN-Netze mit einem zentralen APPN-Netz.
- Gateway 1 ist der einzige Gateway, auf dem eine vollständige und permanente Leitwegtabelle geführt wird.

  Die Gateways 2 und 3 definieren Gateway 1 als ihren Standard-Router. Wenn ein fernes Netz oder Teilnetz dem Gateway 1 bekannt ist, brauchen Gateway 2 und Gateway 3 diese Leitwege nicht explizit zu definieren.

- Wenn Gateway 2 und 3 Daten an nicht definierte Netze oder Teilnetze weiterleiten, werden diese Anforderungen an den Standard-Router, Gateway 1, übermittelt.

  Wenn das Netz oder Teilnetz dem Gateway 1 bekannt ist und ein direkterer Weg verfügbar ist, sendet Gateway 1 eine ICMP-Umleitungsnachricht an den Requester, in der der künftig zu verwendende Pfad angegeben ist. Diese ICMP-Umleitungsnachricht aktualisiert die Leitwegtabelle des Requesters. Die Gateways 2 und 3 erstellen also ihre Leitwegtabellen für ferne Netze und Teilnetze dynamisch nach Bedarf.
- Wenn neue Gateways hinzugefügt werden, muß die permanente Leitwegtabelle von Gateway 1 entsprechend aktualisiert werden. Für Gateway 2 und 3 sind keine expliziten Leitweganweisungen erforderlich.

Modi für Sockets über SNA definieren

Sockets über SNA verwendet LU 6.2-Dialoge, um die Kommunikation zwischen Socket-Anwendungsprogrammen zu ermöglichen. Beim Aufbau eines LU 6.2-Dialogs definiert Sockets über SNA den Modus und die Merkmale der Verbindung. Communications Server identifiziert mit Hilfe des Modusnamens die Merkmale der Verbindung zwischen den beiden Sockets-über-SNA-Knoten.

Der Standardmodus für Sockets über SNA ist BLANK. Der Benutzer kann den Standardmodus verwenden oder einen eigenen Modus definieren. Zum Ändern des Standardmodus für Sockets über SNA im Fenster **Knotenkonfiguration** die Option **AnyNet Sockets über SNA konfigurieren** und danach **Modi** anklicken. Es besteht die Möglichkeit, einen anderen Standardmodus für alle TCP/IP-Übertragungen zu definieren und einem bestimmten TCP/IP-Anschluß einen bestimmten Modus zuzuordnen.

Bei Angabe eines alternativen Modus, der in Communications Server nicht definiert ist, muß der Benutzer die Sitzungsmerkmale für diesen Modus in Communications Server definieren.

Zeitlimit für Inaktivität ändern

Über das Inaktivitätszeitlimit kann festgelegt werden, nach wieviel Sekunden Inaktivität Sockets über SNA den Datagrammdialog unterbricht. Dieses Intervall ermöglicht, zwischen der Verwendung von Systemressourcen bei der Durchführung eines laufenden Datagrammdialogs und dem Zeitverlust beim Einrichten eines neuen Datagrammdialogs abzuwägen. Beispiel: Wenn ein niedriger Wert definiert wird, werden nicht benutzte Datagrammdialoge schneller beendet, aber es dauert länger, bis das nächste Datagramm gesendet wird. Das Standardintervall für das Inaktivitätszeitlimit beträgt 90 Sekunden.

Zum Ändern der Startoption im Fenster **Knotenkonfiguration** die Option **AnyNet Sockets über SNA konfigurieren** anklicken und anschließend **Anzeigen/Ändern/Hinzufügen** sowie die Indexzunge **Erweitert** anklicken und einen neuen Wert für diese Option auswählen.

Planung für Client/Server-Kommunikation

Dieses Kapitel enthält Informationen zur Planung für SNA-API-Clients für Communications Server und Novell IntranetWare für SAA.

SNA-API-Clients

Dieser Abschnitt enthält spezifische Informationen für SNA-API-Clients.

Installation und Konfiguration

Informationen zum Installieren und Konfigurieren von Communications Server-SNA-API-Clients können dem Handbuch *Einstieg* entnommen werden.

Lightweight Directory Access Protocol (LDAP)

LDAP (Lightweight Directory Access Protocol) stellt ein standardisiertes Verfahren für den Zugriff auf Verzeichnisservices zur Verfügung. LDAP ermöglicht das Lesen, Suchen, Hinzufügen und Löschen von Informationen in zentralen oder verteilten Datenbanken. LDAP ähnelt dem älteren X.500 Directory Access Protocol (DAP), jedoch mit geringerem Systemaufwand (z. B. OSI-Schichten für Sitzungen und Darstellung). Mit **API-Client-Konfiguration (LDAP)** können SNA-API-Client-Informationen konfiguriert und auf einem LDAP-Server gespeichert werden.

API-Client-Konfiguration (LDAP) zeigt die logische Anordnung und die Beziehungen zwischen Clients und ihren Konfigurationen

Weitere Informationen zur Verwendung dieser Hauptbereiche können den Hilfetextanzeigen für **API-Client-Konfiguration (LDAP)** entnommen werden.

Verzeichnisbaumstruktur

Die Verzeichnisbaumstruktur (DIT - Directory Information Tree) verbindet alle Verzeichnisserviceagenten (DSA - Directory Service Agents) in einem vordefinierten Modell. Das Modell besteht aus einer erweiterbaren hierarchischen Struktur, mit mehreren Basisobjekten. Eine typische LDAP-DIT geht von einer Basis (Root) aus, in der einzelne Länder (***countries***, c) definiert sind. Von der Länderebene zweigen in der Regel Organisationen (***organizations***, o) ab, und die Organisationen sind wiederum in Einzelpersonen (***individuals***, cn oder uid) oder Organisationseinheiten (***organizational units***, ou) unterteilt. Ein vollständig qualifizierter LDAP-Eintrag würde beispielsweise wie folgt angegeben:

```
c=US, o=firma.com, ou=Verkauf, cn=temp
```

Client-Hierarchie

Die Client-Hierarchie ist angelehnt an die LDAP-DIT, an der die Anmeldung erfolgt ist. In der Client-Hierarchie können Benutzer oder Organisationseinheiten hinzugefügt bzw. entfernt werden.

Konfigurationshierarchie

Die Konfigurationshierarchie stellt in einer grafischen Baumstruktursicht die logische Anordnung der Client-Konfiguration und die Beziehungen zwischen den Konfigurationsdefinitionen dar. In der Konfigurationshierarchie können Definitionen erstellt, geändert und entfernt werden.

Gemeinsamer API-Client für Communications Server für Windows NT und IntranetWare für SAA

Der im Lieferumfang von Communications Server enthaltene Client ermöglicht das Lokalisieren von und Zugreifen auf IBM Communications Server und IntranetWare für SAA-Server (IWSAA-Server) im Netz.

Installationsoptionen für die Konfigurationsposition

Während der Installation des Clients kann der Benutzer die Position für die Client-Konfiguration auswählen. Folgende drei Möglichkeiten stehen zur Wahl:

- INI-Dateikonfiguration - diese Methode wurde in früheren Communications Server-Versionen verwendet; sie ist die Standardmethode zum Installieren des in Communications Server enthaltenen SNA-API-Clients
- Netware Directory Services (NDS) - diese Methode wurde in früheren Versionen von IWSAA verwendet; sie ist die Standardmethode zum Installieren des in IntranetWare für SAA enthaltenen SNA-API-Clients
- Lightweight Directory Access Protocol (LDAP)

Die Konfigurationsposition ist der Ort, an dem Server-Listen, Benutzernamen und alle sonstigen Client-Konfigurationsdaten gespeichert sind.

Konfigurationspositionen

Da die Konfigurationsdaten nicht vom Server-Typ (Communications Server für Windows NT oder IntranetWare für SAA) abhängig sind, können sie in NDS, INI oder LDAP gespeichert werden. Beispielsweise können Communications Server-Namen und -Adressen für den API-Client in NDS, INI oder LDAP gespeichert werden. Da NDS-Verwaltungsprogramme nur mit IntranetWare für SAA geliefert werden, setzt die Konfiguration der SNA-API-Client-Informationen in NDS voraus, daß IntranetWare für SAA im Netz vorhanden ist. Der gemeinsame SNA-API-Client ermöglicht problemloses Integrieren verschiedener Server-Typen im gleichen Netz.

Konfigurationsdienstprogramm

Mit dem Dienstprogramm **Konfigurationsoptionen setzen** kann die Client-Konfigurationsposition (INI, NDS oder LDAP) nach der Installation geändert werden.

Server lokalisieren

Der Client ermöglicht dem Benutzer das Lokalisieren von und den Zugriff auf IBM Communications Server und IWSAA-Server mit dem Transportprotokoll TCP/IP oder SPX.

TCP/IP: Die Methode zum Lokalisieren von Servern mit dem TCP/IP-Transportprotokoll ist die gleiche. Der Netzadministrator kann den Zugriff auf die Server über die Server-Konfiguration steuern. Weitere Informationen können dem Abschnitt „Planung für TCP/IP-Bereiche“ auf Seite 162 entnommen werden.

SPX: Zum Lokalisieren von Servern mit dem SPX-Transportprotokoll sind andere Methoden anzuwenden. Das gleichzeitige Lokalisieren von IBM Communications Servern und von IWSAA-Servern dauert länger als das ausschließliche Lokalisieren von IBM Communications Servern oder IWSAA-Servern.

Der Communications Server-SNA-API-Client versucht zunächst, die IBM Communications Server zu lokalisieren und anschließend die IWSAA-Server. Wenn im Netz keine IWSAA-Server vorhanden sind oder auf diese nicht zugegriffen werden soll, kann der Benutzer das Lokalisieren der IWSAA-Server mit Hilfe einer Umgebungsvariablen inaktivieren. Durch Setzen dieser Variablen kann in Umgebungen, in denen über das SPX-Transportprotokoll ausschließlich auf IBM Communications Server zugegriffen wird, die Verarbeitungsleistung erhöht werden. Diese Umgebungsvariable ist **SNA_API_CLIENT_NO_CC**. Das Setzen dieser Variablen wirkt sich nicht auf die Lokalisierung von Servern aus, die das TCP/IP-Transportprotokoll verwenden.

Lokale Standard-LU zuordnen

Standardaliasnamen für die lokalen LUs können für jeden Benutzer entweder über die INI-Konfigurationsdatei oder über die LDAP-Konfiguration für 32 Bit-Windows-SNA-API-Clients zugeordnet werden.

APPC-Programme können einen Standardaliasnamen der lokalen LU verwenden, anstatt einen Aliasnamen direkt anzugeben. Wenn ein APPC-Programm ein Verb TP_START absetzt, in dem das Feld für den Aliasnamen der lokalen LU nur binäre Nullen oder nur ASCII-Leerzeichen enthält, verwendet die APPC-API den konfigurierten Standardaliasnamen der lokalen LU.

EHNAPPC-Programme können einen Standardaliasnamen der lokalen LU verwenden, anstatt einen Aliasnamen direkt anzugeben. Wenn das Feld für die lokale LU in der AS/400-Konfigurationsanzeige leer ist, wird der konfigurierte Standardaliasname der lokalen LU verwendet.

CPI-C-Programme können einen Standardaliasnamen der lokalen LU verwenden, anstatt einen Aliasnamen direkt anzugeben. Wenn das Feld für den Aliasnamen der lokalen LU in dem CPI-C-Zusatzinformationssatz leer ist und über die Umgebungsvariable APPCLLU kein Wert definiert wurde, verwendet die CPI-C-API beim Einleiten eines Dialogs den konfigurierten Standardaliasnamen der lokalen LU.

Vom Attach-Manager gestartete Programme können einen Standardaliasnamen der lokalen LU verwenden, anstatt einen Aliasnamen direkt anzugeben. Wenn das Feld für den Aliasnamen der lokalen LU im Attach-Manager-Datensatz leer ist, verwendet der Attach-Manager beim Verarbeiten ankommender Dialoganforderungen den konfigurierten Standardaliasnamen der lokalen LU.

Standard-Partner-LU zuordnen

Standardaliasnamen für die Partner-LUs aller Benutzer können entweder über die INI-Konfigurationsdatei oder über die LDAP-Konfiguration für 32 Bit-Windows-SNA-API-Clients zugeordnet werden.

APPC-Programme können einen Standardaliasnamen für die Partner-LU verwenden, anstatt einen Aliasnamen direkt anzugeben. Wenn ein APPC-Programm ein Verb ALLOCATE absetzt, in dem das Feld für den Aliasnamen der Partner-LU und das Feld für die vollständig qualifizierte Partner-LU binäre Nullen oder nur ASCII-Leerzeichen enthält, verwendet die APPC-API den konfigurierten Standardaliasnamen der Partner-LU.

CPI-C-Programme können einen Aliasnamen der Standard-Partner-LU verwenden, anstatt eine direkt eine Partner-LU anzugeben. Wenn das Feld für den Aliasnamen der Partner-LU in den CPI-C-Nebeninformationen leer bleibt, verwendet die CPI-C-API beim Einleiten eines Dialogs den konfigurierten Aliasnamen der Standard-Partner-LU.

Standard-LUA-Sitzungsnamen zuordnen

Standardaliasnamen für die LUA-Sitzungsnamen aller Benutzer können entweder über die INI-Konfigurationsdatei oder über die LDAP-Konfiguration für 32 Bit-Windows-SNA-API-Clients zugeordnet werden.

LUA-Programme (z. B. 3270-Emulationen) können einen Standard-LUA-Sitzungsnamen verwenden, anstatt einen Sitzungsnamen direkt anzugeben. Wenn ein LUA-Programm ein Verb RUI_INIT oder SLI_OPEN absetzt, in dem das Feld für den LUA-LU-Namen binäre Nullen oder nur ASCII-Leerzeichen enthält, verwendet die RUI/SLI-API den konfigurierten Standard-LUA-Sitzungsnamen.

Client/Server-Datenverschlüsselung

Die Client/Server-Datenverschlüsselung ermöglicht dem Client, die Verschlüsselung der Anwendungsdaten für Übertragungsvorgänge zwischen dem SNA-API-Client und Communications Server anzufordern.

Die Datenverschlüsselung kann auf "Ein", "Aus" oder "Wahlfrei" gesetzt werden. Wahlfreie Datenverschlüsselung bedeutet, daß die Verschlüsselung zur Anwendung kommt, wenn sie vom Server unterstützt wird.

Client/Server-Sicherheit

Communications Server ermöglicht SNA-API-Clients unter Windows 95 und Windows NT die Verwendung der Windows NT-Domänensicherheitsfunktion zur Identifikationsüberprüfung der Client-Verbindung zum Server, ohne daß Benutzer-ID und Kennwort erneut eingegeben werden müssen. Der Client muß einer Windows NT-Domäne angehören, und zwar entweder durch seine Teilnahme an einer Communications Server-Domäne oder durch lokale Anmeldung über eine synchronisierte Benutzer-ID mit Kennwort.

Benutzer von SNA-API-Clients außerhalb der Windows NT-Domäne müssen die Benutzer-ID und das Kennwort entweder in einer Eingabeaufforderung oder durch Speichern dieser Werte in der Client-Konfigurationsdatei angeben.

Die berechtigten Client/Server-Benutzer werden in der lokalen Gruppe IBMCSAPI erfaßt, die sich direkt auf dem Communications Server oder auf der Steuereinheit der Domäne befindet, zu der der Communications Server gehört. Diese Benutzergruppe wird während der Installation erstellt und kann mit dem Benutzer-Manager von Windows NT verwaltet werden.

Durch Einstellen des Werts für **LogonControl** auf dem Server auf Null (0) kann festgelegt werden, daß der Client beim Verbindungsaufbau zum Server weder Benutzer-ID noch Kennwort angeben muß.

Prüfprotokolldatensätze für die Client-Verbindungen zum Server werden im Windows NT-Ereignisprotokoll erfaßt. Diese Datensätze können in der Windows NT-Ereignisanzeige durch Anklicken von **Anwendung** angezeigt werden. Wenn Client-Verbindungen zum Server nicht protokolliert werden sollen, kann der Wert für **AuditTrail** auf dem Server auf Null (0) gesetzt werden.

Auf die Einträge **LogonControl** und **AuditTrail** kann im Windows NT-Registrierungseditor unter dem Schlüssel `HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/IBM SNA Client Services` zugegriffen werden.

Novell IntranetWare für SAA-Clients

Communications Server unterstützt über IPX oder TCP/IP verbundene Clients mit Emulationssoftwarepaketen, die die Novell-Architektur für Warteschlangenelemente/Nachrichteneinheiten (QEL/MU - Queue Element/Message Unit) für 3270-Emulation implementieren, und ermöglicht den Clients den Zugriff auf Großrechner-Host-Daten. Dazu gehört auch die Unterstützung häufig verwendeter Client-Funktionen, einschließlich der LU-Kategorien dediziert, im Pool und PUBLIC (gelegentlich auch als Ressourcenarten bezeichnet).

Communications Server unterstützt Novell IntranetWare für SAA-Clients unter Windows 95, Windows NT, Windows 3.1 und OS/2.

TCP/IP, IPX/SPX oder beide sind erforderlich, damit Novell IntranetWare für SAA-Clients mit Communications Server kommunizieren können. Wenn IPX verwendet wird, muß auf dem Server außerdem folgende Software aktiviert sein:

- Gateway Service für Netware
- SAP-Agent
- NWLink IPX/SPX oder ein kompatibles Transportprotokoll

Wenn Communications Server auf einer primären Steuereinheit oder einer Ausweichsteuereinheit ausgeführt wird, müssen den Benutzern Zugriffsberechtigungen in der Gruppe IBMCSAPI erteilt werden, damit sie sich lokal auf dem Server anmelden können.

Planung für Zugriff auf Daten, die mit anderer Software erstellt wurde

Dieses Kapitel enthält Informationen zu Communications Server-Funktionen für den Zugriff auf Host-Informationen.

AS/400 OLE DB Provider

Anwendungen, die OLE-DB oder ActiveX verwenden, können über Communications Server auf Satzebene auf Dateien auf AS/400-Systemen zugreifen. Für den Zugriff auf AS/400-Dateien muß das ferne AS/400-System, auf dem sich die Dateien befinden, als Partner-LU definiert werden.

Der AS/400 OLE DB Provider kann als Communications Server-Komponente oder als Komponente des SNA-API-Clients für Windows 95 installiert werden. Er kann auch als Komponente des SNA-API-Clients für Windows NT installiert werden; dazu ist jedoch Windows NT Workstation oder Server ab Version 4.0 erforderlich. Wenn Microsoft Data Access Components (MDAC) Version 1.5 nicht installiert ist, führt Communications Server diese Installation automatisch aus, wenn diese Komponente installiert wird.

Wird AS/400 OLE DB Provider auf einer Maschine installiert, auf der bereits Client Access Version 3 Release 2 MD (oder niedriger) installiert ist, werden einige Client Access-Funktionen inaktiviert (dazu gehören die Unterstützung für ActiveX sowie OLE-DB-Programme, die mit Client Access auf Datenwarteschlangen, ferne Befehle, verteilte Programmaufrufe, gespeicherte Prozeduren und SQL-Anweisungen von AS/400 zugreifen).

Wenn diese Funktionen auch unter Client Access verfügbar sein sollen, darf die Komponente AS/400 OLE DB Provider nicht während der Installation von Communications Server installiert werden. Wurde die Komponente AS/400 OLE DB Provider während der Communications Server-Installation installiert, können die inaktivierten Client Access-Funktionen durch erneutes Installieren von Client Access wieder verfügbar gemacht werden. Wenn Client Access erneut installiert wird, ist es jedoch nicht möglich, AS/400 OLE DB Provider unter Communications Server zu verwenden.

Erfolgt die Installation von Client Access nach dem Installieren von Communications Server, werden die Daten der Registrierung überschrieben. Soll AS/400 OLE DB Provider unter Communications Server verwendet werden, nachdem Client Access installiert wurde, können durch Ausführen des Hilfsprogramms REGSVR32.EXE an den Dateien cwbzzodb.dll und cwbzzidx.dll die Registrierungsinformationen von AS/400 OLE DB Provider wiederhergestellt werden.

Mit AS/400 OLE DB Provider können Windows 95- und Windows NT 4.0-Clients über Communications Server mit einem oder mehreren AS/400-Systemen verbunden werden, wie in Abb. 27 auf Seite 112 gezeigt. Durch diese Konfiguration erhalten Clients, auf denen AS/400 OLE DB Provider installiert ist, Zugriff auf bestimmte Datensätze in Dateien auf dem AS/400-System.

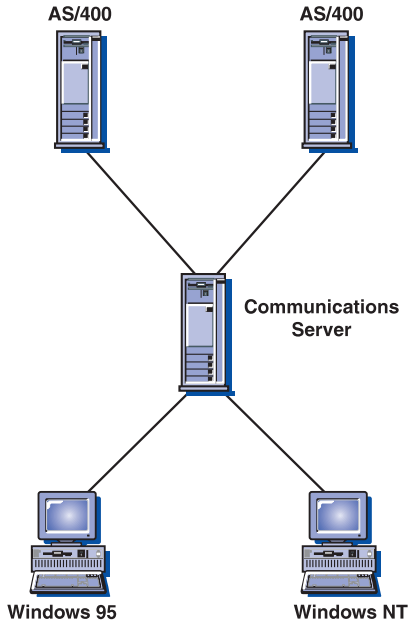


Abbildung 27. AS/400 OLE DB Provider

In dieser Abbildung ist AS/400 OLE DB Provider auf beiden Clients installiert. Die Funktion kann auch auf dem Server installiert und verwendet werden.

Dokumentation zu dieser Funktion sowie Informationen zum Entwickeln von OLE-DB- und ActiveX-Anwendungen mit Client Access enthält das Verzeichnis `csnt\sdk\as400_oledb`.

AS/400-Server für gemeinsam benutzte Ordner

Auf dem Server können Platteneinheiten erstellt werden, die den Datenaustausch mit AS/400-Ordnern über AS/400 IFS (Integrated File System) ermöglichen. Wenn diese Platteneinheiten vom Server zur gemeinsamen Benutzung bereitgestellt werden, können Clients ohne weitere Konfigurationsschritte und Codeinstallation auf der Client-Maschine Verbindung zu diesen Einheiten herstellen und über diese Einheiten auf AS/400-Laufwerke zugreifen. Auf diese Weise können viele Clients die Verbindung zu Ordnern in dem AS/400-System genau so herstellen, als wären sie Laufwerke der lokalen Datenstation.

Unterstützung für gemeinsam benutzte Ordner kann über die Anwendung **Knotenkonfiguration** eingerichtet werden. Wenn eine Platteneinheit für den Benutzer verfügbar ist, fungiert sie als vom System unterstütztes Plattenlaufwerk. Zum Steuern dieser Einheit können die von Windows NT bereitgestellten Schnittstellen verwendet werden. Benutzer können das Laufwerk innerhalb des Netzes gemeinsam benutzen, haben jedoch individuelle Zugriffsberechtigungen beibehalten.

Für den AS/400-Server für gemeinsam benutzte Ordner ist OS/400 ab Version 3.1 erforderlich.

Host Publisher

Host Publisher ermöglicht den Web-Zugriff auf umfangreiche Web-Sites mit dynamischem Inhalt. Mit Host Publisher kann auf Daten auf S/390- oder AS/400-Hosts zugegriffen werden, diese Daten können dann auf Web-Seiten veröffentlicht werden, die dynamisch im Design des Benutzers erstellt wurden.

Host Publisher umfaßt mehrere Komponenten. Beschreibungen der Komponenten und Informationen zur Installation von Host Publisher können im Online-Buch *Einstieg* nachgelesen werden.

Über drei Registrierungswerte kann die Verwendung vorhandener JITs und ein spezifischer Host Publisher-Klassenpfad gesteuert werden. Potentiell inkompatible Java-Implementierungen können auf derselben Maschine wie Host Publisher existieren.

JITCompiler Dieser Wert gibt an, welcher JIT-Compiler für das Host Publisher-Exemplar des VM-Systems verwendet werden soll. Er legt das Systemmerkmal **java.compiler** fest, das darüber entscheidet, wie das VM-System JITs lädt und verwendet.

EnableJIT Dieser Boolesche Werte gibt an, ob das in **JITCompiler** angegebene JIT verwendet wird.

Classpath Dieser Wert gibt den für das VM-System festgelegten Klassenpfad an. Wird der Wert nicht oder als Nullwert angegeben, wird die Systemumgebungsvariable verwendet.

Auf die Einträge **JITCompiler**, **EnableJIT** und **Classpath** kann im Windows NT-Registrierungseditor unter dem Schlüssel

```
HKEY_LOCAL_MACHINE/Software/IBM/Host Publisher/Config
```

zugegriffen werden.

Da Java VM bei der Initialisierung von Host Publisher initialisiert wird, müssen PageServer und Integrator erneut gestartet werden, damit die Änderungen der Registrierung wirksam werden.

Verarbeitung von Web-Seiten

Nachdem mit **Integrator** eine Web-Seite erstellt wurde, muß die Bibliothek (Library) implementiert werden, damit sie von Clients mit Hilfe eines Web-Browsers im Web angezeigt werden kann.

Wenn ein Client einen Knopf auf der Web-Seite anklickt, wird eine Anforderung vom Client-System an einen Web-Server übermittelt. Der Web-Server nimmt Verbindung zum **Adapter** auf. Dieser stellt fest, daß sich die Anforderung auf eine dynamische Web-Seite bezieht, die sich als Web Library-Datei auf einer Netzmaschine befindet, auf der ein **PageServer** installiert ist.

Der **Dispatcher** stellt fest, welcher **PageServer** die Anforderung bearbeiten sollte, und der **Adapter** leitet die Anforderung an den empfohlenen **PageServer** weiter.

Der **PageServer** lokalisiert die Seite in einer seiner Libraries und startet die Verarbeitung der Seite. Er durchsucht die Datei nach DYNA-Befehlen.

- Wenn DYNA-Befehle gefunden werden, durchsucht der **PageServer** die Web Library, um die Position der den DYNA-Befehlen zugeordneten Integrationsobjekte (Integration Objects) festzustellen, und verarbeitet die Befehle, um den dynamischen Inhalt zu extrahieren. Der **PageServer** verarbeitet alle Prozeduren auf der Server-Seite, ersetzt die DYNA-Befehle durch HTML-Befehle, die die aus der Quelle extrahierten Informationen enthalten, und gibt die Seite an den **Adapter** zurück.
- Werden keine DYNA-Befehle gefunden, erstellt der **PageServer** eine Datei und sendet diese an den **Adapter**.

Der **Adapter** sendet die Seite an den Web-Server, der sie an die Client-Maschine weiterleitet.

Konfiguration für Anwendungen mit hoher Verfügbarkeit

Eine Web-Site kann problemlos erweitert werden, wenn die Aktivitäten zunehmen. Um sicherzustellen, daß Clients in einer fehlertoleranten Umgebung arbeiten, kann der **Dispatcher** mit Host Publisher so konfiguriert werden, daß die Verarbeitung mit Ausweichkomponenten fortgesetzt werden kann.

Der **Dispatcher** kann so konfiguriert werden, daß er sowohl über primäre als auch über sekundäre Exemplare verfügt. Fällt der primäre **Dispatcher** aus irgendwelchen Gründen aus, versuchen **Adapter** und **PageServer** sofort, eine Verbindung zum sekundären **Dispatcher** herzustellen. Jeder **Dispatcher** kann mehrere Web-Server unterstützen.

Host Publisher Libraries können auf mehreren **PageServern** vervielfältigt werden. **Dispatcher** und **PageServer** übernehmen zusammen den Lastausgleich und die Ressourcenzuordnung. Client-Anforderungen werden an den **PageServer** mit den meisten verfügbaren Ressourcen übergeben. Bei Zunahme der Client-Anforderungen können zusätzliche **PageServer** gestartet werden.

Client-Zugriff auf CICS-Hosts

Im Lieferumfang von Communications Server ist CICS-Client für Windows NT-Software enthalten, die Clients den Verbindungsaufbau zu CICS-Hosts über Communications Server ermöglicht.

In Abb. 29 ist ein Beispiel dafür dargestellt, wie ein CICS-Client für den Zugriff auf Informationen konfiguriert werden kann, die sich in einer CICS-Datenbank auf einem Host befinden.

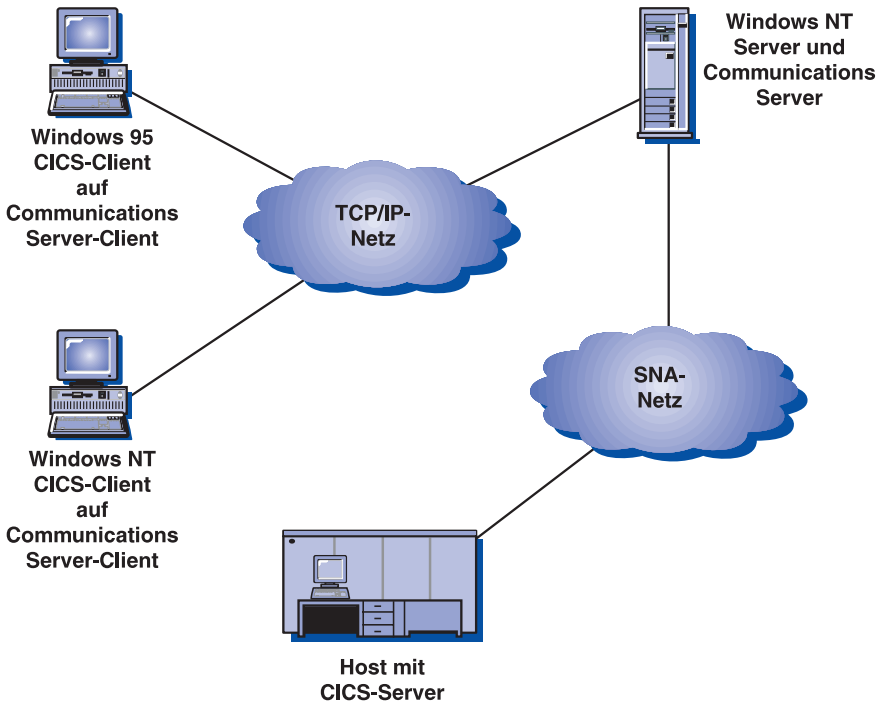


Abbildung 29. CICS-Client-Umgebung

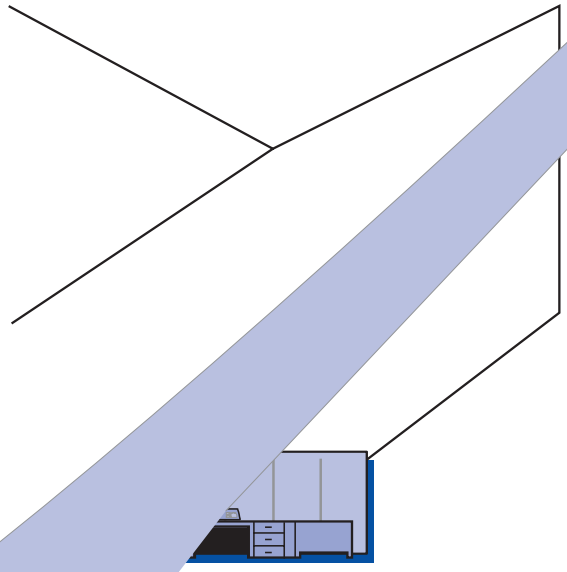
Weitere Informationen zum Konfigurieren von CICS-Clients können im Handbuch *CICS Clients Administration* nachgelesen werden. Dieses Handbuch ist im Internet unter folgender Adresse verfügbar:

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

…ellt wurde

…ations Server ist MQSeries Client für Windows
…ients den Verbindungsaufbau zu MQ-Hosts über
…möglicht.

…spiel dafür dargestellt, wie ein MQSeries Client für den …
…konfiguriert werden kann, die sich in einer MQSeries-Da… …nk
…befinden.

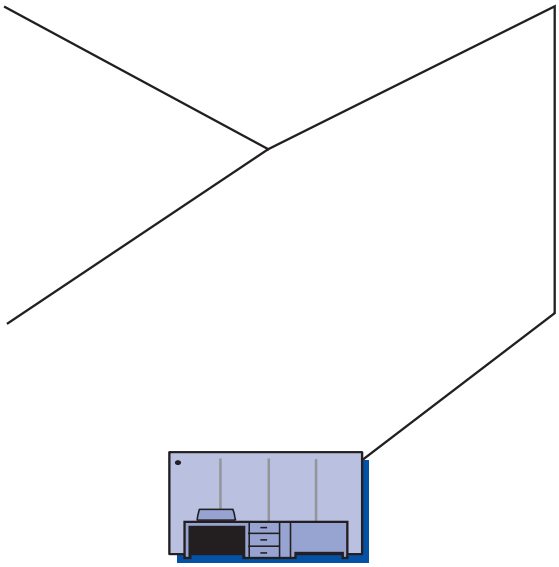


Client-Zugriff auf DB2-Hosts

Communications Server beinhaltet „Testsoftware“ für DB2 Connect Enterprise Edition, ein Host-Konnektivitätsprodukt für mehrere Benutzer. DB2 Connect Enterprise Edition kann auf einem Windows NT-Server installiert werden.

Communications Server beinhaltet außerdem DB2 Client Application Enabler (CAE) für den Client-Zugriff auf den Host. DB2 CAE kann auf einer Client-Maschine unter Windows 3.1, Windows 95, Windows NT oder OS/2 installiert werden.

In Abb. 31 ist ein Beispiel dafür dargestellt, wie DB2 Connect Enterprise Edition für den Zugriff auf Informationen konfiguriert werden kann, die sich in einer DB2-Datenbank auf einem Host befinden.



Planung für HPR

Communications Server unterstützt HPR über Enterprise Extender- (IP), SDLC- (Synchronous Data Link Control- synchrone Datenübertragungssteuerung), LAN-, WAN-, Kanal-, MPC- (Multi-Path Channel) und X.25-Verbindungen.

Automatic Network Routing (ANR) von HPR reduziert die Speicher- und Verarbeitungsanforderungen in Zwischenknoten auf ein Minimum. Dies ist für Hochgeschwindigkeitsnetze mit niedrigen Fehlerraten eine Verbesserung gegenüber der Weitervermittlung eines Sitzungsleitwegs von APPN.

HPR-Unterstützung von Communications Server umfaßt Unterstützung für RTP (Rapid Transport Protocol) und ANR (Automatic Network Routing).

HPR-Verbindungsmerkmale

Um die oben aufgeführten Vorteile bereitstellen zu können, setzt HPR voraus, daß bei Datenübertragungsverbindungen selten Rahmen verlorengehen. HPR wird nach Bedingungen, die zu verlorengegangenen Rahmen führen, fortgesetzt; wenn die Bedingungen jedoch über einen längeren Zeitraum bestehenbleiben, geht HPR davon aus, daß die Netzüberlastung zu groß ist, und der HPR-Durchsatz wird gesenkt. Nur bei entsprechender Konfiguration des Sendeknotens, der Verbindung zwischen den beiden Knoten und des Empfangsknotens wird ein guter HPR-Durchsatz erreicht.

Anmerkung: Möglicherweise ist es wünschenswert, ERP-Werte in den Fällen zu definieren, in denen LAN-Leitungseinrichtungen einen hohen Rahmenverlust haben.

Sendeknoten

Die normalerweise von HPR verwendeten Adapter senden Rahmen an die Verbindung mit niedrigen Fehlerraten. Bei Ethernet-Netzen wird HPR eingeschränkt, wenn das LAN überlastet ist (wenn z. B. die Auslastung ca. 30 bis 40 % über der nominalen Ethernet-Geschwindigkeit liegt). Bei Frame-Relay-Übertragungen sind die Funktionen so zu konfigurieren, daß einzelne Verbindungen mit der Geschwindigkeit der Anschlußleitung übertragen können, ohne eine Überlastung im Frame Relay-Netz zu verursachen.

Leitungseinrichtungen

LAN-Einrichtungen können sehr komplex sein: angefangen bei einer großen Anzahl von Datenstationen, die ein einzelnes LAN-Segment gemeinsam benutzen, über Brücken zwischen LAN-Segmenten (eventuell mit verborgenen Verbindungen mit niedrigerer Geschwindigkeit) bis hin zu simulierten LAN-Segmenten, die über komplexe Teilnetze operieren. Ziel ist es, daß möglichst wenig Rahmen verlorengehen. WAN-Verbindungen zwischen geteilten Brücken müssen z. B. Einrichtungen mit niedriger Fehlerrate oder eine Fehlerbehebung auf Verbindungsebene zwischen den Brücken verwenden. Außerdem müssen z. B. auch Bedingungen, die zu überlaufenden Brückenpuffern führen (eine große Menge an Rundsendebetriebsoperationen oder ein hohes Aufkommen von Rundsenderahmen), vermieden werden.

