eNetwork Communications Server
Version 6.0 for
Windows NT

Quick Beginnings

Version 6.0

GC31-8424-02

eNetwork Communications Server
Version 6.0 for
Windows NT

Quick Beginnings

Version 6.0

GC31-8424-02

Note

Before using this information and the product it supports, be sure to read the information under “Appendix D. Notices” on page 133.

Third Edition (July 1998)

This edition applies to Version 6.0 of Communications Server for Windows NT** and to all subsequent releases and modifications until otherwise indicated in new editions or technical newsletters.

Contents

Welcome to Communications Server

This book describes the Communications Server for Windows NT and explains how to plan for, install, and use it. Hereafter, any reference to Communications Server will refer to the Windows NT version of the product unless otherwise specified.

Road Map

Use the following table to find the information you need to get started with Communications Server.

Table 1. Road Map for Getting Started

If you want to...	**Refer to...**
Read about Communications Server.	"Chapter 1. About IBM Communications Server for Windows NT" on page 1
Install the Communications Server.	"Chapter 3. Installing Communications Server" on page 41
Configure the Communications Server.	"Chapter 4. Configuring Communications Server" on page 49
Start using Communications Server.	"Chapter 5. Using Communications Server" on page 79
Display diagnostic information.	"Chapter 6. Problem Determination and Reporting" on page 93
View or print online documentation.	"Chapter 7. Obtaining Additional Information" on page 101
Contact IBM.	"Contacting IBM" on page 99

Conventions

Knowing the conventions used in this book will help you use it more efficiently.

- **Boldface type** indicates:
  - Verbs, functions, and parameters that you can use in a program or at a command prompt. These values are case sensitive and should be entered exactly as they appear in the text.

  - The names of window controls, such as lists, check boxes, entry fields, push buttons, and menu choices.
- *Italics type* indicates:
  - A variable for which you supply a value
  - Book titles
  - A letter that is being used as a letter or a word that is being used as a word. For example, when you see an *a*, make sure it is not supposed to be an *an*.
- ***Bold italics type*** is used to emphasize a word.
- UPPERCASE indicates constants, file names, keywords, and options that you can use in a program or at a command prompt. You can enter these values in uppercase or lowercase.
- `Example type` indicates information that you are instructed to type at a command prompt or in a window.
- Double quotation marks indicate messages you see in a window. An example of this would be the messages that appear in the operator information area (OIA) of an emulator session.
- Binary numbers are represented as B'xxxx xxxx' or B'x' except in certain instances where they are represented with text (“A value of binary xxxx xxxx is...”).
- Bit positions start with 0 at the right position (least significant bit).
- Decimal numbers over 4 digits are represented in metric style. A space is used rather than a comma to separate groups of 3 digits. For example, the number sixteen thousand, one hundred forty-seven is written 16 147.
- Hexadecimal numbers are represented in text as hex xxxx or X'xxxx' (“The address of the adjacent node is hex 5D, which is specified as X'5D'.”)

This book also uses *icons* (pictures) in the text to help you find different types of information.

This icon represents a note, important information that can affect the operation of Communications Server or the completion of a task.

This icon represents a hint or additional information that can help you complete a task.

Chapter 1. About IBM Communications Server for Windows NT

Today's personal computers offer new ways of networking directly from your desktop. For example, you can communicate and share resources with someone in the next room, the next city, or on another continent. At the same time, an application running on your workstation can be accessing data from a host computer while distributing data to another workstation on a local area network (LAN). You can even have a conference from your personal computer with live video and interactive data exchanges across a network. Distributed processing and client/server applications can also share the personal computer with terminal emulator programs that connect you to applications running on a host computer. These are only a few of the applications of personal networking from your desktop workstation.

IBM's Communications Server for Windows NT provides an industrial-strength networking solution for your workstation. Whether it's for host terminal emulation, client/server and distributed applications, or connectivity across local and wide area networks (LANs and WANs), Communications Server offers a robust set of communications, networking, and system management features.

For true networking flexibility, a wide range of connectivity services and options are provided. With Communications Server, workstations and gateways can communicate using communication protocols such as TCP/IP and SNA. Communication occurs over a variety of data link controls (DLCs). Mobile users can directly access their host system or another Communications Server through public telephone networks.

The versatility of Communications Server extends to the types of applications that can be supported. Communications Server supports a wide variety of application programming interfaces (APIs) and protocols that are ideal for client/server applications and distributed processing. Communications Server also protects your investment in applications by providing compatible APIs for clients and servers. Programs using these APIs can run on any node in the network, whether it is a client or server.

The Common Programming Interface for Communications (CPI-C) and advanced program-to-program communication (APPC) support makes Communications Server the ideal communications platform for peer application environments. The Logical Unit APIs (LUA) for applications that need access to LU 0, 1, 2, and 3 data streams are available for access to many host applications. Refer to the Communications Server Software Development Kit (SDK) for header files, samples, and documentation regarding the APIs.

Advanced Peer-to-Peer Networking (APPN) adds additional power to the basic SNA functions supported by Communications Server. APPN is a protocol that can greatly enhance the management of an SNA network. This is accomplished through reduced configuration requirements, dynamic directory searches, route calculation capabilities, and intermediate session routing.

Communications Server contains a powerful SNA gateway facility. The gateway allows workstations on a local area network to connect to host computers through one set of adapters and physical connections. The Communications Server gateway supports various OS/2, DOS, and Windows workstations. Remote workstations can also dial in to this gateway and then use a common high-speed link to the host. The gateway performs the function of an LU concentrator making LU resources from any number of host and host PUs available to any number of downstream client workstations over any combination of communications media supported by Communications Server. The link to the upstream host can be either traditional SNA subarea or an APPN DLUR link.

Communications Server also delivers solutions to address multiprotocol challenges with its AnyNet, SNA API clients, TN5250 server, and TN3270E server offerings.

AnyNet software enables application programs to communicate over different transport networks and across interconnected networks. Using AnyNet, you can reduce the number of transport networks and therefore reduce operational complexity. These benefits are gained without modification to your existing application programs or hardware.

Communications Server delivers AnyNet SNA over TCP/IP access node and gateway and AnyNet Sockets over SNA access node and gateway. Thus, you can combine SNA and TCP/IP networks without losing application support.

Another way to combine SNA and TCP/IP is by using the SNA API clients that are shipped with Communications Server. Communications Server establishes and manages a session as if the origin were the local node, and then forwards the necessary application data over TCP/IP to the SNA API clients. SNA API clients are supported on OS/2, Windows 3.1, Windows 95, and Windows NT.

The TN3270E server enables TN3270- and TN3270E-compliant clients to gain access to host applications. By configuring a TN3270E server, you can exchange data between TCP/IP workstations running TN3270E applications and a Systems Network Architecture (SNA) mainframe host computer. The

TN3270E server function supports the same upstream DLCs, PU and LU support, and pooling as the SNA gateway.

The TN5250 server enables TN5250 clients on a TCP/IP network to gain access to applications on an SNA-connected AS/400.

Communications Server includes several tools to simplify the administration of SNA networks. These include system and network alerts, message and error logs, trace files, and programming capabilities that allow you to configure and manage networks and build sophisticated management programs. Complementary network and system management products can access all of these facilities.

With Communications Server, IBM also provides an entry-level terminal emulation product from the popular Personal Communications family of products. This product includes both 3270 and 5250 emulation.

You can get up-to-the-minute information about the IBM eNetwork family of products from the Communications Server home page: `http://www.software.ibm.com/enetwork/commserver`. This page includes information and links to headline information, specification sheets, frequently asked questions and answers, maintenance and support information, and more.

What's New for This Release?

The following new functions and enhancements were added for this beta Version 6.0:

- Installation, configuration, and administration enhancements
  - Installation options

    You can now select the Communications Server components that you want to install. This enables you to customize your installation. See "Chapter 3. Installing Communications Server" on page 41.
  - Improved administration and configuration interface

    Communications Server now provides a tree-view diagram of your configuration that enables you to select and modify resources in a hierarchical graphic interface.

    See "Chapter 4. Configuring Communications Server" on page 49 for information about configuring or "Chapter 5. Using Communications Server" on page 79 for information about using Communications Server. For additional information about configuring Communications Server, refer to the online *Tutorial*. For additional information about network administration, refer to the online *Network Administration Guide*.

  - Configuration wizard support

    Communications Server now includes wizards that appear when you use Node Configuration to create a new TN3270E server, TN5250 server, or SNA gateway configuration. These wizards, which guide you through the configuration process, can be disabled using the Options pull-down menu.
  - Directory exploitation

    You can configure multiple clients from a central location using the Lightweight Directory Access Protocol (LDAP) to simplify the configuration process.

    For conceptual information about using directory exploitation, see “Appendix A. Directory Exploitation” on page 105.
  - Tivoli Management Environment (TME) Plus Module

    The provided TME Plus module integrates management of Communications Server into TME. You can use TME to distribute, install, and uninstall Communications Server. You can also use it to check the server’s status, start or stop the server, and display and modify server resources. This module is available in English only, because TME only supports English at this time.

    Refer to the online *Network Administration Guide* for information about using the TME Plus module.
  - Web administration

    You can manage your communications server over an intranet, using a Web browser. The enhanced Web administration interface enables a systems administrator to query node status, obtain information about and modify resources, and display configuration files and message logs. Web administration use is restricted through user authentication based on Windows NT security. Users must be members of the IBMCSADMIN group.

    Refer to the online *Network Administration Guide* for information about administering your network over the Web.
- Host Publisher

  Host Publisher provides access across the Web for high-volume Web sites with dynamic content. You can use Host Publisher to access data on S/390 or AS/400 hosts or on DB2 databases and to publish it on Web pages created dynamically from your design.

  See “Host Publisher” on page 18 for conceptual information. For more detailed information about configuring and using Host Publisher, see the online *Host Publisher User’s Guide*.
- SNA enhancements
  - Branch extender support

Without the branch extender, problems occur if an APPN-topology subnetwork exceeds the smallest network node’s topology database (TDB) storage. This could limit network size to as few as 150 network nodes. (TDB size is a function of the number of network nodes and links, as well as the frequency of state changes.) Many administrators would prefer to install 1500 or more small network nodes as gateways to branch offices, with a LAN at each branch office that is configured as a connection network.

The branch extender enables you to interconnect a branch office with LANs, end nodes and low entry networking nodes with dependent and independent LUs, and PUs such as teller machines, to one or several WANs.

For information about branch extender, refer to the online *Network Administration Guide*.

- SNA Session-Level Encryption

  Communications Server now supports SNA session-level encryption (SLE). SLE enables you to encrypt either all of the data or selected data that is transferred between the workstation and the host. If you want to protect any workstation data by using encryption, the host must also be configured to use encryption.

  Refer to the online *Network Administration Guide* for more information about SLE.

- Data compression

  You can now choose LZ10 (Lempel-Ziv 10) compression for SNA data, as well as LZ9 and Run Length Encoding (RLE).

- Link reactivation

  Communications Server now supports automatic link reactivation.

- Telnet enhancements
  - TN5250 server

    TN5250 server provides connectivity from TN5250 clients on IP networks to AS/400s on SNA networks. The server implements the protocols outlined in RFC1205, enabling the server to exchange 5250 workstation data with the client. Typically, these clients emulate a 5250 display.

    See “TN5250 Server” on page 17 for conceptual information about TN5250 server. For additional information, refer to the online *Network Administration Guide*.

  - Filtering using hostnames

    You can specify which clients can connect to either the TN3270E or TN5250 server, and which resources they can have access to, based on either the client’s IP address or hostname.

  - Load balancing

  Communications Server supports load balancing across TN3270E and TN5250 servers.
  - Secure Sockets Layer–based (SSL-based) security

    You can specify that security is used on connections between Telnet clients and the TN3270E or TN5250 server. This security uses SSL Version 3 to provide data encryption and server authentication using signed certificates.

- SNA API Client Enhancements

  The 32–bit Windows and OS/2 clients have the following enhancements:
  - More detailed trace formatting that can help you debug problems faster
  - Ability to start and stop tracing while the client is running
  - Ability to reinstall the client without uninstalling
  - Support for data encryption between the client and server for LUA and LU 6.2 connections

  The Windows NT and Windows 95 clients now run from the same executable. This executable can be installed on a shared drive; any fixes apply to both clients. The new 32–bit Windows client can communicate with either IBM Communications Servers or Novell IntranetWare or NetWare for SAA servers.

  The 32–bit Windows client now uses the client's existing Windows NT domain logon as the default user ID and password, rather than prompting the user for a second ID and password. You can choose to specify a separate ID and password if you prefer.

  See "SNA API Client Support" on page 22 for conceptual information about the SNA API clients. For detailed information about application development using SNA API client interfaces, refer to the online *Client/Server Communications Programming Reference*.

- Shared folder support

  You can create disk devices on the server that communicate with AS/400. Clients can connect to and use these devices to get access to AS/400 drives without additional configuration or code installation on the client machine.

  For information about shared folders, refer to the online *Network Administration Guide*.

- Load balancing

  Communications Server now supports load balancing for all client types. Load balancing enables you to distribute LU 0 to 3 and LU 6.2 sessions across Communications Server and NetWare for SAA servers. The server advertises services including load factors, which the clients or servers can gather and organize to select a server.

For information about using load balancing in your networks, refer to the online *Network Administration Guide*.

- Hot standby

  Hot standby enables you to ensure that configured connections to a host can continue to function by triggering activation of alternative connections on a backup server when a critical server goes down.

  For information about defining critical and backup servers to enable hot standby, refer to the online *Network Administration Guide*.

- Connectivity enhancements
  - Adapter support

    Communications Server supports shallow (nonprogrammable) adapters for MicroChannel and ISA-bus machines using an open data link control. Communications Server also supports deep (programmable) adapters. Deep adapters can use SDLC, X.25, or other general data link controls through published interfaces. These interfaces enable adapter manufacturers to supply device drivers for their adapters so that Communications Server can support them.

  - Enterprise Extender data link control (DLC)

    Communications Server now provides HPR connections on IP networks, using UDP/IP packets. To the HPR network, the IP backbone appears to be a logical link. To the IP network, the SNA traffic appears to be UDP datagrams. These datagrams are routed without changes to the IP backbone. Because there is no protocol transformation and because packaging takes place at the routing layer without the overhead of additional transport layers, this results in efficient use of the intranet infrastructure for IP clients that access SNA-based data (TN3270 clients or Web browsers using IBM Host on Demand, for example), as well as for SNA clients.

    You can choose this type of connection when you configure devices by selecting IBM-EEDLC from the list. The online *Tutorial* contains additional information about configuring Enterprise Extender.

  - IBM Multi-Path Channel DLC

    The Multi-Path Channel (MPC) DLC provides high-capacity, high-availability fiber connections to one or more S/390 MPC-capable hosts over the ESCON channel adapter card (P/N 9663–001). MPC connections provide high data transmission rates with transparent backup when physical connections break or become temporarily unavailable. This channel-to-channel connection enables you to provide LAN clients ready access to S/390 resources and services.

    You can choose this type of connection when you configure devices by selecting IBM-MPC from the list. The online *Tutorial* contains additional information about configuring MPC.

- API support

Communications Server now supports host access class libraries (ECL) for Java applets and applications. SLI is now supported on the client as well as the server. Refer to the online *Client/Server Communications Programming Reference* for information about APIs.

- Novell NetWare for SAA client (QEL / MU client) support

  Communications Server now includes support for IPX- or TCP / IP-attached clients running emulator software packages that implement Novell's Queue Element / Message Unit (QEL / MU) architecture for 3270 emulation. This includes support for popular client features, including dedicated, pooled, and public LU categories (sometimes referred to as resource types).

  See "Novell NetWare for SAA Client Support" on page 23 for conceptual information about these clients.

- APPN MIB support

  Communications Server now supports simple network management protocol (SNMP) requests for APPN management information from any SNMP management system.

- NetView RUNCMD support

  Communications Server now supports RUNCMD (ROPS) requests. Refer to the online *Network Administration Guide* for information about issuing RUNCMD from TME 10 NetView.

- Host integration

  Communications Server provides client software that enables clients to connect to CICS or MQ hosts through Communications Server.

  Communications Server also includes software and one license for DB2 Connect Personal Edition, a single-user direct connectivity product to the host. You can install this on a client machine running Windows 3.1, Windows 95, Windows NT, or OS / 2.

  For instructions on installing and configuring this product to work with Communications Server, see the Communications Server Hints and Tips Web page: `http://www.software.ibm.com/commserver/tips/csncfgdb2.htm`. Information about ordering additional licenses is included on the DB2 Connect Personal Edition CD-ROM.

- AS / 400 OLE DB Provider support for ActiveX and OLE DB programs

  Applications that use OLE DB or ActiveX can communicate through Communications Server for record-level access to files on an AS / 400. Documentation for this function, as well as information about developing these applications using Client Access, is provided in the csnt \ sdk \ as400_oledb directory.

- Documentation enhancements
  - Product documentation

    Two new books were added to the Communications Server library. These books are provided on the CD-ROM in HTML and PDF formats.

    - *Configuration File Reference*

      This reference provides information about using an ASCII editor to update configuration files.
    - *Network Administration Guide*

      This addition to the Communications Server library contains information designed to help you plan for, configure, and tune your network.
  - Reference documentation

    The following publications are now included on the Communications Server CD-ROM in PDF format:
    - *CPI Communications Reference* (also provided in HTML)
    - *SNA Formats*
    - *SNA Management Services Formats*

Features and Functions of Communications Server for Windows NT

The Communications Server package contains the following product features and functions:

- APPN network node and end node support
- High-Performance Routing (HPR)
  - Rapid Transport Protocol (RTP)
  - Automatic Network Routing (ANR)
  - Enterprise Extender (HPR over IP)
- SNA data compression
- Discovery of service providers
- Dependent LU Requester (DLUR)
- SNA gateway
- TN3270E Server
- TN5250 Server
- Host Publisher
- AS/400 OLE DB Provider
- SNA API client services
- Novell NetWare for SAA client services
- AnyNet SNA over TCP/IP (access node and gateway)
- AnyNet Sockets over SNA (access node and gateway)
- Local and remote configuration and administration support
- Shared folder support
- Load balancing

- 32-bit application programming interfaces (APIs)
  - CPI-C
  - APPC
  - LUA RUI
  - LUA SLI
  - Management Services API
  - Common Services API
  - Node Operations API
- Data security
- LAN support
- Local and wide area connectivity support
- MPC Channel support
- OEM communication adapter support
- Entry-level emulator functions

A machine where Communications Server for Windows NT is installed is often termed a **node**. A Communications Server node can be configured to enable any or all of the features listed above.

Description of the Communications Server for Windows NT Features and Functions

This section gives more information about each of the Communications Server features and functions.

Advanced Peer-to-Peer Networking (APPN) Network and End Node Support

Advanced Peer-to-Peer Networking (APPN) is a networking extension to APPC which simplifies configuration and enhances management of a group of workstations using APPC or CPI-C transaction programs. An APPN network is made up of network nodes and end nodes. The APPN network nodes provide directory services, route selection, and management services to end nodes. The end nodes need only know the location of the network node to communicate with any node in the APPN network. SNA discovery support further simplifies configuration by automatically finding network nodes for the end nodes.

With APPN, you can:

- Add, delete, or move nodes within the network with limited system definition at the affected node, and no other definition at other nodes

- Use defaults for reducing required system definition
- Significantly improve the performance of communications between APPC and CPI-C applications, especially in a LAN environment
- Use the NOF API to automate configuration changes and add network management capabilities

High-Performance Routing

Communications Server supports high-performance routing (HPR), which increases data routing performance and reliability of APPN networking. HPR provides nondisruptive rerouting around network outages, efficient selective retransmission, and end-to-end data integrity and congestion control. Communications Server supports both:

Rapid Transport Protocol (RTP)
This allows a node to be the initiation or termination point of an HPR conversation.

Automatic Network Routing (ANR)
This allows a node to act as an intermediary along the path of an HPR conversation.

Communications Server supports HPR routing over IP, LAN, synchronous data link control (SDLC), and X.25 connections.

HPR routing requires VTAM V4R3 or later for host (mainframe) connections. However, you can use HPR in non-host-oriented networks.

SNA Data Compression

Data compression at the session level increases throughput for large amounts of data across communication links, resulting in the following benefits:

- Enhanced data throughput on low-speed lines
- Reduced costs on high-cost lines
- Faster response times, resulting in productivity improvements

SNA data compression is compatible with the S/390 and AS/400 implementations and can be used with all LU types.

Discovery of Service Providers

Discovery is a LAN address resolution protocol that can be used by a node on the LAN to find another node that matches given search criteria. By adjusting the search parameter, a node can search for APPN network nodes, nodes that provide SNA boundary function, AS/400s, SNA gateways, or user-defined classes of server. A Communications Server for Windows NT server can respond to requests from clients as a network node server, a PU 2.0 gateway, or as a user-defined class of server. A Communications Server can also use discovery to find APPN nodes and SNA gateways.

Dependent LU Requester (DLUR)

Communications Server enables the support in VTAM V4R2 or later for dependent LUs through APPN networks and combined subarea and APPN networks. The dependent LU server function (in VTAM) provides dependent secondary logical unit (SLU) support by establishing an LU 6.2 session between a dependent LU requester node (DLUR), and a dependent LU server node (DLUS).

A DLUR is an APPN end node or network node that uses dependent LUs, but requests that a DLUS provide the system services control point (SSCP) for those dependent LUs through an APPN network. A DLUS controls conversion from a subarea environment to an APPN environment, allowing you to maintain central management of remote dependent LUs while benefiting from an APPN network.

DLUR allows dependent LUs (LU 0, 1, 2, 3, and dependent LU 6.2) to benefit from an APPN network. It supports dynamic and multiple paths through the network and eliminates the need for dependent LUs (or their gateway) to be adjacent to the VTAM host.

SNA Gateway Support

Communications Server provides a full-function Systems Network Architecture (SNA) gateway. The gateway allows multiple LAN-attached workstations to access System/370 or System/390 hosts through one or more physical connections to one or more hosts. This helps reduce the cost per workstation of host connections.

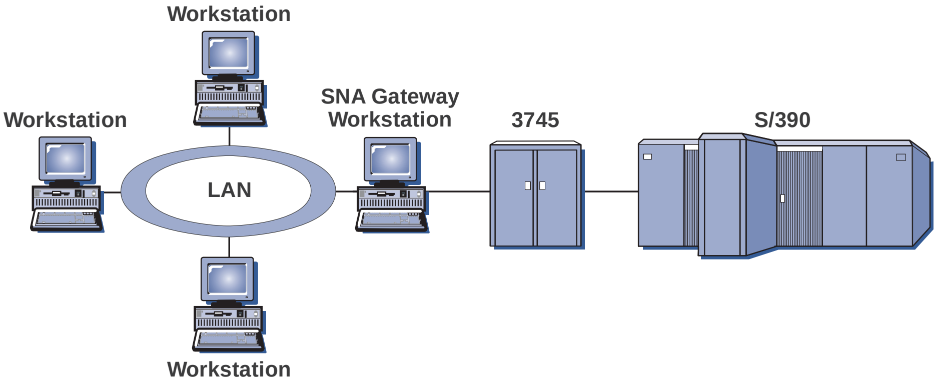

Figure 1. Example of SNA Gateway Configuration

The Communications Server gateway supports the SNA protocols LU 0, 1, 2, 3, and dependent LU 6.2 (APPC). With the AnyNet SNA over TCP/IP function, downstream workstations can now communicate with the SNA gateway over an IP network. The gateway also supports LU 0, 1, 2, or 3 to an AS/400 host using SNA pass-through. The AS/400 host passes the data through to a System/390 host.

A gateway can also act as a protocol converter between workstations attached to a LAN and a WAN host line.

The LUs defined in the gateway can be dedicated to a particular workstation or pooled among multiple workstations. Pooling allows workstations to share common LUs, which increases the efficiency of the LUs and reduces the configuration and startup requirements at the host. You can also define multiple LU pools, each pool associated with a specific application. And you can define common pools that are associated with multiple hosts. When a client connects to the gateway, the gateway retrieves an LU from the pool to establish a session. The LU is returned to the pool for access by other workstations when the session is ended.

In addition, an SNA gateway can support the forwarding of network management vector transports (NMVTs) between the workstations and the host.

Each host views the SNA gateway as an SNA PU 2 node, supporting one or more LUs per workstation. As far as the host is concerned, all LUs belong to the SNA gateway PU. The SNA gateway can have multiple host connections simultaneously and can direct different workstation sessions to specific hosts.

To the supported workstations, the SNA gateway looks like an SNA PU 4 communications controller and forwards such host requests as BIND and UNBIND. The workstation LUs are not aware of the SNA gateway. The SNA gateway, however, is aware of all LUs at the workstations.

Downstream applications using standard SNA connectivity protocols for LU 0, 1, 2, and 3 and dependent 6.2, and communicating through an SNA gateway to a host, are supported by Communications Server. Table 2 summarizes the SNA gateway features.

Table 2. SNA Gateway Summary

Feature	Description
Active workstations	254 (LAN) per adapter 128 (X.25)
DLCs	AnyNet (SNA over TCP/IP) Twinaxial (upstream only) LAN (Any NDIS** compliant network adapter) X.25 SDLC (synchronous, asynchronous, and AutoSync) OEM Channel (upstream only) MPC Channel (upstream only, requires DLUR) Enterprise Extender
Downstream workstations	Any product that supports standard SNA connectivity protocols for LU 0, 1, 2, 3, and 6.2.
Dynamic additions and changes	Yes
Implicit workstation support	Yes
LU pooling	Yes
Maximum number of LUs	254 per PU; no limit on the number of PUs
Mode of operation	Multiple downstream PUs (not apparent to the host) PUs not visible to the host (except when through DLUR)
Multiple PU support	Yes
Segmenting support	Yes
Supported LU types	LU 0, 1, 2, 3, and dependent 6.2

TN3270E Server

The TN3270E server function enables you to configure your network as shown in Figure 2 on page 15.

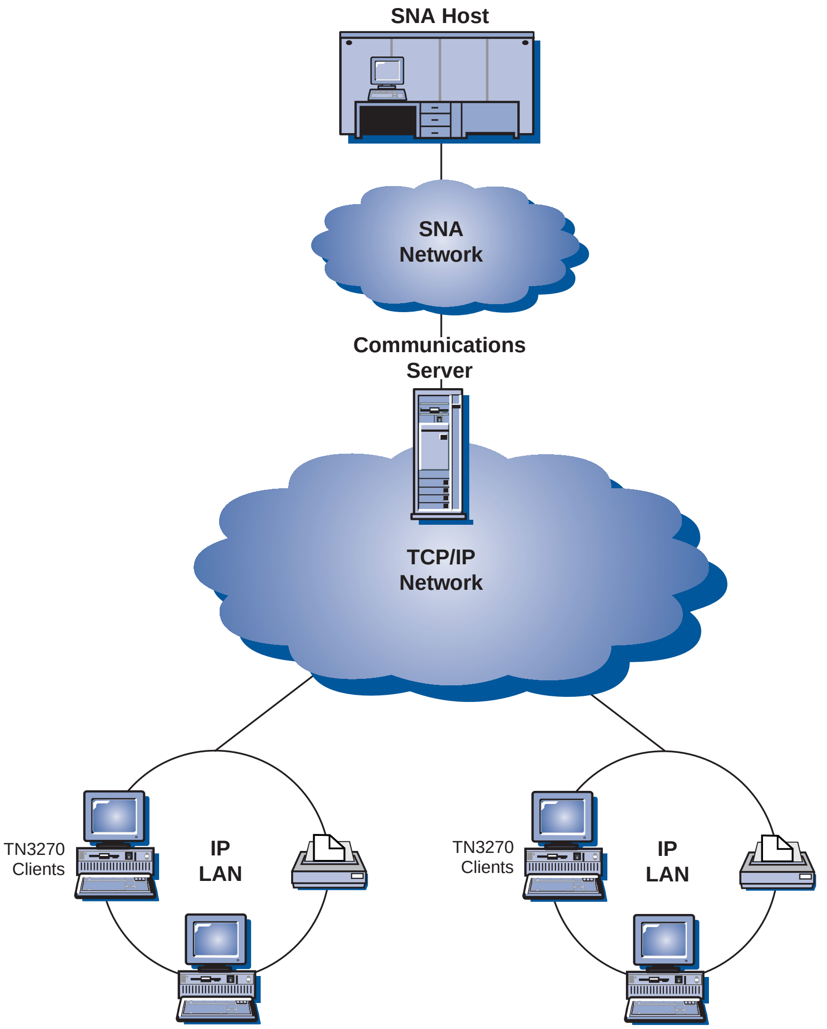

Figure 2. TN3270E Server with Wide Area TCP/IP Network

The TN3270E server function supports:

- Terminal emulation

  TN3270E server supports LU 2, which enables users to run interactive 3270 display application programs.
- Host print

  The Telnet 3270 standard extensions (TN3270E) enable users to print from host applications to printers attached to their workstation. These printers can be locally or network attached. Print sessions can be LU 1 or LU 3.

TN3270E server implements the protocols outlined in RFC 1576, RFC 1646, and RFC 1647, enabling the server to pass LU 1 and LU 3 session data to TN3270E-enabled clients, wait for client confirmation of the print request, and respond to the host.

- Load balancing

  You can load balance TN3270E connections. Refer to the online *Network Administration Guide* for more information about load balancing.

- Client filtering

  TN3270E server enables the user to specify at the server the clients, based on IP address or hostname, that can access the LU names and pools that have been configured for the TN3270E server. This allows controlled access to LUs without modifying the client configurations.

- Support for security

  You can configure a separate port to support Secure Sockets Layer-based (SSL-based) security. If you specify security, the server must have an authenticated certificate provided by a certificate authority such as Verisign. Communications Server provides a utility that generates and manages keys and certificates used by SSL Version 3.

- Response handling

  TN3270E-enabled clients can send both positive and negative responses, which TN3270E Server sends on to the host. TN3270E server generates responses for standard TN3270 clients.

- ATTN and SYSREQ key handling

  TN3270E server can convert and forward information to the host when the client sends an ATTN or SYSREQ key. Although clients that are not TN3270E-enabled have no explicit definition for ATTN and SYSREQ, the TN3270E server uses the following Telnet commands to implement these functions:

Table 3. Command Equivalents

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

- LU classes

  Communications Server categorizes user connections with LU classes. Classes consist of LUs configured with common characteristics; those that require a specific host connection, for example. This simplifies user access, groups users by application needs, and maximizes host resources.

TN3270E server supports both standard and extended Telnet 3270. Typical client programs emulate a 3270 display. Clients that support the TN3270E protocol can emulate LU 1 and LU 3 printers.

TN5250 Server

The TN5250 server function enables TN5250 clients on TCP/IP networks to communicate with AS/400s on SNA networks. It enables you to configure your network as shown in Figure 3.