Empfangsknoten

Die normalerweise von HPR verwendeten Adapter empfangen Rahmen von der Verbindung mit niedriger Fehlerrate. Der Empfang von Rahmen schlägt jedoch bei einigen Adaptern fehl, wenn die aufeinanderfolgenden Rahmen zu schnell ankommen. Der beste HPR-Durchsatz wird erreicht, wenn der empfangende Adapter den Datenaustausch ohne fehlende ankommende Rahmen ausführen kann.

Hat das Netz eine hohe Fehlerrate, stellen Systemadministratoren möglicherweise einen niedrigeren Durchsatz bei HPR-Verbindungen fest als erwartet.

Überlegungen zu HPR

Die HPR-Funktionen können durch zusätzliche Daten in den Rahmenkopfzeilen eingerichtet werden. Werden die HPR-Funktionen nicht benötigt, wird die Netzleistung möglicherweise durch den zusätzlichen Systemaufwand reduziert. Bestehen jedoch Zwischenknoten oder Alternativleitwege, sind die HPR-Funktionen von Vorteil. Ist ein hoher Durchsatz zwischen zwei Knoten erforderlich, die durch eine einzige Leitung ohne unterbrechungsfreie Wiederherstellung bei einer Leitungsstörung miteinander verbunden sind, sollte HPR bei der Konfiguration dieser Verbindung inaktiviert werden.

Bei HPR werden Prioritätswarteschlangen implementiert. Im allgemeinen ist der interaktive Datenaustausch im Netz schneller als der Datenaustausch bei Stapelbetrieb mit niedriger Priorität. Adapter reihen Rahmen ohne Berücksichtigung der Priorität ein und können möglicherweise einen Konflikt mit der HPR-Prioritätswarteschlange verursachen. Daher ist es unter Umständen notwendig, die Warteschlangenlänge des Adapters zu reduzieren, um zu verhindern, daß Datenverkehr mit niedriger Priorität Datenverkehr mit hoher Priorität verzögert. (Anweisungen zur Einstellung der Wartenschlangenlänge von Adaptern können der Adapterdokumentation entnommen werden.)

Viele PCs haben heutzutage eine Funktion zur erweiterten Stromverbrauchssteuerung, die die Stromversorgung von Einheiten (wie Plattenlaufwerken) aussetzt und die Taktgeberrate einer CPU erheblich senkt, um Strom zu sparen, wenn die Tastatur oder Maus nicht verwendet wird. Bei einer Datenstation ist dies eine nützliche Funktion, bei einer Server-Plattform kann diese Funktion jedoch zu einem Zeitpunkt einsetzen, in dem Daten von einem Adapter an einen anderen weitergeleitet werden (und keine Plattenaktivität auftritt). Beim Communications Server wird die erweiterte Stromverbrauchssteuerung und Hardware-Stromverbrauchssteuerung durch Aufrufen der BIOS-Konfiguration beim Booten (normalerweise durch Drücken von F1 beim Initialisieren der Hardware) und Inaktivieren der beiden Optionen inaktiviert.

HPR verwendet mehr LAN-Adapterspeicher aufgrund von höherer Leistungsfähigkeit und der Warteschlangenfunktion. Viele Adapter für gemeinsam benutzten Arbeitsspeicher verwenden standardmäßig 8 Kilobyte gemeinsam benutzten Arbeitsspeicher. Die Größe des gemeinsam benutzten Arbeitsspeichers muß 16 Kilobyte betragen. Informationen zur Anpassung dieser Konfiguration enthält das Handbuch zur Adapterkonfiguration. Dieser Wert wird entweder im Maschinen-BIOS oder durch die Adapterschalterstellung festgelegt.

Anmerkung: Wird der gemeinsam benutzte Arbeitsspeicher nicht auf 16 Kilobyte erhöht, nimmt die Netzleistung ab.

Der gemeinsam benutzte Arbeitsspeicher sollte nicht auf über 16 Kilobyte gesetzt werden, weil 16 Kilobyte die optimale Einstellung für den Adapterspeicher ist.

Fallen HPR-Verbindungen bei hohem Datenaustauschvolumen aus, können die Empfangszeitgeber auf einen höheren Wert gesetzt werden. Dadurch haben die Verbindungen mehr Zeit, eine Bestätigung für gesendete Rahmen zu empfangen.

Bei SDLC-Verbindungen ist dies der primäre Empfangszeitgeber. Der Empfangszeitgeber kann entweder bei der DLC oder bei der Anweisung einer logischen Verbindung gesetzt werden.

Um den minimalen Empfangszeitgeberwert in Zehnteln von Sekunden zu berechnen, folgende Formel verwenden:

```
[(anz_sendefenster * max_größe_des_i_felds * 8) /tatsächl_Übertragungsgeschw]* 10
```

Überlegungen zur Optimierung von Parametern bei LAN-DLCs

Es ist möglich, acht Parameter anzugeben, um festzulegen, wie schnell Communications Server die Wiederherstellung und Fehler von LAN-Verbindungen verarbeitet. Möglicherweise müssen diese Parameter geändert werden, um die besten Ergebnisse zu erzielen, wenn langsame Verbindungen, HPR- oder Sicherungs-Host-Verbindungen verwendet werden.

Folgende Parameter sollten bei der Definition einer LAN-Einheit über die **Knotenkonfiguration** verwendet werden:

Über die Indexzunge **Erweitert**:

Testwiederholungsintervall
Das Testwiederholungsintervall gibt an, wieviel Zeit zwischen den Versuchen vergeht, die angrenzende Verbindungsstation im lokalen Netz (LAN) zu lokalisieren. Wie viele Versuche ausgeführt werden, hängt von dem für das Testwiederholungslimit angegebenen Wert ab.

Der Standardwert ist 8.

Testwiederholungslimit
Das Testwiederholungslimit gibt an, wie viele Versuche zum Lokalisieren der angrenzenden Verbindungsstation im lokalen Netz (LAN) maximal ausgeführt werden, wenn innerhalb der als Testwiederholungsintervall angegebenen Zeit keine Bestätigung empfangen wird.

Der Standardwert ist 5.

Maximale PIU-Größe
Die maximale Größe der Pfadinformationseinheit (PIU - Path Information Unit) ist die maximale Anzahl Byte, die in dem von SNA-Sitzungen für diese Verbindung verwendeten Datenpuffer enthalten sind. Wenn der Wert für die maximale PIU-Größe die vom lokalen Einheitentreiber unterstützte Rahmengröße überschreitet, wird dieser Wert auf die unterstützte Rahmengröße reduziert.

Der Standardwert ist 65535.

Über die Indexzunge **Leistung**:

Zeitlimit für Inaktivität Das Zeitlimit für Inaktivität gibt an, wie lange der LAN-Einheitentreiber auf den Empfang eines Rahmens wartet, bevor die Verbindung als inaktiv deklariert wird.

Der Standardwert ist 30 Sekunden.

Verzögerung der Empfangsbestätigung Die Verzögerung der Empfangsbestätigung gibt an, wie lange die LAN-Einheit die Antwort auf einen empfangenen Rahmen zurückhält, damit weitere Rahmen empfangen und mit der gleichen Nachricht 'Request Ready' (RR) bestätigt werden können.

Der Standardwert ist 100 Millisekunden.

Zeitlimit für Aufrufantwort

Das Zeitlimit für Aufrufantwort gibt an, wie lange die LAN-Einheit auf eine Antwort für einen mit gesetztem POLL-Bit übertragenen Rahmen wartet.

Der Standardwert ist 8000 Millisekunden.

Erwartete anstehende Übertragungen Dieser Parameter gibt an, wie viele Rahmen die LAN-Einheit maximal in die Warteschlange für eine Verbindungsstation einreiht, bevor die Nachricht 'Receive Not Ready' (RNR) an die angrenzende Verbindungsstation übermittelt wird.

Der Standardwert ist 16 Rahmen.

Anzahl Empfangspuffer Die Anzahl Empfangspuffer gibt an, wie viele Speicherpuffer dafür reserviert werden, vom Host erhaltene Daten bis zu ihrer Verarbeitung zwischenzuspeichern. Jeder Puffer hat die Größe der PIU.

Der Standardwert ist 32 Puffer.

HPR-Pfadumschaltungsverarbeitung

HPR stellt eine störungsfreie Pfadumschaltung auf eine andere Verbindung zur Verfügung, wenn eine Verbindung fehlschlägt. Bevor die Pfadumschaltung erfolgt, wird erneut versucht, die fehlgeschlagene Verbindung herzustellen. Die für das Fehlschlagen einer Verbindung und für den Zeitpunkt der Pfadumschaltung maßgeblichen Parameter werden im folgenden erläutert.

Bei Erreichen des als **Zeitlimit für Inaktivität** angegebenen Werts wird ein Keepalive-Rahmen gesendet. Der Standardwert für das **Zeitlimit für Inaktivität** beträgt 30 Sekunden.

Der als **Zeitlimit für Aufrufantwort** angegebene Wert legt fest, wie lange die Einheit auf eine Antwort für den Keepalive-Rahmen wartet. Der Standardwert für das **Zeitlimit für Aufrufantwort** beträgt acht Sekunden (8 000 Millisekunden). Für jeden Keepalive-Rahmen werden 10 Wiederholungsversuche ausgeführt. Dieser Wiederholungszähler kann nicht geändert werden.

Erfolgt keine Reaktion auf den Keepalive-Rahmen, werden TEST-Befehle an das Partnersystem gesendet. Der für **Testwiederholungsintervall** angegebene Wert legt fest, wieviel Zeit zwischen den TEST-Befehlen vergeht, und der Wert für **Testwiederholungslimit** legt fest, wie viele TEST-Befehle maximal gesendet werden. Der Standardwert für das **Testwiederholungsintervall** beträgt 8 Sekunden, und der Standardwert für das **Testwiederholungslimit** sind fünf Versuche.

Nach welcher Zeit eine Verbindung als fehlgeschlagen deklariert und eine Pfadumschaltung eingeleitet wird, läßt sich wie folgt berechnen:

```
(Zeitlimit für Inaktivität) + (Zeitlimit für Aufrufantwort * 10 Wiederhlgen) +
          (Testwiederholungsintervall * Testwiederholungslimit) + 1
```

Bei Verwendung der Standardwerte dieser Parameter kann es bis zu 151 Sekunden dauern, bis eine Verbindung als fehlgeschlagen deklariert und eine Pfadumschaltung eingeleitet wird.

```
(30 Sekunden) + (8 Sekunden * 10 Wiederholungen) +
           (8 Sekunden * 5 Versuche) + 1 = 151 Sekunden
```

Dauert die Pfadumschaltung mit HPR lange (oder schlägt fehl), wenn eine Verbindung fehlschlägt, kann diese Zeit durch Verringern der Werte für die in der Berechnung verwendeten Parameter verkürzt werden.

Planung für SNA-Gateway

Der SNA-Gateway unterstützt:

- Verschiedene SNA-Protokolle
- Verschiedene untergeordnete Datenstationen
- Verschiedene Verbindungsarten zwischen dem Gateway und dem Host
- Zusammenschluß von LUs (Sitzungen) in einem Pool auf dem Gateway
- Definition impliziter Datenstationen
- Dynamisches Ändern oder Hinzufügen von Definitionen für inaktive Datenstationen
- Mehrere Hosts gleichzeitig
- Verschiedene Verbindungsarten (die kombiniert werden können) zwischen den Datenstationen und dem Gateway

Anweisungen zur Konfiguration des SNA-Gateways mit der **Knotenkonfiguration** enthält die Dokumentation *Einstieg*.

Unterstützte Verbindungen zu Datenstationen

Der SNA-Gateway unterstützt Datenstationen, die folgendermaßen angeschlossen sind:

- LAN-Konnektivitäten
  - Token-Ring
  - Ethernet
  - ATM (LAN-Emulation)
- Frame Relay
- SDLC
  - Asynchron
  - Synchron
  - Hayes Autosync
  - Mehrpunktverbindung (Primär)
- X.25-Netz
- AnyNet TCP/IP (für von Microsoft TCP/IP unterstützte Konnektivitäten)
- ISDN-Verbindungen

Der SNA-Gateway kann für jede definierte PU bis zu 254 LUs unterstützen. Für jede Host-Verbindung kann eine andere PU definiert werden. Die LUs werden von den untergeordneten Datenstationen für den Verbindungsaufbau zum Host verwendet. Wie viele untergeordnete Datenstationen unterstützt werden, hängt von verschiedenen Faktoren ab (z. B. von der Konnektivitätsart und der Anzahl der Adapter auf dem Gateway). Beispiel: Wenn auf dem Gateway ein LAN-Adapter vorhanden ist, kann eine Host-Verbindung mit 254 LUs von 253 untergeordneten Datenstationen gleichzeitig verwendet werden. Bei zwei Adaptern werden doppelt so viele untergeordnete Datenstationen unterstützt.

SDLC-Datenstationsverbindungen

SDLC stellt Verbindungen in Punkt-zu-Punkt- und Mehrpunktverbindungskonfigurationen her. Nachdem die Konfiguration abgeschlossen ist, müssen keine weiteren Besonderheiten beachtet werden, um SDLC zwischen der Datenstation und dem Gateway auszuführen.

Bei der Einrichtung von sekundären Datenstationen mit Mehrpunktverbindung müssen die verschiedenen Faktoren berücksichtigt werden, die die Durchlaufzeit für Sendeaufrufe steuern. Es gibt physische Einschränkungen, die die Schnelligkeit beeinflussen können, mit der die primäre Datenstation die sekundäre Datenstation aufrufen kann, die am weitesten entfernt ist. Die Verwendung derselben Parameter bei der Definition aller sekundären Datenstationen vereinfacht die folgende Berechnung.

Zur Berechnung der Mindestzeitspanne für Inaktivität in Sekunden muß folgende Formel verwendet werden:

```
     NS * (SW + RW) * (IS + 2) / (LS / 8)
Dabei gilt folgendes:
     NS  =  Number of Stations (Anzahl Stationen)
     SW  =  Send window size (Größe des Sendefensters)
     RW  =  Receive window size (Größe des Empfangsfensters)
     IS  =  I-field size (Größe des I-Felds)
     LS  =  Line speed (Bit/s) (Übertragungsgeschwindigkeit)
```

Stimmen diese Werte nicht für alle sekundären Datenstationen überein, müssen für jede Gruppe oder Datenstation eine separate Berechnung ausgeführt und die jeweiligen Werte addiert werden, um den korrekten Wert für den Inaktivitätszeitgeber zu bestimmen.

Bei einer Mehrpunktverbindung mit 16 sekundären Datenstationen und einer Geschwindigkeit von 14,4 KBit/s, wobei bei allen Datenstationen die Größe des Sendefensters auf 7, die Größe des Empfangsfensters auf 7 und die Größe des I-Felds auf 521 eingestellt ist, sieht die Berechnung für den Inaktivitätszeitgeber wie folgt aus:

```
16 * (7 + 7) * (521 + 2) / (14400 / 8) = 65,1 Sekunden
```

Anmerkung: Für einen Puffer müssen immer noch ein paar zusätzliche Sekunden hinzugerechnet werden.

X.25-Datenstationsverbindungen

Wird der SNA-Gateway zur ausschließlichen Verwendung fester virtueller X.25-Verbindungen (PVCs - Permanent Virtual Circuits) zu den Datenstationen konfiguriert, empfiehlt es sich, alle Datenstations- und Gateway-PVCs mit zu vereinbarenden Funktionen für die Verbindungsstation zu konfigurieren. Geschieht dies nicht, sind die Datenstationen eventuell nicht in der Lage, die X.25-PVCs zum Gateway herzustellen.

Weitere Informationen zu PVC-Verbindungen und zur Konfiguration enthält der Abschnitt "Planung für X.25".

Unterstützte Verbindungen zu Hosts

Der SNA-Gateway unterstützt die folgenden Verbindungen zum Host:

- LAN-Konnektivitäten
  - Token-Ring
  - Ethernet
  - ATM (LAN-Emulation)
- Frame Relay
- SDLC
  - Synchron
  - Hayes Autosync
-

Überlegungen zum Host

Für die Planung der Host-Verbindung ist folgendes zu beachten:

- Wenn die Umgebung einen Netzsteuerpunkt (NCP - Network Control Point) verwendet, muß der **MAXLU**-Wert des Makros **LINE** für 37*xx* NCPGEN mindestens der Anzahl der LUs im Communications Server entsprechen.
- VTAM-Benutzer können das Zeitintervall steuern, in dem VTAM Daten in den Puffer schreibt, bevor sie zur Steuereinheit gesendet werden (Coattailing). Durch Angabe des VTAM-Coattailing-Parameters **DELAY=0** bei einer PU-Definition kann möglicherweise die Antwortzeit des Hosts beim Senden verkürzt werden, wodurch die Belastung für den Host-Prozessor zunimmt.

  Wird ein DELAY-Wert angegeben, der ungleich Null ist, muß der Host-Prozessor weniger Instruktionen ausführen; jedoch steigt damit die Antwortzeit beim Empfangen an der Communications Server-Datenstation.

  Es ist empfehlenswert, das Coattailing mit dem Standardwert von 0,2 Sekunden zu beginnen. Eine Verzögerung von 0,2 Sekunden hat einen geringen Einfluß auf die Antwortzeit, bei einem Durchsatz von etwa einer Transaktion pro Sekunde oder höher setzt das Coattailing ein.
- Obwohl jede untergeordnete SNA-Datenstation im LAN eine PU mit einer Reihe eigener LUs implementiert, wird der SNA-Gateway so implementiert, daß der Host nur die Gateway-PU zur Kenntnis nimmt. Deshalb wird nur eine PU-Definition auf dem Host codiert. Diese PU-Definition enthält die LUs für ***alle*** Stationen im LAN, die über diesen Gateway eine Verbindung zum Host herstellen.

  Wenn das Host-VTAM selbstdefinierende LUs (SDDLU) unterstützt, kann diese Funktion genutzt werden. Beim Konfigurieren von Host-LUs eine LU-Modellart oder einen LU-Modellnamen angeben, der mit dem Operanden LUSEED übereinstimmt, der im VTAM-Wählleitungshauptknoten definiert und von der VTAM-SDDLU-Beendigungsroutine verwendet wird.

Konfiguration über LAN-Zieladressen

Wird eine der unterstützten LAN-Verbindungen zwischen dem Gateway und dem Host oder zwischen dem Gateway und einer explizit definierten Datenstation verwendet, muß eine Zieladresse zur Verfügung gestellt werden. Bei der Festlegung der richtigen Zieladresse, die in jedes Profil eingetragen werden muß, ist zu beachten, daß sich die richtige Perspektive für beide Adressen aus der Sicht des SNA-Gateways ergibt. Abb. 32 zeigt diese Sicht.

Explizite und implizite Verbindungen verwenden

Es gibt zwei Arten von untergeordneten Datenstationen, die von Gateways unterstützt werden: explizite und implizite. Explizite Datenstationen sind Datenstationen, für die Zieladressen über eine bestimmte DLC-Art definiert sind (z. B. Token-Ring-Netz und SDLC). Zur Konfiguration expliziter Datenstationen muß die Zieladresse oder der vollständig qualifizierte Name des Nachbarsteuerpunkts oder die Nachbarknoten-ID jeder Datenstation bekannt sein und für jede Datenstation eine logische Verbindung zum Gateway definiert sein. LUs, die für explizite Datenstationen definiert sind, können zu einem Pool gehören oder dediziert sein.

Implizite Datenstationen sind einfacher zu konfigurieren; sie können jedoch nur LUs in einem Pool verwenden.

Anstatt eine Verbindung zu jeder Datenstation zu definieren, die den Gateway verwendet, können ein oder mehrere Host-LU-Pools definiert werden und anschließend die Einheiten (DLCs) für die Datenstationsverbindungen konfiguriert werden. Eine implizite Client-Schablone konfigurieren, die als Modell für die LU-Definitionen aller Datenstationen verwendet wird, die Verbindungen zum Gateway herstellen und mit keiner expliziten Definition übereinstimmen. Wenn z. B. jede Datenstation in einem Ethernet-LAN zwei konfigurierte 3270-Sitzungen mit den NAU-Adressen 2 und 3 hat, muß eine Client-Schablone mit zwei LUs (eine für Adresse 2 und eine für Adresse 3) konfiguriert werden. Wenn beide Adressen für Sitzungen zu einem einzigen Host verwendet werden, sind beide Adressen dem gleichen Host-Pool zuzuordnen. Wird jedoch Adresse 2 für die Verbindung zu HOST_A und Adresse 3 für die Verbindung zu HOST_B verwendet, ist jede Adresse dem entsprechenden Host-Pool zuzuordnen. In diesem Beispiel wird jedesmal, wenn eine Datenstation über Ethernet eine Verbindung zum Gateway herstellt und diese Verbindung nicht mit einer expliziten Definition übereinstimmt, dynamisch eine Verbindung hergestellt, und die beiden LUs für NAU 2 und 3 werden vom Host-LU-Pool zugeordnet.

Bei impliziten Datenstationen müssen Benutzer, die eine Verbindung mit dem Gateway aufbauen, nur die Adapteradresse der Gateway-DLC kennen, die für die impliziten Datenstationen konfiguriert ist, und wissen, welche NAU-Werte auf dem Gateway definiert wurden. Diese NAU-Werte müssen zur Definition der 3270-Sitzungen und der logischen Drucker verwendet werden.

Eine mit Communications Server verbundene untergeordnete Personal Communications-Datenstation kann über die LAN-Discovery-Funktion nach dem Gruppennamen `IGO2HOST` suchen, um die Adapteradresse zu finden.

SNA-Gateway-Durchsatz

Der Durchsatz über einen Gateway hängt von vielen Faktoren ab, einschließlich:

- Konfiguration des Gateways
- Verbindung zum Host oder zu den Hosts
- Gesamter Verarbeitungsaufwand auf jedem Host
- Verbindungen zu den unterstützten Datenstationen
- Konfigurationen der unterstützten Datenstationen
- Anzahl der unterstützten Datenstationen
- Anzahl der Sitzungen mit jeder Datenstation
- SNA-Übertragungspriorität
- Flußsteuerung
- Nachrichtendosierungsfenster für alle Sitzungen
- Datenaustausch in Nicht-Gateway-Sitzungen

Die Verwendung einer Datenstation, die einen Software-Gateway für andere Funktionen implementiert, kann ebenfalls den Durchsatz des Gateways beeinträchtigen.

Wird der Durchsatz von keinem der oben genannten Faktoren beeinträchtigt, sollte eine einzelne Datenstation, die unterstützte SNA-Protokolle verwendet, keinen merklichen Unterschied im Durchsatz zwischen einer direkten Verbindung zum Host und einer indirekten Verbindung mittels LAN über einen mit dem Host verbundenen SNA-Gateway bemerken. Wenn die Host-Verbindungen auf dem Gateway aktiv sind, kann die Aktivierung der Datenstation eventuell sogar verbessert werden, indem Verzögerungen durch den Host-Systemaufwand beseitigt werden. Durch die vielen verschiedenen Faktoren kann es ratsam sein, in der Betriebsumgebung Leistungstests durchzuführen, um die gewünschte Ausgewogenheit zwischen Funktionsfähigkeit und Durchsatz zu erreichen.

DLUR-Überlegungen

Die Verwendung des DLUR für die Verbindung zum Host ermöglicht größere Flexibilität bei der Plazierung des SNA-Gateways. Die Verbindung zum Host kann durch jedes APPN-Netz führen und ist nicht auf einen benachbarten HOST/NCP begrenzt. Eine DLUR-zu-DLUS-Pipe wird zu dem DLUS-VTAM erstellt, der für die Steuerungsflüsse abhängiger Sitzungen verwendet wird.

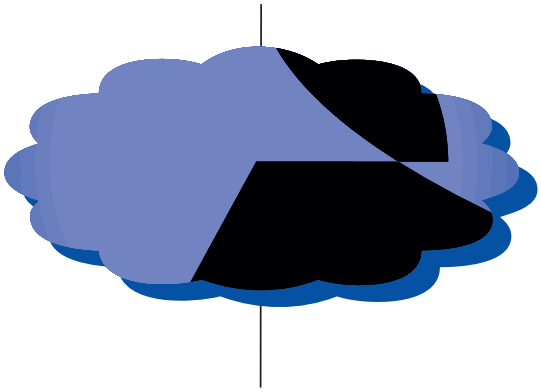
Die empfohlene Konfigurationsmethode für eine DLUR-Verbindung zum Host besteht darin, den Gateway als Netzknoten zu definieren und die DLUS-Informationen zu konfigurieren. Die expliziten und impliziten Clients sollten beim Konfigurieren dem DLUS zugeordnet werden. Dies ist die einfachste Konfiguration, weil sie keine Kenntnisse über die untergeordneten LUs auf dem Gateway voraussetzt und für VTAM die größte Sichtbarkeit der untergeordneten Einheiten ermöglicht, da VTAM die PU kennt.

Wenn die untergeordneten PUs für VTAM nicht bekannt sein sollen, kann auf dem Gateway eine interne PU (statt einer Host-Verbindung) definiert werden, und die untergeordneten Datenstationen können dieser internen PU zugeordnet werden.

Wenn eine untergeordnete Datenstation (z. B. Personal Communications) DLUR-fähig ist, soll diese Datenstation möglicherweise Weiterleitungen über Communications Server vornehmen, so daß anstelle der SNA-Gateway-Funktion die Netzknotenfunktionalität verwendet wird.

Planung für TN3270E-Server

Mittels der TN3270E-Server-Funktion kann ein Netz, wie in Abb. 34 oder Abb. 35 auf Seite 138 gezeigt, konfiguriert werden.



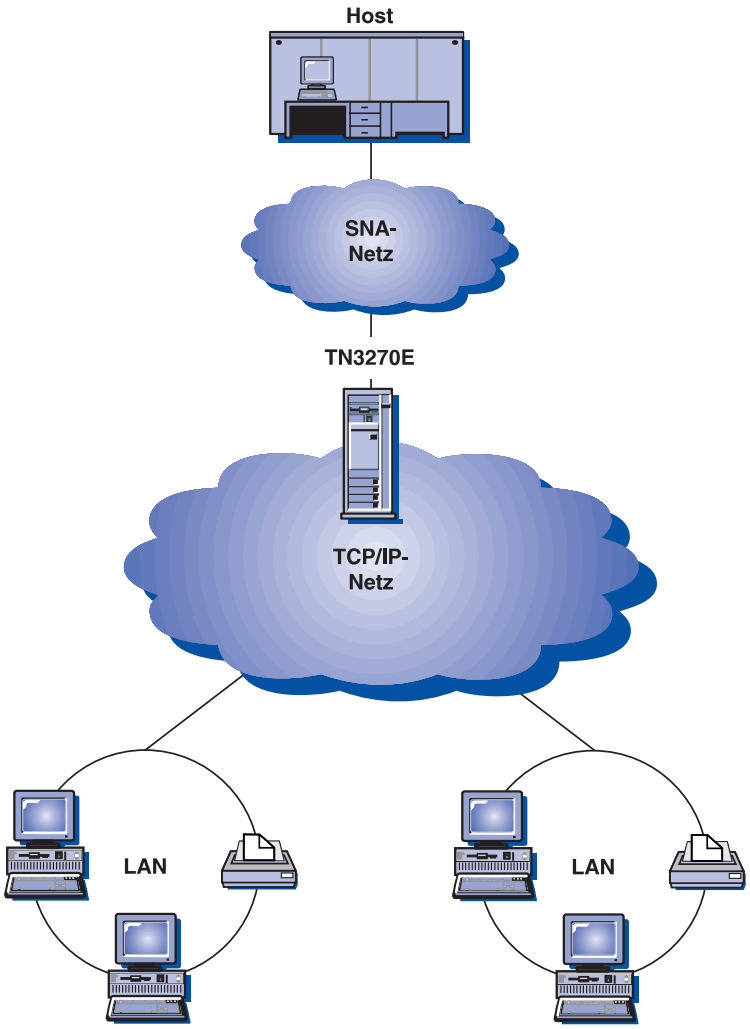


Abbildung 35. Communications Server konfiguriert als TN3270E-Server mit WAN-TCP/IP-Netz

Die TN3270E-Server-Funktion unterstützt folgendes:

- LU-Emulation

  Der TN3270E-Server unterstützt LU 2; dadurch können Benutzer interaktive Anwendungsprogramme für die 3270-Anzeige ausführen.

- Drucken über Host

  Die Telnet-3270-Standarderweiterungen (TN3270E) ermöglichen es Benutzern, von Host-Anwendungen aus auf Druckern zu drucken, die an ihre Datenstation angeschlossen sind. Diese Druckern können lokal oder über ein Netz angeschlossen sein. LU-1- und LU-3-Sitzungen werden unterstützt.

  Der TN3270E-Server implementiert die in RFC 1646 und RFC 1647 erwähnten Protokolle; dadurch kann er LU-1- und LU-3-Sitzungsdaten an TN3270E-fähige Clients senden, auf die Client-Bestätigung der Druckanforderung warten und dem Host antworten.

- IP-Filterung

  Communications Server unterstützt das Angeben von TCP/IP-Client-Filtern über IP-Adressen, Teilnetze, Host-Namen oder Domänennamen. Dieser Funktion ermöglicht die zentrale Verwaltung der Clients, die Verbindungen zum TN3270E-Server herstellen können, und das Angeben von LU-Namen und Pools, auf die Clients zugreifen können.

- Bearbeitung von Antworten

  TN3270E-fähige Clients können sowohl positive als auch negative Antworten senden, die TN3270E-Server an den Host weitersenden. Der TN3270E-Server generiert Antworten auf Anforderungen für TN3270-Standard-Clients.

- Bearbeitung der ATTN- und SYSREQ-Schlüssel

  Der TN3270E-Server kann Informationen umsetzen und an den Host weiterleiten, wenn der Client ATTN- oder SYSREQ-Schlüssel sendet. Obwohl Clients, die nicht TN3270E-fähig sind, keine explizite Definition für ATTN und SYSREQ haben, verwendet der TN3270E-Server zur Implementierung dieser Funktionen die folgenden Telnet-Befehle:

Tabelle 6. Befehlsentsprechungen

Telnet	TN3270E	Standard-TN3270
IP	ATTN	SYSREQ
AO	SYSREQ	SYSREQ
BREAK	N/A	ATTN

- LU-Klassen

  Der Communications Server teilt Benutzerverbindungen in LU-Kategorien ein. Kategorien bestehen aus mit allgemeinen Merkmalen konfigurierten LUs, wie z. B. solche, für die eine bestimmte Host-Verbindung erforderlich ist. Dadurch wird der Benutzerzugriff erleichtert, Benutzer werden nach Anwendungserfordernissen in Gruppen eingeteilt und Host-Ressourcen maximiert.

- SSL-Sicherheit (SSL - Secure Sockets Layer)

  Verbindungen zwischen TN-Clients und dem TN3270E-Server verwenden SSL Version 3, um Datenverschlüsselung und Server-Identifikationsüberprüfung mit unterzeichneten Prüfdokumenten bereitzustellen.

Anweisungen zum Konfigurieren eines TN3270E-Servers enthält das Handbuch *Einstieg*.

Unterstützte Client-Datenstationen unter TN3270E-Server

Der TN3270E-Server unterstützt alle TN3270E- oder TN3270-Clients, die vollständig mit RFC 1576, 1646 oder 1647 übereinstimmen.

Verfügbare Funktionen

Der folgende Abschnitt enthält weitere Informationen zu einigen der Einrichtungen, die für den TN3270E-Server konfiguriert werden können.

Die Standardanschlußnummer ändern

Die Anschlußnummer, die der Server für neue Verbindungen verwendet, kann im Fenster "TN3270E-Optionen" konfiguriert werden. Die Standardanschlußnummer ist 23, aber andere Telnet-Anwendungen (z. B. die TN5250-Server-Unterstützung) verwenden möglicherweise auch diesen Anschluß. Wird der Anschluß 23 von anderen Telnet-Anwendungen genutzt, muß ein anderer Anschluß verwendet werden.

Systemdatenverkehr verwalten

Es gibt zwei Möglichkeiten, zu steuern, wie oft nicht verwendete Verbindungen getrennt werden: Keepalive-Verarbeitung und automatische Abmeldung.

TN3270E-Server verwendet standardmäßig keine Keepalive-Verarbeitung. Wird Keepalive-Verarbeitung verwendet, kann entweder NOP oder Steuermarkierung ausgewählt werden.

- Bei der NOP-Verarbeitung wird ein Telnet-NOP-Befehl nach einem angegebenen Keepalive-Intervall gesendet. Dies bewirkt, daß Daten über die Verbindung übertragen werden, wodurch TCP/IP feststellt, daß die Verbindung unterbrochen wurde. Der Server erwartet keine Antwort vom Client. Es kann eine gewisse, nicht vorhersehbare Zeit dauern, bis TCP/IP den Ausfall einer Verbindung feststellt.
- Bei der Steuermarkierungsverarbeitung wird ein Telnet-Steuermarkierungsbefehl an den Client gesendet. Antwortet der Client nicht innerhalb des angegebenen Zeitraums, wird die Verbindung geschlossen.

Steuermarkierungsverarbeitung verursacht mehr Datenverkehr auf dem System als NOP-Verarbeitung, gibt jedoch nicht verwendete Verbindungen schneller frei.

Wird automatische Abmeldung ausgewählt, trennt der Server jede Sitzung, in der innerhalb des angegebenen Zeitraums kein Datenverkehr auftritt. Datenverkehr aufgrund der Keepalive-Verarbeitung hält die Verbindung nicht aufrecht; die Daten müssen an den Host oder vom Host gesendet werden. Druckersitzungen werden nicht automatisch abgemeldet.

Sind die Client-Emulationen für Keepalive-Verarbeitung konfiguriert, sollte sie auf dem Server inaktiviert werden; wird die Keepalive-Verarbeitung auf dem Server ausgeführt, sollte diese auf dem Client inaktiviert werden, um den Datenaustausch über das Netz zu reduzieren.

IP-Filterung

Communications Server ermöglicht das Konfigurieren von TN3270E-Filtern, um anzugeben, welche TCP/IP-Clients Verbindungen zum Server herstellen können. Clients können unter Verwendung von individuellen IP-Adressen, IP-Teilnetzen, TCP/IP-Host-Namen oder Domänennamen angegeben werden.

SSL-Unterstützung

Eine gesicherte Anschlußnummer, über die der Server sichere Verbindungen herstellen kann, kann vom Fenster mit den TN3270E-Server-Parametern von einer Antwortdatei aus konfiguriert werden.

Um Sicherheit zu ermöglichen, stellt Communications Server das Dienstprogramm **Key-Ring Management** zum Generieren der für SSL erforderlichen Prüfdokumente und Schlüssel zur Verfügung. Weitere Informationen enthält der Abschnitt „Planung für SSL-Sicherheit“ auf Seite 149.

Wenn die Sicherheit konfiguriert und aktiviert ist, können TN3270E-Clients, die SSL Version 3 unterstützen, die Verbindung zu einer gesicherten Anschlußnummer herstellen und sichere Verbindungen aufbauen.

SNA-Verbindungen konfigurieren

Die Host-Verbindung und Host-LUs müssen vor Verwendung der TN3270E-Server-Funktion konfiguriert werden. Die Dokumentation *Einstieg* enthält eine Tabelle, die Host-Parameter beschreibt und erklärt.

Zusammenschluß

Es gibt vier für den TN3270E-Server spezifische Klassen von LU-Definitionen: implizite Datenstation, explizite Datenstation, impliziter Drucker und expliziter Drucker. Diese Klassen entsprechen den in RFC 1647 angegebenen datenstationsgenerischen, daten-
stationsspezifischen, druckergenerischen und druckerspezifischen Klassen.

Definitionen für ***Implizite Datenstationen*** werden in einem Pool definiert, den der TN3270E-Server verwendet, um den Verbindungsanforderungen zu entsprechen. Der Standardpool kann konfiguriert werden, um Anforderungen zu entsprechen, wenn der Client keinen LU- oder Poolnamen angibt. Alle anderen Pools müssen mit Namen angefordert werden.

Es kann auch eine Reihe von LU-Definitionen angegeben werden, die dazu verwendet werden, Anforderungen für einen bestimmten LU-Namen zu erfüllen. Durch diese Definitionen für ***explizite Datenstationen*** wird sichergestellt, daß eine von einer Host-Anwendung benötigte Datenstationseinheit nicht einem Client zugeordnet wird, der sie nicht ausdrücklich angefordert hat.