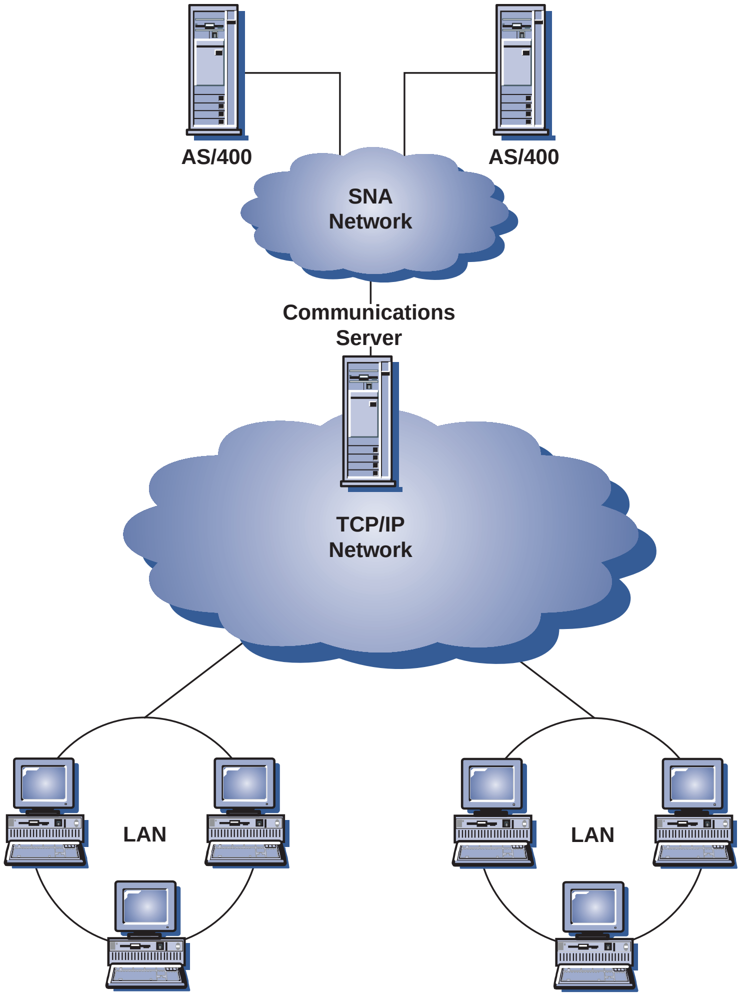

Figure 3. TN5250 Server with Wide Area TCP/IP Network

The TN5250 Server function implements the protocols outlined in RFC 1205. It supports:

- Terminal emulation

  The server provides a gateway between downstream IP-connected RFC 1205–compliant clients (TN5250 clients) and one or more upstream SNA-connected AS/400s. SNA connectivity between the server and the AS/400s is provided using the 5250 Display Station Pass-through datastream on LU 6.2 sessions.
- Client filtering

  TN5250 server enables the user to specify at the server the clients, based on IP address or hostname, that can access the AS/400 servers that have been configured for the TN5250 server. This allows controlled access to AS/400s without modifying the client configurations.
- Support for dynamic local LUs

  This support enables you to exceed the 512 maximum session limit between a single LU and the AS/400 by using additional dynamically defined local LUs.
- Support for multiple AS/400s

  You can enable the server to connect to multiple AS/400s by configuring the server to listen on more than one IP port and specifying the AS/400 that corresponds to each port. The client specifies a port to be used for the connection, using a common configuration parameter. The server then uses the port value to identify the specific AS/400. Clients can connect to multiple hosts by specifying different ports for each emulator session.
- Support for security

  You can configure specific ports to support Secure Sockets Layer-based (SSL-based) encryption. If you specify security, the server must have an authenticated certificate provided by a certificate authority such as Verisign. Communications Server provides a utility that generates certificate requests and manages existing keys and certificates used by SSL Version 3.

Host Publisher

Host Publisher provides access to S/390 and AS/400 host data across the Web on dynamically created Web pages. You can also use Host Publisher's ODBC System Integration Module (SIM) to access databases, such as DB2, and other data sources using ActiveX and Java applications. Host Publisher has several components. These components can run on the same machine or different machines and can be combined to enable load balancing and hot standby.

An *Integrator* is a tool that enables a Web site administrator to generate HTML documents with dynamic content.

An *Adaptor* enables a Web server to intercept requests made to a Host Publisher Web library created with an Integrator. The Adaptor communicates with the Dispatcher to determine which PageServer fulfills each request.

A *Dispatcher* performs two tasks for the Adaptor. First, it directs the Adaptor to the appropriate PageServer to satisfy a request for dynamic data. Second, it load balances requests among multiple PageServers, enabling you to add PageServers as demand increases.

A *PageServer* parses Web pages to determine what information needs to be dynamically generated. It then requests the information from the appropriate data source, processes server-side scripts, and returns the page to the Adaptor.

The *PageTester* enables you to test Host Publisher load balancing and determine how best to distribute pages across PageServers.

The *Monitor* enables a systems administrator to view or change the status of any PageServer.

Data can come from many sources. System Integration Modules (SIMs) communicate with the data source and return information in compatible formats.

Host Publisher also includes a lightweight HTTP server with a built-in Adaptor.

You can use Host Publisher’s components to provide access to selected data using several network configurations. Examples are shown in Figure 4 on page 20 .

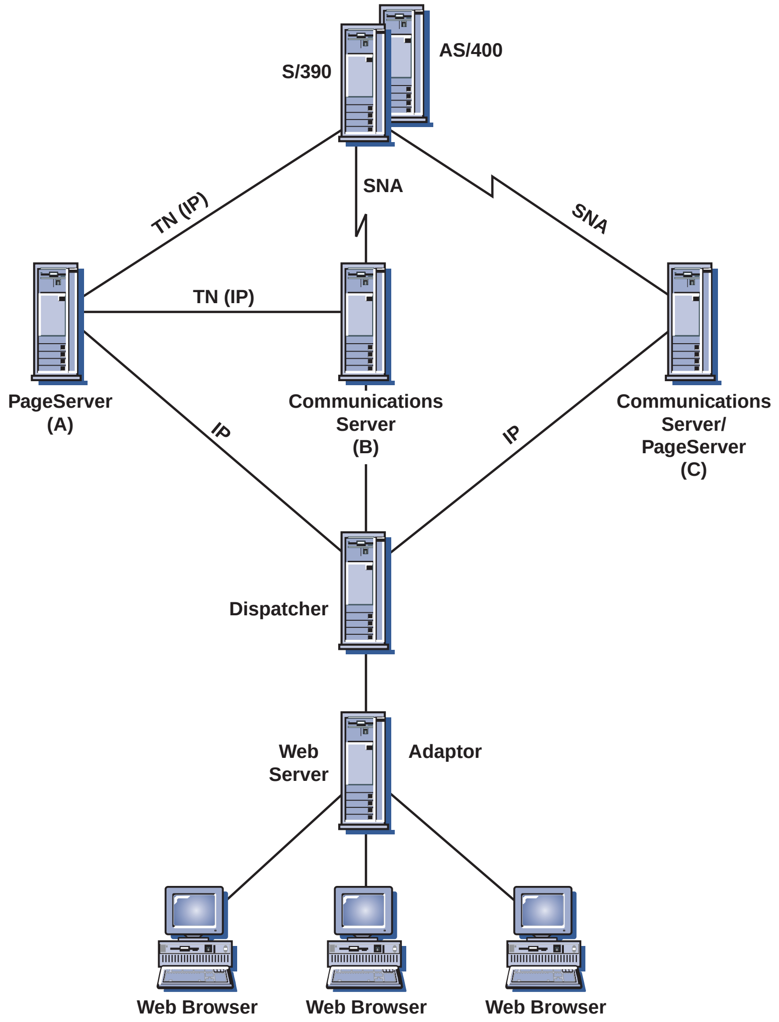

Figure 4. Using Host Publisher on SNA and TCP/IP networks

In this figure, two PageServers are communicating with a host machine. PageServer A can communicate either directly with the host over a Telnet connection, or through a separate Communications Server B with a Telnet connection between the PageServer and Communications Server and an SNA connection between Communications Server and the host. Server C is running Communications Server and a PageServer on the same machine and is communicating with the host directly over an SNA connection. Note that you must purchase Communications Server for each machine where you install the Communications Server, the PageServer, or both.

Clients running browsers request pages from the Web server. The Web server calls the Adaptor, which determines that the requests are associated with dynamic Web pages that exist as Web library files on a PageServer. The Adaptor then asks the Dispatcher which PageServer should service each request and routes the requests to the appropriate PageServers.

For additional information about planning for Host Publisher and Communications Server, refer to the online *Network Administration Guide*. For information about configuring and using Host Publisher, refer to the online help, or to the online *Host Publisher User's Guide*.

AS/400 OLE DB Provider

Applications that use OLE DB or ActiveX can communicate through Communications Server for record-level access to files on AS/400s.

You can use the AS/400 OLE DB Provider to connect Windows 95 and Windows NT 4.0 clients through Communications Server to one or more AS/400s, as shown in Figure 5. This configuration gives clients that have the AS/400 OLE DB Provider installed access to specific records within files on the AS/400.

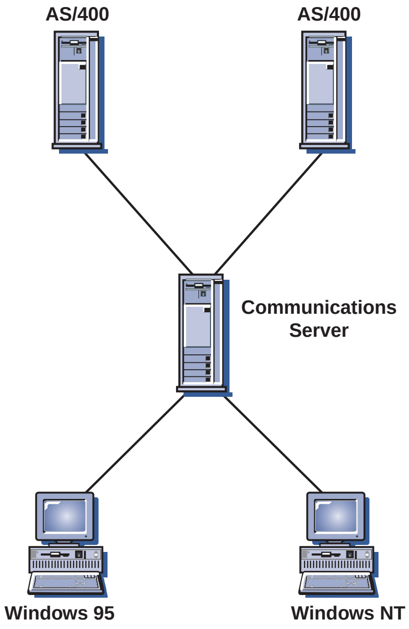

Figure 5. AS/400 OLE DB Provider

In this figure, both clients have the AS/400 OLE DB Provider installed. Alternatively, you can install and use the function from the server.

Documentation for this function, as well as information about developing OLE DB and ActiveX applications using Client Access, is provided in the csnt\sdk\as400_oledb directory.

SNA API Client Support

The Communications Server SNA API client support allows TCP/IP- and IPX-attached clients to access SNA APIs without requiring SNA protocols to flow between the clients and the server. This allows most SNA configuration to take place at the central server.

Communications Server supports SNA API clients on Windows 95, Windows NT, Windows 3.1, and OS/2 as illustrated by Figure 6 on page 23.

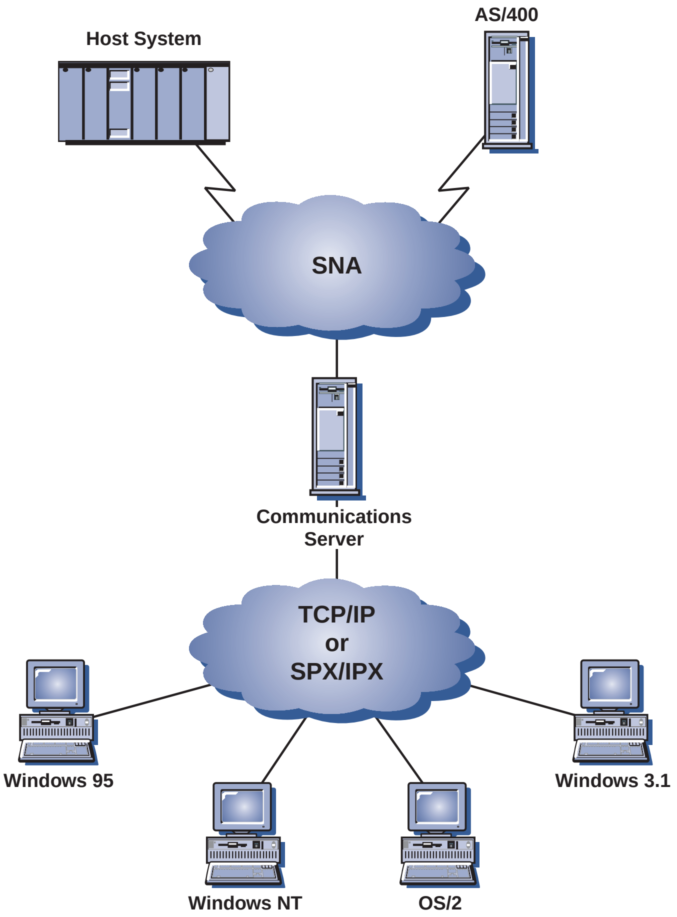

Figure 6. TCP/IP- or IPX-Attached SNA API Clients

The SNA clients provide support for CPI-C APPC, EHNAPPC, LUA RUI, JCPI-C, and HACL API interfaces, while providing the actual SNA processing at the server. These clients are delivered as part of the server but are actually installed and configured at the client.

Refer to "Programming Support" on page 32 for more information about the programming support available and the Software Developers Kit.

Novell NetWare for SAA Client Support

Communications Server Novell NetWare client support enables TCP/IP- and SPX/IPX-attached clients to access mainframe host data.

Communications Server supports Novell NetWare for SAA clients on Windows 95, Windows NT, Windows 3.1, and OS/2 as illustrated by Figure 7.

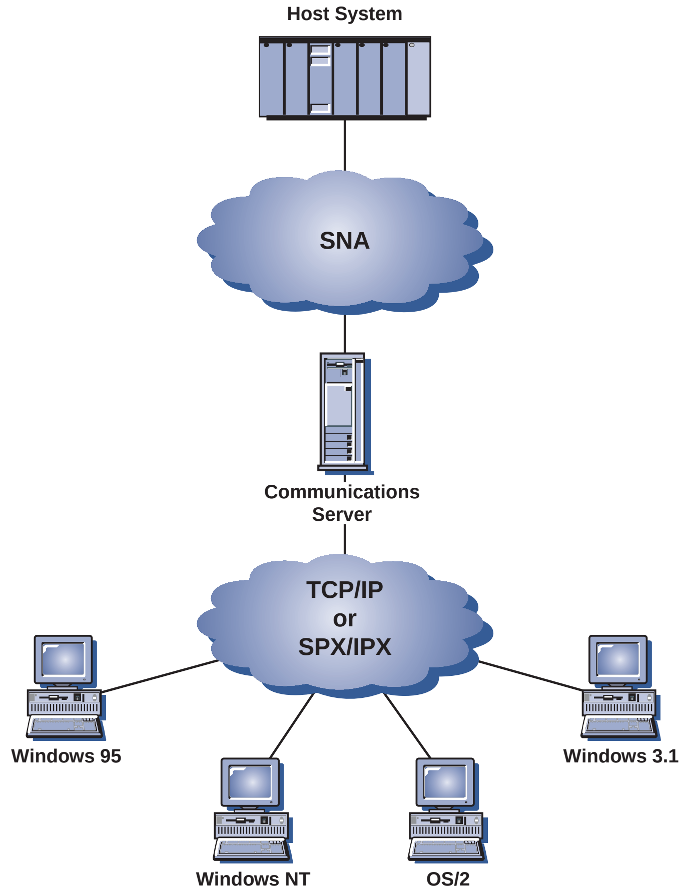

Figure 7. TCP/IP- or IPX-Attached Novell NetWare for SAA Clients

Refer to *Novell NetWare for SAA 3270 Client Interface Guide and Reference* P/N 100–002018–001 for more information about developing these clients.

AnyNet SNA over TCP/IP Access Node and Gateway

The AnyNet SNA over TCP/IP function in Communications Server allows SNA applications to communicate over interconnected IP and SNA networks.

The SNA over TCP/IP access node function allows SNA applications residing on an IP network to communicate. This function supports independent LU6.2

and dependent LU 0, 1, 2, 3, or 6.2 either with or without dependent LU requester (DLUR). In addition, the SNA over TCP/IP access node can be used in conjunction with SNA gateway to enable SNA gateway sessions over TCP/IP.

The SNA over TCP/IP gateway function extends the reach of SNA applications by allowing SNA applications in an SNA network to communicate with SNA applications in an IP network. The SNA over TCP/IP gateway supports independent LU 6.2 sessions.

For more information on how to configure AnyNet SNA over TCP/IP, see the online *Network Administration Guide.*

The following network configurations illustrate how SNA over TCP/IP access nodes and gateways can be used.

Running APPC or CPI-C Applications over a TCP/IP Network

Figure 8 illustrates how you can use the AnyNet SNA over TCP/IP access node function of Communications Server to enable communication between SNA applications over an IP network. Refer to the online Tutorial for configuration instructions.

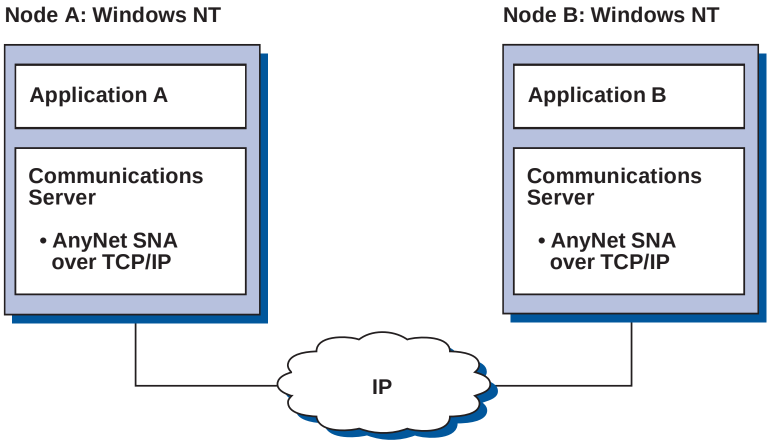

Figure 8. Running APPC or CPI-C Applications over a TCP/IP Network

Using AnyNet SNA over TCP/IP to Connect SNA Applications on Different Platforms

Figure 9 on page 27 illustrates some of the many products with AnyNet SNA over TCP/IP function. AnyNet gateways (Node F) allow SNA applications to communicate across a combination of TCP/IP and SNA networks.

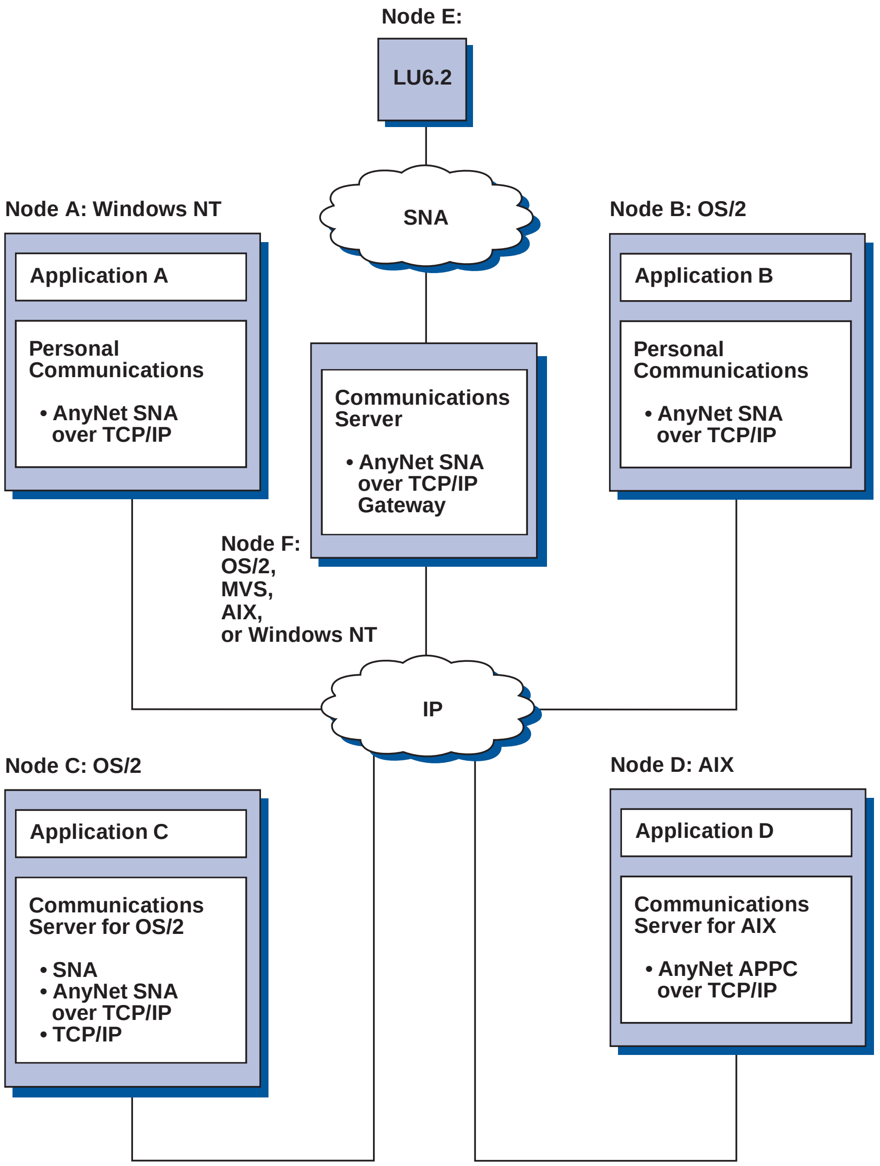

Figure 9. Using AnyNet to Connect SNA Applications on Different Platforms

Using an SNA Gateway for 3270 Emulation over a TCP/IP Network

Figure 10 on page 28 illustrates a configuration that supports dependent LU communication for downstream workstations over a single IP network. All three machines are running AnyNet SNA over TCP/IP. Node A is a dependent LU server (DLUS), and Node B is a dependent LU requester (DLUR). Refer to the online Tutorial for configuration instructions.

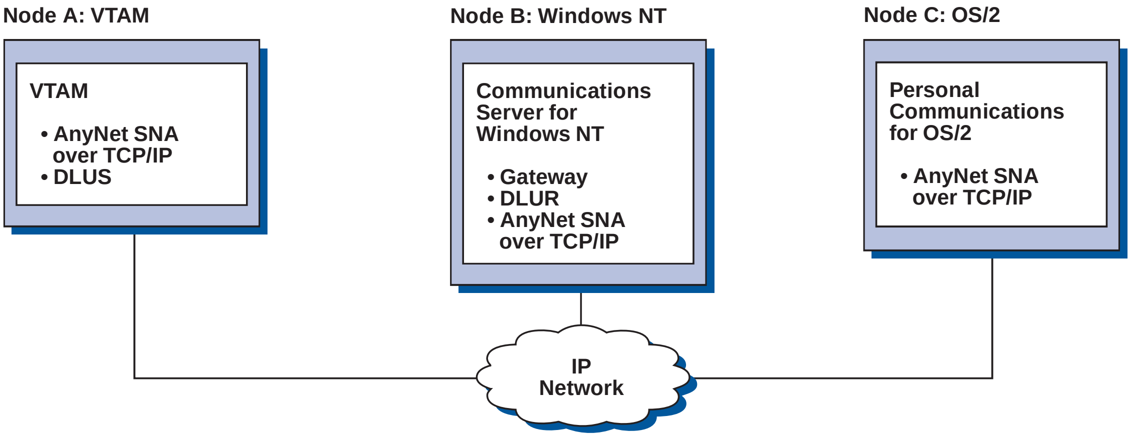

Figure 10. 3270 Emulation through an SNA Gateway over a TCP/IP Network

AnyNet Sockets over SNA Access Node and Gateway

The Sockets over SNA access node function enables TCP/IP application programs using the WinSock 1.1 and WinSock 2.0 socket interface to communicate over an SNA network.

The Sockets over SNA gateway function enables sockets applications in SNA and TCP/IP networks to communicate. Sockets over SNA gateways are often used to connect isolated TCP/IP networks using an SNA backbone network.

Socket Applications Communicating over an SNA Network

Figure 11 on page 29 illustrates a network where Sockets over SNA is configured on each node, but no Sockets gateway function is needed. Socket applications A and B can exchange information as long as they are connected through an SNA network. The SNA transport can take full advantage of the APPN and HPR for enhanced reliability and performance.

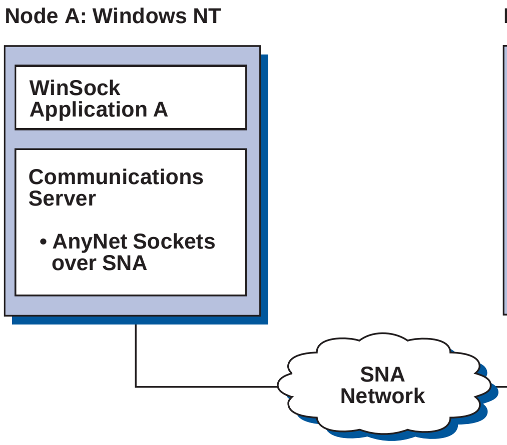

Figure 11. Sockets Applications Communicating over an SNA Network

Connecting Remote TCP/IP Networks Using an SNA Backbone and Sockets over SNA Gateways

Sockets over SNA Gateway can be used to connect remote, native TCP/IP networks across an SNA network. For example, two Sockets over SNA Gateways can be used to connect two TCP/IP networks to an SNA network. In this network configuration, socket applications on either TCP/IP network can use the gateway to communicate with socket applications on the SNA network or with socket applications on the remote TCP/IP network.

In Figure 12 on page 30, Nodes A and C are configured with TCP/IP and run on remote, native TCP/IP networks. Nodes D and E are configured as Sockets over SNA Gateways. Node B is an access node configured with Sockets over SNA and runs on an SNA network. The two Sockets over SNA Gateways enable communication between socket applications on all nodes.

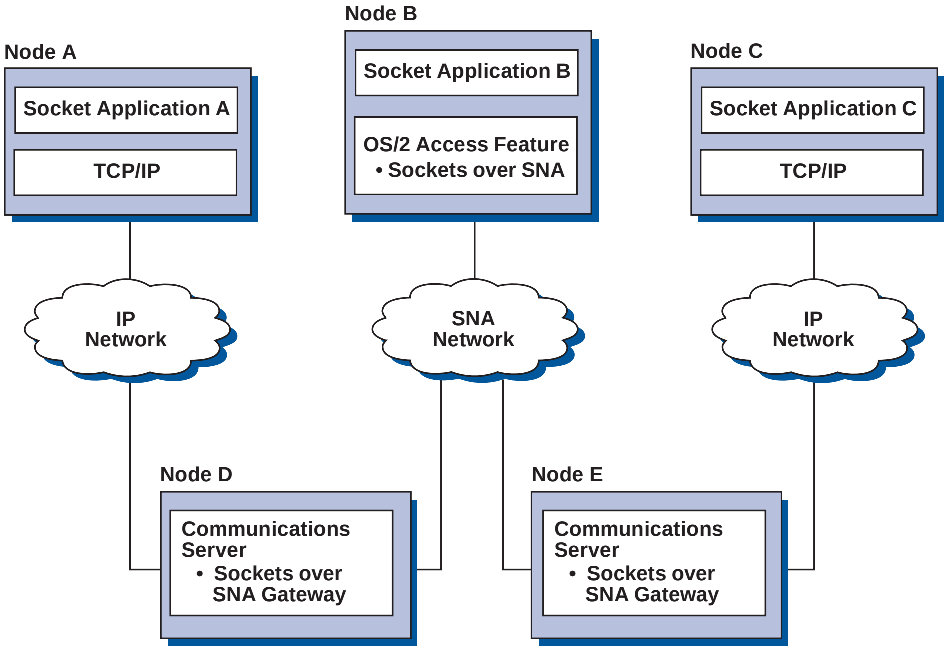

Figure 12. Socket Applications Communicating through Multiple Sockets Gateways

Connecting Sockets over SNA Access Nodes on Different Operating Systems

Figure 13 on page 31 illustrates an SNA network in which socket applications on multiple operating systems are communicating over an SNA network. In this example:

- Node G is configured with Sockets over SNA for MVS which is provided with the VTAM Multiprotocol Transport Feature (MPTF) or the VTAM AnyNet feature.
- Node C is configured with Sockets over SNA for OS/2 which is also provided with Communications Server for OS/2.
- Node D is configured with Sockets over SNA for AIX which is provided as part of the Communications Server for AIX.
- Node A is configured with Windows NT and Sockets over SNA, which is provided with Communications Server for Windows NT.
- Node B is configured with OS/400, which includes the Sockets over SNA function.

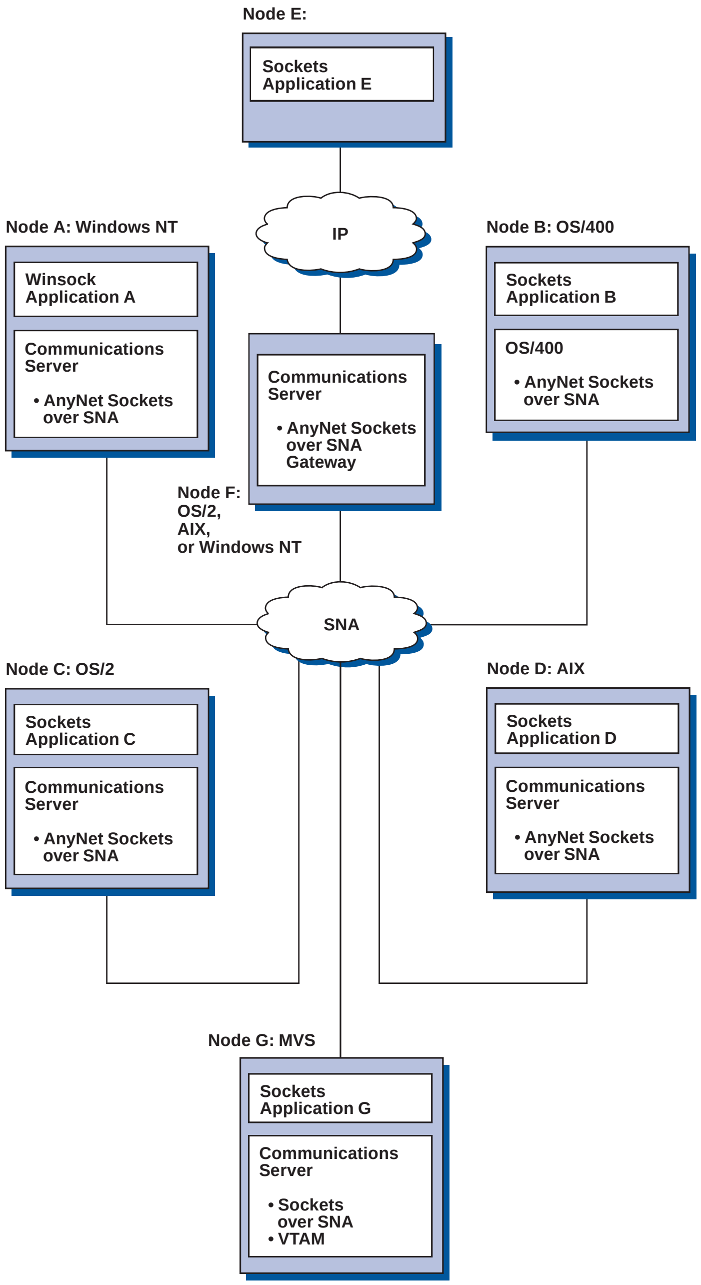

Figure 13. Socket Applications on Multiple Operating Systems Communicating over an SNA Network

Refer to the online *Network Administration Guide* for more information about Sockets over SNA.

Local and Remote Configuration and Administration Support

Communications Server provides a graphic user interface (GUI) for entering configuration data, including wizards that simplify common configuration tasks. Local configuration is supported at both the client and server level. Remote configuration of the server is supported from Windows NT and Windows 95 clients.

The SNA Node Operations application allows you to stop, start, and monitor resources in your network. The SNA Node Operations application is also supported from Windows NT and Windows 95 clients. This support allows Node Operations to connect to and manage remote Communications Servers.

Communications Server includes command line utilities that enable you to perform many of the functions provided by SNA Node Operations. See "Command Line Utilities" on page 87 for more information.