Dementsprechend kann ein Pool von Druckerdefinitionen angegeben werden, die dazu verwendet werden, Verbindungsanforderungen zu erfüllen, für die keine bestimmten LU-Namen erforderlich sind (***impliziter Drucker***), und eine Reihe von Definitionen, die dazu verwendet werden, Anforderungen für einen bestimmten LU-Namen (***expliziter Drucker***) zu erfüllen.

Impliziten und expliziten Datenstationsdefinitionen können Drucker zugeordnet sein. Jeder Datenstationsdefinition kann ein Drucker zugeordnet sein, und jedem Drucker kann eine Datenstationsdefinition zugeordnet sein. Diese Drucker sind nicht in den Definitionen für explizite und implizite Drucker enthalten.

Auf Definitionen für ***zugeordnete Drucker*** kann nur durch Angabe des LU-Namens der Datenstation zugegriffen werden. Sie reduzieren die vom Client-Benutzer benötigte Informationsmenge, da der Benutzer nur den LU-Namen der Datenstation kennen muß, um eine Verbindung zu Datenstations- und Druckersitzungen herzustellen.

Lastausgleich für TN3270E-Server

Communications Server unterstützt auch den Lastausgleich für TN3270-Clients zwischen mehreren TN3270E-Servern. Weitere Informationen enthält der Abschnitt „Planung für den Lastausgleich“ auf Seite 161.

Planung für TN5250-Server

Mittels der TN5250-Server-Funktion kann ein Netz, wie in Abb. 36 oder Abb. 37 auf Seite 144 gezeigt, konfiguriert werden.

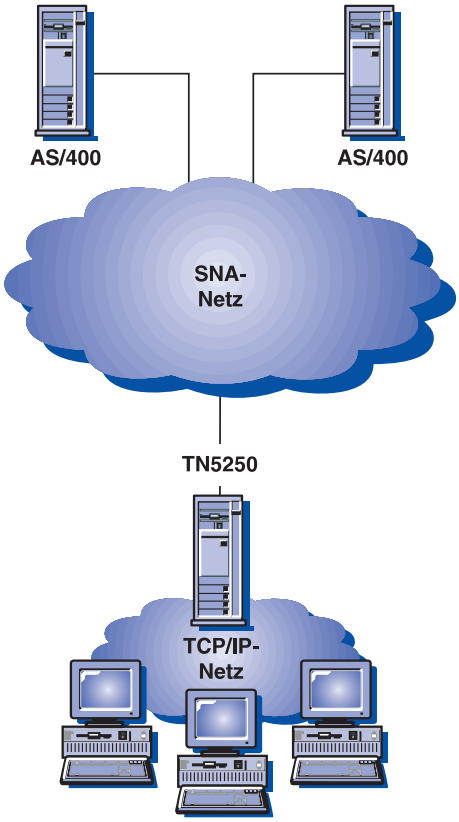
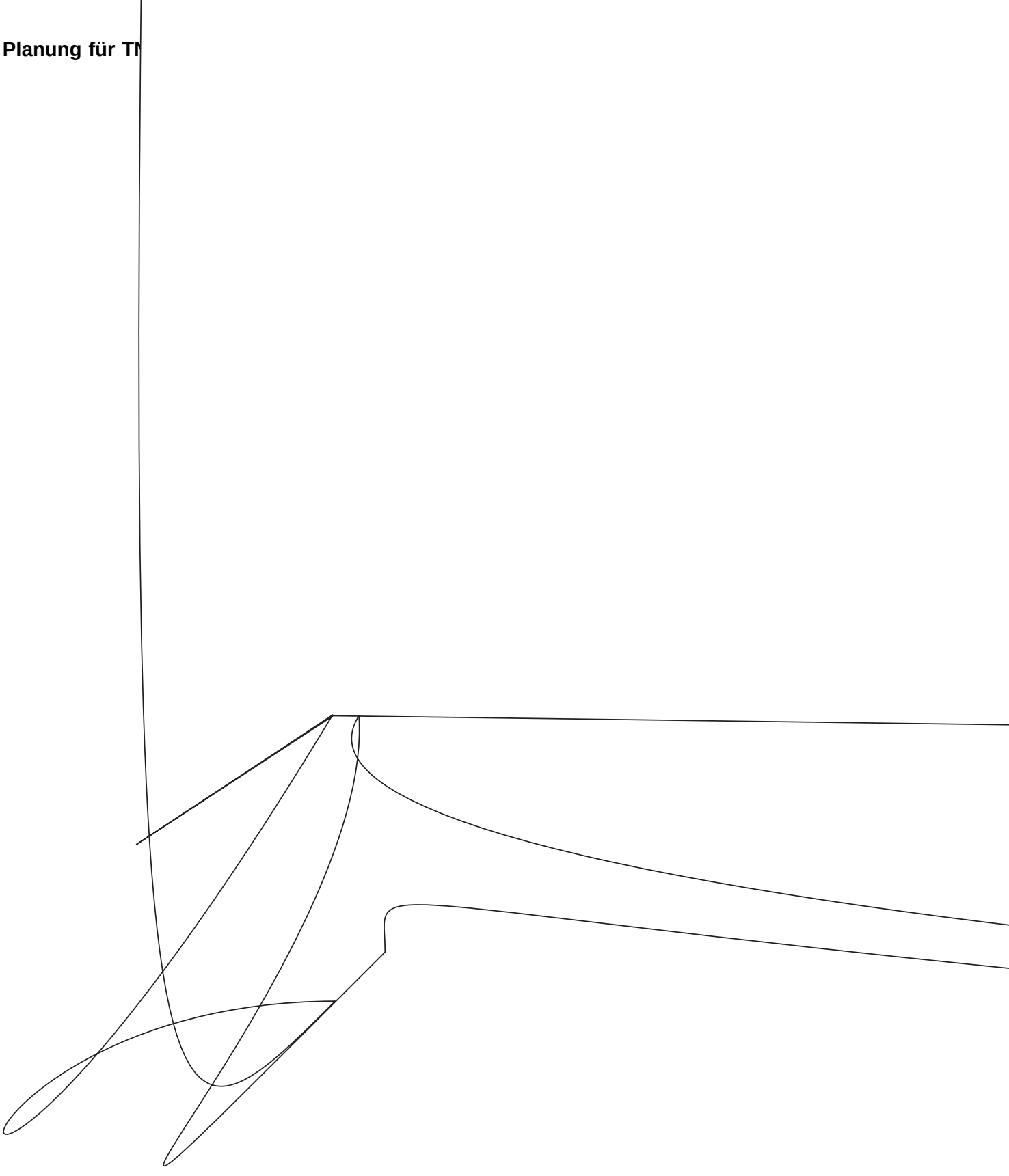


Abbildung 36. Communications Server konfiguriert als TN5250-Server mit WAN-SNA-Netz

Planung für TN



- SSL-Sicherheit (SSL - Secure Sockets Layer)

  Verbindungen zwischen TN-Clients und dem TN3270E-Server verwenden SSL Version 3, um Datenverschlüsselung und Server-Identifikationsüberprüfung mit unterzeichneten Prüfdokumenten bereitzustellen.

Anweisungen zum Konfigurieren eines TN5250-Servers enthält das Handbuch *Einstieg*.

Unterstützte Client-Datenstationen unter TN5250-Server

TN5250-Server unterstützt jeden TN5250-Client, der vollständig mit RFC 1205 übereinstimmt.

Verfügbare Funktionen

Der folgende Abschnitt enthält weitere Informationen zu einigen der Funktionen, die für den TN5250-Server konfiguriert werden können.

Die Standardanschlußnummer ändern

Beim Konfigurieren der TN5250-Server-Unterstützung wird die Anschlußnummer 23 als Standardanschluß definiert, aber andere Telnet-Anwendungen (z. B. die TN3270E-Server-Unterstützung) verwenden möglicherweise auch diesen Anschluß. Wird der Anschluß 23 von anderen Telnet-Anwendungen genutzt, muß ein anderer Anschluß verwendet werden.

Bei der Änderung von Anschlußnummern sollten Nummern vermieden werden, von denen bekannt ist, daß sie von anderen Anwendungen verwendet werden. Verwenden zwei Anwendungen dieselbe Anschlußnummer, schlägt eine der Anwendungen fehl.

Bei der Änderung von Anschlußnummern eine Nummer größer als 1024 verwenden. Nummern, die kleiner als 1 024 sind, sind reserviert. Weitere Informationen zu reservierten Anschlußnummern enthalten die folgenden Internet-Adressen:

http://www.ds1.internic.net

Zum Zeitpunkt der Veröffentlichung dieses Dokuments enthält RFC 1700 die neuesten Standards für reservierte Nummern.

TN5250-Client-Benutzer müssen benachrichtigt werden, wenn die Anschlußnummer geändert wird, da sie ihre Emulationsanwendungen entsprechend ändern müssen.

Systemdatenverkehr verwalten

Es gibt zwei Möglichkeiten, zu steuern, wie oft nicht verwendete Verbindungen getrennt werden: Keepalive-Verarbeitung und automatische Abmeldung.

TN5250-Server verwendet standardmäßig keine Keepalive-Verarbeitung. Wird Keepalive-Verarbeitung verwendet, kann entweder NOP oder Steuermarkierung ausgewählt werden.

- Bei der NOP-Verarbeitung wird ein Telnet-NOP-Befehl nach einem angegebenen Keepalive-Intervall gesendet. Dies bewirkt, daß Daten über die Verbindung übertragen werden, wodurch TCP/IP feststellt, daß die Verbindung unterbrochen wurde. Der Server erwartet keine Antwort vom Client. Es kann eine gewisse, nicht vorhersehbare Zeit dauern, bis TCP/IP den Ausfall einer Verbindung feststellt.
- Bei der Steuermarkierungsverarbeitung wird ein Telnet-Steuermarkierungsbefehl an den Client gesendet. Antwortet der Client nicht innerhalb des angegebenen Zeitraums, wird die Verbindung geschlossen.

Steuermarkierungsverarbeitung verursacht mehr Datenverkehr auf dem System als NOP-Verarbeitung, gibt jedoch nicht verwendete Verbindungen schneller frei.

Wird automatische Abmeldung ausgewählt, trennt der Server jede Sitzung, in der innerhalb des angegebenen Zeitraums kein Datenverkehr auftritt. Datenverkehr aufgrund der Keepalive-Verarbeitung hält die Verbindung nicht aufrecht; Daten müssen an den Host oder vom Host gesendet werden.

Sind die Client-Emulationen für Keepalive-Verarbeitung konfiguriert, sollte diese auf dem Server inaktiviert werden; wird die Keepalive-Verarbeitung auf dem Server ausgeführt, sollte sie auf dem Client inaktiviert werden, um den Datenaustausch über das Netz zu reduzieren.

Zugriff auf AS/400-Systeme mit mehreren Anschlüssen angeben

Communications Server ermöglicht das Konfigurieren von mehreren AS/400-Systemen und von mehreren Anschlüssen, auf denen der TN5250-Server für ankommende Verbindungen empfangsbereit ist. Beim Konfigurieren eines neuen TN5250-Server-Anschlusses kann angegeben werden, welches AS/400-System dem Anschluß zugeordnet werden soll. Ankommende TCP/IP-Verbindungen, die vom TN5250-Server auf diesem Anschluß empfangen werden, greifen dann auf das AS/400-System zu, das diesem Anschluß zugeordnet ist.

Benutzer von TN5250-Clients müssen darüber informiert werden, welche Anschlußnummern konfiguriert werden müssen, damit ihre Emulationsanwendungen Verbindungen zu bestimmten AS/400-Systemen aufnehmen können.

IP-Filterung

Communications Server ermöglicht das Konfigurieren von TN5250-Filtern, um anzugeben, welche TCP/IP-Clients Verbindungen zum Server herstellen können. Clients können unter Verwendung von individuellen IP-Adressen, IP-Teilnetzen, TCP/IP-Host-Namen oder Domänennamen angegeben werden.

Es ist auch möglich, ein AS/400-System mit einem Filter zu konfigurieren, um ein anderes als das dem Anschluß zugeordnete AS/400-System anzugeben. Dadurch können die einem Filter zugeordneten Clients an ein bestimmtes AS/400-System geleitet werden.

In einem Filter können mehrere AS/400-Systeme angegeben werden. Wenn der Verbindungsversuch eines Clients zu dem ersten angegebenen AS/400-System fehlschlägt, wird versucht, eine Verbindung zu anderen im Filter angegebenen AS/400-Systemen aufzunehmen.

SSL-Unterstützung

Beim Konfigurieren eines neuen TN5250-Server-Anschlusses kann angegeben werden, daß der Anschluß für sichere Verbindungen verwendet werden soll. Es können mehrere Anschlüsse als sichere Anschlüsse angegeben werden.

Um Sicherheit zu ermöglichen, stellt Communications Server das Dienstprogramm **Key-Ring Management** zum Generieren der für SSL erforderlichen Prüfdokumente und Schlüssel zur Verfügung. Weitere Informationen enthält der Abschnitt „Planung für SSL-Sicherheit“ auf Seite 149.

Wenn die Sicherheit konfiguriert und aktiviert ist, können TN5250-Clients, die SSL Version 3 unterstützen, die Verbindung zu einer gesicherten Anschlußnummer herstellen und sichere Verbindungen aufbauen.

SNA-Netz konfigurieren

Das SNA-Netz muß so konfiguriert werden, daß der TN5250-Server Verbindung zu den AS/400-Systemen herstellen kann. Informationen zum Konfigurieren des SNA-Netzes für den TN5250-Server enthält das Handbuch *Einstieg*.

Lastausgleich für TN5250-Server

Communications Server unterstützt auch den Lastausgleich für TN5250-Clients zwischen mehreren TN5250-Servern. Weitere Informationen enthält der Abschnitt „Planung für den Lastausgleich“ auf Seite 161.

Planung für SSL-Sicherheit

SSL-Sicherheit (SSL - Secure Sockets Layer) kann für Verbindungen zwischen TN-Clients und dem TN3270E- oder TN5250-Server verwendet werden. Diese Sicherheitsfunktion beinhaltet Datenverschlüsselung über SSL Version 3 und Server-Identifikationsüberprüfung mit unterzeichneten Prüfdokumenten.

Es können bestimmte Anschlüsse für die Unterstützung von SSL-Sicherheit konfiguriert werden. Wenn Sicherheit angegeben wird, muß der Server über ein von einer Zertifizierungsstelle (CA - Certificate Authority) ausgestelltes überprüftes Prüfdokument verfügen. Communications Server stellt ein Dienstprogramm zum Generieren und Verwalten von Schlüsseln und Prüfdokumenten zur Verfügung, die von SSL Version 3 verwendet werden.

Dieses Kapitel enthält eine Übersicht zur Planung für SSL-Sicherheit. SSL-Sicherheit wird beim Konfigurieren von TN3270E-Server und TN5250-Server als Option zur Verfügung gestellt.

Funktionsweise der SSL-Sicherheit

SSL (Secure Sockets Layer) ist ein dem Industriestandard entsprechendes Protokoll, das die Verschlüsselungstechnik mit symmetrischen und allgemeinen Schlüsseln verwendet. Bei der Verschlüsselungstechnik mit symmetrischen Schlüsseln wird derselbe Schlüssel zum Verschlüsseln und zum Entschlüsseln von Nachrichten verwendet. Die Verschlüsselungstechnik mit allgemeinen Schlüsseln verwendet ein Schlüsselpaar, bestehend aus einem allgemeinen und einem privaten Schlüssel. Dabei wird der allgemeine Schlüssel eines Servers veröffentlicht, und der private Schlüssel wird geheimgehalten. Um eine Nachricht sicher an den Server zu übermitteln, verschlüsselt der Client die Nachricht mit dem allgemeinen Schlüssel des Servers. Der Server entschlüsselt die empfangene Nachricht mit seinem privaten Schlüssel.

SSL stellt drei grundlegende Sicherheitsservices zur Verfügung:

- Nachrichtenvertraulichkeit

  Die Nachrichtenvertraulichkeit wird durch eine Kombination aus der Verschlüsselung mit allgemeinen und symmetrischen Schlüsseln sichergestellt. Der gesamte Datenaustausch zwischen einem SSL-Client und einem SSL-Server wird durch einen Schlüssel und einen Verschlüsselungsalgorithmus verschlüsselt, die beim Aufbauen der Sitzung vereinbart werden.

- Nachrichtenintegrität

  Der Service für Nachrichtenintegrität stellt sicher, daß die während der SSL-Sitzung übertragenen Daten auf dem Weg zur Zieladresse nicht verändert werden. SSL gewährleistet die Nachrichtenintegrität mit Hilfe einer Kombination aus allgemeinen/privaten Schlüsseln und Hash-Funktionen.

- Identifikationsüberprüfung

  Die Identifikationsüberprüfung ist ein Verfahren, mit dem sich Client und Server von der korrekten Identität der jeweils anderen Instanz überzeugen. Die Identitäten von Client und Server sind in Prüfdokumenten für allgemeine Schlüssel codiert. Ein Prüfdokument für einen allgemeinen Schlüssel besteht aus folgenden Komponenten:

  – Differenzierter Name des Subjekts
  – Differenzierter Name des Ausstellers
  – Allgemeiner Schlüssel des Subjekts
  – Unterschrift des Ausstellers
  – Gültigkeitsdauer
  – Seriennummer

Anmerkung: Communications Server unterstützt die Identifikationsüberprüfung auf dem Server. Nur der sichere Server verlangt die Identifikationsüberprüfung über die Zertifizierungsstelle (CA - Certificate Authority), bevor eine TN3270E- oder TN5250-Verbindung hergestellt werden kann.

Communications Server-SSL-Unterstützung

Communications Server unterstützt die folgenden Komponenten der SSL-Sicherheit:

- Sichere SSL-Sitzungen zwischen TN3270E-Server und beliebigen TN3270- bzw. TN3270E-Clients, die SSL Version 3 unterstützen
- Sichere SSL-Sitzungen zwischen TN5250-Server und beliebigen TN5250-Clients, die SSL Version 3 unterstützen
- SSL Version 3
- Nachrichtenvertraulichkeit und -integrität
- Identifikationsüberprüfung auf dem Server

SSL-Sicherheit konfigurieren

Beim Konfigurieren von TN3270E-Server und TN5250-Server wird angegeben, welche Anschlüsse SSL-Sicherheit für ihre Verbindungen verwenden. Weitere Informationen zum Konfigurieren sicherer Anschlüsse enthalten die Abschnitte „Planung für TN3270E-Server“ auf Seite 137 und „Planung für TN5250-Server“ auf Seite 143.

Um SSL-Sicherheit mit Server-Identifikationsüberprüfung zu ermöglichen, ist eine Kombination aus allgemeinem/privatem Schlüssel sowie ein dazugehöriges gültiges Prüfdokument für den allgemeinen Schlüssel erforderlich. Communications Server stellt ein Dienstprogramm **Key-Ring Management** zum Erstellen, Verwalten und Speichern der für SSL erforderlichen allgemeinen/privaten Schlüssel und Prüfdokumente zur Verfügung.

Bei Verwendung des Dienstprogramms **Key-Ring Management** ist einer der folgenden Schritte auszuführen:

- Eine Kombination aus allgemeinem/privatem Schlüssel erstellen sowie ein Prüfdokument bei einer der vordefinierten (anerkannten) Zertifizierungsstelle (CA - Certificate Authority) abrufen und speichern.

  Diese Prozedur erfordert einen geringeren Konfigurationsaufwand, weil die Schlüsseldatenbankdatei bereits mit den erforderlichen CA-Stammprüfdokumenten vordefiniert ist, über die die CAs, die das Prüfdokument ausgestellt haben, identifiziert werden.
- Eine Kombination aus allgemeinem/privatem Schlüssel erstellen, eine unbekannte CA definieren (durch Abrufen des CA-Stammprüfdokuments und Speichern dieses Dokuments in der Schlüsseldatenbankdatei), sowie Anfordern und Speichern eines Prüfdokuments von der unbekannten CA.
- Ein selbstunterzeichnetes Prüfdokument erstellen und dieses in der Schlüsseldatenbankdatei speichern.

  Anmerkung: Um zuverlässige Sicherheit für einen Systemstandort zu gewährleisten, sollten selbstunterzeichnete Prüfdokumente nur für überwachte Testvorgänge verwendet werden.

Dienstprogramm Key-Ring Management

Das Communications Server-Dienstprogramm **Key-Ring Management** ermöglicht das Erstellen, Verwalten und Speichern der erforderlichen allgemeinen/privaten Schüssel und Prüfdokumente für die SSL-Kommunikation zwischen Communications Server und dem Client. Vor dem Konfigurieren der SSL-Kommunikation muß die Schlüsseldatenbankdatei von Communications Server geöffnet werden. Zum Öffnen dieser Datei sind folgende Schritte auszuführen:

1. Im Hauptmenü **Schlüsseldatenbankdatei** und **Öffnen** auswählen, um eine vorhandene Schlüsseldatenbank zu öffnen.
2. Im Fenster **Öffnen** das Unterverzeichnis **private** des Verzeichnisses auswählen, in dem das Produkt installiert ist (z. B. C:\IBMCS\PRIVATE).
3. **ibmcs.kdb** als Schlüsseldatenbank auswählen.
4. Nach entsprechender Aufforderung das Kennwort eingeben.

   Anmerkung: Als Kennwort ist zunächst **ibmcs** vordefiniert. Um verläßliche Sicherheit zu erzielen, ***muß*** das Kennwort geändert werden, bevor Operationen mit dem Dienstprogramm **Key-Ring Management** ausgeführt werden.

Kennwort ändern

Mit folgenden Schritten kann das Kennwort der aktuellen Datenbank geändert werden:

1. Im Menü **Schlüsseldatenbankdatei** und **Kennwort ändern** auswählen, um das Kennwort der Schlüsseldatenbank für die aktuelle Datenbank zu ändern. Das Dialogfenster **Kennwort ändern** wird angezeigt.
2. Das gewünschte neue Kennwort eingeben.
3. Das neue Kennwort zur Bestätigung nochmals eingeben.
4. Wenn für das Kennwort ein Ablaufzeitpunkt gelten soll, die Option **Ablaufzeit festlegen** anklicken. Um verläßliche Sicherheit zu gewährleisten, sollte ein Ablaufzeitpunkt für das Kennwort definiert werden.
5. Wenn das Kennwort nur zeitlich begrenzt gültig sein soll, die Anzahl Tage angeben, nach der das Kennwort ungültig wird.
6. **Kennwort verstecken** anklicken, um das Kennwort der aktuellen Datenbank zu verstecken.

SSL über eine anerkannte gesicherte CA konfigurieren

Mit den in diesem Abschnitt beschriebenen Prozeduren kann die SSL-Sicherheit mit einem Prüfdokument von einer anerkannten CA konfiguriert werden. Die folgenden von einer CA unterzeichneten Prüfdokumente sind bereits in der Schlüsseldatenbank gespeichert und als gesicherte Prüfdokumente markiert:

- 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 (auch von VeriSign vergeben)
- VeriSign class 4 public primary CA
- VeriSign class 3 public primary CA
- VeriSign class 2 public primary CA
- VeriSign class 1 public primary CA

Zum Konfigurieren der SSL-Sicherheit über eine anerkannte CA sind die folgenden Schritte erforderlich:

- Anforderung für Schlüssel und Prüfdokument erstellen
- Prüfdokumentanforderung bei der CA einreichen
- Prüfdokument abrufen und in der Schlüsseldatenbank des Servers speichern

Anforderung für Schlüssel und Prüfdokument erstellen

Mit dem Dienstprogramm **Key-Ring Management** die folgenden Schritte ausführen, um eine Anforderung für allgemeinen/privaten Schlüssel und für ein Prüfdokument zu erstellen:

1. In der verdeckten Liste des Hauptmenüs den Eintrag **Persönliche Prüfdokumentanforderungen** auswählen, und die Option **Neu** anklicken, um eine neue Anforderung für ein Schlüsselpaar und ein Prüfdokument zu erstellen. Das Dialogfenster **Neues Schlüsselpaar und Prüfdokument-anforderung erstellen** wird angezeigt.
2. Den Namen (Kennsatz) zur Kennzeichnung des Schlüssels und des Prüfdokuments in der Datenbank angeben.
3. Den Wert für die zu verwendende Schlüsselgröße eingeben. Je größer der Schlüssel, um so zuverlässiger die Sicherheit; aber ein größerer Schlüssel erfordert auch umfangreichere Verarbeitungsoperationen auf dem Client und dem Server beim Herstellen einer Verbindung.
4. Den TCP/IP-Host-Namen des Datenfernverarbeitungs-Servers als allgemeinen Namen eingeben (z. B. wtr05306.raleigh.ibm.com).

5. Einen Organisationsnamen eingeben.
6. Eine Organisationseinheit eingeben (wahlfrei).
7. Eine Stadt bzw. einen Ort eingeben (wahlfrei).
8. Ein Bundesland eingeben (wahlfrei).
9. Einen Postzustellbezirk eingeben (wahlfrei).
10. Einen Landescode eingeben. Hier müssen mindestens zwei Zeichen eingegeben werden (z. B. US).
11. Einen Dateinamen für die Prüfdokumentanforderung eingeben oder den Standarddateinamen verwenden.

Nach Anklicken von **OK** werden die eingegebenen Informationen verarbeitet. Dabei werden die beiden folgenden Dateien erstellt:

ibmcs.rdb Private Schlüsseldatei

certreq.arm Dies ist der Standardname der Prüfdokumentanforderungsdatei. Wenn vom Benutzer ein eigener Dateiname vergeben wurde, wird eine Datei mit diesem Namen erstellt. Die Prüfdokumentanforderungsdatei ist eine Datei des Typs PKCS 10 im Format "armored 64".

Diese Dateien dürfen nicht editiert oder verschoben werden. Wenn die Datei **ibmcs.rdb** nicht gefunden werden kann oder beim Eingeben des Prüfdokuments in die Schlüsseldatenbank beschädigt wurde, muß die Prüfdokumentanforderung erneut bei der CA eingereicht werden.

Prüfdokumentanforderung einreichen

Einen Web-Browser starten und die Web-Seite der CA aufrufen. Die angegebenen Anweisungen befolgen, um die Prüfdokumentanforderung einzureichen. Es folgen die URL-Adressen einiger anerkannter CAs:

- VeriSign: **http://www.verisign.com/**
- Thawte: **http://www.thawte.com/**

Die vom Dienstprogramm **Key-Ring Management** generierte Prüfdokumentanforderung (je nach ausgewählter CA) entweder per E-Mail einreichen oder in das bereitgestellte Formular bzw. die bereitgestellte Datei der CA einfügen.

Nach dem Einreichen einer Prüfdokumentanforderung bei einer CA kann die SSL-Sicherheit durch Erstellen und Speichern eines selbstunterzeichneten Prüfdokuments aktiviert werden. Ein selbstunterzeichnetes Prüfdokument sollte nur für überwachte Testvorgänge verwendet werden. Weitere Informationen enthält der Abschnitt „Selbstunterzeichnetes Prüfdokument erstellen“ auf Seite 158.

>Prüfdokument in der Schlüsseldatenbank speichern

Nach dem Erhalt eines Prüfdokuments von einer CA, das Prüfdokument mit dem Dienstprogramm **Key-Ring Management** in die Schlüsseldatenbankdatei , **ibmcs.kdb** einfügen, die sich auf dem Server befindet.

1. In der verdeckten Liste des Dienstprogramms **Key-Ring Management** den Eintrag **Persönliche Prüfdokumente** auswählen und **Empfangen** anklicken, um die Anforderung für Schlüsselpaar und Prüfdokument in Empfang zu nehmen. Das Dialogfenster **Prüfdokument aus Datei empfangen** wird angezeigt.
2. Sicherstellen, daß als Datentyp **BASE64-verschlüsselte ASCII-Daten** (Format "armored 64") angegeben ist.
3. Den Dateinamen des Prüfdokuments eingeben.
4. Die Position (Pfadname) des Prüfdokuments angeben. **OK** anklicken. Das gespeicherte Prüfdokument wird als erster Eintrag angezeigt.
5. Das gespeicherte Prüfdokument hervorheben und **Anzeigen/Editieren** anklicken. Das Dialogfenster **Schlüsselinformationen** wird angezeigt.
6. Die Option **Prüfdokument als Standardwert einstellen** anklicken. Der ausgewählte Schlüssel wird als Standardeinstellung verwendet.

SSL über unbekannte CA konfigurieren

Zum Konfigurieren der SSL-Sicherheit über eine unbekannte CA (noch nicht in der Datenbank definiert) sind die folgenden Schritte erforderlich:

- Anforderung für Schlüssel und Prüfdokument erstellen
- Prüfdokumentanforderung bei der CA einreichen
- Das Stammprüfdokument und das eigene Prüfdokument von der CA abrufen und in der Schlüsseldatenbank des Servers speichern

Anforderung für Schlüssel und Prüfdokument erstellen

Mit dem Dienstprogramm **Key-Ring Management** die folgenden Schritte ausführen, um eine Anforderung für allgemeinen/privaten Schlüssel und für ein Prüfdokument zu erstellen:

1. In der verdeckten Liste des Hauptmenüs den Eintrag **Persönliche Prüfdokumentanforderungen** auswählen, und die Option **Neu** anklicken, um eine neue Anforderung für ein Schlüsselpaar und ein Prüfdokument zu erstellen. Das Dialogfenster **Neues Schlüsselpaar und Prüfdokumentanforderung erstellen** wird angezeigt.
2. Den Namen (Kennsatz) zur Kennzeichnung des Schlüssels und des Prüfdokuments in der Datenbank angeben.
3. Den Wert für die zu verwendende Schlüsselgröße eingeben. Je größer der Schlüssel, um so zuverlässiger die Sicherheit; aber ein größerer Schlüssel erfordert auch umfangreichere Verarbeitungsoperationen auf dem Client und dem Server beim Herstellen einer Verbindung.
4. Den TCP/IP-Host-Namen des Datenfernverarbeitungs-Servers als allgemeinen Namen eingeben (z. B. wtr05306.raleigh.ibm.com).
5. Einen Organisationsnamen eingeben.
6. Eine Organisationseinheit eingeben (wahlfrei).
7. Eine Stadt bzw. einen Ort eingeben (wahlfrei).
8. Ein Bundesland eingeben (wahlfrei).
9. Einen Postzustellbezirk eingeben (wahlfrei).
10. Einen Landescode eingeben. Hier müssen mindestens zwei Zeichen eingegeben werden (z. B. US).
11. Einen Dateinamen für die Prüfdokumentanforderung eingeben oder den Standarddateinamen verwenden.

Nach Anklicken von **OK** werden die eingegebenen Informationen verarbeitet. Dabei werden die beiden folgenden Dateien erstellt:

ibmcs.rdb Private Schlüsseldatei

certreq.arm Dies ist der Standardname der Prüfdokumentanforderungsdatei. Wenn vom Benutzer ein eigener Dateiname vergeben wurde, wird eine Datei mit diesem Namen erstellt. Die Prüfdokumentanforderungsdatei ist eine Datei des Typs PKCS 10 im Format "armored 64".

Diese Dateien dürfen nicht editiert oder verschoben werden. Wenn die Datei **ibmcs.rdb** nicht gefunden werden kann oder beim Eingeben des Prüfdokuments in die Schlüsseldatenbank beschädigt wurde, muß die Prüfdokumentanforderung erneut bei der CA eingereicht werden.

Prüfdokumentanforderung einreichen

Zum Einreichen der Prüfdokumentanforderung die von der unbekannten CA vorgegebenen Prozeduren ausführen.

Die vom Dienstprogramm **Key-Ring Management** generierte Prüfdokumentanforderung (je nach ausgewählter CA) entweder per E-Mail einreichen oder in das bereitgestellte Formular bzw. die bereitgestellte Datei der CA einfügen.

Nach dem Einreichen einer Prüfdokumentanforderung bei einer CA kann die SSL-Sicherheit durch Erstellen und Speichern eines selbstunterzeichneten Prüfdokuments aktiviert werden. Ein selbstunterzeichnetes Prüfdokument sollte nur für überwachte Testvorgänge verwendet werden. Weitere Informationen enthält der Abschnitt „Selbstunterzeichnetes Prüfdokument erstellen“ auf Seite 158.

>Prüfdokument in der Schlüsseldateidatenbank speichern

Nach Erhalt eines Prüfdokuments von einer CA bei der CA das Stammprüfdokument anfordern. Das CA-Stammprüfdokument muß in der Schlüsseldatenbank gespeichert werden, bevor das angeforderte Prüfdokument gespeichert wird. Das CA-Stammprüfdokument überprüft das angeforderte Prüfdokument. Das CA-Stammprüfdokument mit Hilfe des Dienstprogramms **Key-Ring Management** speichern.

1. In der verdeckten Liste **Prüfdokumente des Unterzeichners** auswählen und **Empfangen** anklicken, um das Schlüsselpaar und das Prüfdokument in Empfang zu nehmen. Das Dialogfenster **Prüfdokument aus Datei empfangen** wird angezeigt.
2. Sicherstellen, daß als Datentyp **BASE64-verschlüsselte ASCII-Daten** (Format "armored 64") angegeben ist.
3. Den Dateinamen des Prüfdokuments eingeben.
4. Die Position (Pfadname) des Prüfdokuments angeben. **OK** anklicken. Die Datei wird als ***gesichert*** markiert und gespeichert.

Um das angeforderte Prüfdokument zu speichern, das Prüfdokument mit dem Dienstprogramm **Key-Ring Management** in die Schlüsseldatenbankdatei **ibmcs.kdb** stellen, die sich auf dem Server befindet.

1. In der verdeckten Liste des Hauptmenüs den Eintrag **Persönliche Prüfdokumente** auswählen und **Empfangen** anklicken, um das Schüsselpaar und das Prüfdokument in Empfang zu nehmen. Das Dialogfenster **Prüfdokument aus Datei empfangen** wird angezeigt.
2. Sicherstellen, daß als Datentyp **BASE64-verschlüsselte ASCII-Daten** (Format "armored 64") angegeben ist.
3. Den Dateinamen des Prüfdokuments eingeben.
4. Die Position (Pfadname) des Prüfdokuments angeben. **OK** anklicken. Das gespeicherte Prüfdokument wird als erster Eintrag angezeigt.
5. Das gespeicherte Prüfdokument hervorheben und **Anzeigen/Editieren** anklicken. Das Dialogfenster **Schlüsselinformationen** wird angezeigt.
6. Die Option **Prüfdokument als Standardwert einstellen** anklicken. Der ausgewählte Schlüssel wird als Standardeinstellung verwendet.

Selbstunterzeichnetes Prüfdokument erstellen

Bis zum Erhalt eines Prüfdokuments von einer anerkannten gesicherten CA können bis zu drei Wochen vergehen. Bis zum Erhalt des allgemeinen Server-Prüfdokuments kann mit einem selbstunterzeichneten Prüfdokument gearbeitet werden, um SSL-Sitzungen zwischen Clients und dem Server zu aktivieren. Ein selbstunterzeichnetes Prüfdokument sollte nur für überwachte Testvorgänge verwendet werden. Um zuverlässige Sicherheit für den Systemstandort zu gewährleisten, sollte ein selbstunterzeichnetes Prüfdokument nicht in einer Produktionsumgebung verwendet werden. Die folgenden Schritte ausführen, um den lokalen Systemstandort mit dem Dienstprogramm **Key-Ring Management** für die Verwendung eines selbstunterzeichneten Prüfdokuments einzurichten:

1. Die Option **Neues selbstunterzeichnetes Prüfdokument** im Menüeintrag **Erstellen** auswählen, um ein neues selbstunterzeichnetes Prüfdokument zu erstellen. Das Dialogfenster **Neues selbstunterzeichnetes Prüfdokument erstellen** wird angezeigt.
2. Den Namen (Kennsatz) zur Kennzeichnung des Schlüssels und des Prüfdokuments in der Datenbank angeben. Als Version des Prüfdokuments **X509 V3** auswählen.
3. Den Wert für die zu verwendende Schlüsselgröße eingeben. Je größer der Schlüssel, um so zuverlässiger die Sicherheit; aber ein größerer Schlüssel erfordert auch umfangreichere Verarbeitungsoperationen auf dem Client und dem Server beim Herstellen einer Verbindung.
4. Den TCP/IP-Host-Namen des Datenfernverarbeitungs-Servers als allgemeinen Namen eingeben (z. B. wtr05306.raleigh.ibm.com).
5. Einen Organisationsnamen eingeben.
6. Eine Organisationseinheit eingeben (wahlfrei).
7. Eine Stadt bzw. einen Ort eingeben (wahlfrei).
8. Ein Bundesland eingeben (wahlfrei).
9. Einen Postzustellbezirk eingeben (wahlfrei).
10. Einen Landescode eingeben. Hier müssen mindestens zwei Zeichen eingegeben werden (z. B. US).
11. Die Gültigkeitsdauer des selbstunterzeichneten Prüfdokuments (Anzahl Tage) eingeben.
12. **OK** anklicken.
13. **Ja** anklicken, um den Schlüssel als Standardschlüssel in der Schlüsseldatenbank zu definieren.