The Web administration application enables you to manage communications servers over an intranet. You can use a Web browser to query node status, obtain information about and modify resources, display and edit configuration files, display message logs, and perform other administrative tasks. To use Web administration, you must have administrator authority and must have a Web server running on the same machine as Communications Server.

Communications Server provides a Tivoli Management Environment (TME) Plus module that integrates management of Communications Server into TME. You can use TME to distribute, install, and uninstall Communications Server. You can also use it to check the server's status, start or stop the server, monitor events, and display and modify server resources. This module is available in English only, because TME only supports English at this time.

Programming Support

Communications Server supports a wide range of 32-bit application programming interfaces (APIs) on the server for the application program developer. These APIs provide convenient ways for application programs to access Communications Server functions and allow applications to address the communication needs of connections to both IBM and other computers. In addition, the provided interfaces support SNA protocols so that standardization is ensured.

The APIs supported include:

- Advanced program-to-program communications (APPC)
- Common Programming Interface for Communications (CPI-C)
- Conventional LU Application Interface (LUA) RUI and SLI
- Host Access Class Libraries (ECL)
- Java CPI-C (JCPI-C)
- WinSock (in conjunction with AnyNet Sockets over SNA)
- Network Operator Facility
- Management Services
- Common Services

On the clients, the Enhanced APPC (EHNAPPC) API is also provided.

The Communications Server Software Developers Tool Kit (which can be separately installed from the Communications Server CD-ROM) is also available for application developers to use. This tool kit contains samples, header files, library files, and online manuals for each of the APIs.

CPI Communications and APPC Support

Advanced program-to-program communications (APPC) supports communications between distributed processing programs, called transaction programs (TPs). APPC uses the LU 6.2 protocol for exchanging data between programs located at different logical units (LUs). In addition, APPC supports multiple concurrent links and parallel sessions. Conversation or session security between the communicating programs is also supported through APPC.

Communications Server supports APPC full duplex conversation, which greatly enhances data transmission capability and improves productivity for programmers who write conversation type applications.

A CPI-C transaction program is similar to an APPC transaction program; both types of transaction programs use APPC support. Rather than building a separate control block for each function, a CPI-C transaction program invokes each CPI-C function with a call to the function that passes the appropriate parameters on the call.

APPC is a single entry point API where complex control blocks are required to cause different functions. CPI-C provides many functions, each with its own parameters, which enhances readability and portability.

The CPI-C and APPC verbs provide similar services. However, CPI-C provides an API that is portable across multiple platforms.

Data Security

Communications Server provides basic and enhanced security support at session and conversation levels. There is security in limiting which Windows NT users may access SNA resources through the SNA API clients. Conversation security includes support for password substitution. There is also enhanced LU-LU security.

Communications Server also provides session-level encryption (SLE), which enables you to encrypt either all of the data or selected data that is transferred between the workstation and the host. If you want to protect any workstation data by using encryption, the host must also be configured to use encryption.

Conformance with SNA

Communications Server supports conformance with Systems Network Architecture (SNA), the set of conventions and protocols used in IBM networks. SNA helps ensure standardization of network configurations and accurate transmission of data across networks.

An SNA network is organized as a system of *nodes* and *links*. Each node is classified according to its capabilities and the extent of control it has over other nodes in the network. The node type is not necessarily associated with a specific type of hardware, and the node's capabilities can be performed by different devices. For example, a workstation acting as a gateway can perform the same functions as a communications controller. Communications Server workstations can communicate using LAN, SDLC, MPC, X.25, twinaxial (for upstream communication), and SNA over TCP/IP.

A link is the combination of the link connection (the transmission medium) and two link stations (nodes), one at each end of the link connection. A link connection can be shared among multiple links in a multipoint or token-ring configuration.

LU Support

Communications Server provides support for SNA LU types 0, 1, 2, and 3, which provide communications with host applications that support devices such as:

- LU type 0, for 3650 and 4700 financial terminals
- LU type 1, for 3270 printers
- LU type 2, for 3270 interactive displays
- LU type 3, for 3270 printers

Communications Server also supports LU type 6.2 or APPC. LU type 6.2 supports communications between two programs located at type 5 subarea nodes or type 2.1 peripheral nodes, or both, and between programs and devices. Communications Server supports LU 6.2 through the APPC or CPI Communications APIs.

Management Services

Management services are functions distributed among network components to operate, manage, and control a network. This capability is based on the SNA management services architecture documented in *Systems Network Architecture Management Services Reference*.

Communications Server provides programming support that allows installation of focal point, service point, and entry point applications.

System Management

You can monitor and manage your SNA networks with several network management tools, including:

- ***Message logs and error logs***

  Communications Server writes its message-log and error-log entries to the log files maintained on each workstation.
- ***Trace files***

  Communications Server provides trace tools for problem determination.
- ***Configuration and management***

  You can use the SNA Node Operations application to help manage the resources in your network. Also, the systems management programming capabilities of Communications Server enable you to configure and manage the nodes within your SNA network. To accomplish this, Communications Server provides a subset of system management verbs that you can use to configure your node and to build sophisticated management programs for your active node.
- ***System management tools***

  Communications Server provides a variety of tools to assist you in network management. The tools include:
  - SNA Node Operations
  - Trace Services
  - Tivoli Plus Module

  SNA Node Operations is an online facility for monitoring and controlling communications resources maintained by Communications Server. It is used by individuals performing installation, testing, tuning, and special development activities of Communications Services. It can also be used to assist during problem determination.

For example, you can use the SNA Node Operations facility to display the status of a transaction program you are having problems with.

Trace services are described in “Chapter 6. Problem Determination and Reporting” on page 93.

For information about the Tivoli Plus module, refer to the online *Network Administration Guide*.

In addition to these tools, Communications Server provides several productivity aids and an online message and help facility.

Entry-Level Emulator Functions

Communications Server includes an entry-level version of the popular Personal Communications 3270 and 5250 emulator for administrative purposes. This emulator provides basic 5250 and 3270 support on the server that includes a subset of the features and functions that are in the full-function IBM Personal Communications family of emulators.

The entry-level emulation functions provided include:

- Color mapping
- Command line transfer (3270 only)
- Full font set
- Screen sizes mod 2-5
- Two sessions

Although graphical keyboard remapping is not supported for the entry-level emulator, you can use the remap files generated by the full-function emulator.

Chapter 2. Planning for the Installation of Communications Server

This chapter describes the requirements for installing the elements shipped with Communications Server and gives an overview of the installation process.

Before You Start

Before you install Communications Server:

- Review the information found in the README.TXT file on the CD-ROM or the installation source directory.
- Review the available features and functions by referring to "Features and Functions of Communications Server for Windows NT" on page 9.
- Obtain access to the installation media (either a CD-ROM or the appropriate LAN environment).
- Obtain an administrator user ID with local authority to use when installing Communications Server.

Introduction to Installing Communications Server

Communications Server provides an interactive interface for installing the product.

Prerequisite Software

Communication Server requires Microsoft Windows NT Server 4.0 with service pack 3 or later. Consult the Windows NT documentation to determine the memory and hard disk storage requirements for your operating system.

TCP/IP is required for TN3270E and TN5250 servers.

TCP/IP, IPX/SPX, or both, is required for SNA API clients, Novell NetWare for SAA clients, and Remote Administration clients to communicate with Communications Server. If you are running IPX, you also need the following software enabled on the server:

- Gateway Service for NetWare
- SAP agent
- NWLink IPX/SPX or a compatible transport

Remote Administration clients require Windows 95 or Windows NT Workstation or Server Version 4.0 or later.

SNA API clients require one of the following:

- OS/2 Warp Version 3.0 or later
- Windows 3.11 or later
- Windows 95 with service pack 1 and the following fix:

  ```
  Microsoft Knowledge Base article id: Q128366
       Creation date:  11Mar96
       Web site for downloading fix:
       www.microsoft.com/windows/servpak1/sphome.htm
  ```
- Windows NT Workstation or Server 3.51 with service pack 4 or later
- Windows NT Workstation or Server 4.0 or later

TCP/IP or IPX is required for communication with the server. If you are running IPX, you also need the following software:

- Gateway Service for NetWare
- SAP agent
- NWLink IPX/SPX or a compatible transport

The AS/400 OLE DB Provider can be installed as a component of Communications Server, or as a component of the SNA API client for Windows 95. It can also be installed as a component of the SNA API client for Windows NT; however, it requires Windows NT Workstation or Server 4.0 or later. If you do not have the Microsoft Data Access Components (MDAC) Version 1.5 installed, Communications Server will install it for you when you install this component.

If you install the AS/400 OLE DB Provider on a machine that already has Client Access Version 3 Release 2 MD (or lower) installed, some Client Access function will be disabled, including support for ActiveX and OLE DB programs that use Client Access for access to AS/400 data queues, remote commands, distributed program calls, stored procedures, and SQL statements.

Host Publisher requires a Web server running in your network and the Java Runtime Environment (JRE) that is provided with Communications Server.

Web administration requires a Web server running on the Communications Server system and a Web browser running on any system on your intranet. Communications between the systems must use Sockets over SNA or TCP/IP. Supported Web servers include:

- IBM Internet Connection Server for Windows NT
- Lotus Domino
- Lotus GO

- Microsoft Internet Information Server for Windows NT
-

Other Web servers can be used, but are not supported and may have limitations. Microsoft Peer Web Server, which is supplied with Microsoft Windows NT Workstation, cannot be used because of its limitations.

Supported Web browsers include:

- Netscape Navigator 4.0 or later
- Microsoft Internet Explorer 4.0 or later

Other Web browsers that support Java 1.1 or later, JavaScript, frames, and cookies can be used, although they are not supported.

Many other functions and features of Communications Server require a Web browser. The Web browser you use must support HTML 3.0 documents.

Refer to the latest Microsoft Windows NT Service Pack.

Communications Server will not install successfully on a machine that has Microsoft SNA Server** installed and will not coexist with SNA Server or other SNA stack providers.

Communications Server does not provide the link control protocol (LCP) required to support a Point-to-Point Protocol (PPP) connection between the server and a modem for ISDN connections. If your modem provides the LCP independently from the application support, then Communications Server should work.

Refer to README.TXT on the installation CD for more up-to-date information.

Prerequisite Hardware

Communications Server Version 6.0 can be used on all Intel**-based systems that are supported by Windows NT Server, Version 4.0 or later. An Intel Pentium machine, 100 MHz CPU with 32 MB of RAM, is the minimum recommended server hardware.

Configurations requiring multiple protocols, such as TN3270E, TN5250, AnyNet, or SNA API clients require a minimum of 32MB of RAM on the server. More may be required based on the size of the environment. These components require both SNA and TCP/IP and a corresponding increase in memory.

Planning for Installing Communications Server

Prepare to use a minimum of 75 MB of disk space for Communications Server. Depending upon your Communications Server requirements, you may require more resources.

MPC connections require a PCI ESCON Channel adapter, a multimode (LED) fiber connection, and an S/390 host with VTAM V4R4 or later.

Refer to README.TXT on the product CD for more information.

Startup Drive Requirements during Installation

Communications Server requires 20 MB of disk space on the startup drive (the drive that contains the Windows NT operating system) for temporary files used during installation. These files are erased after installation completes.

Chapter 3. Installing Communications Server

The Communications Server package contains the Communications Server product files, the Communications Server documentation, and the Adobe Acrobat Library Reader which can be used to view the online books. You can view and print the documentation from the CD without installing, if desired.

In addition to the Communications Server product files, the following features can be selectively installed from the CD.

- Clients for SNA API client services (installation images; cannot be installed over Communications Server)
  - OS/2
  - Windows 3.x
  - Windows 95
  - Windows NT
- Remote administration and configuration clients (installation images; cannot be installed over Communications Server)
- IBM Host On-Demand (a Web-based emulator)
- Entry-Level Personal Communications Emulator (install only after the Communications Server product and only on the server)

Considerations before Installing

Communications Server should be installed on an Intel-based computer running Windows NT Server 4.0. To install the Communications Server, you must have a Windows NT administrator user ID with local administrative authority.

Beginning Installation

Before beginning to install Communications Server, close other application programs that you are running.

Either Communications Server or the SNA API client should be installed prior to installing any version of the Personal Communications product (including the entry-level emulation program shipped with Communications Server). If Personal Communications is already installed on your server, remove it prior to installing Communications Server or the SNA API client.

If you have any version of Communications Server for Windows NT already running, stop it before starting to install.

Your machine must be running in VGA mode to install Adobe Acrobat. If you are running in another mode, change to VGA mode before starting to install.

Installing Communications Server for Windows NT

1. Insert the Communications Server for Windows NT CD-ROM into the CD-ROM drive and follow the steps provided in the interface. If you do not have autorun enabled on your machine, access the CD-ROM drive manually and run SETUP.EXE to launch the installation interface. Use any editor to read the README.TXT file for the latest product notes. Click **Help** to get online help throughout the installation procedure.
2. Choose **Install Products**. A window appears that asks whether you want to install server or client products. Select **Server** and then click **Next**.
3. Select the server options you want to want to install and then click **Next**.
4. Check that the options you wanted are listed on the summary window. To continue, click **Finish**. To add or remove options, click **Back**.
5. The InstallShield** Wizard for Communications Server begins installing. When installed, the wizard will guide you through the installation procedures. A progress bar indicates how far along you are in the installation procedures. Upon completion of the installation of the wizard, a Welcome to IBM Communications Server window appears. Click **Next** to continue.
6. The next window asks you to choose the drive and directory where you want to install Communications Server and its components. The default is C:\IBMCS. Click **Browse** to display a dialog box that will allow you to change your drive or directory by typing in a new path name or choosing a directory from the provided list. Click **Next** to continue.
7. The Select Components window enables you to choose the Communications Server components you want to install. When you click on a component, its description appears in the box below the component list. After you select the components, click **Next** to continue.
8. If you selected Web Administration, the Configuration of Web Administration window appears. This window lists the Web servers that were detected on your system. You can select which of these servers you want Communications Server to configure for you. Click **Next** to continue.
9. The Select Program Folder window shows which program folder will contain the Communications Server icons. The IBM Communications Server folder is the default. If you want to use a different folder, type the name of the desired folder in the entry box. If you select a new name, a new folder will be created. You can also select a folder from the Existing Folders list. Click **Next** to continue.
10. The next window asks for the name of one existing user ID to be initially added to the group; more user IDs can be added later using the Windows NT User Manager. This window is used to establish the

IBMCSADMIN group, which allows users to be authorized to remotely configure and administer Communications Server. Type a user ID and click **Next**.

11. The Number of Concurrent Licenses window appears. Type the number of concurrent user licenses that you have purchased and click **Next**.
12. The Start Copying Files window shows your current settings for the installation of Communications Server. To change a setting, click **Back** to go backward through the previously mentioned installation screens and make the necessary changes.
13. Click **Next** to begin copying the Communications Server files onto your system. Once the horizontal Progress Bar appears on the screen to indicate copying has started, do not stop the installation procedure.

    During the copying procedure, there are vertical progress bars at the left of the window that enable you to watch the installation's progress. The progress bar on the far left monitors how much data remains in each file as it is being transferred. The progress bar in the middle shows the percentage of the installation files that have been copied. The progress bar on the right shows how much disk space remains for you to use during the installation process.
14. When all product files have been copied, the Installing NT Services window appears.
15. After the services have been installed, a window appears that asks whether you would like to register Communications Server now. Click **Yes** or **No**.
16. At the end of the installation, a dialog box asks if you would like to install the IEEE 802.2 interface for the Local Area Network (LAN) using the IBM LLC2 protocol interface. If you know that you will use Communications Server over a LAN adapter or if you are not sure, choose **Yes**. If you know that you will not use Communications Server over a LAN adapter, choose **No**.
17. Once you have completed the installation, you will be prompted to reboot your machine.

If you want to install the online documentation on an additional machine, such as a publications server, you can install it later by performing a drag-and-drop (using Windows Explorer) of the documentation files to the desired path. After you have created icons in the appropriate folder, you will need to associate these files with the Adobe Acrobat Library reader. See the Adobe Acrobat README.TXT file for more information.

Removing Communications Server for Windows NT

To remove Communications Server, follow these steps:

1. Click the **Uninstall Communications Server** icon in the Communications Server folder.
2. If you have the IBM LLC2 protocol interface installed, a help panel will help you remove the LLC2 protocol.

> 1. We recommend that you back up your configuration files periodically in case a problem occurs with the configuration. By default, your configuration files (.ACG files) are located in the **\private** subdirectory of your Communications Server installation directory. These files are not removed when Communications Server is removed.
> 2. Attempting to remove while an application that uses Communications Server (APING or Personal Communications, for example) is running will cause the removal to hang until the application ends. Close all applications that use Communications Server before you remove the product.

Reinstalling Communications Server for Windows NT

To reinstall Communications Server, you must first remove the product. After you have successfully removed Communications Server and have rebooted the machine, reinstall the product. Use the previous two sections for guidance in installing and removing the product.

> We recommend that you back up your configuration files periodically in case a problem occurs with the configuration. By default, your configuration files (.ACG files) are located in the **\private** subdirectory of your Communications Server installation directory.

Registering Communications Server for Windows NT

The IBM eNetwork Software Servers offer a common method for registering the server products. The Axtive Registration Tool is used for registering the Communications Server. The benefit of registering the server with IBM is that you can be notified of future service updates and of future releases of the product.

You are given the opportunity to register when you install and the first time you start the product. Follow the instructions of the registration tool. If you decline to register, then once every eight days you will again be prompted to register. In addition to the initial registration, a follow-up registration survey will be offered one year after you have installed Communications Server and once more after two years.

License Management

If you purchase a licensed version of Communications Server, then the license certificate is contained in a file on the CD. This license is installed along with the product. During installation you are prompted to enter the number of concurrent licenses you purchased. Refer to the License Agreement for details on what constitutes a concurrent user.

If the number of concurrent users exceeds the number of concurrent licenses that you have purchased, then an error message is logged. No product function is disabled even in the case of the licenses being exceeded. Further connections are still allowed with an error message being logged for each connection as long as the license count is exceeded. You are expected to monitor the log and purchase additional licenses if you consistently exceed your initial license quantity.

The Node display in the Node Operations application can be used to view the number of licenses purchased, the number in use, and the highest number of licenses ever used. If you purchase additional licenses, use the **cslic** command to update the number of licenses purchased. For example, if you initially purchased 20 licenses and later purchased 20 more, go to a command prompt window on the Communications Server machine and type `cslic 40` to update the number of licenses to 40.

You do not need to reinstall the product in order to convert from a trial version to a licensed version, however, there are two steps you need to perform:

1. Copy the license certificate file (CSNT60.LIC in the \csnt directory of the licensed product CD-ROM) to the directory where you installed Communications Server (usually C:\IBMCS).
2. Use the **cslic** command to indicate the number of concurrent licenses you purchased. If you purchased 20 licenses, enter `cslic 20` at a command prompt. The next time you start the product the license information will be loaded.

You can also remove the trial version, then install the licensed version of Communications Server.

If you have obtained a trial version of Communications Server, then the license certificate file is not contained on the CD. You may use all the functions of Communications Server for a period of ninety days. After that time the product will fail to start. You can convert the trial version of Communications Server to a licensed version by purchasing a license.

Installing Host Publisher

You can select the Host Publisher component from the installation interface provided on the CD-ROM. Follow the instructions in the interface and refer to the online help for detailed instructions.

You can choose any or all of the components in the following categories:

Design tool
Integrator

Documentation
Host Publisher User's Guide (HTML)

Extensions
Java Integrator and Active Server

Runtime environment
Adaptor, Dispatcher, Monitor, PageServer, and Web Server

Test Page Tester

Toolkit
Software Developer's Kit

Accessing and Installing the SNA API Clients

Once you have installed Communications Server, you will be able to access the SNA API clients that work with the server. SNA API clients are provided for the following operating systems:

- OS/2
- Windows 3.x
- Windows 95 and Windows NT

1. The SNA API client for OS/2 cannot be used in conjunction with IBM Communications Server for OS/2. Communications Server for OS/2 must be removed before you install the SNA API client for OS/2.
2. IBM Personal Communications Version 4.1 for Windows 95, Windows 3.1, or OS/2 cannot be used in conjunction with SNA API clients.
3. The SNA API client for OS/2 cannot be installed on the same machine as IBM eNetwork Communications Server for OS/2 (CS/2). You must uninstall CS/2 before you install the SNA API client.
4. To use IBM Personal Communications for Windows NT or IBM Personal Communications Version 4.2 for Windows 95, install the SNA API client for Windows NT and Windows 95 before installing Personal Communications. When removing, remove Personal Communications and reboot before you remove the SNA API client.

The client installation packages are located in the following directories under your Communications Server installation directory, provided you chose to install them:

- clients\win32
- clients\win16
- clients\OS2

To install a package on a client, the client must have access to the information in these directories (for instance, using **net use**, **ftp**, or diskette transfer).

Change to the appropriate drive and at the command prompt type **install** to access the OS/2 client and **setup** to access any of the other clients.

You can also install the SNA API clients directly from the CD-ROM onto a client machine instead of from a server. Follow the steps on the Communications Server CD-ROM.

Accessing the Remote Administration Client

The remote administration client for Windows NT and Windows 95 is used to remotely administer and configure the server. The remote administration client is located in the following directory under your Communications Server installation directory, provided you chose to install it:

- clients\admin

To install a package on a client, the client must have access to the information in these directories (for instance, using **net use**, **ftp**, or diskette transfer).

Change to the appropriate drive and at the command prompt type **setup** to access the clients.

You can also install the remote administration client directly from the CD-ROM onto a client machine instead of from a server. Follow the steps on the Communications Server CD-ROM.

You do not need to put the remote administration and configuration clients on the same machine as your server because they are already available on that machine.

Chapter 4. Configuring Communications Server

This chapter explains the basics of how to use the configuration program provided with Communications Server.

SNA Node Configuration provides configuration options that enable you to define SNA nodes and associated resources. You can define the following SNA characteristics:

- Network functions such as APPN, host connectivity, or LU 0
- Link characteristics
- Session partners and parameters
- Transaction programs on the local node that can be accessed through the SNA network (also known as target TPs)

The set of objects that must be configured depends on the environment in which Communications Server operates and the specific functions Communications Server is to support.

Back up your configuration files periodically in case a problem occurs with the configuration. By default, your configuration files (.ACG files) are located in the **\private** subdirectory of your Communications Server installation directory.

Detailed configuration instructions are available online as part of the Tutorial. You can get to this information from a configuration scenario by selecting any step and pressing F1.

Deciding What to Configure

How you configure and use Communications Server depends on the task you are trying to accomplish. Scan the list of common configuration types below to find the section of this chapter that discusses your configuration needs. Each configuration scenario is self-contained and divided into steps.

Configuration Type	**Refer To:**
Use Communications Server as a SNA gateway allowing clients to access host applications through this server	"SNA Gateway Configuration" on page 52
Use Communications Server as a TN3270E server	"TN3270E Server Configuration" on page 53
Use Communications Server as a TN5250 server	"TN5250 Server Configuration" on page 54

Configuration Type	Refer To:
Define an APPN network node (with HPR and connection networks)	"APPN Network Node Configuration" on page 55
Define the node as a dependent LU requester (DLUR) over an APPN network, or as a gateway between a downstream DLUR and an upstream DLUS (dependent LU server)	"DLUR/DLUS Configuration" on page 57
Define an AnyNet SNA over TCP/IP gateway	"AnyNet SNA over TCP/IP Gateway Configuration" on page 59
Define AnyNet Sockets over SNA	"AnyNet Sockets over SNA Configuration" on page 60
Configure Communications Server to support SNA API clients running APPC applications	"SNA API Client Configuration for APPC" on page 61
Configure Communications Server to support SNA API clients running 3270 or other LUA applications	"SNA API Client Configuration for LUA" on page 68
Run APPC or CPI-C applications or 5250 emulation to an AS/400 system	"CPI-C or APPC Configuration" on page 72
Run APPC or CPI-C applications on this node to a host through a subarea network	"Dependent LU 6.2 Sessions to a Host" on page 74
Access host applications using a 3270 emulator	"3270 Configuration" on page 75
Define a focal point	"Focal Point Configuration" on page 76
Use AS/400 shared folders	"AS/400 Shared Folders Configuration" on page 77

As a starting point, choose the scenario that most closely matches your configuration. The online *Network Administration Guide* contains information that can help you decide which type of configuration you should use. You can then use the information in the online help to alter the configuration as necessary.

You can also use these scenarios to create a basic configuration for multiple machines. Refer to the online *Configuration File Reference* for detailed information about customizing your configuration.

Getting Started

To begin configuring, follow these steps:

1. Click **SNA Node Operations** in the Communications Server folder. On the toolbar, click **Configuration Utility**.

2. Select **New** on the Welcome to Communications Server Configuration! window to create a new configuration. Click **Next>**.
3. Select the scenario you want from the Choose a Configuration Scenario window. Click **Finish**.
4. A window appears that lists the steps you need to follow and shows a diagram of the resources you need to configure. Click the help button for a step to get detailed instructions. Click the action button for a step to bring up the configuration window and add a definition for that step.
5. To modify a definition, double-click its entry in the tree-view diagram.

This section only lists required steps. Optional steps are listed in the online scenarios.

Testing Your Configuration

The steps you need to take to test your configuration are listed in each scenario and described fully online. Usually, testing involves the following steps:

1. Start the node

   Click **Start/Stop Node** on the SNA Node Operations toolbar to start the local node. Specify a configuration with which to start the node. Select the file you have just configured and click **Open**. It may take a moment for the node to start and to establish all the defined links.
2. Verify that the link is active

   Once the node has started, you should see a view of the active node with the control point name displayed that you specified in Step 1. (It may take a few moments to establish the link.) To verify that the link you configured is active:

   a. Find the **Host Resources** icon in the left side of the SNA Node Operations window. Expand the list of resources by clicking the plus mark (+) next to the icon.

   b. Click **Connections** (for CPI-C and APPC configurations, click **Peer Connections**. Defined links are displayed in the right side of the SNA Node Operations window.

   c. To display details about the displayed links, click the **Details** icon on the toolbar.
3. Establish a session

   For most configurations, have clients establish a session through the gateway to the host. The client configurations need to specify the gateway's network addressing information, such as the token-ring address for the gateway's token-ring card.

For APPN network node, AnyNet SNA over TCP/IP, and CPI-C and APPC configurations, you can use the Check Connection (APING) application from the Communications Server program group on the desktop to verify that a remote LU in the network is reachable. When you invoke the application, specify the fully qualified partner LU. Click **OK** to continue. The application will send test packets of data to the remote node's APINGD application. These packets will in turn be returned to the local application.

For AnyNet Sockets over SNA, use the **ping** application to reach another Sockets over SNA node in your network:

```
ping IPaddress
```

If successful, you will receive test frames indicating that packets were transmitted to the remote node and returned. You can also use the ping application, or any other socket application, to reach the local node from another Sockets over SNA node in the same network. Run the application on that node, specifying the local node's AnyNet Sockets over SNA IP address.

SNA Gateway Configuration

This section describes the steps to configure Communications Server as an SNA gateway for passing sessions between SNA clients and hosts.

By configuring an SNA gateway, you are able to exchange data between downstream client workstations and a Systems Network Architecture (SNA) mainframe host computer. The gateway performs the function of a concentrator, which makes LU resources from one or more hosts and host PUs available to downstream SNA client workstations over any combination of communications media supported by Communications Server.

Before proceeding with this configuration, locate **all** the information listed in "Before You Begin". If the following configuration steps do not mention some field names that appear on the configuration panels, you can accept the default values for those fields.

Before You Begin

Before you begin this procedure, collect the following information:

- A local node ID (XID) corresponding to the host's PU (for switched physical media) *or* a local secondary station address corresponding to the host's PU (for non-switched physical media)

A local node ID consists of a block ID followed by a PU ID.

- At least one local LU address available on the same host PU
- Addressing information for contacting the host’s communication controller (such as the token-ring address)
- The physical network type your downstream clients are using (for example, token ring)
- If you are using AnyNet SNA over TCP/IP:
  - The IP address of your machine
  - The IP address of your gateway or partner
  - The domain name suffix administered by your site administrator.

    See the online *Network Administration Guide* for more information.

Summary of Steps

To begin configuring, follow the steps listed in “Getting Started” on page 50.

If you have wizards enabled, a wizard will appear for this scenario instead of the window described in “Getting Started” on page 50.

This type of configuration requires the following steps:

1. Node setup
2. Device configuration
3. Define host connections and LUs
4. Define gateway clients
5. Start the node
6. Verify that the link is active
7. Establish a session

TN3270E Server Configuration

By configuring a TN3270E server, you are able to exchange data between downstream TCP/IP client workstations running TN3270E (or TN3270) applications and a Systems Network Architecture (SNA) mainframe host computer. The server performs the function of a concentrator, making LU resources from one or more hosts and host PUs available to downstream TN3270E (or TN3270) sessions over any combination of communications media supported by Communications Server.

Before proceeding with this configuration, locate **all** the information listed in “Before You Begin”. If the following configuration steps do not mention some field names that appear on the configuration panels, you can accept the default values for those fields.

Before You Begin

Before you begin this procedure, collect the following information:

- A local node ID (XID) corresponding to the host’s PU (for switched physical media) *or* a local secondary station address corresponding to the host’s PU (for nonswitched physical media)

  A local node ID consists of a block ID followed by a PU ID.

- At least one local LU address available on the same host PU
- Addressing information for contacting the host’s communication controller (such as the token-ring address)

Summary of Steps

To begin configuring, follow the steps listed in “Getting Started” on page 50.

If you have wizards enabled, a wizard will appear for this scenario instead of the window described in “Getting Started” on page 50.

This type of configuration requires the following steps:

1. Node setup
2. Device configuration
3. Define host connections and LUs
4. Define TN3270E server properties
5. Start the node
6. Verify that the link is active
7. Establish a session

TN5250 Server Configuration

By configuring a TN5250 server, you are able to exchange data between downstream client workstations on a TCP/IP network running TN5250 applications and an AS/400 on an SNA network. The server performs the function of a gateway, making AS/400 display sessions available to downstream TN5250 clients over any combination of communications media supported by Communications Server.

Before proceeding with this configuration, locate **all** the information listed in “Before You Begin” on page 54. If the following configuration steps do not mention some field names that appear on the configuration panels, you can accept the default values for those fields.

Before You Begin

Before you begin this procedure, collect the following information:

- At least one AS/400 fully-qualified control point name
- If the AS/400 requires it, a user ID and password needed to access that AS/400
- A partner LU for LEN connections (optional)
- Addressing information for contacting the AS/400 (such as the token-ring address)

Summary of Steps

To begin configuring, follow the steps listed in “Getting Started” on page 50.

This type of configuration requires the following steps:

1. Node setup
2. Device configuration
3. Connection configuration
4. Define AS/400 server properties
5. TN5250 defaults configuration
6. Start the node
7. Verify that the link is active
8. Establish a session

APPN Network Node Configuration

This section describes how to configure the local node as an APPN network node. Network nodes are responsible for maintaining and routing information through an APPN network. They maintain a directory of all resources (LUs) available on directly attached end nodes, as well as maintain a topology of all network nodes in the APPN network. When an independent LU 6.2 session is requested by a node in the network, the network node is responsible for locating the remote resource requested by the session and, once located, for establishing and routing the session between the two nodes.

Before proceeding with this configuration, locate **all** the information listed in “Before You Begin”. If the following configuration steps do not mention some field names that appear on the configuration panels, you can accept the default values for those fields.