Wenn IBM eNetwork Host On-Demand oder ein anderer SSL-Client verwendet wird, der die Angabe des selbstunterzeichneten Prüfdokuments erfordert, mit dem Dienstprogramm **Key-Ring Management** die folgenden Schritte ausführen:

1. In der verdeckten Liste den Eintrag **Persönliche Prüfdokumente** auswählen, das selbstunterzeichnete Prüfdokument hervorheben und **Prüfdokument extrahieren** anklicken. Das Dialogfenster **Prüfdokument in eine Datei extrahieren** wird angezeigt.
2. Als Datentyp die Option **Binäre DER-Daten** auswählen.
3. Den Dateinamen des Prüfdokuments eingeben. Die Datei sollte die Erweiterung **der** haben (z. B. ibmcs.der).
4. Die Position (Pfadname) des Prüfdokuments angeben.
5. **OK** anklicken.

Die Prüfdokumentdatei muß auf jeden Client gestellt werden, der zum Verbindungsaufbau mit dem Server berechtigt ist. Anweisungen zum Speichern des selbstunterzeichneten Prüfdokuments als CA-Stammprüfdokument in der Klassendatei oder Schlüsseldateidatenbank des Servers enthält die Client-Dokumentation.

Planung für den Lastausgleich

Dieses Kapitel enthält eine Übersicht zur Planung für den Lastausgleich. Es wird die Planung für den Lastausgleich für abhängige LU und LU 6.2 beschrieben.

Lastausgleich für abhängige LU

Der Lastausgleich ermöglicht das Verteilen von abhängigen Host-Sitzungen auf die verfügbaren Server. Der Lastausgleich für LUx-API-Anwendungen wird durch SNA-API-Clients, 3270-Emulationen und TN3270-Emulationen unterstützt.

Beim Beantworten von Client-Anforderungen sortiert Communications Server diejenigen Server, die den angeforderten Pool unterstützen, entsprechend ihrer Auslastung.

Die Auslastung abhängiger LUs gibt an, wieviel Prozent der Ressourcen eines bestimmten Servers verfügbar sind. Der Prozentwert für die Auslastung ergibt sich aus der Division der Anzahl aktiver Anwendungsverbindungen durch die Gesamtzahl verfügbarer LUs (0 bis 3).

Der Benutzer kann die Berechnung der Auslastung durch Angeben eines Belastungsfaktors für LU 0 bis 3 (Belastungsfaktor für Host-Sitzung) modifizieren, um Unterschiede zwischen zwei Servern (z. B. verfügbarer Speicher, Prozessorgeschwindigkeit und CPU-Auslastung) auszugleichen. Mit dem Belastungsfaktor für LU 0 bis 3 kann die Auslastung auch zwischen Communications Servern und Novell IntranetWare für SAA-Servern aufgeteilt werden.

Anmerkungen:

1. Welche Server am Lastausgleich teilnehmen, wird anhand der Zugehörigkeit zu LU-Pools und der Bereichszugehörigkeit festgelegt. Alle Communications Server mit LUs, die Pools mit gleichen Namen angehören, nehmen am Lastausgleich teil.
2. Clients, die das TCP/IP-Protokoll verwenden, können am Lastausgleich teilnehmen. Für TCP/IP-Clients kann der Lastausgleich jedoch nur zwischen IBM Communications Servern erfolgen. Der Lastausgleich wird durch konfigurierte Bereiche festgelegt.

Wenn in Communications Server LU-Pools, die sich auf verschiedenen Servern befinden, den gleichen Namen haben, werden sie beim Lastausgleich wie ein Pool behandelt. Beim Zuordnen von LUs zu einem LU-Pool unter den Host-Verbindungen des Servers eine Auswahl treffen und LUs der ausgewählten Host-Verbindung dem LU-Pool zuordnen. Diese LUs müssen nicht den gleichen LU-Typ aufweisen. Außerdem kann der resultierende Pool LUs von mehreren Verbindungen enthalten.

Lastausgleich für LU 6.2

Der Lastausgleich ermöglicht das Verteilen von unabhängigen LU 6.2-Sitzungen auf mehrere Server. Der Lastausgleich für APPC-API-Anwendungen wird durch SNA-API-Clients und TN5250-Emulationen unterstützt.

Die Auslastung für LU 6.2 gibt an, wieviel Prozent der Ressourcen eines bestimmten Servers verfügbar sind. Der Prozentwert für die Auslastung ergibt sich aus der Division der Gesamtzahl der auf allen lokalen LUs eines bestimmten Servers geführten Dialoge durch das kumulative maximale Sitzungslimit für alle lokalen LUs. Das maximale Sitzungslimit ist das bei der Konfiguration angegebene LU 6.2-Sitzungslimit. Wenn das maximale Sitzungslimit auf Null (0) gesetzt ist, d. h., es ist kein Sitzungslimit festgelegt, wird bei der Lastberechnung das maximale Standardsitzungslimit für lokale LU-Sitzungen (512 pro lokale LU) verwendet. Das Standardsitzungslimit für lokale LU-Sitzungen kann auch beim Konfigurieren angegeben werden. Der Benutzer kann die Lastberechnung durch Angeben eines LU 6.2-Belastungsfaktors (Belastungsfaktor für APPC-Sitzung) modifizieren, um Unterschiede zwischen zwei Servern (z. B. verfügbarer Speicher, Prozessorgeschwindigkeit und CPU-Auslastung) auszugleichen. Mit dem LU 6.2-Belastungsfaktor kann die Auslastung auch zwischen Communications Servern und Novell IntranetWare für SAA-Servern aufgeteilt werden.

Anmerkung: Clients, die das TCP/IP-Protokoll verwenden, können am LU 6.2-Lastausgleich teilnehmen.

Planung für TCP/IP-Bereiche

Mit dem Parameter ***Scope*** (Bereich) kann der Zugriff von TCP/IP-Clients auf Server in einem Netz gesteuert und verwaltet werden. Dieser Parameter stimmt mit dem in RFC 2165 genannten SLP-Bereich (SLP = Service Location Protocol) überein. SLP wird von Communications Server zum Implementieren des TCP/IP-gestützten Lastausgleichs verwendet.

Die Angabe des Steuerbereichs ist aus folgenden zwei Gründen erforderlich:

- Mit dem Anwachsen des Netzes, der Anzahl Clients und der Anzahl Server wird es erforderlich, den Zugriff auf diese Server durch die wachsende Anzahl von Clients aufzuteilen, um die Gesamtauslastung des Netzes zu reduzieren.
- Der Steuerbereich ermöglicht Administratoren, die Benutzer und die Server in Verwaltungsgruppen einzuteilen.

Die Bedeutung der Bereichswerte wird vom Netzadministrator definiert. Diese Werte können jede beliebige Definitionseinheit darstellen. In der Regel erfolgt die Aufteilung in Bereiche nach Abteilungen, Organisationen oder geografischen Grenzen.

Nach erfolgter Konfigurierung können Clients das SNA-Netz über Server erreichen, die für denselben Bereich konfiguriert sind, oder denen kein Bereich zugeordnet ist (Services oder Server ***ohne Bereich***).

Anmerkung: Wenn ein Server ohne Bereich konfiguriert ist, antwortet er auf Anforderungen für bestimmte SLP-Bereiche **und** Anforderungen, die an keinen bestimmten Bereich gerichtet sind. Wenn der SNA-API-Client für den Verbindungsaufbau zu Servern ohne Bereich konfiguriert ist, antworten nur Server ohne Bereich.

Bereiche und Client/Server-Sicherheit

Communications Server ermöglicht Novell IntranetWare für SAA-Clients die Verwendung der Windows NT-Domänensicherheitsfunktion zur Identifikationsüberprüfung der Client-Verbindung zum Server, ohne daß Benutzer-ID und Kennwort erneut eingegeben werden müssen. Der Client muß einer Windows NT-Domäne angehören, und zwar entweder durch seine Teilnahme an einer Communications Server-Domäne oder durch lokale Anmeldung über eine synchronisierte Benutzer-ID mit Kennwort.

Die berechtigten Client/Server-Benutzer werden in der lokalen Gruppe IBMCSAPI erfaßt, die sich direkt auf dem Communications Server oder im Steuerprogramm der Domäne befindet, zu der der Communications Server gehört. Diese Benutzergruppe wird während der Installation erstellt und kann mit dem Benutzer-Manager von Windows NT verwaltet werden.

Benutzer von Novell IntranetWare für SAA-Client außerhalb der Windows NT-Domäne müssen die Benutzer-ID und das Kennwort auf allen Servern angeben, die für denselben Bereich konfiguriert sind.

Wo wird der Bereich konfiguriert?

Jedem Server werden über die **Knotenkonfiguration** ein oder mehrere Bereiche zugeordnet. Clients, die diese Server verwenden, müssen so konfiguriert sein, daß sie zu Servern innerhalb eines bestimmten Bereichs oder zu Servern ohne Bereich Verbindungen aufbauen. Weitere Informationen zum Konfigurieren von Clients können im Handbuch *Client/Server Communications Programming* nachgelesen werden.

Wie verhält sich der Bereich zu SLP?

Der Bereich bei Communications Server steht in direktem Zusammenhang zum SLP-Bereich (SLP = Service Location Protocol). Deshalb können sich SLP-Verzeichnisagenten in dem Netz befinden, das die von Communications Server konfigurierten Bereiche enthält. Wenn zugelassen werden soll, daß Communications Server-Services von den Clients nach Bereichen lokalisiert werden, ist zu bedenken, in welcher Relation die Bereiche zum gesamten Netz stehen. Gibt es in einem Netz sowohl Services ohne Bereich als auch Services, für die ein bestimmter Bereich konfiguriert ist, können die Services ohne Bereich alle Anforderungen für einen bestimmten Bereich erfüllen. Dies kann zu einer stärkeren Belastung der Service- und Verzeichnisagenten führen, die die Services ohne Bereich unterstützen.

Anmerkung: Wenn der SNA-API-Client für den Verbindungsaufbau zu Servern ohne Bereich konfiguriert ist, antworten nur Server ohne Bereich.

Wenn im Standortnetz Verzeichnisagenten (für Aufwärtsskalierung) verwendet werden sollen, sollten sie so konfiguriert werden, daß sie dieselben Bereiche verarbeiten, die auch für Communications Server konfiguriert sind. Wenn Services ohne Bereich in Netzen mit Verzeichnisagenten verwendet werden sollen, sollte außerdem mindestens ein Verzeichnisagent ohne Bereich konfiguriert werden.

Communications Server beinhaltet einen SLP-Serviceagenten, der auf jedem Server installiert wird, auf dem Communications Server installiert wird. Im Netz braucht keine weitere SLP-Unterstützung installiert zu werden, damit TCP/IP-Lastausgleich und die Discovery-Funktion von Communications Server ordnungsgemäß funktionieren.

Aktuelle Auslastung überwachen

Die aktuelle Auslastung von LU 6.2 und von abhängigen LUs kann mit dem Systemmonitor von Windows NT überwacht werden. Die Leistungsüberwachung kann über die Auswahl **Verwaltung (Allgemein)** im Menü **Programme** gestartet werden.

In der Anzeige "Systemmonitor" die Option **Diagramm erweitern** im Aktionsmenü **Bearbeiten** auswählen. Im Feld **Objekt** die Option **IBM SNA-Lastausgleich** auswählen. Die beiden folgenden Zähler werden aufgelistet:

LU0/LU3-Last Mit diesem Zähler kann die Auslastung abhängiger LUs überwacht werden.

LU6.2-Last Mit diesem Zähler kann die Auslastung von LUs 6.2 überwacht werden.

Die Ergebnisse der Lastüberwachung können zur späteren Verwendung gespeichert werden.

Planung für Sicherungs-Host-Verbindungen

Für Umgebungen, in denen Sicherungs-Host-Verbindungen zu den von Datenstationsemulationssitzungen verwendeten primären Verbindungen erforderlich sind, stellt Communications Server entsprechende Optionen zur Verfügung. Damit können Host-Verbindungen konfiguriert werden, die in Reaktion auf Fehlerbedingungen aktiviert werden. Welche Optionen dafür verwendet werden können, hängt von der gewünschten Sicherungsstufe ab:

- Um vollständige Systemdatensicherung zwischen Server-Knoten zu ermöglichen, die IP- oder IPX-Datenstationsemulationssitzungen im LAN unterstützen, sollte die verwendete Umgebung über den fehlertoleranten Modus verfügen.
- Um vollständige Systemdatensicherung zwischen Server-Knoten zu ermöglichen, die IP- oder IPX-Datenstationsemulationssitzungen außerhalb eines LANs unterstützen, darf die verwendete Umgebung nicht über den fehlertoleranten Modus verfügen. In diesem Fall sollte auf dem Sicherungssystem eine zweite identische Communications Server-Installation konfiguriert werden.
- Um die Sicherung innerhalb eines Server-Knotens zu aktivieren, darf der fehlertolerante Modus nicht verwendet werden. In diesem Fall sollten für die Verbindungsdefinitionen in der Sicherungsumgebung die normalen Optionen verwendet werden.

Diese Optionen werden in den nächsten Abschnitten beschrieben.

Planung für Ausweichverbindungen zwischen Servern mit fehlertolerantem Modus

Unter Communications Server können Host-Verbindungen so konfiguriert werden, daß sie automatisch aktiviert werden, wenn ein kritischer Server ausfällt. Dies bedeutet, daß konfigurierte Verbindungen zu einem Host durch Aktivierung alternativer Verbindungen auf einem Sicherungs-Server weiter benutzt werden können. Diese Funktion wird als fehlertoleranter Modus bezeichnet.

Für Benutzer einer Datenstationsemulationssitzung mit einer Host-Maschine, deren einleitende Verbindung infolge eines Communications Server-Fehlers ausfällt, ermöglicht der fehlertolerante Modus den Versuch, die Verbindung zur Host-Maschine über einen anderen Communications Server automatisch wiederherzustellen. Der Server, über den die einleitende Verbindung hergestellt wird, wird als ***kritischer Server*** bezeichnet. Der Server, über den nach Ausfall des kritischen Servers eine Verbindung zur Host-Maschine hergestellt wird, wird als ***Sicherungs-Server*** bezeichnet. Wenn ein Ausfall des kritischen Servers festgestellt wird, startet der Sicherungs-Server automatisch bestimmte Verbindungen und übernimmt die Lizenz für die Host-Konnektivität des kritischen Servers.

Ein Server kann zugleich kritischer Server und Sicherungs-Server sein. Server können wechselseitig als Sicherungs-Server füreinander fungieren.

Der fehlertolerante Modus ermöglicht Sicherungs-Server-Unterstützung für IP- und IPX-Emulationssitzungen im LAN. Der fehlertolerante Modus bietet keine Sicherungs-Server-Unterstützung für die SNA-Umgebung.

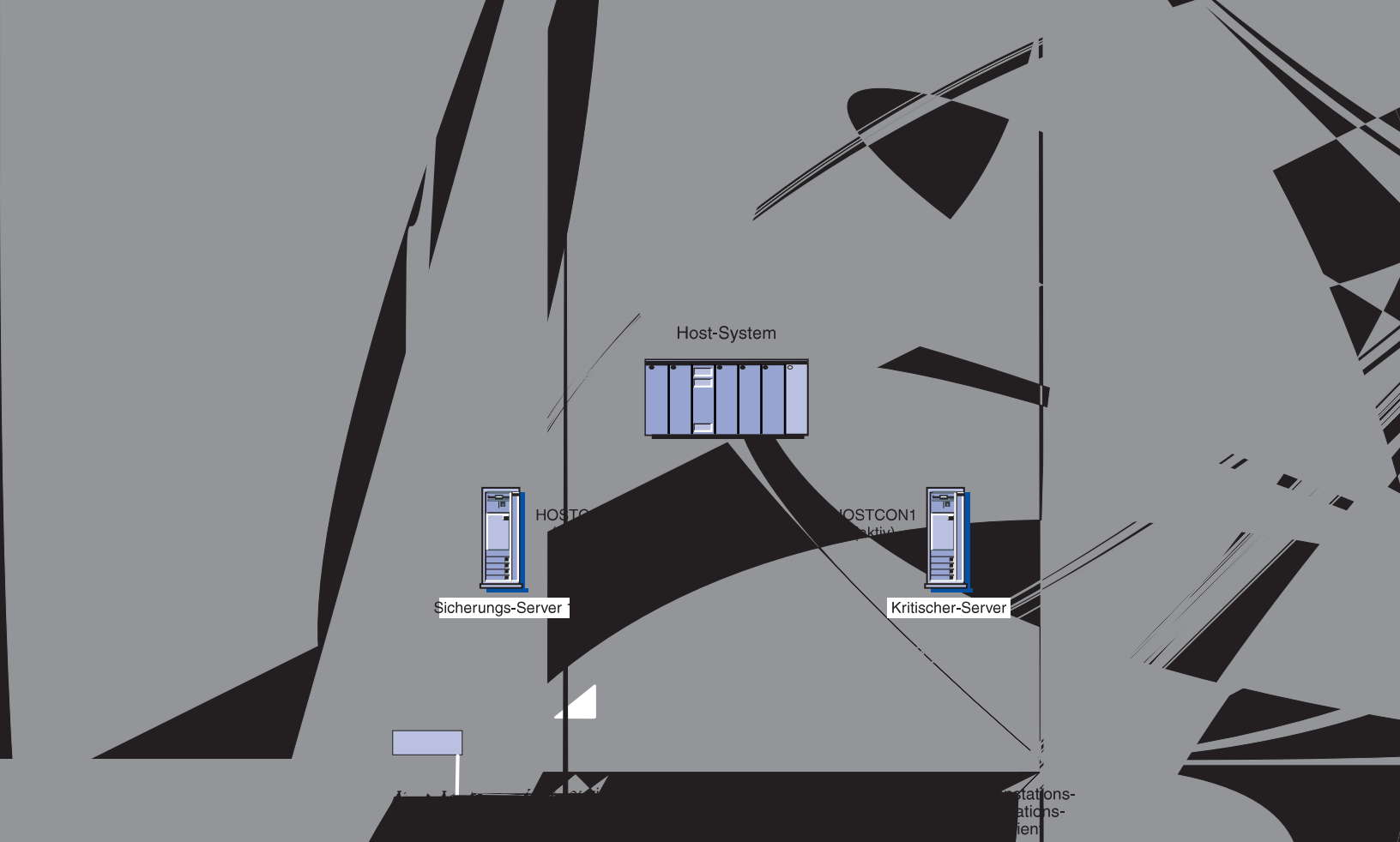


Abbildung 38. Kritischer Server mit einem Sicherungs-Server

In Abb. 39 ist jeder Sicherungs-Server mit einer Teilausweichverbindung für HOSTCON1 konfiguriert (HOSTCON1 stellt die primäre Host-Konnektivität auf dem kritischen Server zur Verfügung). Die beiden Sicherungs-Server stellen zusammen eine vollständige Sicherung für HOSTCON1 zur Verfügung. Die gestrichelten Linien zwischen den Sicherungs-Servern und den Datenstationsemulations-Clients sind nicht aktiv, solange der kritische Server betriebsbereit ist.

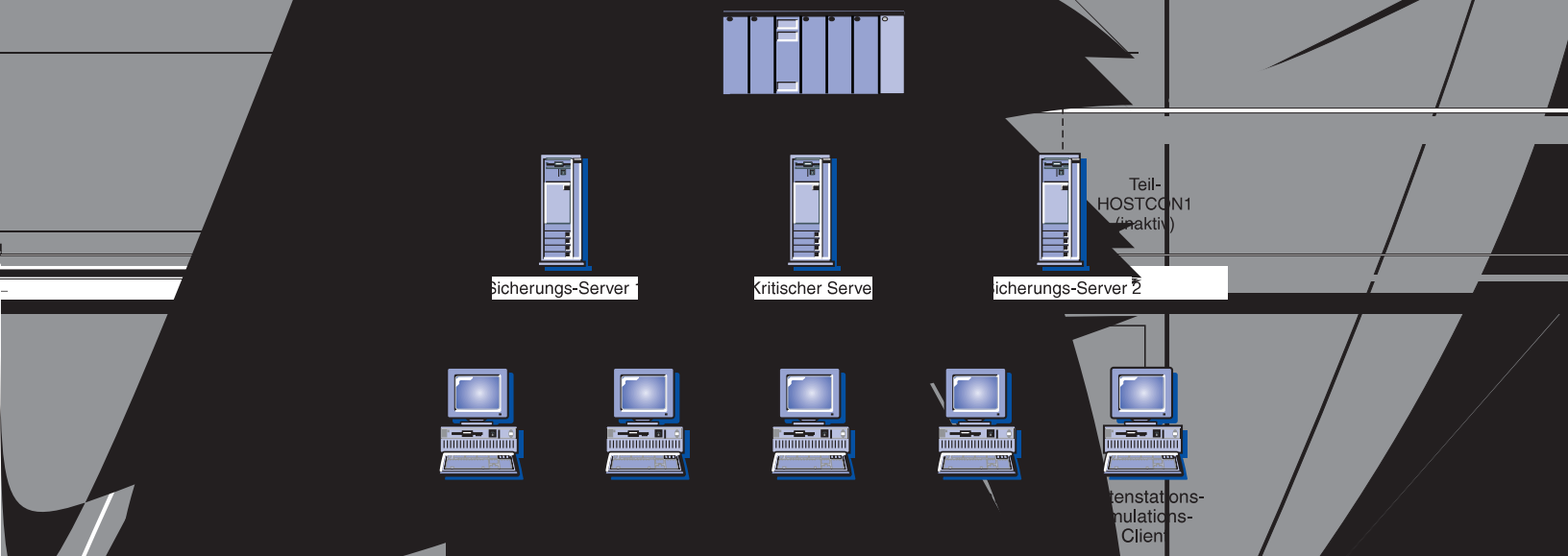


Abbildung 39. Kritischer Server mit zwei Sicherungs-Servern

Wenn der kritische Server ausfällt, wird die Wiederherstellung wie folgt ausgeführt:

1. Der Sicherungs-Server, der Host und die Datenstationsemulationssoftware auf der Datenstation stellen den Ausfall ungefähr zur gleichen Zeit fest.
2. Die in der kritischen Server-Konfiguration des Sicherungs-Servers angegebenen Verbindungen werden automatisch aktiviert, und ihre Konnektivität zur Host-Maschine wird hergestellt.
3. Die Datenstation leitet eine neue Sitzung mit dem Sicherungs-Server ein, der zuvor seine kritischen Server-Verbindungen aktiviert hat.
4. Die Datenstation nimmt Kontakt zur Host-Maschine auf und zeigt eine Anmeldeaufforderung für den Benutzer an.

Anmerkung: Wenn der kritische Server wieder betriebsbereit wird, werden die bei seinem Ausfall aktivierten Sicherungs-Server-Verbindungen nicht automatisch inaktiviert. Der Benutzer muß die Sicherungs-Server-Verbindungen manuell inaktivieren.

Produktions-Server oder dedizierten Sicherungs-Server für fehlertoleranten Modus verwenden

Es ist nicht zulässig, die gleichen Communications Server-Lizenzen auf mehreren Servern zu installieren, die sich in einem Netz befinden. Zum Installieren von Communications Servern auf mehreren Servern muß für jeden Server ein zusätzliches Communications Server-Paket gekauft werden.

Vor dem Konfigurieren eines Communications Servers für den fehlertoleranten Modus muß entschieden werden, ob der Communications Server als Produktions- und Sicherungs-Server oder als dedizierter Sicherungs-Server verwendet werden soll.

Produktions-Server verwenden

Ein ***Produktions-Server*** ist ein Communications Server, mit dem die täglichen DFV-Anforderungen abgedeckt werden. In dieser Umgebung wird Communications Server mit Host-Verbindungen konfiguriert, die unabhängig von einem Ausfallszenario für den kritischen Server aktiviert werden. Zum Aktivieren und Verwenden solcher Verbindungen müssen zunächst die erforderlichen Lizenzen erworben. Es ist nicht zulässig, die gleichen Communications Server-Lizenzen auf mehreren Servern zu installieren. Zum Installieren von Communications Server als Produktions-Server auf mehreren Systemen muß für jede Server-Installation ein zusätzliches Communications Server-Paket gekauft werden.

Für die gleichzeitige Verwendung eines Communications Servers als Produktions-Server und als Sicherungs-Server gelten keine besonderen Lizenzierungsvoraussetzungen. Es genügt, Communications Server und die erworbenen Produktions-Server-Lizenzen für Communications Server zu installieren.

Für die Verwendung von Communications Server als Produktions-Server sind keine zusätzlichen Lizenzen erforderlich. Hierfür genügen die ordnungsgemäß erworbenen Basislizenzen der kritischen Server, die der Communications Server als Sicherungs-Server überwachen soll. Für den Sicherungs-Server sind keine speziellen Lizenzen erforderlich. Wenn der Sicherungs-Server den Ausfall eines kritischen Servers feststellt, aktiviert er automatisch die für diesen kritischen Server konfigurierten Verbindungen und paßt die Sicherungs-Server-Lizenzen an die für

den kritischen Server geltenden Lizenzen an. Communications Server führt die Lizenzverwaltung im fehlertoleranten Modus ohne Benutzereingriffe aus.

Wurden die für den kritischen Server konfigurierten Verbindungen jedoch außerhalb eines Ausfallszenarios für kritische Server aktiviert, werden die für den kritischen Server geltenden Lizenzen vom Sicherungs-Server nicht automatisch angepaßt, d. h., die Lizenzierung des Sicherungs-Servers muß separat erfolgen.

Dedizierten Server verwenden

Ein ***dedizierter*** Sicherungs-Server fungiert nicht als Produktions-Server und aktiviert keine Verbindungen außerhalb eines Ausfallszenarios für kritische Server. Auf einem solchen Server können weder beim Systemstart noch manuell Verbindungen aktiviert werden. Er übernimmt ausschließlich die Überwachung eines oder mehrerer kritischer Server.

Für einen dedizierten Sicherungs-Server sind keine zusätzlichen Lizenzen erforderlich, vielmehr genügen die ordnungsgemäß erworbenen Basislizenzen der kritischen Server, für deren Überwachung dieser Server konfiguriert ist. Communications Server führt die Lizenzverwaltung im fehlertoleranten Modus ohne Benutzereingriffe aus.

Planung für vollständige Umgebung mit fehlertolerantem Modus

Szenarios für den fehlertoleranten Modus beinhalten normale Funktionsszenarios von Communications Server zur Unterstützung von Emulations-Clients über IP oder IPX im LAN sowie einige spezielle Operationen für den fehlertoleranten Modus.

Beim Konfigurieren einer Umgebung mit fehlertolerantem Modus gelten die beiden folgenden Grundbedingungen:

- Zwei oder mehr Datenfernverarbeitungs-Server müssen so konfiguriert werden, daß kompatible Verbindungen zu einer Host-Maschine zur Verfügung gestellt werden. Der Sicherungs-Server muß über eine Konfiguration als kritischer Server für denjenigen Server verfügen, der die primäre Konnektivität zur Host-Maschine bereitstellt.
- Die Datenstationsemulations-Client-Software, die über den Server Emulationssitzungen auf der Host-Maschine für Benutzer bereitstellt, muß bei Ausfall des kritischen Servers Ausweichpfade zum Sicherungs-Server aktivieren können.

Manche Emulations-Clients stellen möglicherweise keine Ausweichpfade zur Verfügung. Bei der Planung für Umgebungen mit fehlertolerantem Modus müssen die Emulationssoftware und die verwendete Konnektivitätsart zwischen Client und Server sorgfältig berücksichtigt werden. Es folgen einige Auswahlmöglichkeiten für Ausweichpfade:

- **Dynamischer Wechsel** - Ein Emulations-Client unterstützt die Konfiguration mehrerer benannter Server, die in einer bestimmten Reihenfolge kontaktiert werden, um über den Server eine Verbindung zur Host-Maschine für eine Emulationssitzung herzustellen. Der dynamische Wechsel ermöglicht es, den Sicherungs-Server so zu konfigurieren, daß er kontaktiert wird, wenn der kritische Server nicht erreichbar ist. Wenn beim Ausfall des kritischen Servers Ressourcen auf dem Sicherungs-Server aktiviert werden, kontaktiert der Emulations-Client den Sicherungs-Server und richtet über ihn einen Ausweichpfad für die Verbindung zur Host-Maschine ein.

- **LU-Pools** - Ein Emulations-Client unterstützt den dynamischen Verbindungsaufbau zur Host-Maschine für eine Emulationssitzung über den Server, der momentan auf die Anfragen nach verfügbaren LUs in einem benannten Pool reagiert. Durch die LU-Poolunterstützung können Sicherungs-Server und kritische Server LUs für denselben Pool bereitstellen. Der Sicherungs-Server ist zwar definiert, jedoch zunächst nicht aktiv. Wenn beim Ausfall des kritischen Servers die Ressourcen auf dem Sicherungs-Server aktiviert werden, reagiert der Sicherungs-Server auf Anforderungen des Emulations-Clients für eine LU aus dem Pool und richtet einen entsprechenden Ausweichpfad für die Verbindung mit der Host-Maschine ein. LU-Pools beinhalten die folgenden Arten von Client-Unterstützung für LU-Pools:
  - Vor SLP: Bevor SLP von Communications Server unterstützt wurde, erfolgte der Client-Zugriff auf LU-Pools nach dem Zufallsprinzip oder in einer angegebenen Server-Reihenfolge.
  - SLP: Die SLP-Unterstützung von Communications Server stellt Client-Zugriff auf LU-Pools zur Verfügung; dabei wird die Sitzungsauslastung auf die an dem Pool beteiligten Server verteilt.
- **Mehrere Emulationssitzungen** - Ein Emulations-Client unterstützt das Konfigurieren von mehreren Emulationssitzungen, d. h., der Benutzer kann getrennte Sitzungen über den Sicherungs-Server und die kritischen Server konfigurieren, um die Verbindung zur Host-Maschine herzustellen. Die Verwendung von mehreren Emulationssitzungen ist komplexer als die Unterstützung für dynamischen Wechsel oder LU-Pools, weil sie manuelle Eingriffe des Emulationsbenutzers erfordert, um bei einem Server-Ausfall Ausweichpfade bereitzustellen. Wird die Verbindung zum kritischen Server unterbrochen, leitet der Benutzer manuell die Sitzung ein, mit der über den Sicherungs-Server die Verbindung zur Host-Maschine wiederhergestellt wird.

Die Unterstützung von IBM Personal Communications für TN3270E-, TN5250-, API- und QEL/MU-Emulations-Clients beinhaltet Optionen zum Bereitstellen von Ausweichpfaden über eine oder mehrere der folgenden Optionen: dynamischer Wechsel, LU-Pools und mehrere Emulationssitzungen. Einige Emulations-Clients anderer Hersteller stellen Optionen für Ausweichpfade zur Verfügung.

Fehlertoleranten Modus auf dem Sicherungs-Server konfigurieren

Zum Konfigurieren des fehlertoleranten Modus auf dem Sicherungs-Server kann die Konfigurationsoption **Kritische Server im fehlertolerantem Modus** in der Anzeige "Erweitert" der **Knotenkonfiguration** verwendet werden.

Auf dem kritischen Server muß keine Konfiguration für den fehlertoleranten Modus erstellt werden, aber der Sicherungs-Server erfordert eine solche Konfiguration. Über die Option "Erweitert" in der Anzeige **Knotenkonfiguration** können auf dem Sicherungs-Server Definitionen für kritische Server konfiguriert werden. Eine Definition für kritischen Server gibt den Namen des kritischen Servers an, der vom Sicherungs-Server überwacht wird, sowie die Namen der Verbindungen, die beim Ausfall des kritischen Servers aktiviert werden. Es können mehrere solcher Definitionen erstellt werden, über die der Sicherungs-Server mehrere kritische Server überwachen und Ausweichverbindungen für sie aktivieren kann. Nach dem Erstellen von Definitionen für kritische Server auf dem Sicherungs-Server muß der Sicherungs-Server-Knoten erneut gestartet werden, damit die Änderungen wirksam werden. Ausführliche Informationen zum Konfigurieren des fehlertoleranten Modus können der Online-Hilfe der **Knotenkonfiguration** entnommen werden.

Umgebung für fehlertolerantem Modus konfigurieren

Eine Umgebung mit fehlertolerantem Modus kann wie folgt konfiguriert werden:

1. **Den kritischen Server konfigurieren:** Der kritische Server wird ohne spezielle Konfigurationsschritte für den fehlertoleranten Modus konfiguriert. Die Host-Konnektivität ist so zu konfigurieren, daß sie mit dem mit den Emulations-Clients verwendeten Ausweichpfad übereinstimmt.
2. **Den Sicherungs-Server konfigurieren:** Hierbei gelten die beiden folgenden Grundprinzipien:
   a. Die Konfiguration der Host-Konnektivität auf dem Sicherungs-Server entspricht in etwa der des kritischen Servers, allerdings werden die Host-Verbindungen für manuelle Einleitung konfiguriert.
   b. Konfiguration des kritischen Servers auf dem Sicherungs-Server, um die bei einem Ausfall des kritischen Servers zu startenden Host-Verbindungen zu definieren.
3. **Die Emulations-Clients konfigurieren:** Die Datenstationsemulations-Clients werden so konfiguriert, daß sie der von den Servern bereitgestellten Konnektivität einen entsprechenden Ausweichpfad zuordnen.
4. **Knoten für kritischen Server und Sicherungs-Server starten:** Die Knoten sind in der üblichen Weise zu starten. Die **SNA-Knotenoperationen** können den Status des fehlertoleranten Modus für die kritischen Server und Sicherungs-Server überprüfen.
5. **Ausfall des kritischen Servers:** Wenn der kritische Server ausfällt, wird die Wiederherstellung wie folgt ausgeführt:
   a. Der Sicherungs-Server, der Host und die Datenstationsemulationssoftware auf dem Client stellen den Ausfall ungefähr zur gleichen Zeit fest.
   b. Die in der Konfiguration für kritischen Server auf dem Sicherungs-Server angegebenen Verbindungen werden aktiviert, und die Konnektivität zur Host-Maschine wird hergestellt.
   c. Der Datenstationsemulations-Client leitet eine neue Sitzung mit dem Sicherungs-Server ein. Der Sicherungs-Server führt Sitzungen mit der Host-Maschine über die Verbindung, die vom Sicherungs-Server beim Ausfall des kritischen Servers aktiviert wurde.
   d. Die Datenstation nimmt Kontakt zur Host-Maschine auf und zeigt eine Anmeldeaufforderung für den Benutzer an.
6. **Kritischer Server wieder betriebsbereit:** Wenn der kritische Server wieder aktiv ist, verwenden neue Datenstationsemulationssitzungen die Host-Konnektivität des kritischen Servers. Die über den Sicherungs-Server geleiteten Datenstationsemulationssitzungen bleiben aktiv, bis die Sitzungen beendet werden.

   Die vom Sicherungs-Server hergestellten Host-Verbindungen müssen vom Benutzer manuell inaktiviert werden. Die manuelle Inaktivierung der Sicherungs-Server-Verbindungen sollte außerhalb der üblichen Arbeitszeiten erfolgen. Die Benutzer von Datenstationsemulationssitzungen über den Sicherungs-Server sollten entsprechend informiert werden, bevor diese Verbindungen inaktiviert werden.

Planung für Ausweichverbindungen zwischen Servern ohne fehlertoleranten Modus

Der fehlertolerante Modus steht nur in Umgebungen zur Verfügung, die IP- oder IPX-Datenstationsemulationssitzungen im LAN unterstützen. Dies bedeutet, daß manche Umgebungen keine Ausweichkonnektivität im fehlertoleranten Modus bereitstellen können. Viele der Überlegungen zur Planung von Sicherungsumgebungen ohne fehlertoleranten Modus entsprechen der Planung für Umgebungen mit fehlertolerantem Modus. Eine Sicherungsumgebung ohne fehlertoleranten Modus kann wie folgt konfiguriert werden:

1. Auf dem Sicherungs-Server ein zusätzlich erworbenes Communications Server-Paket mit entsprechenden Lizenzen für Sicherungs-Host-Verbindungen zum primären Server installieren.
2. Auf dem Sicherungs-Server Host-Verbindungen konfigurieren, die bei Bedarf als Ausweichverbindungen aktiviert werden können.
3. Die Datenstationsemulations-Clients so konfigurieren, daß sie automatische Weiterleitung zu den Ressourcen auf dem Sicherungs-Server bereitstellen, wenn der primäre Server ausfällt. Diese Weiterleitung zum Sicherungs-Server sollte nur ermöglicht werden, wenn der Ausfall des primären Servers festgestellt wird.
4. Beide Knoten werden gestartet, aber zunächst stellt nur der primäre Knoten mit seinen aktiven übergeordneten Verbindungen die Konnektivität zum Host bereit.
5. Wenn der primäre Server ausfällt, versuchen die Datenstationsemulations-Clients, Verbindungen über den Sicherungs-Server herzustellen. Die Host-Verbindungen auf dem Sicherungs-Server werden aktiviert.
6. Die auf dem Sicherungs-Server installierte doppelte Lizenz gewährleistet, daß der Sicherungs-Server für Clients zur Verfügung steht, die vorher Verbindungen über den primären Server geleitet haben.
7. Wenn der primäre Server wieder betriebsbereit ist, müssen die Verbindungen auf dem Sicherungs-Server manuell inaktiviert werden.