Before You Begin

Before you begin this procedure, collect the following information:

- The physical communications media (for example, token ring or X.25) over which links to the APPN network will be established.
- If any low-entry networking (LEN) nodes will be served by this network node, you must obtain each LEN node’s control point (CP) name, as well as any LU names on that node which should be made available to other nodes in the network. LEN nodes do not support APPN, so the network node must ensure that the LEN node’s resources are reachable.
- Determine if this network node will be establishing a link with another node or if other nodes will be calling into this network node. If this network node will establish links into other nodes, the addressing information for those nodes is required (for example, token-ring adapter address).

  You can use the discovery function (available over LAN devices only) to do this.
- Determine if this network node will participate in a connection network (available over LAN devices only). If so, the connection network name is required. Connection networks allow non-adjacent nodes to establish direct links to one another over which sessions will be routed. This method is faster than having the session routed over multiple nodes in the APPN network.
- If you are using AnyNet SNA over TCP/IP:
  – The IP address of your machine
  – The IP address of your gateway or partner
  – The domain name suffix administered by your site administrator.

  See *Network Administration Guide* for more information.

Summary of Steps

To begin configuring, follow the steps listed in “Getting Started” on page 50.

This type of configuration requires the following steps:

1. Node configuration

2. Device configuration
3. Connection configuration
4. Start the node
5. Verify that the link is active
6. Establish a session

DLUR/DLUS Configuration

This task describes the steps to configure Communications Server to support dependent LU sessions over APPN networks. This feature requires that the Communications Server function as a dependent LU requester (DLUR) that requests routing services from a dependent LU server (DLUS), which resides on a host.

Communications Server supports DLUR for local sessions and devices, as well as downstream sessions and devices. Because of these two types, this task includes two subtasks:

- Local DLUR Support
- DLUR Support for Downstream LUs

In either case, the local node must be configured to connect into an APPN network; to do this, use the APPN Network Node Configuration task (see “APPN Network Node Configuration” on page 55). You may also use this task to configure the local node as an APPN end node; to do this, on the Node Setup step, select **End node** as the node type, and disregard the Partner LU 6.2 Configuration step.

Before proceeding with this configuration, locate **all** the information listed in “Before You Begin”. If the following configuration steps do not mention some field names that appear on the configuration panels, you can accept the default values for those fields.

Before You Begin

Before you begin this procedure, collect the following information:

- The fully qualified DLUS name (network name and LU name) representing your primary dependent LU server as defined in VTAM
- The fully qualified backup DLUS name representing your backup dependent LU server, if you have one
- For local DLUR support:
  - A local node ID (XID) corresponding to the host’s PU that will be served by the DLUS

A local node ID consists of a block ID followed by a PU ID.

– At least one available LU address on the host's PU for each session

If you are using AnyNet SNA over TCP/IP:

- The IP address of your machine
- The IP address of your gateway or partner
- The domain name suffix administered by your site administrator.

  See *Network Administration Guide* for more information.

Summary of Steps

To begin configuring, follow the steps listed in "Getting Started" on page 50.

This type of configuration requires the following steps:

Subtask: DLUR Support for Local LUs

1. APPN configuration
   a. Node setup
   b. Device configuration
   c. Connection configuration
2. DLUR PUs configuration
3. Start the node
4. Verify that the link is active
5. Establish a session

Subtask: DLUR Support for Downstream LUs

1. APPN configuration
   a. Node setup
   b. Device configuration
   c. Connection configuration
2. Assign DLUS to clients
3. Start the node
4. Verify that the link is active
5. Establish a session

AnyNet SNA over TCP/IP Gateway Configuration

This section describes the steps to configure Communications Server as an AnyNet SNA over TCP/IP Gateway. The function of the SNA over TCP/IP gateway is to route SNA traffic (independent LU 6.2) between TCP/IP and SNA networks. The SNA over TCP/IP gateway, for example, allows APPC or CPI-C applications running on another AnyNet SNA over TCP/IP access node to communicate with SNA peer nodes on an SNA network.

The AnyNet SNA over TCP/IP Gateway must be configured as an APPN network node. This will allow APPC sessions to be routed to appropriate SNA peer nodes.

If you want to route dependent LU sessions from downstream AnyNet SNA over TCP/IP workstations to upstream hosts, use the SNA Gateway function along with AnyNet SNA over TCP/IP. See “SNA Gateway Configuration” on page 52 to set up the local node for this function.

Do not proceed with Step 1 until you can answer all questions and locate **all** the information in “Before You Begin”.

Before You Begin

Before you begin this procedure, collect the following information:

- The fully qualified LU name(s) (NetworkID.LUName) of the LUs (on the SNA and IP networks) that will be communicating through the AnyNet SNA over TCP/IP gateway(s).
- The IP addresses of the gateway(s) and access node(s) that will be using AnyNet SNA over TCP/IP for communication.

Summary of Steps

To begin configuring, follow the steps listed in “Getting Started” on page 50.

This type of configuration requires the following steps:

1. Node setup
2. Configure AnyNet SNA/IP gateway device
3. Configure other devices
4. Connection configuration
5. Partner LU 6.2 configuration
6. Map the LU names to TCP/IP addresses

7. Start the node
8. Verify that the link is active
9. Establish a session

AnyNet Sockets over SNA Configuration

This section describes the steps to configure Communications Server to support TCP/IP sockets applications over an SNA network. The complexity of this configuration depends on whether Communications Server will connect to an APPN network.

There are two types of AnyNet Sockets over SNA nodes: access nodes and gateway nodes. Access nodes allow TCP/IP sockets applications to run locally and communicate with other access nodes or gateways somewhere in the SNA network. The AnyNet Sockets over SNA gateway serves as a protocol converter, allowing applications on a TCP/IP network to communicate with socket applications running on an access node in the SNA network. Using two gateways, separate TCP/IP networks can be connected across an SNA network.

The steps to configure an AnyNet Sockets over SNA access node and gateway node are identical. In fact, the difference lies in whether or not the sockets application is running locally. The configuration task below will set up the local node for both an AnyNet Sockets over SNA access node and gateway node.

Before proceeding with this configuration, answer all questions and locate **all** the information listed in “Before You Begin”. If the following configuration steps do not mention some field names that appear on the configuration panels, you can accept the default values for those fields.

Before You Begin

Before you begin this procedure, collect the following information:

- A control point name for this node. The name must be unique within the network.
- The name of the network in which this node will operate.

If you are not using APPN and if you do not know what the value should be, you can make up a fictitious name.

- The IP address to assign to this AnyNet Sockets over SNA node and its associated subnet mask. This IP address must be unique among all IP addresses (both Sockets over SNA and native TCP/IP) in the network.

- Will this node operate in an APPN network? If so, will it function as an APPN end node or as an APPN network node? This information is used to set the control point type in Step 1.
- If you are not connecting Communications Server to an APPN network, and you are establishing a session from the local node to another node in the network (instead of receiving a session request from another node), you need the control point name of the remote node and the LU name on that node to establish your session. Step 5 makes use of this information.
- Will you establish an SNA link from this node to another node, or will another node call into this node? If you need to establish a link with another node, then you must know the addressing information for establishing that link. Use Step 3 to configure that link.
- The LU name template and mask to be used by all AnyNet Sockets over SNA nodes in the network. This template and mask is used to generate TCP/IP address–to–LU name mappings.

Summary of Steps

To begin configuring, follow the steps listed in “Getting Started” on page 50.

This type of configuration requires the following steps:

1. Node setup
2. Device configuration
3. Connection configuration
4. Partner LU 6.2 configuration
5. Local TCP/IP address configuration
6. Start the node
7. Start the session

SNA API Client Configuration for APPC

This section describes the steps to configure the Communications Server for supporting SNA API clients. SNA API clients are separate machines from the Communications Server which have the ability to run SNA applications while using the SNA code on the Communications Server node to actually manage the session. Communications Server simply establishes and manages a session as if the origin were the local node, but forwards the application data to the SNA API client instead of to its own application APIs.

SNA API clients give you the ability to run SNA applications without having to install an SNA communications stack, such as the Communications Server for Windows NT, on the same machine. Smaller, less powerful machines can thus be used to run the SNA applications while a centralized, more powerful machine can be dedicated as the SNA server for these SNA API clients.

SNA API clients support two types of applications: APPC (independent LU 6.2) applications and LUA API applications, such as 3270 emulators. For support of LUA applications, see “SNA API Client Configuration for LUA” on page 68 . Configuring for SNA API client support involves two sub-tasks: configuring the Communications Server to support SNA API clients and their applications, and configuring the SNA API client to communicate with Communications Server.

Configuring Communications Server for SNA API Client Support

Before proceeding with this configuration, locate **all** the information listed in “Before You Begin”. If the following configuration steps do not mention some field names that appear on the configuration panels, you can accept the default values for those fields.

This section describes using the configuration interface to configure SNA API clients. If you will be using directory services (LDAP) to provide configuration access across your clients, see “Appendix A. Directory Exploitation” on page 105 for an overview of LDAP as it refers to Communications Server SNA API clients.

Before You Begin

Before you begin configuring Communications Server, collect the following information:

- The user IDs with which the API clients will connect into the local NT system to access Communications Server.
- Determine what type of applications the SNA API clients will run: APPC or 3270 (LUA) applications. This will help you decide which path to take when configuring Communications Server.

Communications Server may be configured to support SNA API clients running both APPC and 3270 applications. Some of the steps will be similar between the two sub-tasks; you may be able to reuse portions of one configuration in the other.

If you are configuring Communications Server to allow SNA API clients to run APPC applications, you must know:

- A control point name for this node. The name must be unique within the network.

If you do not know what value the control point name should take, a good rule of thumb is to use the first 8 characters of the local node's TCP/IP host name, as an example of a unique name, which is found by entering **hostname** on the command line.

- The name of the network in which this node will operate.

If you are not using APPN and do not know what the value should be, you can make up a fictitious name.

- Will this node operate in an APPN network? If so, will it function as an APPN end node or as an APPN network node? This information is used to set the control point type in Step 1.
- If you are not connecting Communications Server to an APPN network, and you are establishing a session from the local node to another node in the network (instead of receiving a session request from another node), you need the control point name of the remote node and the LU name on that node to establish your session. Step 5 makes use of this information.
- Will you establish a link from this node to another node, or will another node call into this node? If you need to establish a link with another node, you must know the addressing information for establishing that link. Use Step 3 to configure that link.
- The local LU 6.2 LUs to be accessed by clients
- The Transaction Programs (TPs), along with their attributes, to be configured on the clients

Configuring Communications Server to Support SNA API Clients Running APPC Applications

Summary of Steps

To begin configuring, follow the steps listed in "Getting Started" on page 50.

This type of configuration requires the following steps:

Configuring Communications Server to support SNA API clients running APPC applications:

1. Node setup
2. Device configuration
3. Connection configuration
4. Local LU 6.2 configuration
5. Partner LU 6.2 configuration
6. Transaction program configuration

Configuring the SNA API client to run APPC applications:

1. Configure global data
2. Configure server location
3. Configure transaction program definition
4. Configure CPI-C side information definition

Testing the configuration:

1. Start the Communications Server node
2. Verify that all configured links are active
3. Establish the connection from the SNA API client

Administering User IDs

You can restrict which SNA API clients can connect with the Communications Server by adding user IDs and global group IDs to the local group IBMCSAPI. Only clients using a user ID under this group will be allowed access to Communications Server.

To define the IBMCSAPI user group and all user IDs and passwords:

1. Invoke the User Manager application for Windows NT 4.0 to view the local system security database. From the Start menu, select **Programs**, **Administrative Tools**.
2. From the groups list, double-click on the IBMCSAPI group, which is created for you during Communications Server installation, to invoke the change dialog for the group. Add the user IDs and global group IDs that you want to give access to, if they are not listed.
3. Exit the User Manager application.

Configuring the SNA API Client to Run APPC Applications

Because SNA API client configuration differs slightly between operating systems, this section will address the steps necessary to configure the SNA API client as generally as possible so as to apply to all operating system clients.

Before proceeding with this configuration, locate **all** the information listed in “Before You Begin”. If the following configuration steps do not mention some field names that appear on the configuration panels, you can accept the default values for those fields.

Before You Begin

Before you begin configuring the SNA API client, collect the following information:

- The user IDs configured in the IBMCSAPI group on the NT system where Communications Server resides.
- The TCP/IP address, IPX name, or host name of the NT system where Communications Server resides.
- If transaction programs on the SNA API client will need to be run by remote SNA nodes, create a transaction program definition in Step 3 under the APPC configuration subtask below.
- If you will be running an APPC application locally, what does it require in terms of session information? Does it require that you specify a partner LU name and mode name as parameters? (You can assign default local LUs and default Partner LUs. Refer to the online *Network Administration Guide* for more information) Does it require that you specify the remote transaction program to execute? Or does it require that you specify a CPI-C Side Information definition for providing all of this information? If a CPI-C Side Information definition is required, Step 4 under the APPC configuration subtask is also required.

Step 1: Configure Global Data

You can configure the user ID and password that will give the SNA API client access to Communications Server. Choose one of the user IDs configured under the IBMCSAPI user group on the Windows NT system where Communications Server resides. If you do not configure the user ID and password, Communications Server prompts the user to supply it each time the client attempts to connect to the server, unless the user logs on to the Windows NT domain with a user ID or password from the IBMCSAPI user group.

Step 2: Configure Server Location

When configuring the server location, choose the type of transport: TCP/IP or IPX. For TCP/IP, specify either the host name or address of the Communications Server machine. For IPX, specify the server name of the Communications Server machine. This will direct the SNA API client to that machine when requesting services from Communications Server.

Step 3: Configure Transaction Program Definition

If an APPC or CPI-C transaction program is to be run locally by remote SNA nodes, a transaction program definition is required. In this definition, specify the TP name by which the application will be known to the SNA network. Also specify the location of the executable file within the SNA API client's file system.

Step 4: Configure CPI-C Side Information Definition

If a CPI-C transaction program is to be run locally by a user and it asks that a CPI-C side information definition be supplied in order to provide session characteristics, then this definition is required. In the CPI-C Side Information definition, you must provide the information which the application cannot gather by itself. You must specify a symbolic destination name by which this definition will be known, and an asterisk (*) for the local LU name. This tells the Communications Server to which the SNA API client will connect to choose on behalf of the client an LU 6.2 LU configured for SNA API client traffic.

You should define a local LU name on the server on the SNA API client if you want the server to run applications to the client.

You must specify the fully qualified (NetworkID.LUName) partner LU name (or partner LU alias) with which the SNA API client will establish a session. You must also provide the remote transaction program to invoke and what mode name to use for providing session parameters.

If you specify a mode other than a provided default mode, that mode definition must exist on Communications Server as well.

When you are finished, save your configuration. The current working configuration is normally called CSNTAPI.INI, but you can save your configuration under a different name. To use a renamed configuration, set the environment variable CSNTAPI. For example, to use the configuration named *MYCONFIG.INI*, use the command `SET CSNTAPI=MYCONFIG`.

You can also use configuration files in other directories, including shared files in remote directories. To use the configuration *CSNTUSER.INI* in a remote directory *P:\MYUSER*, use the command `SET CSNTAPI=P:\MYUSER\CSNTUSER.INI`.

Testing the Configuration

Step 1: Start the Communications Server node

Start the SNA Node Operations application under the Communications Server program group if it is not already started. Click **Start** on the toolbar to start the local node. Specify the configuration file you used earlier in this task. It may take a moment for the node to start and to establish all the defined links.

Step 2: Verify that all configured links are active

If you configured any connection definitions for Communications Server, such as a host link, ensure that these start successfully by clicking on **Connections** from the toolbar. Any configured links should be shown in the list box. If they do not become active after a short period of time, ensure that the remote nodes are ready to receive link activation requests from Communications Server.

If you are configured as a network node, it may be that a remote node must start a link with Communications Server in order to connect into an APPN network, in which case no link definitions are necessary on Communications Server. Ensure that any remote nodes with links defined to Communications Server have been started.