Planung für Ausweichverbindungen in einem einzelnen Server

In einem einzelnen Server kann kein fehlertoleranter Modus für Ausweichkonnektivität verwendet werden, weil der fehlertolerante Modus nur für Umgebungen mit Ausweichverbindungen zwischen mehreren Servern zur Verfügung steht. Einige der Überlegungen zur Planung von Sicherungsumgebungen in einem einzelnen Server entsprechen jedoch der Planung für den fehlertoleranten Modus.

Die Unterschiede sind in den folgenden Schritten für Ausweichverbindungen in einem einzelnen Server zusammengefaßt:

1. Auf dem Server, der als Gateway zum Host dient, primäre Verbindungen und Ausweichverbindungen konfigurieren, die LUs für den gleichen LU-Pool bereitstellen. Die Ausweichverbindung muß jedoch so konfiguriert werden, daß sie nur auf Anforderung aktiviert wird.
2. Die Datenstationsemulations-Clients so konfigurieren, daß sie Verbindungen über den LU-Pool herstellen.
3. Wenn die primären Verbindungen ausfallen oder im Pool keine weiteren LUs verfügbar sind, löst der nächste Versuch, eine Verbindung zu dem Pool herzustellen, die Aktivierung der Ausweichverbindung aus.
4. Wenn der primäre Server wieder betriebsbereit ist, müssen die Verbindungen auf dem Sicherungs-Server manuell inaktiviert werden.

Planung für X.25

Die Konfiguration des X.25-Netzes muß sorgfältig geplant werden. Folgendes muß beachtet werden:

- Um ein öffentliches Netz mit Paketvermittlung zu benutzen, muß für jede benötigte Leitung (Verbindung) eine Genehmigung zur Netzteilnahme beantragt werden. Da es etwas dauern kann, bis eine Verbindung bereitgestellt wird, sollte der X.25-Netzbetreiber frühzeitig informiert werden.
- Es sollte bekannt sein, welche Funktionen auf dem X.25-Netz verfügbar sind und welche Funktionen benötigt werden. Der Netzbetreiber liefert normalerweise ein technisches Handbuch zum Netz, das der Benutzer erwerben und konsultieren sollte.
- Die Informationen zu logischen Kanälen, die für PVCs und SVCs erforderlich sind, zusammenstellen.
  - Bis zu 16 Gruppen von je 256 logischen Kanälen können definiert werden.
  - Die Gruppennummer liegt zwischen 0 und 15.
  - Die Nummern der logischen Kanäle innerhalb der Gruppe liegen zwischen 0 und 255.

    Durch Multiplikation der Gruppennummer mit 256 und Hinzufügung der Nummer des logischen Kanals ergibt sich eine Nummer zwischen 0 und 4095, durch die ein logischer Kanal eindeutig gekennzeichnet wird. Diese Kombination wird manchmal als Nummer des logischen Kanals bezeichnet.

    Anmerkungen:

    1. Wenn für CCITT 1984 oder 1988 angegeben wird, beträgt die maximale Anzahl logischer Kanäle 4095.
    2. Wenn für CCITT 1980 angegeben wird, beträgt die maximale Anzahl logischer Kanäle 1024.
  - Gruppen logischer Kanäle können als Nur ankommend (reserviert für Anrufe von anderen DEEs), als Nur abgehend (reserviert für Anrufe bei anderen DEEs) oder als abgehend und ankommend definiert werden.
- Anzahl der virtuellen Verbindungen, die bei der Verwendung von SNA benötigt wird
- Art der benötigten PVCs
- Die Kombination der nur ankommenden, nur abgehenden und abgehenden und ankommenden logischen Kanäle
- Die maximal benötigte Paketgröße und welche Größe vom X.25-Netz unterstützt wird
- Genaue Informationen darüber, welche wahlfreien X.25-Funktionen die X.25-Anwendungsprogramme verwenden

  Die X.25-Empfehlungen von CCITT definieren eine Reihe wahlfreier Funktionen, die das Netz möglicherweise unterstützt.

Einige Funktionen haben Parameter, die das Anwendungsprogramm während des Anrufaufbaus und der Anrufauflösung über die Funktionsfelder in den Rufanforderungs-, Rufannahme- und Auflöseanforderungspaketen angeben oder vereinbaren kann.

Die X.25-Verbindung kann so konfiguriert werden, daß sie während des Anrufaufbaus folgende Funktionen unterstützt:

- Geschlossene Benutzergruppe
- Netzbenutzer-ID
- Paket- und Fenstergrößenvereinbarung
- Gebührenübernahme

Die Funktionen werden während der Konfiguration der X.25-DLC definiert.

- Genaue Informationen zu speziellen Anforderungen für Rahmen- und Paketparameter. Die Standardwerte für diese Konfigurationsparameter wurden sorgfältig ausgewählt, um den meisten Situationen gerecht zu werden. Eventuell legt der Netzbetreiber bestimmte Werte fest oder empfiehlt bestimme Werte.

  Um Fehler zu vermeiden, müssen die Konfigurationsparameter mit der Genehmigung der Netzteilnahme übereinstimmen. Wurden z. B. 20 logische Kanäle für SVCs konfiguriert, aber nur für 10 liegt eine Teilnehmerberechtigung vor, stellt die DÜE beim Versuch, den 11. logischen Kanal zu verwenden, einen Fehler fest.

Mögliche X.25-Verbindungen

Abb. 40 zeigt, wie ein X.25-Netz eine Verbindung von einem SNA-Gateway zu einem Host zur Verfügung stellen kann.

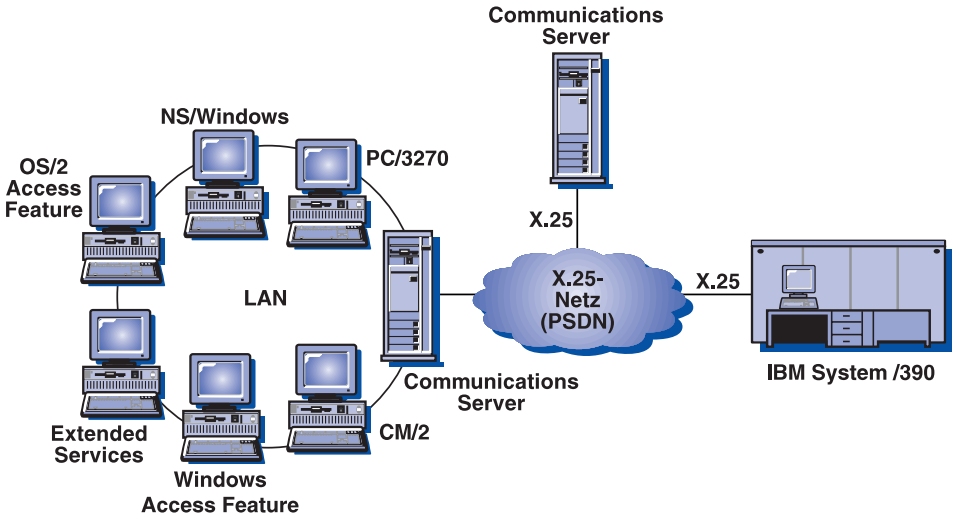


Abbildung 40. X.25- und SNA-Gateway-Konnektivität

X.25-Netzgebühren

Die tatsächlichen Gebühren hängen von den Modalitäten der X.25-Netzbetreiber ab; aber Gebühren bestehen normalerweise aus einigen oder allen der folgenden Elemente:

- Installationsgebühr

  Eine einmalige Installationsgebühr bei der ersten Genehmigung für das X.25-Netz.

- Regelmäßige Mietgebühr

  Diese Gebühr hängt von den Funktionen ab, die vom Netzbetreiber bereitgestellt werden. Wahrscheinlich ist beispielsweise eine Gebühr für jede wahlfreie Netzeinrichtung zu bezahlen, für die eine Genehmigung erworben wurde. Außerdem wird vermutlich eine Gebühr für jeden logischen Kanal fällig. PVCs kosten in der Regel mehr als SVCs, da sie dedizierte Netzressourcen benötigen.

- Benutzungsgebühr

  Diese Gebühr hängt davon ab, wie lange die logische Verbindung zum Netz besteht, möglicherweise ist eine Mindestgebühr zu entrichten.

- Mengengebühr

  Diese Gebühr hängt von der Datenmenge ab, die während eines Berechnungszeitraum über das Netz übertragen wird.

Host-Konnektivität konfigurieren

Datenstationen, auf denen IBM Communications Server ausgeführt wird, können mit IBM System /390-Hosts (einschließlich IBM System /370) oder IBM AS/400-Hosts verbunden werden. Viele der beim Konfigurieren von Communications Server angegebenen Werte werden auch beim Konfigurieren des Hosts verwendet. In diesem Kapitel wird die Zuordnung der Communications Server-Konfigurationsparameter zu den Host-Konfigurationsparametern beschrieben. Es enthält außerdem Tabellen der Parameter, mit denen die allgemeinen Parameter in den zwischen Communications Server und dem Host abgesetzten Makros nicht mehr erforderlich sind.

Anmerkung: Viele von den LINE-, PU- und LU-Makros abgesetzte NCP-Parameter können aus Gründen der Lesbarkeit und einfachen Codierung im Makro GROUP angegeben werden. Durch diesen Parameterabgleich wird es unnötig, in jedem nachfolgenden Makro allgemeine Parameter anzugeben. Die Möglichkeit zum Überschreiben der Parameter bleibt jedoch weiterhin erhalten.

NCP Token-Ring (NTRI) mit VTAM und Communications Server

Tabelle 7 vergleicht Host-Parameter mit den Communications Server-Parametern für IBM Token-Ring-Netzverbindungen.

Tabelle 7. Host-/PC-Parameterzuordnung: IBM Token-Ring-Netz - NTRI-Definition

NTRI/NCP	Communications Server-Profil/-Parameter	Bemerkungen
GROUP ECLTYPE = PHY	DLC-Art: LAN	
LINE LOCADDR	Verbindungen konfigurieren LAN **Zieladresse**	Der unter Communications Server für diesen Parameter festgelegte Wert muß die Adresse des IBM Token-Ring-Netzadapters auf der Host-Steuereinheit sein.

Token-Ring mit VTAM-Wählnetz und Communications Server

Tabelle 8 vergleicht Host-Parameter mit den Communications Server-Parametern für IBM Token-Ring-Netzverbindungen über ein VTAM-Wählnetz.

Tabelle 8 (Seite 1 von 2). Host-/PC-Parameterzuordnung: IBM Token-Ring-Netz - VTAM-Wählnetz

VTAM	Communications Server-Profil/-Parameter	Bemerkungen
IDBLK=	Knoten konfigurieren ID des lokalen Knotens **Block-ID**	Der Host-Parameter IDBLK muß mit den ersten drei hexadezimalen Zeichen der **ID des lokalen Knotens** übereinstimmen, die für Communications Server standardmäßig X'05D' lauten. Diesen Parameter bei Verwendung von Wählleitungen angeben und bei Verwendung von CPNAME= weglassen.

Tabelle 8 (Seite 2 von 2). Host-/PC-Parameterzuordnung: IBM Token-Ring-Netz - VTAM-Wählnetz

VTAM	Communications Server-Profil/-Parameter	Bemerkungen
IDNUM=	Knoten konfigurieren ID des lokalen Knotens **ID der physischen Einheit**	Der Host-Parameter IDNUM muß mit den letzten 5 hexadezimalen Zeichen von **ID des lokalen Knotens** übereinstimmen. Diesen Parameter bei Verwendung von Wählleitungen angeben und bei Verwendung von CPNAME= weglassen.
CPNAME=	Knotendefinition Knoten konfigurieren **Vollständig qualifizierter CP-Name** (zweites Feld)	Diesen Parameter bei Verwendung von Wählleitungen angeben und bei Verwendung von IDBLK= und IDNUM= weglassen.
LOCADDR	Host-LUs konfigurieren **NAU-Adresse**	Diese Parameter müssen denselben Wert haben. Bei unabhängigen LUs empfiehlt VTAM, anstelle der Codierung LOCADDR=0 eine CDRSC-Definition zu erstellen oder den Operanden DYNLU zu verwenden. Weitere Informationen zum Codieren von CDRSC-Definitionen für unabhängige LUs enthält der *VTAM Network Implementation Guide*. Für abhängige LUs sind keine Host-Definitionen erforderlich, wenn SDDLU oder dynamische Definition für unabhängige LUs unter VTAM 3.4 oder höher verwendet wird.
MAXDATA	LAN-Einheit konfigurieren **Maximale PIU-Größe** (265–65535)	Diese Werte müssen nicht übereinstimmen.
MAXOUT	LAN-Einheit konfigurieren **Anzahl Empfangspuffer** (2–64)	Die **Anzahl Empfangspuffer** in Communications Server sollte dem Wert des Host-Parameters MAXOUT entsprechen.

Token-Ring-Netzadapter IBM 9370 und Communications Server

Tabelle 9 vergleicht 9370-Host-Parameter mit den Communications Server-Parametern für IBM Token-Ring-Netzverbindungen.

Tabelle 9. Host-/PC-Parameterzuordnung: IBM Token-Ring-Netz 9370-VTAM-LAN

VTAM	Communications Server-Profil/-Parameter	Bemerkungen
VBUILD TYPE = LAN	DLC-Art: LAN	
PORT MACADDR=	Verbindung konfigurieren LAN **Zieladresse**	Die beim Anpassen von Communications Server angegebene Zieladresse muß die Adresse des Token-Ring-Adapters IBM 9370 sein.
PORT SAPADDR=04	Verbindung konfigurieren LAN **Ferner SAP**	Diese Werte müssen übereinstimmen.
ADDR=04 (nur abgehend)	Verbindung konfigurieren LAN **Lokaler SAP**	Diese Werte müssen übereinstimmen.

Establishment Controller IBM 3174 und Communications Server

Tabelle 10 vergleicht die Parameter des Establishment Controller IBM 3174 mit den Communications Server-Parametern für IBM Token-Ring-Verbindungen.

Tabelle 10. Parameterzuordnung zwischen Establishment Controller IBM 3174 (Token-Ring) und Communications Server

IBM 3174	Communications Server-Profil/-Parameter	Bemerkungen
Obere Adreßgrenze größer als 104: CUA	DLC-Art: LAN	
Token-Ring-Adresse für Gateway	Verbindungen konfigurieren LAN **Zieladresse**	Diese Werte müssen übereinstimmen.
Ringübertragungsdefinition. W= max. abgehende Fenster F=0, W = 1-7, F=1, W = 1-7, F=2, W = 1-4, F=3, W = 1-2	Einheiten konfigurieren LAN **Anzahl Empfangspuffer** (1–8)	Der Communications Server-Parameter **Anzahl Empfangspuffer** sollte den Wert 3174 W haben.

VTAM-PU des Establishment Controller IBM 3174 und Communications Server

Tabelle 11 vergleicht die VTAM-PU-Parameter des Establishment Controller IBM 3174 mit den Communications Server-Parametern für IBM Token-Ring-Verbindungen.

Tabelle 11 (Seite 1 von 2). Host-/PC-Parameterzuordnung: IBM Token-Ring-Netz - VTAM-PU des Establishment Controller IBM 3174 und Communications Server

VTAM	Communications Server-Profil/-Parameter	Bemerkungen
CUADDR (lokal) oder ADDR (fern)	(keine)	Wird von dem Establishment Controller IBM 3174 der IBM Token-Ring-Adresse zugeordnet
MAXDATA (nur fern)	Einheiten konfigurieren LAN **Maximale PIU-Größe** (99–65535)	Der auf der Communications Server-Datenstation festgelegte Wert für maximale PIU-Größe muß mit dem auf dem Host definierten Wert übereinstimmen.
MAXOUT (nur fern)	Einheiten konfigurieren LAN **Anzahl Empfangspuffer** (2–64)	Der Communications Server-Parameter **Anzahl Empfangspuffer** sollte dem Wert MAXOUT entsprechen.

Tabelle 11 (Seite 2 von 2). Host-/PC-Parameterzuordnung: IBM Token-Ring-Netz - VTAM-PU des Establishment Controller IBM 3174 und Communications Server

VTAM	Communications Server-Profil/-Parameter	Bemerkungen
LOCADDR	Host-LUs konfigurieren **NAU-Adresse**	Diese Parameter müssen denselben Wert haben. Bei unabhängigen LUs empfiehlt VTAM, anstelle der Codierung LOCADDR=0 eine CDRSC-Definition zu erstellen oder den Operanden DYNLU zu verwenden. Weitere Informationen zum Codieren von CDRSC-Definitionen für unabhängige LUs enthält der *VTAM Network Implementation Guide*. Für abhängige LUs sind keine Host-Definitionen erforderlich, wenn SDDLU oder dynamische Definition für unabhängige LUs unter VTAM 3.4 oder höher verwendet wird.

Ethernet mit VTAM-Wählnetz und Communications Server

Tabelle 12 vergleicht Host-Parameter mit den Communications Server-Parametern für Ethernet-Netzverbindungen über ein VTAM-Wählnetz.

Tabelle 12 (Seite 1 von 2). Host-/PC-Parameterzuordnung: Ethernet-VTAM-Wählnetz

VTAM	Communications Server-Profil/-Parameter	Bemerkungen
IDBLK=	Knoten konfigurieren ID des lokalen Knotens **Block-ID**	Der Host-Parameter IDBLK muß mit den ersten drei hexadezimalen Zeichen der **ID des lokalen Knotens** übereinstimmen, die für Communications Server standardmäßig X'05D' lauten. Diesen Parameter bei Verwendung von Wählleitungen angeben und bei Verwendung von CPNAME= weglassen.
IDNUM=	Knoten konfigurieren ID des lokalen Knotens **ID der physischen Einheit**	Der Host-Parameter IDNUM muß mit den letzten 5 hexadezimalen Zeichen von **ID des lokalen Knotens** übereinstimmen. Diesen Parameter bei Verwendung von Wählleitungen angeben und bei Verwendung von CPNAME= weglassen.
CPNAME=	Knotendefinition Knoten konfigurieren **Vollständig qualifizierter CP-Name** (zweites Feld)	Diesen Parameter bei Verwendung von Wählleitungen angeben und bei Verwendung von IDBLK= und IDNUM= weglassen.

Tabelle 12 (Seite 2 von 2). Host-/PC-Parameterzuordnung: Ethernet-VTAM-Wählnetz

VTAM	Communications Server-Profil/-Parameter	Bemerkungen
LOCADDR	Host-LUs konfigurieren **NAU-Adresse**	Diese Parameter müssen denselben Wert haben. Bei unabhängigen LUs empfiehlt VTAM, anstelle der Codierung LOCADDR=0 eine CDRSC-Definition zu erstellen oder den Operanden DYNLU zu verwenden. Weitere Informationen zum Codieren von CDRSC-Definitionen für unabhängige LUs enthält der *VTAM Network Implementation Guide*. Für abhängige LUs sind keine Host-Definitionen erforderlich, wenn SDDLU oder dynamische Definition für unabhängige LUs unter VTAM 3.4 oder höher verwendet wird.
MAXDATA	LAN-Einheit konfigurieren **Maximale PIU-Größe** (265–65535)	Diese Werte müssen nicht übereinstimmen.
MAXOUT	LAN-Einheit konfigurieren **Anzahl Empfangspuffer** (2–64)	Die **Anzahl Empfangspuffer** in Communications Server sollte dem Wert des Host-Parameters MAXOUT entsprechen.

VTAM/NCP und Communications Server (SDLC)

Tabelle 13 vergleicht VTAM/NCP-Host-Parameter mit den Communications Server-Parametern für SDLC-Verbindungen.

Tabelle 13 (Seite 1 von 3). Host-/PC-Parameterzuordnung: SDLC

VTAM/NCP	Communications Server-Profil/-Parameter	Bemerkungen
NETID=	Knoten konfigurieren **Vollständig qualifizierter CP-Name** (erstes Feld)	Dieser Parameter kann für Standleitungen und für Wählleitungen verwendet werden. Dieser Parameter kennzeichnet das SNA-Netz, zu dem mit Communications Server eine Verbindung hergestellt wird.
NAME PU		Ein PU-Name muß immer verwendet werden. Dieser PU-Name sollte ein Name sein, der sich vom lokalen CP-Namen unterscheidet, damit eine LU für den Steuerpunkt definiert werden kann.
IDBLK=	Knoten konfigurieren ID des lokalen Knotens **Block-ID**	Der Host-Parameter IDBLK muß mit den ersten drei hexadezimalen Zeichen der **ID des lokalen Knotens** übereinstimmen, die für Communications Server standardmäßig X'05D' lauten. Diesen Parameter bei Verwendung von Wählleitungen angeben und bei Verwendung von CPNAME= weglassen.
IDNUM=	Knoten konfigurieren ID des lokalen Knotens **ID der physischen Einheit**	Der Host-Parameter IDNUM muß mit den letzten 5 hexadezimalen Zeichen von **ID des lokalen Knotens** übereinstimmen. Diesen Parameter bei Verwendung von Wählleitungen angeben und bei Verwendung von CPNAME= weglassen.

Tabelle 13 (Seite 2 von 3). Host-/PC-Parameterzuordnung: SDLC

VTAM/NCP	Communications Server-Profil/-Parameter	Bemerkungen
CPNAME=	Knotendefinition Knoten konfigurieren **Vollständig qualifizierter CP-Name** (zweites Feld)	Diesen Parameter bei Verwendung von Wählleitungen angeben und bei Verwendung von IDBLK= und IDNUM= weglassen.
LNCTL=SDLC	DLC-Art: SDLC-WAC, SDLC-MPA, COM-Anschluß (je nach verwendeter Hardware)	SDLC muß hier ausgewählt sein. Dieser Parameter wird für Standleitungen und für Wählleitungen verwendet.
LOCADDR	Host-LUs konfigurieren **NAU-Adresse**	Diese Parameter müssen denselben Wert haben. Bei unabhängigen LUs empfiehlt VTAM, anstelle der Codierung LOCADDR=0 eine CDRSC-Definition zu erstellen oder den Operanden DYNLU zu verwenden. Weitere Informationen zum Codieren von CDRSC-Definitionen für unabhängige LUs enthält der *VTAM Network Implementation Guide*. Für abhängige LUs sind keine Host-Definitionen erforderlich, wenn SDDLU oder dynamische Definition für unabhängige LUs unter VTAM 3.4 oder höher verwendet wird.
NRZI=YES/NO	Verbindungen konfigurieren SDLC-WAC, SDLC-MPA, COM-Anschluß **NRZI-Verschlüsselung**	Communications Server verwendet USE_NRZI_ENCODING=0 und USE_NRZI_ENCODING=1. Dieser Parameter findet sich nur in PCMs für folgende Modemtypen: synchrone Wählleitung, synchrone Standleitung und AutoSync. Das Verschlüsselungsschema NRZI oder NRZ muß an beiden Enden einer Verbindung gleich konfiguriert sein. Wenn die Verschlüsselungsschemata nicht übereinstimmen, können die Modems zwar eine Verbindung herstellen, aber die Datenübertragung schlägt fehl, und die Verbindung wird von Communications Server nach der Überschreitung eines Zeitlimits auf Verbindungsebene (normalerweise 40 Sekunden) unterbrochen. Für Verbindungen zu einem X.25-Netz, das einen IBM Wide Area Connector verwendet, ist das Verschlüsselungsschema NRZ zu empfehlen.
DUPLEX= FULL/HALF	Verbindungen konfigurieren nur SDLC-WAC und COM-Anschluß **Vollduplex-übertragung**	Die an beiden Enden definierten Werte müssen mit dem Modemtyp und der Konfiguration übereinstimmen. Dieser Parameter wird für Standleitungen und für Wählleitungen verwendet.
(TRANSFR * BFRS) –47	Einheiten konfigurieren SDLC-WAC, SDLC-MPA, COM-Anschluß **Maximale PIU-Größe** (265–4105)	Die Wert für die maximale Größe des I-Felds muß kleiner oder gleich dem auf dem Host angegebenen Wert (TRANSFR * BFRS) - 47 sein. Dieser Parameter wird für Standleitungen und für Wählleitungen verwendet.

Tabelle 13 (Seite 3 von 3). Host-/PC-Parameterzuordnung: SDLC

VTAM/NCP	Communications Server-Profil/-Parameter	Bemerkungen
MAXDATA=	Einheiten konfigurieren SDLC-WAC, SDLC-MPA, COM-Anschluß **Maximale PIU-Größe** (265–4105)	Diese Werte müssen nicht übereinstimmen. Dieser Parameter wird für Standleitungen und für Wählleitungen verwendet. Der niedrigste Wert wird verwendet.
MAXOUT=	Einheiten konfigurieren SDLC-WAC, SDLC-MPA, COM-Anschluß **Anzahl Empfangsfenster** (1–30)	Die **Anzahl Empfangsfenster** in Communications Server sollte dem Wert des Host-Parameters MAXOUT entsprechen. Dieser Parameter wird für Standleitungen und für Wählleitungen verwendet.
ADDR=	Einheiten konfigurieren SDLC-WAC, SDLC-MPA, COM-Anschluß **Adresse der Verbindungsstation** (01–FE)	Diese Parameter müssen denselben Wert haben. Die Angabe erfolgt in hexadezimaler Codierung für Communications Server und für VTAM/NCP. Dieser Parameter wird für Standleitungen und für Wählleitungen verwendet.

VTAM und Communications Server (APPC)

Tabelle 14 vergleicht VTAM-Host-Parameter mit den Communications Server-Parametern für APPC-Verbindungen.

Tabelle 14 (Seite 1 von 2). Host-/PC-Parameterzuordnung: APPC

VTAM	Communications Server-Profil/-Parameter	Bemerkungen
LU NAME	Host-LU konfigurieren **Name der lokalen LU** oder: Knoten konfigurieren **Vollständig qualifizierter CP-Name** (zweites Feld)	
LOCADDR	Host-LUs konfigurieren **NAU-Adresse**	Diese Parameter müssen denselben Wert haben. Bei unabhängigen LUs empfiehlt VTAM, anstelle der Codierung LOCADDR=0 eine CDRSC-Definition zu erstellen oder den Operanden DYNLU zu verwenden. Weitere Informationen zum Codieren von CDRSC-Definitionen für unabhängige LUs enthält der *VTAM Network Implementation Guide*. Für abhängige LUs sind keine Host-Definitionen erforderlich, wenn SDDLU oder dynamische Definition für unabhängige LUs unter VTAM 3.4 oder höher verwendet wird.
NETID APPL	Partner-LU 6.2 konfigurieren **Name der Partner-LU**	
VTAM-Interpretationstabelle	Partner-LU 6.2 konfigurieren **Name der Partner-LU**	Dies gilt nur für abhängige LUs.
LOGMODE-Tabelle LOGMODE=	Modus konfigurieren **Modusname**	Diese Parameter müssen übereinstimmen.

Tabelle 14 (Seite 2 von 2). Host-/PC-Parameterzuordnung: APPC

VTAM	Communications Server-Profil/-Parameter	Bemerkungen
LOGMODE-Tabelle RUSIZES=	Modus konfigurieren **Maximale RU-Größe** (256–32767)	Die Endwerte sind zu vereinbaren.

VTAM und Communications Server (MPC)

Tabelle 15 und Tabelle 16 vergleichen IOCP/HCD- und VTAM-Host-Parameter mit Communications Server-Parametern für MPC-Verbindungen.

Tabelle 15. IOCP/HCD-Parameterzuordnung: MPC

IOCP/HCD	Communications Server-Profil/-Parameter	Bemerkungen
IOCP IODEVICE UNIT=SCTC	DLC-Art: IBM-MPC	
HCD Einheitentyp SCTC	DLC-Art: IBM-MPC	

Tabelle 16 (Seite 1 von 2). VTAM-Parameterzuordnung: MPC

VTAM-Definitionsanweisung	Operand	Communications Server-Profil/-Parameter	Bemerkungen
VBUILD,TYPE=TRL	LNCTL= ition sf n ö		

Tabelle 16 (Seite 2 von 2). VTAM-Parameterzuordnung: MPC

VTAM-Definitionsanweisung	Operand	Communications Server-Profil/-Parameter	Bemerkungen
VBUILD,TYPE=LOCAL	CONNTYPE=APPN	Verbindungen konfigurieren IBM-MPC **APPN-Unterstützung**	Für Communications Server IBM-MPC-Verbindung ist APPN erforderlich.
	XID=YES	Verbindungen konfigurieren IBM-MPC **APPN-Unterstützung**	Für Communications Server IBM-MPC-Verbindung ist PU2.1 erforderlich.
	CPCP=YES	Verbindungen konfigurieren IBM-MPC **APPN-Unterstützung**	Für Communications Server IBM-MPC-Verbindung ist APPN erforderlich.
	HPR=YES	Verbindungen konfigurieren IBM-MPC **HPR-Unterstützung**	Für Communications Server IBM-MPC-Verbindung ist HPR erforderlich.
	NN	Knoten konfigurieren **Knotentyp**	Der VTAM-PU-Knotentyp muß mit der Communications Server-Definition übereinstimmen.
	DELAY		Kann sich auf den Durchsatz und/oder die VTAM-CPU-Auslastung auswirken

ES/9000 und Communications Server (SDLC)

Tabelle 17 vergleicht die Parameter für das Informationssystem IBM 9370 mit den Communications Server-Parametern für SDLC-Verbindungen.

Tabelle 17 (Seite 1 von 2). Host-/PC-Parameterzuordnung: Informationssystem IBM 9370 über SDLC

9370/VTAM	Communications Server-Profil/-Parameter	Bemerkungen
QFI: NRZI (Non-Return to Zero Inverted; Mikrocodekonfiguration)	Verbindungen konfigurieren SDLC-WAC, SDLC-MPA, COM-Anschluß **NRZI-Verschlüsselung**	Diese Parameter müssen übereinstimmen. Dieser Parameter wird für Standleitungen und für Wählleitungen verwendet. Communications Server verwendet USE_NRZI_ENCODING=0 und USE_NRZI_ENCODING=1. Dies ist der Synchrondatenstrom.
QFI: Protocol (Mikrocodekonfiguration) VTAM: GROUP LNCTL=SDLC	DLC-Art SDLC-WAC, SDLC-MPA COM-Anschluß	Die Mikrocode- und VTAM-Parameter müssen übereinstimmen. Dieser Parameter wird für Standleitungen und für Wählleitungen verwendet.
MAXDATA	Einheiten konfigurieren SDLC-WAC, SDLC-MPA, COM-Anschluß **Maximale PIU-Größe** (265–4105)	Diese Werte müssen nicht übereinstimmen. Dieser Parameter wird für Standleitungen und für Wählleitungen verwendet.
MAXBFRU * IOBUF-Größe	Einheiten konfigurieren SDLC-WAC, SDLC-MPA, COM-Anschluß **Maximale PIU-Größe** (265–4105)	Der Wert für die maximale Größe des I-Felds muß kleiner oder gleich dem Multiplikationsergebnis der auf dem Host angegebenen Werte für MAXBFRU und IOBUF-Größe sein. Dieser Parameter wird für Standleitungen und für Wählleitungen verwendet.

Tabelle 17 (Seite 2 von 2). Host-/PC-Parameterzuordnung: Informationssystem IBM 9370 über SDLC

9370/VTAM	Communications Server-Profil/-Parameter	Bemerkungen
MAXOUT=	Einheiten konfigurieren **Anzahl Empfangsfenster** (1–30)	Die **Anzahl Empfangsfenster** in Communications Server sollte dem Wert des Host-Parameters MAXOUT entsprechen. Dieser Parameter wird für Standleitungen und für Wählleitungen verwendet.
ADDR=	Einheiten konfigurieren **Adresse der Verbindungsstation** (01–FE)	Die für diese Parameter festgelegten Werte müssen übereinstimmen. Dieser Parameter wird für Standleitungen und für Wählleitungen verwendet.
IDBLK=	Knoten konfigurieren ID des lokalen Knotens **Block-ID**	Der Host-Parameter IDBLK muß mit den ersten drei hexadezimalen Zeichen der **ID des lokalen Knotens** übereinstimmen, die für Communications Server standardmäßig X'05D' lauten. Diesen Parameter bei Verwendung von Wählleitungen angeben und bei Verwendung von CPNAME= weglassen.
IDNUM=	Knoten konfigurieren ID des lokalen Knotens **ID der physischen Einheit**	Der Host-Parameter IDNUM muß mit den letzten 5 hexadezimalen Zeichen von **ID des lokalen Knotens** übereinstimmen. Diesen Parameter bei Verwendung von Wählleitungen angeben und bei Verwendung von CPNAME= weglassen.
CPNAME=	Knoten konfigurieren **Vollständig qualifizierter CP-Name** (zweites Feld)	Diesen Parameter bei Verwendung von Wählleitungen angeben und bei Verwendung von IDBLK= oder IDNUM= weglassen.
LOCADDR	Host-LUs konfigurieren **NAU-Adresse**	Die Parameter LOCADDR und NAU müssen denselben Wert haben. Bei unabhängigen LUs empfiehlt VTAM, anstelle der Codierung LOCADDR=0 eine CDRSC-Definition zu erstellen oder den Operanden DYNLU zu verwenden. Weitere Informationen zum Codieren von CDRSC-Definitionen für unabhängige LUs enthält der *VTAM Network Implementation Guide*. Dieser Parameter wird für Standleitungen und für Wählleitungen verwendet.

Host und Communications Server (DLUR)

Tabelle 18 vergleicht Host-Parameter und Communications Server-Parameter für VTAM-Verbindungen über DLUR.

Tabelle 18. VTAM-/Communications Server-Parameterzuordnung: Mit DLUR

VTAM	Communications Server	Bemerkungen
IDBLK=	DLUR-PUs konfigurieren **Block-ID**	IDBLK muß mit den ersten 3 hexadezimalen Zeichen der Knoten-ID übereinstimmen, die für Communications Server standardmäßig X'05D' lauten. Diesen Parameter angeben, wenn CPNAME= NICHT verwendet wird.
IDNUM=	DLUR-PUs konfigurieren **ID der physischen Einheit**	IDBLK muß mit den letzten 5 hexadezimalen Zeichen der Knoten-ID übereinstimmen. Diesen Parameter angeben, wenn CPNAME= NICHT verwendet wird.
CPNAME=	DLUR-PUs konfigurieren **PU-Name**	CPNAME muß mit dem Namen der lokalen PU übereinstimmen. Diesen Parameter angeben, wenn IDNUM= und IDBLK= NICHT verwendet wird.

Tabelle 19 listet die folgenden Parameter in der PATH-Anweisung auf, die beim Herstellen einer Verbindung vom Host zur Datenstation verwendet werden.

Tabelle 19. VTAM-/Communications Server-DLUR-Parameterzuordnung: Verbindungen vom Host zur Datenstation

VTAM	Communications Server	Bemerkungen
DLURNAME=	Knoten konfigurieren **Vollständig qualifizierter CP-Name** (zweites Feld)	DLURNAME gibt den Namen des DLUR-Knotens an, der Eigner der DLUR-PU ist. Für Communications Server ist dies der vollständig qualifizierte CP-Name.
DLCADDR= (1,C,INTPU)		Erforderlich. Dieser Parameter teilt dem DLUR mit, daß die Verbindung für eine interne PU verwendet wird.
DLCADDR=(2,X,zzzzzzzz)	DLUR-PUs konfigurieren **Block-ID und** **ID der physischen Einheit**	Die Angabe zzzzzzzz in DLCADDR=(2,X,zzzzzzzzz) muß mit der Knoten-ID übereinstimmen. Diesen Parameter angeben, wenn DLCADDR=(3,C,puname) NICHT verwendet wird.
DLCADDR= (3,C,puname)	DLUR-PUs konfigurieren **PU-Name**	Der PU-Name in DLCADDR=(3,C,puname) muß mit dem Namen der lokalen PU übereinstimmen. Diesen Parameter angeben, wenn DLCADDR=(2,X,zzzzzzzz) NICHT verwendet wird.

NPSI und Communications Server (X.25)

Die X.25-Unterstützung von Communications Server ermöglicht das Übertragen von SNA-Rahmen in einem X.25-Netz. X.25 behandelt SNA-Rahmen als Rohdaten und überträgt sie als Daten-in-Daten-Pakete. Die beiden Netzknoten sind nicht direkt verbunden, sondern über eine Zwischeninstanz, die als Netz mit Paketvermittlung (PSDN - Packet-Switching Data Network) bezeichnet wird. Das X.25-Netz kann jede der X.25-Konnektivitäten enthalten.

Die Software zur Interaktion mit PSDN und zum Packen der SNA-Daten in Pakete sowie zum fehlerfreien Extrahieren der Daten aus den Paketen ist integraler Bestandteil von Communications Server. Auf der Seite des S/370-Host-Systems werden die X.25-Funktionen von einem speziellen Softwareprodukt, dem X.25 NPSI (Network Control Program Packet Switching Interface), ausgeführt. Die NPSI-Definitionen werden zusammen mit dem NCP generiert, und die NPSI-Software wird im Einklang mit dem NCP auf derselben Steuereinheit IBM 3705-, 3725-, 3720- oder 3745 ausgeführt.

Die Mehrzahl der in Communications Server und in NPSI angegeben X.25-Parameter erhalten Werte, die nicht von den beiden Knoten sondern vom lokalen Benutzer und dem Betreiber des X.25-Netzes vereinbart werden.

Beispiel:

Bei einer SDLC-Verbindung über eine Standleitung wird die Host-Steuereinheit (NCP) so konfiguriert, daß sie eine bestimmte Sekundäradresse abfragt. Communications Server ist so konfiguriert, daß er auf diese Adresse über eine physische Verbindung zwischen der Communications Server-Datenstation und dem Host reagiert.

NPSI-Verbindungen über X.25

Tabelle 20 vergleicht Host-Parameter und Communications Server-Parameter für NPSI-Verbindungen über X.25.

Tabelle 20. Host-/PC-Parameterzuordnung: NPSI-Verbindungen über X.25

NPSI	Communications Server-Profil/-Parameter	Bemerkungen
X25.LINE TYPE=	DLC-Art X.25-COM-Anschluß, X.25-WAC	Bei der NPSI-X.25-Leitungsdefinition für PVCs **TYPE=P** und für SVCs **TYPE=S** angeben.
CALL= (nur für TYPE=S)	Einheiten konfigurieren X.25-COM-Anschluß, X.25-WAC **Bereiche für virtuelle Verbindungen**	Die Bereiche für virtuelle Verbindungen müssen mit der X.25-Netzteilnehmerberechtigung übereinstimmen.
MAXDATA=	Einheiten konfigurieren X.25-COM-Anschluß, X.25-WAC **Maximale PIU-Größe** (256–4105)	Diese Werte müssen nicht übereinstimmen.
VWINDOW	Einheiten konfigurieren X.25-COM-Anschluß, X.25-WAC **Fenstergröße** (1–7)	Die **SVC/PVC-Fenstergröße** muß mit den X.25-Teilnehmerberechtigungen übereinstimmen.
MWINDOW	Einheiten konfigurieren X.25-COM-Anschluß, X.25-WAC Rahmenwerte **Fenstergröße** (1–7)	
FRMLGTH	Einheiten konfigurieren X.25-COM-Anschluß, X.25-WAC Rahmenfolge **Modulo**	Der Host-Wert für **FRMLGTH** muß mindestens MAXPKT + 3 betragen, wenn Modulo 8 verwendet wird, oder MAXPKT + 4, wenn Modulo 128 verwendet wird. Die Modulo-Größe von Host und Communications Server sowie die Paketgrößen müssen mit der X.25-Teilnehmerberechtigung übereinstimmen.
MAXPKTL	Einheiten konfigurieren X.25-COM-Anschluß, X.25-WAC **Paketgröße**	Die **SVC/PVC-Paketgrößen** für den Host müssen mit dem Wert der X.25-Teilnehmerberechtigung übereinstimmen.

VTAM/NCP und Communications Server (X.25)

Tabelle 21 vergleicht Host- und Communications Server-Parameter für X.25 (VTAM/NCP).

Tabelle 21. Host-/PC-Parameterzuordnung: X.25 (VTAM/NCP)

VTAM/NCP	Communications Server-Profil/-Parameter	Bemerkungen
NETID=	Knoten konfigurieren **Vollständig qualifizierter CP-Name** (erstes Feld)	Dieser Parameter gibt das SNA-Netz an, zu dem mit Communications Server eine Verbindung hergestellt wird.
PU NAME		Ein PU-Name muß immer verwendet werden. Dieser PU-Name sollte sich vom lokalen CP-Namen unterscheiden, damit eine LU für den Steuerpunkt definiert werden kann.
IDBLK=	Knoten konfigurieren ID des lokalen Knotens **Block-ID**	Die ersten 3 hexadezimalen Zeichen der **ID des lokalen Knotens**, die für Communications Server standardmäßig X'05D' lauten. Diesen Parameter bei Verwendung von Wählleitungen angeben und bei Verwendung von CPNAME= weglassen.
IDNUM=	Knoten konfigurieren ID des lokalen Knotens **ID der physischen Einheit**	Der Host-Parameter IDNUM muß mit den letzten 5 hexadezimalen Zeichen von **ID des lokalen Knotens** übereinstimmen. Diesen Parameter bei Verwendung von Wählleitungen angeben und bei Verwendung von CPNAME= weglassen.
CPNAME=	Knoten konfigurieren **Vollständig qualifizierter CP-Name** (zweites Feld)	Diesen Parameter bei Verwendung von Wählleitungen angeben und bei Verwendung von IDBLK= und IDNUM= weglassen.
(TRANSFR * BFRS) – 47	Einheiten konfigurieren X.25-COM-Anschluß, X.25-WAC **Maximale PIU-Größe** (265–4105)	Der Wert für **Maximale PIU-Größe** muß mit dem auf dem Host definierten Wert übereinstimmen.
MAXDATA=	Einheiten konfigurieren X.25-COM-Anschluß, X.25-WAC **Maximale PIU-Größe** (265–4105)	Diese Werte müssen nicht übereinstimmen.
LOCADDR	Host-LUs konfigurieren **NAU-Adresse**	Diese Parameter müssen denselben Wert haben. Bei unabhängigen LUs empfiehlt VTAM, anstelle der Codierung LOCADDR=0 eine CDRSC-Definition zu erstellen oder den Operanden DYNLU zu verwenden. Weite d ´ Wá de D elle egen - R=0 eine CDRSC etedeŸ DY ben. Bei vabhängi e B f der á

APPC über X.25

Tabelle 22 enthält die Parameterzuordnung für eine Communications Server-Datenstation mit APPC (Advanced Program-to-Program Communications), die über X.25 die Verbindung zu einem Host herstellt.

Tabelle 22. Host-/PC-Parameterzuordnung: APPC in einem IBM Token-Ring-Netz mit Host-Verbindung über X.25

NCP	Communications Server-Profil/-Parameter	Bemerkungen
LU NAME	Lokale LU 6.2 konfigurieren **Name der lokalen LU** oder: Knoten konfigurieren **Vollständig qualifizierter CP-Name** (zweites Feld)	
LOCADDR	Host-LUs konfigurieren **NAU-Adresse**	Diese Parameter ***müssen*** denselben Wert haben. Bei unabhängigen LUs empfiehlt VTAM, anstelle der Codierung LOCADDR=0 eine CDRSC-Definition zu erstellen oder den Operanden DYNLU zu verwenden. Weitere Informationen zum Codieren von CDRSC-Definitionen für unabhängige LUs enthält der *VTAM Network Implementation Guide*. Für abhängige LUs sind keine Host-Definitionen erforderlich, wenn SDDLU oder dynamische Definition für unabhängige LUs unter VTAM 3.4 oder höher verwendet wird.
NETID APPL	Partner-LU 6.2 konfigurieren **Name der Partner-LU**	
VTAM-Interpretationstabelle	Partner-LU 6.2 konfigurieren **Name der Partner-LU**	Dies gilt nur für abhängige LUs.
LOGMODE-Tabelle LOGMODE=	Modus konfigurieren **Modusname**	Diese Parameter ***müssen*** übereinstimmen.
LOGMODE-Tabelle RUSIZES=	Modus konfigurieren **Maximale RU-Größe** (256–32767)	Diese Werte müssen übereinstimmen.

AS/400-Host-Leitungsdefinitionen

Zu den AS/400-Host-Leitungsdefinitionen gehört die Zuordnung von OS/400-Host-Programmparametern zu Communications Server-Parametern. Tabelle 23 auf Seite 192 enthält die SDLC-Leitungsparameter.

Tabelle 23. AS/400-/Communications Server-Parameterzuordnung: OS/400-Host-Programm-Leitungsdefinition

OS/400	Communications Server-Profil/-Parameter	Bemerkungen
NRZI= Datenverschlüsselung	Verbindungen konfigurieren SDLC-WAC, SDLC-MPA, COM-Anschluß **NRZI-Verschlüsselung**	Communications Server verwendet USE_NRZI_ENCODING=0 und USE_NRZI_ENCODING=1. Dieser Parameter findet sich nur in PCMs für folgende Modemtypen: synchrone Wählleitung, synchrone Standleitung und AutoSync.

Tabelle 23. AS/400-/Communications Server-Parameterzuordnung: OS/400-Host-Programm-Leitungsdefinition

OS/400	Communications Server-Profil/-Parameter	Bemerkungen
Auswahl der Modem-übertragungsgeschwindigkeit	Einheiten konfigurieren nur COM-Anschluß **Modem konfigurieren**	Die Parameter für Modemverbindungsart "asynchrone Wählverbindung" müssen auf beiden Systemen übereinstimmen.
Maximale Rahmengröße (MAXFRAME)	Einheiten konfigurieren SDLC-WAC, SDLC-MPA, COM-Anschluß **Anzahl Empfangsfenster** (1–30)	Werte für asynchrone Standleitungen müssen nicht übereinstimmen.
Maximal anstehende Rahmen (MAXOUT)	Einheiten konfigurieren SDLC-WAC, SDLC-MPA, COM-Anschluß **Anzahl Empfangsfenster** (1–30)	Die **Anzahl Empfangsfenster** in Communications Server sollte dem Wert des Parameters MAXOUT auf dem AS/400-Host entsprechen.

AS/400-Host-Steuereinheitendefinitionen

Zum Definieren der AS/400-Host-Steuereinheit gehört die Zuordnung der OS/400-Host-Programmparameter zu Communications Server-Parametern.

Tabelle 24 zeigt die OS/400-Host-Programmparameter.

Tabelle 24 (Seite 1 von 2). AS/400-/Communications Server-Parameterzuordnung: Steuereinheitenparameter

OS/400	Communications Server-Profil/-Parameter	Bemerkungen
Verbindungsart: *SDLC	DLC-Art SDLC-WAC, SDLC-MPA COM-Anschluß	Die Verbindungsart muß auf beiden Systemen übereinstimmen. Dieser Parameter gehört zur Leitungsbeschreibung, sollte aber der Vollständigkeit halber angegeben werden.
Angeschlossene Standleitung	Einheiten konfigurieren SDLC-WAC, SDLC-MPA, COM-Anschluß **Wählleitung**	Dieser Parameter gilt für festgeschaltete Verbindungen. Dieser Wert muß mit einer zuvor festgelegten Host-Leitungsdefinition übereinstimmen.
Wählleitungsliste	(keine)	Dieser Parameter gilt für Wählverbindungen. Dieser Wert muß mit einer zuvor festgelegten Host-Leitungsdefinition übereinstimmen.
Maximale Rahmengröße	Einheiten konfigurieren SDLC-WAC, SDLC-MPA, COM-Anschluß **Maximale PIU-Größe** (265–4105)	Diese Werte müssen nicht übereinstimmen.
ID des fernen Netzes	Knoten konfigurieren **Vollständig qualifizierter CP-Name** (erstes Feld)	Diese Werte müssen übereinstimmen.
Name des fernen Steuerpunkts	Knoten konfigurieren **Vollständig qualifizierter CP-Name** (zweites Feld)	Diese Werte müssen übereinstimmen.

Tabelle 24 (Seite 2 von 2). AS/400-/Communications Server-Parameterzuordnung: Steuereinheitenparameter

OS/400	Communications Server-Profil/-Parameter	Bemerkungen
Funktion der Datenverbindung	Verbindungen konfigurieren SDLC-WAC, SDLC-MPA, COM-Anschluß **Funktion der Verbindungsstation**	Die Parameter auf beiden Systemen sind komplementär. Wenn der Host eine primäre Funktion hat, muß die Communications Server-Datenstation als sekundär oder als zu vereinbaren konfiguriert werden. Wenn keine Mehrpunktverbindung (*MP) verwendet wird, empfiehlt es sich, die Funktion der Datenverbindung auf als zu vereinbaren (*NEG) zu setzen.
Stationsadresse	Einheiten konfigurieren SDLC-WAC, SDLC-MPA, COM-Anschluß **Adresse der Verbindungsstation** (01–FE)	Diese Werte müssen übereinstimmen.
APPN-CP-Sitzungsunterstützung: (Ja/Nein)	Verbindungen konfigurieren SDLC-WAC, SDLC-MPA, COM-Anschluß **APPN-Unterstützung**	Diese Werte müssen übereinstimmen, wenn CP-CP-Sitzungen verwendet werden sollen.
APPN-Knotentyp	Verbindungen konfigurieren SDLC-WAC, SDLC-MPA, COM-Anschluß **Art des benachbarten CP**	Diese Werte müssen übereinstimmen.

AS/400-Host-Einheitendefinitionen

Der AS/400-Host kann eine Einheitendefinition erstellen, wenn die Communications Server-Datenstation die Verbindung ohne eine zuvor festgelegte Einheitendefinition herstellt.

Tabelle 25 enthält die Einheitenparameter des OS/400-Host-Programms.

Tabelle 25 (Seite 1 von 2). AS/400-/Communications Server-Parameterzuordnung: Einheitenparameter

OS/400	Communications Server-Profil/-Parameter	Bemerkungen
Name des fernen Standorts	Lokale LU 6.2 konfigurieren **Name der lokalen LU** oder: Knoten konfigurieren **Vollständig qualifizierter CP-Name** (zweites Feld)	Diese Werte müssen übereinstimmen.
Angeschlossene Steuereinheit	(keine)	Dieser Parameter gilt für festgeschaltete Verbindungen. Dieser Wert muß mit einer zuvor festgelegten Host-Leitungsdefinition übereinstimmen.
Name des lokalen Standorts		Den vorgegebenen Standardwert verwenden.
ID des fernen Netzes	Knoten konfigurieren **Vollständig qualifizierter CP-Name** (erstes Feld)	Den vorgegebenen Standardwert verwenden.
Modus	Modus konfigurieren **Modusname**	Den vorgegebenen Standardwert verwenden.

AS/400-Host-Leitungsbeschreibung und Communications Server

Tabelle 26 enthält die Leitungsbeschreibung des AS/400-Host-Programms.

Tabelle 26. Host-/PC-Parameterzuordnung: Leitungsbeschreibung

OS/400	Communications Server-Profil/-Parameter	Bemerkungen
Adresse des lokalen Adapters:	Verbindungen konfigurieren **LAN-Zieladresse**	Die beiden Adressen müssen übereinstimmen, damit eine Kommunikation möglich ist.

AS/400-Host-Steuereinheitenbeschreibung und Communications Server

Tabelle 27 enthält die Steuereinheitenbeschreibung des OS/400-Host-Programms.

Tabelle 27. Host-/PC-Parameterzuordnung: Steuereinheitenbeschreibung

OS/400	Communications Server-Profil/-Parameter	Bemerkungen
Aktive Wählleitung	(keine)	Dieser Parameter gilt für festgeschaltete Verbindungen. Dieser Wert muß mit einer zuvor definierten Host-Leitungsdefinition übereinstimmen.
Ferner Steuerpunkt	Knoten konfigurieren **Vollständig qualifizierter CP-Name** (zweites Feld)	Die Namen müssen übereinstimmen.
ID des fernen Netzes	Knoten konfigurieren **Vollständig qualifizierter CP-Name** (erstes Feld)	Den Standardwert verwenden oder die Parameter abgleichen, wenn sie von der lokalen Netz-ID des AS/400-Systems abweichen.
Beschreibung der Modellsteuereinheit		Dieser Parameter muß auf YES gesetzt werden, wenn das AS/400-System ein Verbindungsnetz verwendet.
ID des Verbindungsnetzes und CP-Name des Verbindungsnetzes	Verbindungsnetze konfigurieren **Verbindungsnetzname**	Diese Werte müssen für alle Knoten, die an einem Verbindungsnetz beteiligt sind, übereinstimmen.

AS/400-Host (Twinaxial) - Beschreibungen

Tabelle 28 auf Seite 195 enthält die Beschreibung für ein twinaxiales AS/400-System.

Tabelle 28. Host-/PC-Parameterzuordnung: Steuereinheitenbeschreibung

AS/400	Communications Server-Profil/-Parameter	Bemerkungen
Angeschlossene Standleitung	(keine)	Dieser Parameter gilt für festgeschaltete Verbindungen. Dieser Wert muß mit einer zuvor definierten Host-Leitungsdefinition übereinstimmen.

Tabelle 28. Host-/PC-Parameterzuordnung: Steuereinheitenbeschreibung

AS/400	Communications Server-Profil/-Parameter	Bemerkungen
Ferner Steuerpunkt	Knoten konfigurieren **Vollständig qualifizierter CP-Name** (zweites Feld)	Die Namen müssen übereinstimmen.
ID des fernen Netzes	Knoten konfigurieren **Vollständig qualifizierter CP-Name** (erstes Feld)	Den Standardwert verwenden oder die Parameter abgleichen, wenn sie von der lokalen Netz-ID des AS/400-Systems abweichen.
Funktion der Datenverbindung=*SEC:	Verbindungen konfigurieren SDLC-WAC, SDLC-MPA COM-Anschluß **Funktion der Verbindungsstation**	Die Parameter auf beiden Systemen sind komplementär. Wenn der Host eine primäre Funktion hat, muß die Communications Server-Datenstation als sekundär oder als zu vereinbaren konfiguriert werden. Wenn keine Mehrpunktverbindung (*MP) verwendet wird, empfiehlt es sich, die Funktion der Datenverbindung auf als zu vereinbaren (*NEG) zu setzen.

AS/400-Host-Leitungsdefinitionen (X.25)

Zu den AS/400-Host-Leitungsdefinitionen gehört die Zuordnung von OS/400-Host-Programmparametern zu Communications Server-Parametern. Tabelle 29 enthält die X.25-Leitungsparameter.

Tabelle 29 (Seite 1 von 2). AS/400-/Communications Server-Parameterzuordnung: OS/400-Host-Programm-Leitungsdefinition (X.25)

OS/400	Communications Server-Profil/-Parameter	Bemerkungen
Lokale Netzadresse	Einheiten konfigurieren **Lokale Adresse**	Beide Adressen werden normalerweise vom Netzbetreiber festgelegt.
Verbindungsart	Einheiten konfigurieren X.25-COM-Anschluß X.25-WAC **Wählleitung**	Die Verbindungsart muß auf beiden Systemen übereinstimmen.
X.25-DÜE-Unterstützung	--	Muß auf YES gesetzt sein, wenn beide Systeme durch eine Punkt-zu-Punkt-Verbindung verbunden sind, die nicht durch ein X.25-Netz führt.
Maximale Rahmengröße	Einheiten konfigurieren X.25-COM-Anschluß X.25-WAC **Maximale PIU-Größe**	Die maximale Rahmengröße muß auf beiden Systemen übereinstimmen.
Standardpaketgröße	Einheiten konfigurieren X.25-COM-Anschluß X.25-WAC **Paketgröße**	Dieser Wert wird vom Netzbetreiber festgelegt und ist beim Senden und Empfangen gleich.
Maximale Paketgröße	--	Dieser Wert wird vom Netzbetreiber festgelegt.
Modulus	Einheiten konfigurieren X.25-COM-Anschluß X.25-WAC **Reihenfolge**	Dieser Wert wird vom Netzbetreiber festgelegt.

Tabelle 29 (Seite 2 von 2). AS/400-/Communications Server-Parameterzuordnung: OS/400-Host-Programm-Leitungsdefinition (X.25)

OS/400	Communications Server-Profil/-Parameter	Bemerkungen
Standardfenstergröße	Einheiten konfigurieren X.25-COM-Anschluß X.25-WAC **Fenstergröße**	Dieser Wert wird vom Netzbetreiber festgelegt und ist beim Senden und Empfangen gleich.
Netzadresse einfügen	Einheiten konfigurieren X.25-COM-Anschluß X.25-WAC	Dieser Wert wird vom Netzbetreiber festgelegt und sollte für beide Systeme gleich sein.
Einträge für logischen Kanal	Einheiten konfigurieren X.25-COM-Anschluß X.25-WAC **Bereiche für virtuelle Verbindung**	Diese Werte werden vom Netzbetreiber und durch die Art der virtuellen X.25-Verbindung festgelegt.

AS/400-Host-Steuereinheitendefinitionen (X.25-PVC)

Zum Definieren der AS/400-Host-Steuereinheit gehört die Zuordnung der OS/400-Host-Programmparameter zu Communications Server-Parametern.

Tabelle 30 zeigt die OS/400-Host-Programmparameter für X.25-PVC.

Tabelle 30 (Seite 1 von 2). AS/400-/Communications Server-X.25-PVC-Parameterzuordnung: Steuereinheitenparameter

OS/400	Communications Server-Profil/-Parameter	Bemerkungen
ID des logischen X.25-Kanals	Verbindungen konfigurieren X.25-COM-Anschluß, X.25-WAC **Nummer des logischen Kanals**	Diese Werte werden vom Netzbetreiber festgelegt.
Verbindungsart: *X25	Verbindungen konfigurieren	Die Verbindungsarten müssen auf beiden Systemen übereinstimmen.
Wählverbindung: *NO		Alle PVCs sind festgeschaltet.
Maximale Rahmengröße	Einheiten konfigurieren X.25-COM-Anschluß X.25-WAC **Maximale PIU-Größe**	Die Werte für die maximale Rahmengröße müssen nicht übereinstimmen.
Funktion der Datenverbindung	Einheiten konfigurieren X.25-COM-Anschluß X.25-WAC **Funktion der Verbindungsstation**	Die Parameter auf beiden Systemen sind komplementär. Wenn der Host eine primäre Funktion hat, muß die Communications Server-Datenstation als sekundär oder zu vereinbaren konfiguriert werden.
X.25-Netzebene	Einheiten konfigurieren X.25-COM-Anschluß X.25-WAC **CCITT-Übereinstimmung**	Diese Werte werden vom Netzbetreiber festgelegt.
Protokoll für X.25-Verbindungsebene: *QLLC		Dieser Wert muß auf QLLC gesetzt sein.

AS/400-Host-Steuereinheitendefinitionen (X.25-SVC)

Zum Definieren der AS/400-Host-Steuereinheit gehört die Zuordnung der OS/400-Host-Programmparameter zu Communications Server-Parametern.

Tabelle 31 zeigt die OS/400-Host-Programmparameter für X.25-SVC.

Tabelle 31. AS/400-/Communications Server-X.25-SVC-Parameterzuordnung: Steuereinheitenparameter

OS/400	Communications Server-Profil/-Parameter	Bemerkungen
Verbindungsart: *X25	Verbindungen konfigurieren	Die Verbindungsarten müssen auf f arauf , % ë

Communications Server-Konfigurationen implementieren

Nachfolgend wird eine Prozedur zur Installation und Konfiguration der Software für das Netz vorgeschlagen:

1. Plan für Hardware
2. Plan für Softwareanwendungen
3. Namenskonventionen erstellen
4. Netzadressen definieren
5. Hilfsprogramme für die Konfiguration und Installation auswählen
6. Schablonenkonfiguration definieren
7. Konfigurationen erstellen und installieren
8. Benutzermaterial erstellen
9. Netz verwalten

Dieses Kapitel enthält die Informationen, die zum Ausführen der vorgeschlagenen Prozedur erforderlich sind.

Einführung

In einer Schablonenkonfiguration werden die Konfigurationsdaten definiert, die für eine Gruppe von Servern gelten. Es kann hilfreich sein, eine oder mehrere Schablonenkonfigurationen zu erstellen. Jede Server-Konfigurationsdatei beginnt mit der Schablonenkonfiguration und kann die speziellen Parameter enthalten, die zum Anpassen der Konfiguration für diesen Server erforderlich sind. Dadurch wird das Konfigurieren des Servers vereinfacht.

In der Schablonenkonfiguration können auch Konfigurationsoptionen angegeben werden, die in den Antwortdateien nicht angegeben werden können.

Informationen zum Ausführen von Installation und Konfiguration mit Hilfe von Antwortdateien und Schablonendateien können dem Abschnitt „Konfiguration mit Schablonen- und Antwortdateien“ auf Seite 210 entnommen werden.

Beim Zusammenstellen der Informationen in den nachfolgenden Schritten den Gesamtbedarf an Arbeitsspeicher und Plattenspeicherplatz für jede Datenstation berechnen. Dadurch kann sichergestellt werden, daß die Benutzer über adäquate Hardware verfügen, wenn sie mit der ausgewählten Software zu arbeiten beginnen.

Schritt 1. Plan für Hardware

Wurde bereits entschieden, daß vorhandene Server verwendet werden können, muß sichergestellt werden, daß die vorhandene Hardware über ausreichend Hauptspeicher und Festplattenspeicherplatz verfügt. Bei der Hardware ist außerdem zu berücksichtigen, daß die richtigen Systemeinheiten, Bildschirme, Drucker, Tastaturen, Adapter, Modems und Kabel für die Software vorhanden sind, die installiert wird.

Beim Erwerb neuer Server die Hardware auf den Arbeitsblättern auflisten, die für die Benutzer vorbereitet werden.

Speicherbedarf

Angaben zum Speicherbedarf für Communications Server können im Handbuch *Einstieg* nachgelesen werden.

Speicherkapazität

Beim Planen der Hardware für Communications Server ist unbedingt darauf zu achten, wie die Server-Kapazität genutzt werden soll. Dies hängt auch von den Sitzungsarten ab, die Communications Server unterstützt. Dazu gehören unter anderem TN3270E-Sitzungen, SNA-API-Client-Sitzungen und herkömmliche SNA-Sitzungen mit einem Host. Ausgehend von dieser Zahl kann anschließend die durchschnittliche Auslastung des Servers errechnet und die entsprechende Speicherkapazität für den Server bestimmt werden.

Anmerkung: Diese geschätzten Zahlen sind zu den Erfordernissen des Basisbetriebssystems (Windows NT-Server) und der übrigen, gleichzeitig auf demselben System auszuführenden Anwendungen zu addieren.

Anhand der folgenden Tabelle kann bestimmt werden, wie die durchschnittliche Auslastung des Servers aussehen wird:

Tabelle 32. Speicherkapazität

Art der Client-Sitzung	Speicherbelegung je Sitzung
SNA-Gateway (traditionell)	29,9 KB
SNA-API-Client	25,2 KB
TN3270E	15,8 KB

Der geschätzte Speicherbedarf eines aktiven Communications Servers ohne aktive Verbindungen oder Sitzungen beträgt 21 MB. Um den Leistungsabfall zu minimieren, empfiehlt es sich, die Seitenwechselrate (Auslagern von Speichersegmenten auf die Platte) möglichst gering zu halten. Dazu sollte im System soviel Realspeicher verfügbar sein wie von der ausgeführten Software benötigt wird, plus 5 - 10 MB als Puffer. Beispiel: Für eine Communications Server-Installation, die 1000 TN3270E-Client-Sitzungen unterstützt, wären die folgenden Speicherkapazitäten erforderlich (basierend auf den Werten aus Tabelle 32).

Betriebssystem: Microsoft Windows NT-Server	ca. 19,0 MB
Communications Server für Windows NT	21,0 MB
TN3270E-Sitzungen (1000 X 15,8 KB)	15,8 MB
Speicherreserve	10,0 MB
Gesamte empfohlene Speicherkapazität	65,8 MB

Anmerkung: Diese 65,8 MB sind nicht die erforderliche Speicherkapazität für 1000 TN3270E-Sitzungen. Sie sind vielmehr ein Empfehlungswert, um optimale Leistungswerte zu erzielen.

CPU-Geschwindigkeit

Beim Festlegen der Mindestgeschwindigkeit für den Prozessor ist zunächst zu berücksichtigen, wie viele Transaktionen der Server durchschnittlich pro Minute verarbeiten soll. Der Begriff Transaktion bezeichnet jeden mit Hilfe des Servers abgewickelten Datenaustausch zwischen Client und Host, sei es eine Bildschirmaktualisierung oder ein angeforderter Datenbankeintrag.

Beim Berechnen der durchschnittlichen CPU-Auslastung ist die durchschnittliche Sitzungsanzahl mit der durchschnittlichen Anzahl der pro Minute und Sitzung zu verarbeitenden Transaktionen und mit dem Belastungsfaktor der folgenden Tabelle (nach Sitzungsart) zu multiplizieren.

Art der Client-Sitzung	CPU-Belastungsfaktor (100 MHz)	CPU-Belastungsfaktor (166 MHz)
SNA-Gateway (traditionell)	0,004	0,002
SNA-API-Client	0,021	0,011
TN3270E	0,011	0,006

Beispiel: Zur Unterstützung von 1000 gleichzeitig ablaufenden TN3270E-Sitzungen mit durchschnittlich 6,7 Transaktionen pro Minute, beträgt die durchschnittliche Belastung für die CPU (166 MHz) 1000 x 6,7 x 0,006 oder 40,2%. Die Leistung nimmt deutlich ab, wenn die CPU-Auslastung 80% übersteigt. Eine schnellere CPU würde die Verarbeitungsgeschwindigkeit von Communications Server und die Systemleistung erhöhen. Das bedeutet, der Server könnte von mehr Benutzern und Transaktionen gleichzeitig genutzt werden. Die von Communications Server unterstützte CPU-Geschwindigkeit ist nach oben unbegrenzt, die Geschwindigkeit sollte jedoch mindestens 100 MHz betragen.

Schritt 2. Plan für Softwareanwendungen

Softwareanwendungen stellen Anforderungen, die über die Systemvoraussetzungen für Communications Server hinausgehen. Weitere Informationen können der Dokumentation zu der jeweiligen Softwareanwendung entnommen werden.

Schritt 3. Namenskonventionen erstellen

Bei mit dem Communications Server erstellten Netzen müssen zahlreiche Namen für viele Objekte im Netz erstellt und verwendet werden. Einige Namen können auf allen Servern identisch sein, andere Namen müssen jedoch im Netz eindeutig sein, um Konflikte zwischen den Servern zu vermeiden, die auf die Netzressourcen zugreifen wollen.

Beispiel: In zwei LANs sind dieselben Domänennamen definiert. Solange diese LANs nicht verbunden waren, traten keine Konflikte auf. Sollen sie jedoch zu einem späteren Zeitpunkt zu einem zentralen LAN verbunden werden, treten Namenskonflikte in dem LAN auf.

Dies bedeutet, daß Namenskonventionen erstellt werden müssen. Namenskonventionen sind Regeln und Standards, die beim Zuordnen von Namen zu den verschiedenen Netzressourcen verwendet werden.

In den folgenden Abschnitten werden die Namenskonventionen aufgelistet, für die eine Planung erforderlich ist. Wurde bereits festgelegt, welche Namenskonventionen verwendet werden sollen, diese bei der Planung des Netzes notieren.

Benennungskriterien

Beim Erstellen von Namenskonventionen folgendes festlegen:

- Welche Kriterien zum Erstellen von Namen und Adressen im Netz zu verwenden sind
- Wie diese Namen und Adressen konsistent und gegebenenfalls im Netz eindeutig bleiben

Wird ein Server an ein Host-Computernetz angeschlossen, kann es zum Beispiel sein, daß die meisten Namen, die im Netz verwendet werden müssen, von der Host-Benutzerunterstützung ausgewählt wurden. In diesem Fall ist es Aufgabe des Netzadministrators, die vorgegebenen Namen der für den Host erforderlichen physischen und logischen Einheiten für die Server-Konfigurationsdateien aufzuzeichnen.

Alle Server im Netz können auch nach dem jeweiligen Benutzer benannt werden, der mit ihnen arbeitet. In einem kleinen Netz kann dies praktikabel sein, solange nur eine geringe Anzahl von Namen benötigt wird und diese Namen eindeutig sind. Dies ist jedoch nicht möglich für ein größeres Netz, da in der Regel nicht alle Benutzernamen eindeutig sind. Für ein großes Netz ist eine andere Konvention zur Benennung der Datenstationen erforderlich.

Die für die Benennung geltenden Kriterien müssen auf jeden Fall aufgezeichnet werden. So besteht jederzeit Zugriff auf die entsprechenden Informationen, wenn dem Netz neue Ressourcen hinzugefügt werden.

Namenstypen und Einschränkungen

Die meisten Namen müssen in dem Netz eindeutig sein, in dem sie benutzt werden. In den folgenden Abschnitten werden die Namenstypen aufgelistet, die beim Planen, Installieren und Konfigurieren eines Netzes möglicherweise auftreten. Der Netzadministrator sollte sich vor der Netzplanung mit diesen Namen vertraut machen.

Zu jedem Namen werden folgende Informationen angegeben:

- Eine Definition
- Ob der Name im Netz eindeutig sein muß
- Einschränkungen

Von mehreren Komponenten verwendete Namen

Folgende Namen werden von mehreren Komponenten verwendet:

- Netz-IDs
- Kennwörter
- Benutzer-IDs
- Namen adressierbarer Netzeinheiten (Network Adressable Unit, NAU)

Netz-IDs: Netz-IDs sind die Namen von Netzen, die von allen Servern und Datenstationen (Knoten) in einem spezifischen Netz verwendet werden, damit für alle angeschlossenen Netze eine eindeutige Kennung vorhanden ist. Die Netz-ID wird auch in Fehlerprotokollen und Alerts zur Netzverwaltung verwendet, die mit Netzsystemfehlern zusammenhängen.

Es gibt zwei unterschiedliche Betrachtungsweisen für ein Netz. Zum einen gibt es ein physisches Netz, das aus einem “Ring” in einer Token-Ring-Umgebung oder einer “Reihe” in einer Ethernet- oder PC-Netz-Umgebung besteht. Zum anderen gibt es ein logisches Netz, das nicht unbedingt mit dem physischen Netz identisch ist. Zwei oder mehr physische Netze (z. B. zwei Token-Ring-"Ringe" und eine Ethernet-"Reihe") können zu einem logischen Netz miteinander verbunden werden. Die Netz-IDs müssen bei logischen Netzen eindeutig sein, sonst wären die Netze logisch dasselbe Netz. In einem logischen Netz müssen die LU-Namen eindeutig sein, um Namenskonflikte zu vermeiden. Netzübergreifend sind die Namen aufgrund der Netz-ID eindeutig. Ein LU-Name kann in zwei logischen Netzen identisch sein, durch die Netz-ID für jedes logische Netz wird der vollständig qualifizierte LU-Name jedoch eindeutig. Auch wenn die Netze zur Zeit nicht verbunden sind, sollten die Netz-IDs eindeutig sein, falls geplant ist, die Netze in Zukunft miteinander zu verbinden.

Die Netz-IDs sollten bei IBM registriert werden. Dadurch wird sichergestellt, daß SNA-Netze zu einem späteren Zeitpunkt ohne Adreßkonflikte miteinander verbunden werden können. Bei der IBM Geschäftsstelle sind weitere Informationen zum Registrieren der Netz-IDs erhältlich.

Folgende Einschränkungen gelten für Netz-IDs:

- **Länge**: Zwischen 1 und 8 Zeichen
- **Zulässige Zeichen**: A bis Z, 0 bis 9, $, @, #

Kennwörter: Bei Kennwörtern handelt es sich um Sicherheitsfunktionen, die von entsprechend konfigurierten Anwendungen und Services zum Schutz von Daten und zum Einschränken des Zugriffs auf Ressourcen erforderlich sind. Kennwörter müssen im Netz nicht eindeutig sein. Kennwörter sind benutzerspezifisch.

Für LU-LU-Kennwörter gelten folgende Einschränkungen:

- **Länge**: Zwischen 1 und 8 Zeichen
- **Zulässige Zeichen**: Alle hexadezimalen Zeichenfolgen

Für andere Kennwörter, z. B. in CPI-C- und AS/400-Verbindungen, gelten folgende Bedingungen:

- **Länge**: Zwischen 1 und 10 Zeichen
- **Zulässige Zeichen**: Alle ASCII-Zeichenfolgen

Benutzer-IDs: Benutzer-IDs sind eindeutige Kennungen, die den Benutzern der Netzressourcen zugeordnet werden, damit sie auf Datenbank- und LAN-Ressourcen oder über eine Emulation auf Host-Ressourcen zugreifen können.

Benutzer-IDs müssen im Netz eindeutig sein.

Für Benutzer-IDs gelten folgende Einschränkungen:

- **Länge**: Zwischen 1 und 8 Zeichen
- **Zulässige Zeichen**: A bis Z, a bis z, 0 bis 9, $, @, #

Namen adressierbarer Netzeinheiten (NAUs)

Folgende Namenstypen müssen möglicherweise bei Communications Server angegeben werden:

- CP-Namen (Namen lokaler Knoten)
- LU-Namen

CP-Namen (Namen lokaler Knoten): Der Steuerpunkt (CP - Control Point) hat die Funktion, den Knoten und seine Ressourcen zu verwalten. In einem APPN-Endknoten muß der Steuerpunkt mit dem Steuerpunkt eines benachbarten Netzknotens kommunizieren, um APPN-Netzservices zu erhalten. In einem APPN-Netzknoten muß der Steuerpunkt mit den Steuerpunkten benachbarter Netzknoten kommunizieren, um das Netz zu verwalten. Der Steuerpunkt steuert Funktionen wie die Aktivierung und Inaktivierung von Adaptern und Verbindungen und unterstützt LUs bei der Initialisierung und der Beendigung einer Sitzung.

Der Steuerpunktname ist die zweite Hälfte des vollständig qualifizierten CP-Namens in der Knotendefinition (NODE) von Communications Server.

Steuerpunktnamen müssen in einem Netz eindeutig sein. In einem Knoten sind jedoch mehrere PU-Namen möglich, die in der Verbindungsdefinition (**LINK_STATION**) festgelegt sind und über XID3 mit verschiedenen Hosts ausgetauscht werden. Diese PU-Namen müssen auf dem Knoten und auf dem angeschlossenen Host eindeutig sein.

Für das Unterbereichs-VTAM sind die PU und der Steuerpunkt nicht dasselbe. Ein PU-Name für jeden peripheren Knoten in einer VTAM-Domäne wird in diesem VTAM definiert und stellt die VTAM-Sichtweise der peripheren Knoten dar. Die PU-Namen bei VTAM sind den peripheren Knoten nicht bekannt, d. h., VTAM sendet die PU-Namen nicht an die peripheren Knoten. Soll der PU-Name auf einem peripheren Knoten mit dem bei VTAM definierten identisch sein, muß dies koordiniert werden. Dies wird empfohlen, ist jedoch für SNA nicht erforderlich.

Für VTAM ist der Steuerpunkt eine LU, die zur Aktivierung von LU 6.2-Sitzungen zwischen dem Steuerpunkt und einer VTAM-LU (z. B. CICS) verwendet wird. Der im peripheren Knoten definierte Steuerpunktname muß einer LU-Definition in VTAM entsprechen, wenn VTAM LU 6.2-Sitzungen mit dem Steuerpunkt initialisiert. Andernfalls erfährt VTAM den Steuerpunktnamen, wenn der periphere Knoten eine Sitzung mit einer VTAM-LU initialisiert.

Der Communications Server behandelt den Steuerpunktnamen (die Netz-ID nicht eingeschlossen) als Steuerpunktnamen des lokalen Knotens und als Namen seiner PU. Der einzige Datenfluß, der den PU-Namen des peripheren Knotens enthält, ist ein Alert. Wenn jedoch der Communications Server (APPC/APPN) einen Alert sendet, enthält der Alert den Steuerpunktnamen (Ressourcenart ist CP) und nicht einen PU-Namen.

Wenn Emulationen einen PU-Namen in den Alerts senden, ist der Name mit dem Steuerpunktnamen identisch (weil der Communications Server den Steuerpunktnamen als PU-Namen des Knotens verwendet). Host-ZAVS kann nur für eine Verbindung definiert werden, bei der PU-Name und Steuerpunktname identisch sind. Außerdem sind bei Host-Verbindungen, bei denen sich PU-Name und Steuerpunktname unterscheiden, keine CP-CP-Sitzungen mit dem Host oder Weiterleitungen von APPN-Übertragungen über die Verbindung möglich. Alle Alerts beinhalten den Steuerpunktnamen, auch wenn der Alert durch eine Bedingung bei einer Verbindung verursacht wurde, die eine andere PU verwendet.

Für Namen von lokalen Knoten gelten folgende Einschränkungen:

- **Länge**: Zwischen 1 und 8 Zeichen
- **Zulässige Zeichen**: A bis Z, 0 bis 9, $, @, #
- **Erstes Zeichen**: A bis Z, $, @, #

Namen logischer Einheiten (LUs): LU-Namen werden logischen SNA-Definitionseinheiten in einem Knoten gegeben, die Unterstützungsfunktionen zur Transaktionsverarbeitung bereitstellen. Dadurch können sie mit anderen LUs im Netz, einschließlich Host-Anwendungen, kommunizieren.

Für LU-Namen gelten folgende Einschränkungen:

- **Länge**: Zwischen 1 und 8 Zeichen
- **Zulässige Zeichen**: A bis Z, 0 bis 9, $, @, #

Sockets-über-SNA-LU-Namen: Der Sockets-über-SNA-Gateway muß über einen für den Gateway konfigurierten LU-Namen verfügen, damit er erfolgreich initialisiert werden kann. Sockets-über-SNA-Gateway definiert den für Communications Server konfigurierten LU-Namen dynamisch bei der Initialisierung.

Bei der Verwendung einer vordefinierten Namenskonvention für Sockets-über-SNA-LUs können Namen bei folgenden Aufgaben hilfreich sein:

- Feststellen, welche Namen Sockets-über-SNA-Gateway-LUs sind und welche Namen für andere LUs im Netz stehen
- Analyse und Auflösung von Zuordnungs- und Weiterleitungsfehlern, falls diese auftreten
- Ermöglichen algorithmischer Zuordnung bei der Zuordnung von IP-Adressen zu Sockets-über-SNA-LU-Namen

Weitere Informationen zum Zuordnen von IP-Adressen zu LU-Namen können in „AnyNet Sockets über SNA konfigurieren“ auf Seite 96 nachgelesen werden.

Schritt 4. Netzadressen definieren

Es muß sichergestellt werden, daß die Adressen im Netz konsistent und eindeutig sind. Alle Adressen müssen eindeutig sein. Welche Adressen definiert werden müssen, hängt von der Konfiguration des Netzes ab. In den weiteren Abschnitten werden folgende Adressen beschrieben:

- LAN
- SDLC
- X.25

Die verwendeten Adressen notieren, um sicherzustellen, daß kein Adreßkonflikt auftritt und daß sie mit den ausgewählten Namenskonventionen übereinstimmen.

LAN-Adapteradressen

LAN-Adapteradressen sind aus 12 Zeichen bestehende Hexadezimalzahlen, die vom Hersteller im Adapter codiert sind (universell vergebene Adapteradresse) oder vom Netzadministrator zugeordnet werden (lokal vergebene Adresse). Alle Netzadapterkarten in der Datenstation, die für die Datenübertragung über LAN konfiguriert wird, müssen eine eindeutige Adresse haben.

Für die Netzadapterkarten können entweder die universell vergebenen Adressen, auch als „ursprüngliche Adressen“ bezeichnet, verwendet oder lokal vergebene Adressen zugeordnet werden. LAN-Adapteradressen müssen im Netz eindeutig sein. Werden lokal vergebene Adressen verwendet, sicherstellen, daß die Adressen im Netz eindeutig sind.

Lokal vergebene Adressen sind von Vorteil, wenn ein Adapterfehler auftritt, der das Ersetzen des Adapters erforderlich macht. Die vorhandene Adresse kann dem Ersatzadapter zugeordnet werden, so daß keine Konfigurationen geändert werden müssen, die diese Adresse enthalten. Werden universell vergebene Adressen verwendet, muß die Adresse des Netzadapters für alle Datenstationen geändert werden, die auf fehlerhafte Adapterkarten zugreifen.

Für die Konfiguration von LAN-Adapteradressen gelten folgende Einschränkungen:

- **Länge**: 12 Zeichen
- **Zulässige Zeichen**: A, B, C, D, E, F, 0-9
- **Bereich**: X'400000000000' bis X'7FFF FFFF FFFF'

Im LAN kann festgelegt werden, daß lokal vergebene LAN-Adapteradressen verwendet werden sollen. In diesem Fall werden den LAN-Adaptern Hexadezimalzahlen als Adresse zugeordnet, anstatt die in den LAN-Adaptern codierten universell vergebenen LAN-Adapteradressen zu verwenden. Es kann eine Konvention mit folgenden Kriterien verwendet werden:

- Die ersten 4 Stellen sind immer X'4000'
- Die folgenden 3 Stellen sind immer X'268' zur Angabe der Abteilung
- Die letzten Stellen liegen im Bereich von X'01000' bis X'FFFFF' und geben die jeweilige Datenstation im Netz an

Universell vergebene Adressen bei Ethernet haben Ethernet-Format. Das Format (Ethernet oder Token-Ring) kann angegeben werden, wenn lokal vergebene Adressen verwendet werden. Bei der Konfiguration der Zieladresse bei SNA-Verbindungen sicherstellen, daß das Adreßformat mit dem Format übereinstimmt, daß bei der fernen Datenstation angegeben wurde. Werden Netze über Brücken verbunden, ist es möglich, daß sich die lokale Datenstation in einem Token-Ring-Netz und die ferne Station in einem Ethernet-Netz befindet und eine Adresse im Ethernet-Format (mit Byte-Austauschformat) verwendet wird.

SDLC-Sekundärstationsadressen

Über Stationsadressen werden Sekundärstationen im Netz gekennzeichnet.

Sekundärstationsadressen müssen im Netz eindeutig sein. Die Primärstation benötigt zur Kommunikation mit der Sekundärstation die Adresse der Sekundärstation. Die Sekundärstation verwendet ihre eigene Adresse zur Kommunikation mit der Primärstation.

Unterstützt die Sekundärstation die Rundsendeadresse X'FF', erkennt die Primärstation bei Punkt-zu-Punkt-Verbindungen die Adresse der fernen Sekundärstation. Die Adresse der Sekundärstation kann ein beliebiger Wert zwischen X'01' und X'FE' sein.

Bei Primärstationen, die die Rundsendeadresse nicht unterstützen, muß für die Sekundärstation derselbe Wert angegeben sein, der an der Primärstation definiert ist. Der Wert muß zwischen X'01' und X'FE' liegen.

Anmerkung: Die meisten Stationen unterstützen die Rundsendeadresse, so daß für die Adresse der Sekundärstation auf der Primärstation X'FF' verwendet werden sollte.

Bei zu vereinbarenden Stationen sind lokale Sekundärstationsadressen zwischen X'01' und X'FE' konfiguriert. Es wird die Adresse der Station verwendet, die als Sekundärstation vereinbart wurde.

Bei Sekundärstationen in einer Mehrpunktverbindung muß die Adresse dem Wert auf dem Knoten entsprechen, der die Funktion für den Mehrpunkt-Primär-Server zur Verfügung stellt. Die Adresse liegt im Bereich von X'01' bis X'FE'.

X.25-Adressen

X.25-Adressen werden verwendet, um in X.25-Netzen kommunizierende Ressourcen zu kennzeichnen. X.25-Netze implementieren die CCITT-Empfehlung, in der die Schnittstelle zwischen Datenendeinrichtungen und Netzen mit Paketvermittlung definiert wird. X.25-Adressen müssen im Netz eindeutig sein. Diese Adressen können beim X.25-Netzbetreiber angefragt werden.

Internet-Adressen

Internet Protocol-Adressen (IP-Adressen) werden zur Weiterleitung von Daten im Netz verwendet. Jedem TCP/IP-Host ist mindestens eine eindeutige IP-Adresse zugeordnet. Die dem Host zugeordnete IP-Adresse definiert keinen Host im Netz; sie definiert eine Netzschnittstelle auf diesem Host zu einem Netz.

Ein Communications Server-Knoten muß für jede Netzschnittstelle, die TCP/IP-Daten über den Knoten weiterleitet, eine eindeutige IP-Adresse haben. Beispiel: Ein Communications Server-Knoten, der TCP/IP-Daten über ein SNA-Netz weiterleitet (mit Hilfe der Sockets-über-SNA-Gateway-Funktion) benötigt eine eindeutige IP-Adresse sowohl für das SNA-Netz als auch für das TCP/IP-Netz. Die IP-Adresse der TCP/IP-Schnittstelle kennzeichnet die Verbindung des Sockets-über-SNA-Gateways zum IP-Netz, während die IP-Adresse die Verbindung zum SNA-Netz kennzeichnet, das für das System wie ein "virtuelles" TCP/IP-Netz aussieht.

Eine IP-Adresse besteht aus einem zweiteiligen 32-Bit-Adreßfeld:

- Der erste Teil des Adreßfelds enthält die Netzadresse; der zweite Teil enthält die Host-Adresse.
- Die Anzahl der für die Netz- und Host-Abschnitte einer IP-Adresse verwendeten Bit sind variabel und hängen von der Adreßkategorie der IP-Adresse ab.
- Mit Hilfe einer Netzmaske kann ein Teil des Host-Abschnitts der IP-Adresse als eine Teilnetzadresse verwendet werden.

Die Kategorie der IP-Adresse wird durch Lesen der ersten 3 (oberen) Bit der Adresse festgelegt. Wie in Tabelle 33 gezeigt, unterstützt der Communications Server die Adreßkategorien A, B und C. Weitere Informationen können dem *Guide to Sockets over SNA* entnommen werden.

Tabelle 33. Vom Communications Server unterstützte IP-Adreßkategorien

Adreß-kategorie	**Standard-netz-maske**	**Bit-Verteilung für Netz- und Host-Adressen**	**Für IP-Adressen in Schreibweise mit Trennzeichen in Form von *a.b.c.d* ist der Wertebereich für *a* folgender:**
A	255.0.0.0	8-Bit Netzadresse; 24-Bit Host-Adresse	1–127 9.0.0.0 ist z. B. eine IP-Netzadresse der Kategorie A.
B	255.255.0.0	16-Bit Netzadresse; 16-Bit Host-Adresse	128–191 132.11.0.0 ist z. B. eine IP-Netzadresse der Kategorie B
C	255.255.255.0	24-Bit Netzadresse; 8-Bit Host-Adresse	192–223 220.11.44.0 ist z. B. eine IP-Netzadresse der Kategorie C.

Schritt 5. Hilfsprogramme für die Konfiguration und Installation auswählen

Der Communications Server verwendet die in den nächsten Abschnitten beschriebenen Hilfsprogramme für die Konfiguration. Weitere Informationen zu diesen Hilfsprogrammen können der Dokumentation *Einstieg* entnommen werden.

Knotenkonfigurationsanwendung

Die Anwendung **Knotenkonfiguration** hat eine grafische Oberfläche zum Verwalten von SNA-Konfigurationsdaten. Die SNA-Konfigurationsdaten werden in einer Baumstruktursicht dargestellt, um die Beziehungen zwischen den Definitionen aufzuzeigen. Der Benutzer erhält beim Erstellen einer Konfiguration Hilfe zum Ausführen von Aufgaben durch eine integrierte Task-Liste, durch den Online-*Lerntext* und durch die Kontexthilfe. Die Anwendung ermöglicht das Erstellen von Benutzerkonfigurationsdateien und das Prüfen der angegebenen Daten.

Fernkonfiguration

Die **Knotenkonfiguration** kann auch verwendet werden, um eine Verbindung zu einem fernen Communications Server herzustellen und dessen Ressourcen direkt zu konfigurieren. Der Benutzer kann die Konfiguration für einen Communications Server von jeder Stelle im Netz aus fern verwalten.

Ein Fernverwaltungs-Client installiert nur die Verwaltungsanwendungen, einschließlich der Anwendung **Knotenkonfiguration**, auf einem Client. Von diesem Client aus kann ein Benutzer jeden Communications Server im Netz vollständig verwalten und konfigurieren.

Fernverwaltungs-Clients unter Windows 95 und Windows NT verwenden die Windows NT-Domänensicherheitsfunktion zur Identifikationsüberprüfung der Client-Verbindung zum Server, ohne daß Benutzer-ID und Kennwort erneut eingegeben werden müssen. Der Client muß einer Windows NT-Domäne angehören, und zwar entweder durch seine Teilnahme an einer Communications Server-Domäne oder durch lokale Anmeldung über eine synchronisierte Benutzer-ID mit Kennwort.

Benutzer von Fernverwaltungs-Clients außerhalb der Windows NT-Domäne müssen die Benutzer-ID und das Kennwort entweder in einer Eingabeaufforderung oder durch Speichern dieser Werte in der Client-Konfigurationsdatei angeben.

Die berechtigten Benutzer von Fernverwaltungs-Clients werden in der lokalen Gruppe IBMCSADMIN erfaßt, die sich direkt auf dem Communications Server oder auf der Steuereinheit der Domäne befindet, zu der der Communications Server gehört. Diese Benutzergruppe wird während der Installation erstellt und kann mit dem Benutzer-Manager von Windows NT verwaltet werden. Benutzern von Fernverwaltungs-Clients müssen die Benutzerberechtigungen der Gruppe IBMCSADMIN zum lokalen Anmelden an den Server erteilt werden.

ASCII-Konfigurationsdatei

Die Communications Server-Anwendung **Knotenkonfiguration** speichert ihre Konfigurationsdaten in einer ASCII-Konfigurationsdatei. Dadurch kann der Benutzer Konfigurationsdateien auch ohne die Anwendung **Knotenkonfiguration** ändern. (Weitere Informationen zu dieser Datei und ihrer Syntax können in der *Configuration File Reference* nachgelesen werden.) In dieser Datei kann ein Netzadministrator mit Hilfe automatisierter Tasks (z. B. Skript- oder Softwareverteilungsservices wie Tivoli TME10 oder Microsoft System Management Server) innerhalb kurzer Zeit Änderungen an der Konfiguration vornehmen.

Beim Erstellen von Konfigurationen für eine größere Anzahl zu implementierender Server kann der Netzadministrator eine Schablonenkonfigurationsdatei mit den gemeinsamen Konfigurationselementen aller Server erstellen. Bei Verwendung von Antwortdateien, die nur die für die einzelnen Server erforderlichen Änderungen enthalten, kann der Administrator die Schablonen- und Antwortdatei verteilen und miteinander mischen, um die Zielkonfiguration zu erstellen. Ausführliche Informationen zur Verwendung von Schablonen- und Antwortdateien für Konfiguration und Installation können dem Abschnitt „Konfiguration mit Schablonen- und Antwortdateien“ entnommen werden.

Verwaltung über das Web

Mit Hilfe der Verwaltung über das Web kann ein Benutzer eine Communications Server-Konfigurationsdatei durch Laden der Datei in ein Editierfenster ändern. Die vorgenommenen Änderungen werden zum Server übertragen, überprüft und für die sofortige Verwendung gespeichert. Der Benutzer kann den Server stoppen und mit den Änderungen erneut starten oder die Konfigurationsänderungen auf ein aktives System anwenden.

Konfiguration mit Schablonen- und Antwortdateien

Die Schablonen- und Antwortdateien des Communications Server ermöglichen es, eine Konfiguration mit Hilfe eines Editors zu erstellen oder zu ändern. Alle Schlüsselwörter und Parameter der Communications Server-Konfiguration können mit Antwortdateien konfiguriert werden. Sowohl die Schablonen- als auch die Antwortdateien haben dasselbe Format wie die Communications Server-Konfigurationsdateien (.ACG).

Anmerkung: Das Format der .ACG-Dateien ist in der Datei OCDNTS50.DAT dokumentiert, die sich im Communications Server-Installationsverzeichnis (z. B. C:\IBMCS) befindet. Weitere Informationen zu den in .ACG-Dateien verwendeten Schlüsselwörtern und Parametern können der *Configuration File Reference* entnommen werden.

Schablonendateien vereinfachen das Verteilen zahlreicher Konfiguration auf ferne Server. In einer Schablonendatei können Schlüsselwörter angegeben werden, die mehreren Servern gemeinsam sind. Beispiel: Wenn mehrere Server als SNA-Gateways mit Unterstützung impliziter Clients konfiguriert werden, sind viele der erforderlichen Schlüsselwörter identisch. In diesem Fall kann eine Schablonenkonfigurationsdatei mit den gemeinsamen Schlüsselwörtern erstellt werden.

Mit Antwortdateien können Schlüsselwörter in einer Schablonendatei hinzugefügt, geändert oder gelöscht werden. Dabei bleibt die ursprüngliche Schablonenkonfigurationsdatei unverändert. Durch Angeben des Schlüsselworts INCLUDE am Ende einer Schablonendatei kann eine Antwortdatei in die Schablonendatei gemischt werden. Beispiel: Wenn die zu verwendende Antwortdatei *myconfig.rsp* heißt, muß die letzte Zeile der Schablonendatei, die die Antwortdatei verwenden soll, `INCLUDE = myconfig.rsp` lauten. Nach dem Mischen der Antwortdatei und der Schablonendatei kann der resultierenden Konfigurationsdatei ein Dateiname mit der Erweiterung .ACG zugeordnet werden, der sie von anderen .ACG-Dateien unterscheidet.

Beim Erstellen von Konfigurationen mit Schablonen- und Antwortdateien durchsucht das Prüfdienstprogramm die Verzeichnisse in folgender Reihenfolge:

1. Das lokale Verzeichnis, in dem das Prüfdienstprogramm aufgerufen wird
2. Das Unterverzeichnis PRIVATE im Communications Server-Installationsverzeichnis

Um sicherzustellen, daß die Schablonen- und Antwortdateien vom Prüfdienstprogramm gefunden werden, sollten sie im Unterverzeichnis PRIVATE gespeichert werden. Im Unterverzeichnis PRIVATE werden auch die Konfigurationsdateien (.ACG) gespeichert.

Schlüsselfelder

Das Schlüsselfeld ist derjenige Parameter in einem Schlüsselwort, der das Schlüsselwort benennt und eindeutig von anderen Schlüsselwörtern des gleichen Typs unterscheidet. Der Parameter @KEY_NAME gibt das Schlüsselfeld für das Schlüsselwort an.

Das Schlüsselfeld ist in einem Schlüsselwort, das über ein Schlüsselfeld verfügt, immer der erste Parameter (z. B. **MODE_NAME** im Schlüsselwort **MODE**).

Manche Schlüsselwörter verfügen nicht über Schlüsselfelder, weil sie in einer Konfigurationsdatei nur einmal angegeben werden dürfen. Ein solches Schlüsselwort, das nur einmal angegeben werden darf, ist beispielsweise **TN3270E_DEF**.

Einer Schablonendatei Schlüsselwörter hinzufügen

Beim Hinzufügen einer neuen Schlüsselwortdefinition mit Hilfe einer Antwortdatei muß das Schlüsselwort vollständig angegeben werden. Das Schüsselfeld muß zusammen mit einem eindeutigen Wert angegeben werden. Wenn untergeordnete Felder des Schlüsselworts weggelassen werden, werden die Standardwerte für diese Felder verwendet. Beispielsweise könnte die Antwortdatei das folgende Schlüsselwort enthalten, um der Konfiguration ein Schlüsselwort **MODE** hinzuzufügen:

```
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
)
```

Der Inhalt dieser Antwortdatei geht davon aus, daß die Schablone kein Schlüsselwort **MODE** mit dem Parameter `MODE_NAME=MYMODE` enthält. Ist ein solches Schlüsselwort vorhanden, würden die Parameter durch die in der Antwortdatei angegebenen Werte aktualisiert.

Wenn der Parameter `MODE_NAME` in der Antwortdatei fehlt, tritt bei der Konfigurationsprüfung ein Fehler auf, weil der Parameter `MODE_NAME` nicht eindeutig identifiziert werden kann. In der Antwortdatei sind nicht alle für das Schüsselwort **MODE** verfügbaren Parameter angegeben. Für die nicht angegebenen Parameter werden die in der Datei OCDSNT50.DAT zugeordneten Standardwerte verwendet. Daraus ergibt sich der folgende Zusatz in der Konfigurationsdatei:

```
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
)
```

Ein Schlüsselwort in einer Schablonendatei ändern

Wenn eine vorhandene Schlüsselwortdefinition mit Hilfe einer Antwortdatei geändert werden soll, sollte das Originalschlüsselwort in der Schablonendatei enthalten sein. Ist dies nicht der Fall, fügt die Antwortdatei der neuen Konfiguration einen Eintrag hinzu. Der Schlüsselparameter muß in der Antwortdatei angegeben sein, um das Zielschlüsselwort zu kennzeichnen. Nur die im Schlüsselwort der Antwortdatei angegebenen Parameter werden im Schlüsselwort der Schablonendatei aktualisiert. Parameter, die in der Antwortdatei nicht angegeben sind, bleiben unverändert. Beispiel: In der Schablonendatei ist das folgende Schlüsselwort **MODE** angegeben:

```
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 )
```

Und in der Antwortdatei ist folgendes Schüsselwort angegeben:

```
MODE=(
     MODE_NAME=#INTER
     AUTO_ACT=10
)
```

Die daraus resultierende Konfiguration würde folgende Definition des Schlüsselworts **MODE** enthalten:

```
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
)
```

Ein Schlüsselwort aus einer Schablonendatei löschen

Wenn ein Schlüsselwort mit Hilfe einer Antwortdatei aus der Schablone gelöscht wird, müssen der Schüsselparameter und der Wert zur Kennzeichnung des Schlüsselworts zusammen mit dem Schlüsselwort `DELETE` angegeben werden. Beispiel: In der Schablonendatei ist das folgende Schlüsselwort angegeben:

```
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
)
```

Und die Antwortdatei enthält folgendes Schlüsselwort:

```
MODE=(
     MODE_NAME=#INTER
     DELETE
)
```

Die daraus resultierende Konfiguration enthält nicht die Definition für den Modus `#INTER`.

Das Schlüsselwort **DELETE** kann auf eine Angabe *parameter=wert* folgen oder in einer separaten Zeile vor oder nach dem Parameter stehen. Beispielsweise sind die folgenden Verwendungsweisen des Schlüsselworts **DELETE** zulässig:

```
MODE=(
     MODE_NAME=#INTER
     DELETE
)
MODE=(
     DELETE
     MODE_NAME=#INTER
)
MODE=(
     MODE_NAME=#INTER DELETE
)
```

Das Schlüsselwort **DELETE** darf **nicht** vor einer Angabe *parameter=wert* in der gleichen Zeile stehen. Beispielsweise ist die folgende Verwendungsweise des Schlüsselworts **DELETE** nicht zulässig:

```
MODE=(
     DELETE MODE_NAME=#INTER
)
```

Um alle Schlüsselwörter eines bestimmten Typs zu löschen oder ein einziges Schlüsselwort, das kein Schlüsselfeld hat, muß nur das betreffende Schlüsselwort zusammen mit dem Schlüsselwort **DELETE** angegeben werden. Beispiel:

```
TN3270E_DEF=(
     DELETE
)
```

Schritt 6. Communications Server-Funktionen auswählen

Die unterstützten Funktionen für Communications Server werden nachfolgend beschrieben. Für die vorhandene Verbindungsart werden möglicherweise einige oder alle dieser Funktionen unterstützt:

SNA-Gateway-Konfiguration

Eine SNA-Gateway-Konfiguration ermöglicht den Datenaustausch zwischen untergeordneten Client-Datenstationen und einem SNA-Großrechner-Host. Der Gateway übernimmt die Funktion eines Konzentrators, der die LU-Ressourcen eines oder mehrerer Hosts und Host-PUs über die von Communications Server unterstützten Übertragungsmedien für untergeordnete SNA-Client-Datenstationen zur Verfügung stellt.

TN3270E-Server-Konfiguration

Eine TN3270E-Server-Konfiguration ermöglicht den Datenaustausch zwischen untergeordneten TCP/IP-Client-Datenstationen, auf denen TN3270E-Anwendungen (oder TN3270-Anwendungen) ausgeführt werden, und einem SNA-Großrechner-Host. Der Server übernimmt die Funktion eines Konzentrators, der die LU-Ressourcen eines oder mehrerer Hosts und Host-PUs über die von Communications Server unterstützten Übertragungsmedien für untergeordnete TN3270E-Sitzungen (oder TN3270-Sitzungen) zur Verfügung stellt.

TN5250-Server-Konfiguration

Eine TN5250-Server-Konfiguration ermöglicht den Datenaustausch zwischen untergeordneten Client-Datenstationen in einem TCP/IP-Netz, auf denen TN5250-Anwendungen ausgeführt werden, und einem AS/400-System in einem SNA-Netz. Der Server übernimmt die Funktion eines Gateways, der AS/400-Anzeigesitzungen über die von Communications Server unterstützten Übertragungsmedien für untergeordnete TN5250-Clients zur Verfügung stellt.

APPN-Netzknotenkonfiguration

Netzknoten sind zuständig für die Verwaltung und Weiterleitung von Informationen über ein APPN-Netz. Sie verwalten ein Verzeichnis sämtlicher Ressourcen (LUs), die auf direkt verbundenen Endknoten verfügbar sind, sowie eine Topologie aller Netzknoten in dem APPN-Netz. Wird von einem Knoten im Netz eine unabhängige LU 6.2-Sitzung angefordert, ist der Netzknoten dafür zuständig, die von der Sitzung angeforderte ferne Ressource zu lokalisieren, die Sitzung einzurichten und zwischen den beiden Knoten weiterzuleiten.

DLUR/DLUS-Konfiguration

Communications Server unterstützt abhängige LU-Sitzungen über APPN-Netze. Dazu muß Communications Server die Funktion eines abhängigen LU-Requesters (DLUR - Dependent LU Requester) übernehmen, der Leitwegservices von einem abhängigen LU-Server (DLUS - Dependent LU Server) anfordert, der sich auf einem Host befindet.

Communications Server unterstützt DLUR sowohl für lokale als auch für untergeordnete Sitzungen und Einheiten. In beiden Fällen muß der lokale Knoten so konfiguriert sein, daß er die Verbindung zu einem APPN-Netz herstellt.

AnyNet-SNA-über-TCP/IP-Gateway-Konfiguration

Der SNA-über-TCP/IP-Gateway übernimmt die Weiterleitung von SNA-Datenverkehr (unabhängige LU 6.2) zwischen TCP/IP- und SNA-Netzen. Der SNA-über-TCP/IP-Gateway ermöglicht beispielsweise die Kommunikation zwischen APPC- oder CPI-C-Anwendungen auf einem anderen AnyNet-SNA-über-TCP/IP-Zugriffsknoten und SNA-Peer-Knoten in einem SNA-Netz.

Der AnyNet-SNA-über-TCP/IP-Gateway muß als APPN-Netzknoten konfiguriert werden. Dadurch können APPC-Sitzungen an geeignete SNA-Peer-Knoten weitergeleitet werden.

AnyNet-Sockets-über-SNA-Konfiguration

Es gibt zwei Arten von AnyNet-Sockets-über-SNA-Knoten: Zugriffsknoten und Gateway-Knoten. Zugriffsknoten ermöglichen die lokale Ausführung von TCP/IP-Sockets-Anwendungen sowie die Kommunikation mit anderen Zugriffsknoten oder Gateways im SNA-Netz. Der AnyNet Sockets über SNA-Gateway-Server übernimmt die Funktion eines Protokollumsetzers, der Anwendungen in einem TCP/IP-Netz die Kommunikation mit Socket-Anwendungen auf einem Zugriffsknoten im SNA-Netz ermöglicht. Bei Verwendung von zwei Gateways können separate TCP/IP-Netze über ein SNA-Netz verbunden werden.

SNA-API-Client-Konfiguration

SNA-API-Clients sind von Communications Server unabhängige Maschinen, auf denen SNA-Anwendungen ausgeführt werden können. Dabei wird der SNA-Code auf dem Communications Server zum Verwalten der Sitzung verwendet. Communications Server erstellt und verwaltet einfach eine Sitzung als sei der Ursprung der lokale Knoten, leitet aber die Anwendungsdaten nicht an die eigenen Anwendungs-APIs, sondern an den SNA-API-Client weiter.

SNA-API-Clients ermöglichen dem Benutzer, SNA-Anwendungen auszuführen, ohne auf der jeweiligen Maschine einen SNA-Übertragungsstapelspeicher (wie z. B. Communications Server für Windows NT) zu installieren. Auf diese Weise können kleinere Maschinen mit geringerer Verarbeitungsleistung zum Ausführen der SNA-Anwendungen verwendet werden, während eine zentrale Maschine mit größerer Verarbeitungsleistung als SNA-Server für diese SNA-API-Clients dediziert werden kann.

SNA-API-Clients unterstützen zwei Arten von Anwendungen: APPC-Anwendungen (unabhängige LU 6.2) und LUA-API-Anwendungen (z. B. 3270-Emulationen).

CPI-C oder APPC-Konfiguration

Communications Server unterstützt CPI-C- oder APPC-Anwendungen (z. B. APPC-3270- oder -5250-Emulation auf einem AS/400-System). Der APPC-Netzbetrieb ist außerordentlich flexibel und vielseitig und kann daher sehr komplex sein. Der Komplexitätsgrad dieser Konfiguration hängt davon ab, wie Communications Server verwendet werden soll und in welchem Umfang die Anwendung genutzt werden soll.

Abhängige LU 6.2-Sitzungen mit einem Host

Communications Server unterstützt abhängige LU 6.2-Sitzungen mit einer Host-PU.

3270-Konfiguration

Communications Server unterstützt 3270-Sitzungen mit einem Host.

ZAVS-Konfiguration

Communications Server unterstützt ferne zentrale Alert-Verarbeitungssysteme (ZAVS) zur Weiterleitung von Alert-Informationen für bestimmte Verwaltungsserviceanwendungen. Der lokale Knoten lokalisiert ferne zentrale Alert-Verarbeitungssysteme über ein APPN-Netz.

Konfiguration für gemeinsam benutzte AS/400-Ordner

Mit Communications Server können Platteneinheiten auf dem Server erstellt werden, die den Datenaustausch mit AS/400-Ordnern über AS/400 IFS (Integrated File System) ermöglichen. Wenn der Server diese Platteneinheiten zur gemeinsamen Benutzung bereitstellt, können Clients mit NET USE die Verbindung zu ihnen herstellen. Auf diese Weise können viele Clients die Verbindung zu Ordnern in dem AS/400-System so herstellen, als wären sie Laufwerke der lokalen Datenstation.

Schritt 6.1. Planung für Anwendungsprogramme

Die Anwendungen überprüfen und sicherstellen, daß alle für ihre Ausführung erforderlichen Voraussetzungen erfüllt sind. Im besonderen folgende Voraussetzungen überprüfen:

- Modi
- Transaktionsprogramme (TPs)
- LU-Definitionen (Host, LU 6.2)
- Partner-LUs

Schritt 7. Konfigurationen erstellen und installieren

Es muß festgelegt werden, wie Communications Server auf den Servern des Benutzers konfiguriert und installiert werden soll. Es bestehen folgende Möglichkeiten:

- Der Netzadministrator kann den Benutzern Anweisungen zur Installation und Konfiguration des Communications Server geben. Er kann eigene Anweisungen vorbereiten oder Kopien der Dokumentation *Einstieg* drucken. Außerdem muß er die speziellen Informationen für jeden Server bereitstellen, wie z. B. Netz-ID, Steuerpunktname und Netzadresse.
- Er sollte den Benutzern Anweisungen zur Installation des Communications Server mit einer vorhandenen Konfigurations- oder Schablonendatei geben. Außerdem muß er für jeden Server eine angepaßte Antwortdatei bereitstellen sowie Communications Server-CD-ROMs oder Zugriff auf CD-ROM-Abbilder.
- Der Netzadministrator kann den Communications Server selbst auf Benutzer-Servern konfigurieren und installieren. Sofern es sich nicht um eine sehr kleine Gruppe von Benutzern handelt, kann der Einsatz eines Programms erwogen werden, das die Konfiguration, Installation und Verteilung von Software für mehrere Datenstationen unterstützt. Beispiele für solche Produkte sind IBM NetView Distribution Manager/2 (NVDM/2), Tivoli TME-10 und Microsoft System Management (SMS).

Konfiguration und Installation mit Hilfe einer Antwortdatei

Informationen zum Ausführen von Installation und Konfiguration mit Hilfe einer Antwortdatei können dem Abschnitt „Konfiguration mit Schablonen- und Antwortdateien“ auf Seite 210 entnommen werden.

Schritt 8. Benutzermaterial erstellen

Nachdem die Planung für das Netz beendet und die Implementierung des Planes festgelegt wurde, muß Benutzermaterial erstellt werden. Das heißt im einzelnen, daß Dokumentation zur Installation, Konfiguration und für den täglichen Betrieb erstellt werden muß und daß Sicherungsprozeduren vorbereitet werden müssen.

Dokumentation vorbereiten

Für die Benutzer muß Dokumentation zum Installieren, Konfigurieren und Verwenden des Communications Server und lokaler Anwendungen erstellt werden, die den speziellen Erfordernissen der einzelnen Benutzer entsprechen. Die folgenden Abschnitte enthalten Vorschläge dazu, welche Informationen in der Dokumentation enthalten sein sollten.

Material und Prozeduren zur Konfiguration und Installation

Informationen zur Installation des Communications Server kann der Benutzer der Dokumentation *Einstieg* und der Online-Hilfe zur Installation entnehmen. Der Benutzer muß den Anweisungen des Netzadministrators entnehmen können, welche der folgenden Schritte auszuführen sind, wenn Software installiert wird:

- In welchen Fällen Konfigurationsdateien gesichert werden müssen
- Ob die Standardwerte zum Erstellen einer Communications Server-Konfigurationsdatei übernommen werden können

  Möglicherweise müssen Netzinformationen wie LAN-Adapteradressen, Netznamen usw. angegeben werden.
- In welchen Fällen die Installation mit einer Antwortdatei ausgeführt werden muß, die vom Netzadministrator zur Verfügung gestellt wird
- In welchen Fällen mit einer angepaßten Konfigurationsdatei installiert werden muß, die vom Netzadministrator zur Verfügung gestellt wird

Falls erforderlich, den Benutzern die entsprechende Dokumentation zur Verfügung stellen.

Material und Prozeduren für Communications Server

Folgendes Material wird zur Verwendung mit Communications Server-Funktionen und -APIs empfohlen:

- *Einstieg*
- Vom Benutzer erstellte Programme für die ausgewählten Communications Server-APIs

Communications Server starten und stoppen

Die Prozedur zum Starten oder Stoppen des Communications Server kann der Dokumentation *Einstieg* entnommen werden.

Hat der Netzadministrator andere Anweisungen zum Starten oder Stoppen vorbereitet, muß er diese Anweisungen den Benutzern zur Verfügung stellen.

- Rufnummer für Hilfe bei der Host-Fehlerbestimmung (die Host-Benutzerunterstützung kontaktieren)
- Anmeldeverfahren für Host-Systeme und -Anwendungen
- Prozeduren zum Stoppen der Host-Anwendung

  Die Host-Benutzerunterstützung kontaktieren.
- Abmeldeverfahren

  Die Anweisungen sollten alle speziellen Anforderungen zum Abmelden von Systemen oder Anwendungen enthalten. Diese Informationen können bei der Host-Benutzerunterstützung angefragt werden.

Material und Prozeduren für Anwendungsprogramme

Der Netzadministrator sollte den Benutzern Prozeduren und andere Informationen für die Anwendungsprogramme zur Verfügung stellen, die möglicherweise im Netz verwendet werden. Im allgemeinen ist folgendes zur Verfügung zu stellen:

- Prozeduren zum Starten von Anwendungsprogrammen
- Prozeduren zum Ausführen von Anwendungsprogrammen
- Prozeduren zum Reagieren auf Nachrichten, die vom Anwendungsprogramm generiert wurden
- Prozeduren zur Fehlerbestimmung
- Falls erforderlich, Prozeduren zum Stoppen des Anwendungsprogramms

Informationen zu den aufgelisteten Prozeduren beim Anwendungsprogrammierer anfordern.

Material und Prozeduren zur Fehlerbestimmung

Informationen zu Fehlerbestimmung und Fehlerberichten enthält das Handbuch *Einstieg*.

Sicherungsprozeduren vorbereiten

Es kann vorkommen, daß Benutzer versehentlich die Konfigurationsdateien, die Registrierung, das Dateisystem, Anwendungsprogramme oder andere lokal erstellte Programme oder Dateien löschen oder ändern. Auch auf den Servern können Daten gelöscht oder geändert werden, besonders, wenn viele Benutzer während eines Arbeitstags auf die Server-Datenstationen zugreifen.

Aus diesem Grund müssen Sicherungsprozeduren für das Netz vorbereitet und dokumentiert werden. Es ist auch möglich, die Attribute ausgewählter Dateien auf den Servern in Read-Only (Nur-Lesen) zu ändern, so daß diese Dateien von Benutzern nicht geändert werden können.

Schritt 9. Das Netz verwalten

Sind Planung, Installation und Konfiguration des Netzes beendet und wird täglich mit dem Netz gearbeitet, ist es Aufgabe des Netzadministrators, das Netz zu verwalten. Das Hinzufügen, Ändern und Löschen von Ressourcen und Benutzern im Netz sowie Maßnahmen zur Fehlerbehebung müssen geplant werden.

Für die Änderungen am Netz sind dieselben Planungs- und Implementierungsschritte wie bei der ursprünglichen Einrichtung des Netzes auszuführen. Für Änderungen am Netz dieselben Schritte ausführen, die bei der ursprünglichen Planung, Installation und Konfiguration ausgeführt wurden.

Beim Communications Server stehen folgende Hilfsprogramme zur Überwachung der täglichen Netzleistung zur Verfügung:

- **SNA-Knotenoperationen**
- Befehlszeilendienstprogramme
- Web-Verwaltung
- Fernverwaltungs-Client
- Systemverwaltungs-API
- SNMP-Subagent
- NT-Systemmonitor

Die folgenden Programme dienen ebenfalls zur täglichen Verwaltung des Netzes:

- IBM NetView
- IBM LAN Netzwerk-Manager
- Tivoli TME-10

Steuerung und Verwaltung eines Netzes

Systemverwaltungseinrichtungen

Dieses Kapitel enthält eine Übersicht über die Systemverwaltungseinrichtungen von Communications Server und beschreibt die gemeinsamen Funktionen der Einrichtungen. Jede Einrichtung verfügt außerdem über spezifische Funktionen, die separat beschrieben werden.

Die Systemverwaltungseinrichtungen ermöglichen das Überwachen und Steuern der DFV-Ressourcen von Communications Server. Mit Hilfe dieser Funktionen kann der Netzadministrator diese Ressourcen anpassen, um die Effizienz von SNA-DFV-Services zu steigern oder diese Services während der Fehlerbestimmung zu überwachen und zu testen.

Eine Liste der Ressourcen, die verwaltet werden können, enthält das Handbuch *Einstieg*.

Communications Server kann mit den folgenden Einrichtungen verwaltet werden:

- **SNA-Knotenoperationen**
- Fernverwaltung
- Befehlszeilendienstprogramme
- Verwaltung über das Web
- ActiveX-Steuerung der SNA-Knotenoperationen
- Tivoli Plus-Modul
- APPN-MIB-Unterstützung
- S/390 Remote Operations Support (ROPS)

Bei der Verwaltung von Communications Server können diese Einrichtungen in jeder beliebigen Kombination zum Einsatz kommen.

Gemeinsame Funktionen der Systemverwaltungseinrichtungen

Jede Systemverwaltungseinrichtung kann die folgenden Aktionen an Ressourcen ausführen:

- Ressourceninformationen anzeigen
- Ressourcen starten
- Ressourcen stoppen
- Ressourcen löschen
- Pfadumschaltung einleiten

Wie in Tabelle 34 auf Seite 226 gezeigt, kann ein Teil dieser Aktionen für die einzelnen Ressourcen ausgeführt werden.

Tabelle 34. Verwaltungsaktionen für Communications Server-Ressourcen

Ressource	Anzeigen	Starten	Stoppen	Löschen	Pfadum-schaltung
Verbindungen	X	X	X	X	
CPI-C-Zusatzinformationen	X			X	
Einheiten	X	X	X	X	
DLUR-PUs	X	X	X		
Lokale LU 0 bis 3	X			X	
Lokale LU 6.2	X			X	
LU 6.2-Sitzungen	X		X		
PU 2.0/DLUR-Gateway	X			X	
RTP-Verbindungen	X				X
TN3270E-Sitzungen	X		X		
TN5250-Sitzungen	X		X		

SNA-Knotenoperationen

SNA-Knotenoperationen ist eine Online-Einrichtung zum Überwachen und Steuern der von Communications Server verwalteten DFV-Ressourcen. Die **SNA-Knotenoperationen** ermöglichen das Stoppen, Starten und Überwachen von Ressourcen im verwendeten Netz.

Die **SNA-Knotenoperationen** unterstützen den Administrator beim Verwalten der Netzressourcen. Die Programmierfunktionen der Systemverwaltung des Communications Server ermöglichen die Konfiguration und Verwaltung der Knoten auf dem SNA-Netz. Die **SNA-Knotenoperationen** stellen eine Baumstruktursicht der Konfiguration zur Verfügung, in der über eine Grafikschnittstelle mit hierarchischer Anzeige Ressourcen ausgewählt und geändert werden können.

Im Hauptfenster der **SNA-Knotenoperationen** können mehrere Fenster verwaltet werden.

Der Benutzer kann mehrere Communications Server-Konfigurationen definieren und nach Bedarf zwischen ihnen wechseln. Beim Starten von Communications Server wird die Standardkonfiguration als erste Auswahlmöglichkeit für die Knotenkonfiguration oder für Knotenoperationen angeboten, sofern der Benutzer keine andere Konfiguration angibt. Sobald eine neue Konfiguration erstellt ist, kann diese als Standardkonfiguration verwendet werden. Mit den **SNA-Knotenoperationen** kann die neue Konfiguration angewendet werden, und es kann sichergestellt werden, daß die betreffende Produktkomponente gemäß dieser Konfiguration ausgeführt wird.

Mit Hilfe der **SNA-Knotenoperationen** können andere Communications Server-Programme (z. B. **Protokollanzeigefunktion**, **Trace-Einrichtung** oder **Knotenkonfiguration**) gestartet werden.

Fernverwaltung

Die **SNA-Knotenoperationen** ermöglichen außerdem den Verbindungsaufbau zu einem fernen Communications Server und die direkte Verwaltung seiner Ressourcen. Der Benutzer kann die Ressourcen für einen Communications Server von jeder beliebigen Stelle im Netz aus fern verwalten.

Ein Fernverwaltungs-Client installiert nur die Verwaltungsanwendungen, einschließlich der **SNA-Knotenoperationen**, auf einem Client. Von diesem Client aus kann ein Benutzer jeden Communications Server im Netz vollständig verwalten.

Fernverwaltungs-Clients unter Windows 95 und Windows NT verwenden die Windows NT-Domänensicherheitsfunktion zur Identifikationsüberprüfung der Client-Verbindung zum Server, ohne daß Benutzer-ID und Kennwort erneut eingegeben werden müssen. Der Client muß einer Windows NT-Domäne angehören, und zwar entweder durch seine Teilnahme an einer Communications Server-Domäne oder durch lokale Anmeldung über eine synchronisierte Benutzer-ID mit Kennwort.

Benutzer von Fernverwaltungs-Clients außerhalb der Windows NT-Domäne müssen die Benutzer-ID und das Kennwort entweder in einer Eingabeaufforderung oder durch Speichern dieser Werte in der Client-Konfigurationsdatei angeben.

Die berechtigten Benutzer von Fernverwaltungs-Clients werden in der lokalen Gruppe IBMCSADMIN verwaltet, die sich direkt auf dem Communications Server oder auf der Steuereinheit der Domäne befindet, zu der der Communications Server gehört. Diese Benutzergruppe wird während der Installation erstellt und kann mit dem Benutzer-Manager von Windows NT verwaltet werden. Benutzern von Fernverwaltungs-Clients müssen die Benutzerrechte der Gruppe IBMCSADMIN zum lokalen Anmelden an den Server erteilt werden.

Befehlszeilenprogramme

Befehlszeilenprogramme ermöglichen das Absetzen von Befehlen über ein Windows NT-Befehlszeilenfenster. Die Ausgabe der Befehle wird auf dem Bildschirm angezeigt; sie kann aber auch in eine Datei umgeleitet werden.

Eine Liste der verfügbaren Befehlszeilenprogramme enthält das Handbuch *Einstieg*.

Verwaltung über das Web

Die web-gestützte Verwaltungsfunktion von Communications Server ermöglicht das Verwalten des Servers über ein Intranet von jedem System aus, das über einen Web-Browser verfügt. Damit die Web-Verwaltungsfunktion verwendet werden kann, muß auf der Communications Server-Maschine ein Web-Server gestartet sein. Obwohl mehrere Communications Server verwaltet werden können, kann nur jeweils auf einen Server zugegriffen werden. Zum Ausführen von Verwaltungsfunktionen muß sich der Benutzer auf der Windows NT-Maschine, auf der Communications Server ausgeführt wird, als Mitglied der Gruppe IBMCSADMIN an die Web-Verwaltung anmelden.

Diese Funktion kann von der Communications Server CD-ROM installiert werden. Die meisten Funktionen der **SNA-Knotenoperationen** können über einen Web-Browser ausgeführt werden. Dazu gehört das Abfragen von Knotenstatus und Ressourceninformationen, das Ändern von Ressourcen, das Anzeigen und Editieren von Konfigurationsdateien, das Anzeigen von Nachrichtenprotokollen und das Ausführen anderer Verwaltungsaufgaben. Die Web-Verwaltungsfunktion ermöglicht ebenfalls das Editieren von Konfigurationsdateien und das Anzeigen der Protokolldatei. Die erforderlichen Schritte zum Verwenden dieser Funktionen sind auf der Web-Seite **Willkommen bei der Communications Server Web-Verwaltung** beschrieben.

ActiveX-Steuerung der SNA-Knotenoperationen

Für die **SNA-Knotenoperationen** steht eine Version mit ActiveX-Steuerung zur Verfügung. Diese Steuerung ermöglicht das Einbetten der **SNA-Knotenoperationen** in jede Anwendung, die eingebettete Steuerelemente unterstützt (z. B. Microsoft Management Console, MMC). Der Name dieser Steuerung lautet CSNTACTX und befindet sich im Produktinstallationsverzeichnis. Diese Steuerung bietet alle Funktionen der **SNA-Knotenoperationen** und ermöglicht das Einbetten der **SNA-Knotenoperationen** in andere Anwendungen und damit die produktunabhängige Verwaltung.

Tivoli Plus-Modul

Wenn Einheiten und Anwendungen im Netz mit TME (Tivoli Management Environment) zentral verwaltet werden, ermöglicht es das Tivoli Plus-Modul, auch Communications Server mit TME zu verwalten. Das Tivoli Plus-Modul für Communications Server kann auf dem TME-Server installiert werden. Ein installierbares Abbild von TME befindet sich im Verzeichnis TME der Communications Server CD-ROM. Zum Aufrufen der installierten TME Plus-Funktionen, doppelt auf das TivoliPlus-Symbol klicken, das zur TME-Anzeige **Desktop for Administrator** hinzugefügt wurde. Nach Doppelklicken auf das IBM CSPlus-Symbol können mit Hilfe der in der Anzeige enthaltenen Symbole folgende Aktionen ausgeführt werden:

- Communications Server verteilen, installieren und die Installation entfernen
- Den Server starten, stoppen und abfragen
- Server-Ressourcen anzeigen und ändern
- Konfigurationsdateien auflisten
- Fehlernachrichten von Communications Server an eine Tivoli Enterprise-Konsole weiterleiten
- Überwachungen und Schwellenwerte für wichtige Communications Server-Attribute einrichten

Nach dem Doppelklicken auf ein Symbol in der IBM CSPlus-Anzeige können in den Feldern des angezeigten Dialogfensters Informationen eingegeben werden. Hilfetexte zu den Feldern des Dialogfensters können aufgerufen werden.

APPN-MIB-Unterstützung

Communications Server unterstützt SNMP-Anforderungen (SNMP - Simple Network Management Protocol) für APPN-Verwaltungsinformationen von jedem SNMP-Verwaltungssystem aus.

Der SNMP-Service kann über die Indexzunge **Dienste** im Dialogfenstermenü **Netzwerk** der Windows NT-Systemsteuerung installiert werden. Nach dem Installieren muß die SNMP-Service-Software mit gültigen Informationen konfiguriert werden, damit SNMP verwendet werden kann.

Zum Konfigurieren von SNMP muß der Benutzer als Mitglied der Administratorgruppe des lokalen Computers angemeldet sein.

Die SNMP-Konfigurationsdaten kennzeichnen Benutzergemeinschaften und Alarmnachrichtenziele.

S/390 ROPS (Remote Operations Support) für das Programm NetView

Wenn RUNCMD von NetView ausgegeben wird, muß der Wert für den Parameter APPL als APPL=CSRCMDS angegeben werden.

Wenn der Befehl RUNCMD ausgegeben wird, werden alle Informationen, einschließlich ID und Kennwort, unverschlüsselt und ungesichert übertragen, sofern nicht das NetView-Unterdrückungszeichen verwendet wird. Diese Informationen werden auf dem Bildschirm angezeigt und im NetView-Protokoll aufgezeichnet. Wenn Kennwörter an den ROPS-Service übertragen werden, ist der Benutzer für die Sicherheit der NetView-Datenstation und der NetView-Protokolle verantwortlich, so daß sensible Daten nicht gefährdet werden.

Anhänge

Anhang A. Planung für Communications Server

Dieser Anhang enthält Informationen, die zur Planung der Communications Server-Umgebung erforderlich sind.

Kompatible Hardware

In diesem Abschnitt wird die IBM Hardware beschrieben, die den Communications Server unterstützt. Diese Beschreibungen enthalten Informationen zu folgenden Komponenten:

- DFV-Adapter
- Modems
- Adapter für Verschlüsselung auf Sitzungsebene

DFV-Adapter

Eine Liste der von Communications Server unterstützten DFV-Adapter enthält die folgende URL-Adresse im Internet:

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

Modems

Communications Server unterstützt die folgenden Modemtypen:

- Asynchronmodems:
  - Modems 100 % kompatibel mit dem Hayes AT-Befehlssatz
  - IBM Modems, die den Schnittstellenstandards ITU-T (CCITT) V.24/V.28 (EIA RS-232-D) und V.35 entsprechen.
  - Asynchronmodems von anderen Herstellern werden auch unterstützt ebenso wie die Basisfunktion der Standardschnittstelle ITU-T (CCITT) V.24 (EIA RS-232-D) zwischen DEE und DÜE für asynchrone Übertragung
  - Modems, die der RS-232-D-Standardschnittstelle zwischen DEE und DÜE entsprechen
- Synchronmodems und CSU/DSU-Einheiten, die den V.24bis-Befehlssatz unterstützen
- Modems 100 % kompatibel mit dem Hayes AutoSync-Protokoll

X.25-Benutzer benötigen entweder einen Synchronmodem und CSU/DSU-Einheiten, die den V.24bis-Befehlssatz unterstützen, oder einen mit dem Hayes AutoSync-Protokoll kompatiblen Modem. Netzlieferanten informieren über empfohlene Verbindungsart und Modem.

Eine Liste der von Communications Server unterstützten Modems enthält die folgende URL-Adresse im Internet:

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

Adapter für Verschlüsselung auf Sitzungsebene

Damit die Verschlüsselung auf Sitzungsebene verwendet werden kann, werden das Programm Programmed Cryptographic Facility und einer der folgenden Adapter benötigt:

- IBM SecureWay 4758 PCI Cryptographic Coprocessor Adapter
- Andere Adapter, die mit der IBM Common Cryptographic Architecture übereinstimmen

Anmerkung: Wird ein anderer Adapter als der Adapter IBM 4758 verwendet, sind statt dessen verschlüsselte API-Verben erforderlich. Weitere Informationen können der Dokumentation *Communications Server Programming Guide and Reference* entnommen werden.

Emulationssoftware

Eine Liste der von Communications Server unterstützten Emulationssoftware enthält die folgende URL-Adresse im Internet:

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

Überlegungen zur Datenkomprimierung

Bevor die SNA-Datenkomprimierung verwendet werden kann, müssen verschiedene Konfigurationsschritte auf den betreffenden Systemen ausgeführt werden. SNA-Datenkomprimierung wird von folgenden Programmen unterstützt:

- VTAM Version 3, Release 4.1 oder höher
- OS/400 Version 2, Release 3 oder höher

Bei der Komprimierung werden alle RUs unabhängig voneinander komprimiert, und ein Komprimierungsvorsatz wird der RU hinzugefügt. Übertragungskopf und Nachrichtenvorsatz werden nicht komprimiert. Es erfolgt keine Komprimierung, wenn die RU kleiner als 20 Byte oder größer als 64 KB ist oder wenn die komprimierten Daten, einschließlich des Komprimierungsvorsatzes, größer als die Originaldaten sind. Letzteres gilt jedoch nur im Fall von RLE.

Bevor mit der Konfiguration der entsprechenden Funktionen des Communications Server für die Datenkomprimierung begonnen wird, sicherstellen, daß das Partnersystem Datenkomprimierung unterstützen kann und für diese Funktion vorbereitet ist.

Host/VTAM-Verbindung planen

Bevor Datenkomprimierung bei einer Sitzung mit einem IBM System /370- oder IBM System /390-Host mit 3270-Emulation oder mit LU 6.2-Übertragung angefordert werden kann, muß VTAM Version 3, Release 4.1 installiert und konfiguriert sein, damit solche Anforderungen ausgehandelt werden können.

Host-VTAM-Systemprogrammierer sollten die für die Datenkomprimierung erforderlichen VTAM-Definitionen bereitstellen. Es folgt eine Liste der erforderlichen Definitionen. Nach der Liste folgen Beispiele.

- Die VTAM-Startoptionen müssen den Parameter **CMPVTAM**=x enthalten.
- Mit dem Parameter **COMPRES=** ist ein Eintrag LOGMODE erforderlich.
- Dieser Eintrag LOGMODE muß in der verwendeten Modustabelle enthalten sein.
- Für die verwendete Anwendung ist eine VTAM-APPL-Anweisung bei den Parametern **CMPAPPLI=** und **CMPAPPLO=** erforderlich.
- In der VTAM-LU-Definition für die Sitzung müssen der LOGMODE und die Modustabelle angegeben werden, die für die Komprimierung definiert wurden.

CMPVTAM

Dies ist der Parameter für die VTAM-Startoptionen, mit dem die maximal zulässige Komprimierungsstufe für alle an diesen Host angeschlossenen Sitzungen angegeben wird. Die Syntax dieses Parameters lautet folgendermaßen:

```
CMPVTAM=n
```

Dabei ist n die für eine Anforderung zulässige Komprimierungsstufe im Bereich von 0 bis 4. Der empfohlene Wert ist 4; bei Angabe dieses Wertes können alle Stufen der Datenkomprimierung verwendet werden.

COMPRES

Dies ist der VTAM-MODEENT-Tabelleneintrag in der LOGMODE-Definition, die von der LU verwendet wird. Die Syntax lautet folgendermaßen:

```
COMPRES=wert
```

Dabei steht wert für SYSTEM, REQUESTED (Angefordert) oder PROHIBITED (Verhindert). SYSTEM sollte für alle unterstützten LU-Typen codiert werden.

CMPAPPLO

Dies ist der VTAM-Anwendungsdefinitionsparameter (APPL), mit dem die angeforderte Komprimierungsstufe für abgehende RU-Daten festgelegt wird. Die Syntax lautet folgendermaßen:

```
CMPAPPLO=n
```

Dabei steht "n" für die angeforderte Datenkomprimierungsstufe für abgehende Daten (PLU -> SLU). Für alle vom Communications Server unterstützten LU-Sitzungen kann der Wert für "n" 0, 1 oder 2 für die Datenkomprimierungsstufen 0, 1 und 2 sein. Für die LU-Typen 0, 1, 2 und 3 reserviert der Communications Server jedoch immer Komprimierungsressourcen auf Stufe 2.

CMPAPPLI

Dies ist der VTAM-Anwendungsdefinitionsparameter (APPL), mit dem die angeforderte Komprimierungsstufe für ankommende RU-Daten festgelegt wird. Die Syntax lautet folgendermaßen:

```
CMPAPPLI=m
```

Dabei steht "m" für die angeforderte Datenkomprimierungsstufe für ankommende Daten (SLU -> PLU). Der Wert für "m" hängt von dem für die Sitzung verwendeten LU-Typ ab:

- Für 3270-LU-Sitzungen kann der Wert für "m" 0 oder 1 sein.
- Bei LU 6.2-Sitzungen kann der Wert für "m" 0, 1 oder 2 sein.

Anmerkung: VTAM stellt immer die primäre LU (PLU) dar und der Communications Server die sekundäre LU (SLU) für die LU-Typen 0, 1, 2 und 3.

Es folgen aus den Original-VTAM-Listen extrahierte Codebeispiele zu Verwendung und Position der oben beschriebenen Parameter. Die hervorgehobenen Zeilen sind besonders zu beachten.

```
************************************************************
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)
************************************************************
```

Abbildung 41. VTAM-Startparameter. Bei diesem VTAM ist 4 als maximale Komprimierungsstufe zulässig.

```
*********************************************************************
* LOGMODE FOR COMPRESSION TEST - BASED ON D4C32XX3                   *
*********************************************************************
*                                                                   *
*              3274 MODEL 1C (REMOTE SNA)                    @OY02946*
*              PRIMARY SCREEN 24 X 80 (1920)                        *
*              ALTERNATE SCREEN TO BE DETERMINED BY APPLICATION     *
*                                                                   *
*********************************************************************
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
```

Abbildung 42. VTAM-LOGMODE-Tabelle. Makro MODEENT konfiguriert mit angeforderter Datenkomprimierung

```
      VBUILD TYPE=APPL
*********************************************************************
* VTAM APPL STATEMENTS FOR 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
```

Abbildung 43. VTAM-Anwendungsanweisung. Sie steuert die maximal für diese Sitzung unterstützten Stufen.

```
WTCC1102   PU   ADDR=13,
                IDBLK=05D,
                IDNUM=32289,
           etc.
                DLOGMOD=D4C3COMP
                MODETAB=AMODETAB
           etc.

RACC1102   LU   LOCADDR=2,DLOGMOD=D4C3COMP,MODETAB=AMODETAB
           LU
           etc.
```

Abbildung 44. VTAM-PU- und -LU-Definitionen. Die LU RACC1102 verwendet den LOGMODE D4C3COMP, der in der Modustabelle AMODETAB enthalten ist.

AS/400-Datenkomprimierung planen

Beim Anschluß an ein System IBM AS/400 wird IBM OS/400 Version 2, Release 3 benötigt, damit Datenkomprimierung verwendet werden kann. Es muß lediglich sichergestellt werden, daß eine Modusdefinition vorhanden ist, in der Komprimierungsunterstützung angegeben ist. Drei Parameter sind im Profil „Modusbeschreibung erstellen“ erforderlich, das über den Befehl CRTMODD oder über die Menüs aufgerufen wird. Die drei Parameter sind:

DTACPR Dieser Parameter steuert die Verwendung der Datenkomprimierung. Gültige Parameter:

- **NETATR** Den Systemnetzwert für diesen Parameter verwenden.
- **NONE** Datenkomprimierung ist nicht zulässig.
- **ALLOW** Wenn das ferne System Datenkomprimierung anfordert, läßt das lokale System den Sitzungsaufbau zu.
- **REQUEST** Das lokale System fordert Datenkomprimierung an.
- **REQUIRE** Die Verwendung der Datenkomprimierung ist erforderlich. Kann eines der Systeme keine Datenkomprimierung auf der angeforderten Stufe ausführen, wird die Sitzung nicht aufgebaut.

Wenn Datenkomprimierung zulässig ist und angefordert wird, handeln beide Systeme die bei dieser Sitzung zu verwendende Datenkomprimierungsstufe anhand der Werte für die Parameter **INDTACPR** und **OUTDTACPR** aus.

INDTACPR Dieser Wert steht für die maximale Komprimierungsstufe für ankommende Daten.

OUTDTACPR Dieser Wert steht für die maximale Komprimierungsstufe für abgehende Daten.

Bei LU 6.2-Sitzungen werden die Datenkomprimierungsstufen 0, 1 und 2 für ankommende und für abgehende Daten unterstützt.

Informationen zum Einrichten des Communications Server für Datenkomprimierung können der Dokumentation *Einstieg* entnommen werden.

Überlegungen zur Leistung

Die Übertragungsleistung eines Computers und besonders von Communications Server hängt von einer großen Anzahl von Faktoren ab. Nachfolgende Abschnitte enthalten einige Informationen über Faktoren, die sich auf die Übertragungsleistung in einer Communications Server-Umgebung auswirken.

Die Übertragungsleistung hängt von der Geschwindigkeit der DFV-Leitung ab. Diese Geschwindigkeit wird normalerweise durch die Anzahl von Bit angegeben, die pro Sekunde über die Leitung übertragen werden können (Bit/s). Je höher der Wert für Bit/s, desto höher ist die Leistung, die über eine Leitung erreicht werden kann.

Außer der Bitübertragungsrate wirken sich noch andere die Leitung betreffende Faktoren auf die Übertragungsleistung aus. Über einige Leitungen können Daten beispielsweise nicht gleichzeitig in zwei Richtungen übertragen werden. Um die Übertragungsrichtung zu ändern (wer sendeberechtigt ist), gibt die Station eine ***Anforderung zum Senden*** (RTS - Request to Send) aus und wartet darauf, daß ein ***Sendebereitschaftssignal*** (CTS - Clear to Send) ausgegeben wird. Diese ***Leitungsumschaltung*** (die modemabhängig ist) nimmt zusätzliche Zeit in Anspruch. Ein weiterer Faktor ist die Übertragungsqualität der DFV-Leitung. Von den meisten Protokollen wird ein Leitungsfehler festgestellt, und die Daten werden erneut gesendet. Treten weniger Übertragungsfehler auf, erhöht sich der Durchsatz.

Ein größerer Durchsatz wird auch erreicht, wenn die Protokolle den ***Duplex***modus für die Datenübertragung verwenden, bei dem das Protokoll gleichzeitig empfangen und übertragen kann. LAN und X.25 sind Duplexprotokolle. SDLC kann im Duplex- oder Halbduplexmodus ausgeführt werden.

Um Duplex für SDLC zu verwenden, ist ein geeigneter Adapter erforderlich (der MPA-Adapter kann Duplex nicht unterstützen). Die ferne Datenstation kann ebenfalls Duplex unterstützen.

Durch die Erhöhung der Übertragungsgeschwindigkeit wird die Übertragungsleistung nicht mehr so sehr durch die Bitübertragungsrate beeinträchtigt. Statt dessen wirken sich Verzögerungen innerhalb der Einheiten, die die DFV-Leitungen verwenden (Modems, Steuereinheiten oder der Computer), negativ auf die Leistung aus. Bei sehr hohen Übertragungsgeschwindigkeiten beeinträchtigen diese Verzögerungen die Übertragungsleistung mehr als die Bitübertragungsrate der Leitung.

Die Analyse dieser Situationen ist schwierig. Verzögerungen bei der Übertragung, die länger dauern als erwartet, können z. B. eine der folgenden Ursachen haben:

- Überlastung der DFV-Leitung
- Überlastung des Host-Systems
- Überlastung der Steuereinheit IBM 3X74
- Überlastung der Netzsteuereinheit 37*xx*
- Keine optimale VTAM- oder NCP-Definition
- Netzentwurf und Netzverwaltung sind inadäquat
- Überbelegung und Auslagerung des Betriebssystemspeichers

In einer Übertragungsumgebung für hohe Geschwindigkeiten wie in einem LAN ist die Bitübertragungsrate von geringerer Bedeutung, da die Übertragungsleistung hauptsächlich von der Geschwindigkeit der DFV-Einheiten bestimmt wird. Häufig kann eine höhere Übertragungsleistung erreicht werden, indem die Verarbeitungsleistung der Datenstation, des Hosts oder anderer Netzkomponenten erhöht wird. Dies bedeutet nicht, daß die Bitübertragungsrate eines LAN nie zu einer Beeinträchtigung der Übertragungsleistung führt; erst wenn mehrere Computer gleichzeitig die Datenübertragungsfunktion stark beanspruchen, kann dies dazu führen, daß die Leistung des LAN in größerem Maße reduziert wird.

Zusammenfassend läßt sich sagen, daß die Leistung des Communications Server in vielen Fällen durch Faktoren bestimmt wird, die mit dem verwendeten DFV-Netz zusammenhängen. Damit Übertragungsleistung zu angemessenen Kosten zur Verfügung gestellt werden kann, sind gute Kenntnisse des Netzes und die Analyse der einzelnen Komponenten erforderlich.

Anhang B. Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden. Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, daß nur Programme, Produkte oder Dienstleistungen von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Dienstleistungen können auch andere ihnen äquivalente Produkte, Programme oder Dienstleistungen verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte der IBM verletzen. Die Verantwortung für den Betrieb von Fremdprodukten, Fremdprogrammen und Fremdservices liegt beim Benutzer.

Für in dieser Veröffentlichung beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanfragen sind schriftlich an folgende Adresse zu richten:

IBM Europe
Director of Licensing
92066 Paris La Defense Cedex
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Die Änderungen werden in Überarbeitungen oder in Technical News Letters (TNLs) bekanntgegeben. IBM kann jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängigen, erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Deutschland
Informationssysteme GmbH
Abteilung 4985, SW Service
Laatzener Str. 1
30532 Hannover

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des im Handbuch aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt im Rahmen der IBM Kundenvereinbarung oder einer äquivalenten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer gesteuerten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Garantie, daß diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen.

Informationen über Produkte anderer Hersteller als IBM wurden von den Herstellern dieser Produkte zur Verfügung gestellt, bzw. aus von ihnen veröffentlichten Ankündigungen oder anderen öffentlich zugänglichen Quellen entnommen. IBM hat diese Produkte nicht getestet und übernimmt im Hinblick auf Produkte anderer Hersteller keine Verantwortung für einwandfreie Funktion, Kompatibilität und andere Ansprüche. Fragen hinsichtlich des Leistungsspektrums von Produkten anderer Hersteller als IBM sind an den jeweiligen Hersteller des Produkts zu richten.

Marken

Folgende Namen sind in gewissen Ländern Marken der IBM Corporation:

Advanced Peer-to-Peer Networking
AIX
AnyNet
APPN
AS/400
AT
BookManager
CICS
DB2/2
eNetwork
Enterprise System/9000
ESCON
ES/9000
FFST/2
First Failure Support Technology/2
Global Network
IBM
IBMLink
IMS
MICRO CHANNEL
NetView
OS/2
OS/400
Personal System/2
Portmaster
Presentation Manager
PS/2
System/370
System/390
SystemView
S/370
S/390
TalkLink
VTAM
WebExplorer

Andere Namen von Unternehmen, Produkten oder Dienstleistungen können Marken anderer Unternehmen sein.

C-bus ist eine Marke von Corollary, Inc.

Java und HotJava sind Marken von Sun Microsystems, Inc.

Microsoft, Windows und Windows 95 Logo sind Marken der Microsoft Corporation.

PC Direct ist eine Marke der Ziff Communications Company und wird von der IBM Corporation unter Lizenz verwendet.

ActionMedia, LANDesk, MMX, Pentium und ProShare sind in gewissen Ländern Marken der Intel Corporation.

Eine vollständige Auflistung aller Marken von Intel befindet sich unter folgender Adresse: www.intel.com/tradmarx.htm.

UNIX ist eine eingetragene Marke und wird ausschließlich von der X/Open Company Limited lizenziert.

Index

Numerische Stichwörter

A

B

C

D

E

F

G

H

I

K

L

M

N

P

R

S

T

U

V

W

X

Z

Antwort

eNetwork Communications Server
Version 6.0 für Windows NT
Handbuch für die Netzverwaltung

IBM Form SC12-2577-00

Anregungen zur Verbesserung und Ergänzung dieser Veröffentlichung nehmen wir gerne entgegen.
Bitte informieren Sie uns über Fehler, ungenaue Darstellungen oder andere Mängel.

Senden Sie Ihre Anregungen bitte an die angegebene Adresse.

IBM Deutschland
Informationssysteme GmbH
SW NLS

70548 Stuttgart

Kommentare:

Zu Ihrer weiteren Information:

Zur Klärung technischer Fragen sowie zu Liefermöglichkeiten und Preisen wenden Sie sich bitte entweder an Ihre *IBM Geschäftsstelle*, Ihren *IBM Geschäftspartner* oder Ihren *Händler*. Unsere Telefonauskunft **„Hallo IBM“** (Telefonnr.: 0180 3/31 32 33) steht Ihnen ebenfalls zur Klärung allgemeiner Fragen zur Verfügung.

Printed in the European Union

SC12-2577-00