Once Communications Server has been started and all links into the SNA network have been established, you are ready to have your SNA API client connect with Communications Server.

Step 3: Establish the connection from the SNA API client

If you are running an APPC or LUA application locally, a connection to Communications Server will be established when the application is started.

If you are using the SNA API client for Windows 95 or Windows NT, you can use the LU 6.2 Connection Tester utility to test the connection. Click the **LU62 Connection Tester** icon in the SNA API client folder to start the utility. The connection tester attempts to open a connection between the client and the server using the current configuration. If the connection completes successfully, a window appears with information about the connection. If the connection does not complete successfully, the connection tester provides an error message that includes probable reasons the connection failed. The connection tester is designed to enable you to check the connection between the client and the server that LU 6.2 applications residing on the client will use. It does not determine the status of the complete connection between the client APPC node and eventual partner APPC nodes.

If you have applications on the SNA API client to which you want to give other SNA nodes access, start the Attach Manager application. Attach Manager automatically starts transaction programs configured to start with Attach Manager.

SNA API Client Configuration for LUA

This section describes the steps to configure the Communications Server for supporting SNA API clients. SNA API clients are separate machines from the Communications Server which have the ability to run SNA applications while using the SNA code on the Communications Server node to actually manage the session. Communications Server simply establishes and manages a session as if the origin were the local node, but forwards the application data to the SNA API client instead of to its own application APIs.

SNA API clients give you the ability to run SNA applications without having to install an SNA communications stack, such as the Communications Server for Windows NT, on the same machine. Smaller, less powerful machines can thus be used to run the SNA applications while a centralized, more powerful machine can be dedicated as the SNA server for these SNA API clients.

SNA API clients support two types of applications: APPC (independent LU 6.2) applications and LUA API applications, such as 3270 emulators. For support of APPC applications, see “Configuring the SNA API Client to Run APPC Applications” on page 64. Configuring for SNA API client support involves two sub-tasks: configuring the Communications Server to support SNA API clients and their applications, and configuring the SNA API client to communicate with Communications Server.

Before proceeding with this configuration, locate **all** the information listed in “Before You Begin”. If the following configuration steps do not mention some field names that appear on the configuration panels, you can accept the default values for those fields.

Configuring Communications Server for SNA API Client Support

Before You Begin

Before you begin configuring Communications Server, collect the following information:

- The user IDs and passwords with which the API clients will connect into the local NT system to access Communications Server.
- Determine what type of applications the SNA API clients will run: APPC or 3270 (LUA) applications. This will help you decide which path to take when configuring Communications Server.

Communications Server may be configured to support SNA API clients running both APPC and 3270 applications. Some of the steps will be similar between the two sub-tasks; you may be able to reuse portions of one configuration in the other.

SNA API Client Configuration for LUA

If you are configuring Communications Server to allow SNA API clients to run 3270 (LUA) applications, you must know:

- A local node ID (XID) corresponding to the host's PU (for switched physical media) *or* a local secondary station address corresponding to the host's PU (for nonswitched physical media)

  A local node ID consists of a block ID followed by a PU ID.

- At least one local LU address available on the same host PU
- Addressing information for contacting the host's communication controller (such as the token-ring address)
- The LU pool that will be the default pool for client usage, if any

Summary of Steps

To begin configuring, follow the steps listed in "Getting Started" on page 50.

This type of configuration requires the following steps:

Configuring Communications Server to support SNA API clients running 3270 or other LUA applications:

1. Node setup
2. Device configuration
3. Connection configuration
4. Define host connections and LUs
5. Enable SNA API client support

Configuring the SNA API client to run 3270 or other LUA applications:

1. Configure global data
2. Create an LUA definition

Testing the configuration:

1. Start the Communications Server node
2. Verify that all configured links are active
3. Establish the connection from the SNA API client

Configuring Communications Server to Support SNA API Clients Running 3270 or Other LUA Applications

Administering User IDs

You can restrict which SNA API clients can connect with the Communications Server by defining user IDs and passwords under the user group IBMCSAPI. Only clients using a user ID under this group are allowed access to Communications Server. See "Administering User IDs" on page 64 for information about how to define this group.

Configuring the SNA API Client to Run 3270 or Other LUA Applications

Because SNA API Client configuration differs slightly between operating systems, this section will address the steps necessary to configure the SNA API client as generally as possible so as to apply to all operating system clients.

Before proceeding with this configuration, locate **all** the information listed in "Before You Begin". If the following configuration steps do not mention some field names that appear on the configuration panels, you can accept the default values for those fields.

Before You Begin

Before you begin configuring the SNA API client, collect the following information:

- The user IDs and passwords configured in the IBMCSAPI group on the Windows NT system where Communications Server resides.
- The TCP/IP address or host name of the NT system where Communications Server resides.
- The LU name of an LU 0 to 3 LU configured on Communications Server if you require a specific LU address. If you do not, you may configure the SNA API client to simply request the next available LU in the default pool.

Step 1: Configure Global Data

You can configure the user ID and password that will give the SNA API client access to Communications Server. Choose one of the user IDs configured under the IBMCSAPI user group on the Windows NT system where Communications Server resides. If you do not configure the user ID and password, Communications Server prompts the user to supply it each time the client attempts to connect to the server, unless the user logs on to the Windows NT domain with a user ID and password from the IBMCSAPI user group.

Step 2: Create an LUA Definition

When creating the LUA definition, give a meaningful session name by which this definition will be known. You must configure a line within this definition for each application you want to run concurrently on the SNA API client.

For TCP/IP, specify the host name or address of the Communications Server machine on each line. For IPX, specify the server name of the Communications Server machine on each line.

Also, specify whether the session should use a dedicated LU or an LU from the default pool. If you specify that a dedicated LU be used, provide the LU name as configured in Communications Server. The easiest configuration is to specify that an available LU be chosen from the default pool, which was configured as the PUBLIC pool on Communications Server. If the definition requires you to specify a pool name, use PUBLIC.

When you are finished, save your configuration. The current working configuration is usually called CSNTAPI.INI, but you can save your configuration under a different name. To use a renamed configuration, set the environment variable CSNTAPI. For example, to use the configuration named *MYCONFIG.INI*, use the command `SET CSNTAPI=MYCONFIG`.

You can also use configuration files in other directories, including shared files in remote directories. To use the configuration *CSNTUSER.INI* in a remote directory *P:\MYUSER*, use the command `SET CSNTAPI=P:\MYUSER\CSNTUSER.INI`.

Testing the Configuration

Step 1: Start the Communications Server Node

Start the SNA Node Operations application under the Communications Server program group if it is not already started. Click **Start** on the toolbar to start the local node and specify the configuration file you used earlier in this task.

Step 2: Verify that All Configured Links Are Active

If you configured any connection definitions for Communications Server, such as a host link, ensure that these start successfully by clicking on **Connections** from the toolbar. Any configured links should be shown in the list box. If the links do not become active after a short period of time, ensure that the remote nodes are ready to receive link activation requests from Communications Server.

If your machine is configured as a network node, it may be that a remote node must start a link with Communications Server in order to connect into an APPN network, in which case no link definitions are necessary on Communications Server. Ensure that any remote nodes with links defined to Communications Server have been started.

After Communications Server has been started and all links into the SNA network have been established, you are ready to have your SNA API client connect with Communications Server.

Step 3: Establish the Connection from the SNA API Client

If you are running an APPC or LUA application locally, a connection to Communications Server will be established when the application is started.

If you have applications on the SNA API client to which you want to give other SNA nodes access, you need to start the Attach Manager application. Attach Manager automatically starts transaction programs configured to start with Attach Manager.

CPI-C or APPC Configuration

This section describes the steps to configure Communications Server to support CPI-C or APPC applications (for example, APPC3270 or 5250 emulation to an AS/400 system). APPC networking is very flexible and versatile and, therefore, it can be complicated. The complexity of this configuration depends on how you will use Communications Server and how much work your application will do for you.

Only the following steps are absolutely required: Step 1 (Node Setup) and Step 2 (Device Configuration). The remaining steps may also be required, depending on your responses to the questions in “Before You Begin”.

Read **all** of the documentation that came with your application before proceeding with this configuration. There are a number of questions which you must answer before proceeding, and your application documentation can help you answer them.

Before You Begin

Before you begin this procedure, collect the following information:

- A control point name for this node. The name must be unique within the network.

- The name of the network in which this node will operate.

  If you are not using APPN and if you do not know what the value should be, you can make up a fictitious name.

- Will this node operate in an APPN network? If so, will it function as an APPN end node or as an APPN network node? This information is used to set the control point type in Step 1.
- Will you run APPC applications (such as 5250 emulators) locally? If so, you do not need to create a Transaction Program definition, and Step 4 is not required.

  However, if you will be configuring applications for other nodes to access, Step 4 is required.
- If you are not connecting Communications Server to an APPN network, and you are establishing a session from the local node to another node in the network (instead of receiving a session request from another node), you need the control point name of the remote node and the LU name on that node to establish your session. Step 5 makes use of this information.
- If you are running an APPC application locally, what does it require in terms of session information? Does it require that you specify a partner LU name and mode name as parameters (to the application itself, not the Communications Server)? Or does it require that you specify a CPI-C Side Information Profile? If it requires that you specify a CPI-C Side Information Profile, Step 6 is required.
- Will you establish a link from this node to another node, or will another node call into this node? If you need to establish a link with another node, then you must know the addressing information for establishing that link. Use Step 3 to configure that link.
- If you are using AnyNet SNA over TCP/IP:
  - The IP address of your machine
  - The IP address of your gateway or partner
  - The domain name suffix administered by your site administrator.

    See *Network Administration Guide* for more information.

Summary of Steps

To begin configuring, follow the steps listed in “Getting Started” on page 50.

This type of configuration requires the following steps:

1. Node setup
2. Device configuration
3. Connection configuration
4. Transaction program configuration

5. Partner LU 6.2 configuration
6. CPI-C side information configuration
7. Start the node
8. Verify that the link is active
9. Start the session

Dependent LU 6.2 Sessions to a Host

This section describes the steps to configure Communications Server to support dependent LU 6.2 sessions with a host's PU.

Before proceeding with this configuration, locate **all** the information listed in "Before You Begin". If the following configuration steps do not mention some field names that appear on the configuration panels, you can accept the default values for those fields.

Before You Begin

Before you begin this procedure, collect the following information:

- A local node ID (XID) corresponding to the host's PU (for switched physical media) *or* a local secondary station address corresponding to the host's PU (for nonswitched physical media)

  A local node ID consists of a block ID followed by a PU ID.

- A single LU 6.2 address available on the same host PU
- The partner LU name corresponding to the application you want to use on the host
- Addressing information for contacting the host's communication controller (such as the token-ring address)
- If you are using AnyNet SNA over TCP/IP:
  - The IP address of your machine
  - The IP address of your gateway or partner
  - The domain name suffix administered by your site administrator.

    See *Network Administration Guide* for more information.

Summary of Steps

To begin configuring, follow the steps listed in "Getting Started" on page 50.

This type of configuration requires the following steps:

1. Node setup
2. Device configuration
3. Define host connections and LUs
4. CPI-C side information configuration
5. Start the node
6. Verify that the link is active
7. Start the session

3270 Configuration

This section describes the steps to configure Communications Server for a 3270 session with a host. For APPC 3270 configuration, go to “CPI-C or APPC Configuration” on page 72.

Before proceeding with this configuration, locate **all** the information listed in “Before You Begin”. If the following configuration steps do not mention some field names that appear on the configuration panels, you can accept the default values for those fields.

Before You Begin

Before you begin this procedure, collect the following information:

- A local node ID (XID) corresponding to the host’s PU (for switched physical media) *or* a local secondary station address corresponding to the host’s PU (for nonswitched physical media)

  A local node ID consists of a block ID followed by a PU ID.

- At least one local LU address available on the same host PU
- Addressing information for contacting the host’s communication controller (such as the token-ring address)
- If you are using AnyNet SNA over TCP/IP:
  - The IP address of your machine
  - The IP address of your gateway or partner
  - The domain name suffix administered by your site administrator.

    See *Network Administration Guide* for more information.

Summary of Steps

To begin configuring, follow the steps listed in “Getting Started” on page 50.

This type of configuration requires the following steps:

1. Node setup
2. Device configuration
3. Define host connections and LUs
4. Start the node
5. Verify that the link is active
6. Start the application

Focal Point Configuration

Use this section to define remote focal point locations for routing alert information for specific management services applications. The local node will locate remote focal points through an APPN network, so you must configure the local node to operate there; to accomplish this, use “APPN Network Node Configuration” on page 55. You may also use this task to configure the local node as an APPN end node; to accomplish this, select **End node** as the node type and disregard the Partner LU 6.2 Configuration step.

Before proceeding with this configuration, locate **all** required information listed in “Before You Begin”. If the following configuration steps do not mention some field names that appear on the configuration panels, you can accept the default values for those fields.

Before You Begin

Before you begin this procedure, collect the following information:

- The control point name of the primary focal point
- The control point name of the backup focal point, if applicable
- The management services category for which you want to forward alert data to the specified focal point
- The applications on the focal points which are used to process the alert data

Before you continue, make sure that the local node is configured to connect into an APPN network as described above. The following steps assume that local node configuration is complete.

Summary of Steps

To begin configuring, follow the steps listed in "Getting Started" on page 50.

This type of configuration requires the following steps:

1. Node setup
2. Device configuration
3. Connection configuration
4. Focal-point configuration
5. Start the node
6. Verify that the link is active
7. Establish a session

AS/400 Shared Folders Configuration

Use this section to define disk devices on the server that communicate with AS/400 folders through the AS/400 integrated file system (IFS). If the server shares these disk devices, clients can NET USE to them; that is, use them as if they were drives on the client workstations.

Before proceeding with this configuration, locate **all** required information listed in "Before You Begin". If the following configuration steps do not mention some field names that appear on the configuration panels, you can accept the default values for those fields.

Before You Begin

Before you begin this procedure, collect the following information:

- At least one local LU address available on the same host's PU
- Addressing information for contacting the AS/400
- The path to a folder you want to provide access to in the AS/400 Integrated File System

Summary of Steps

To begin configuring, follow the steps listed in "Getting Started" on page 50.

This type of configuration requires the following steps:

1. Node setup
2. Device configuration
3. Peer connection configuration

4. AS/400 server definition
5. Local LU 6.2 configuration
6. Configure modes
7. Connection network configuration
8. Start the node
9. Verify that the link is active
10. Establish a session

Chapter 5. Using Communications Server

Use the SNA Node Operations application of Communications Server to start, stop, and monitor resources in your network.

Starting Communications Server

1. From the Start menu, select **Programs**, **IBM Communications Server**, then **SNA Node Operations**.
2. The Communications Server SNA Node Operations window appears. Either click **Operations** and then click **Start Node**, or click the Start/Stop Node icon.
3. The Open File window appears. Select the appropriate configuration.
4. Click **Open** to start the node.

After the node is started, you can close the Node Operations panel.

Alternatively, you can use the **csstart** command to start Communications Server. See "Command Line Utilities" on page 87 for details.

Stopping Communications Server

To stop all Communications Server connections and any application or emulator sessions that you are supporting through the server:

1. From the Start menu, select **Programs**, click **IBM Communications Server**, and then click **SNA Node Operations**.
2. The Communications Server SNA Node Operations window appears. Click **Operations**, then **Stop Node**, or click the Start/Stop Node icon.
3. Click **OK** at the verification prompt.

Alternatively, you can use the **csstop** command to stop Communications Server. See "Command Line Utilities" on page 87 for details.

Replacing the Default Configuration

You can define more than one Communications Server configuration and then switch between configurations as your needs require.

When you start Communications Server, the default configuration is offered as the first choice for node configuration or node operation unless you specify another configuration. After you complete a new configuration, you can replace the default configuration with your new one.

To replace a default configuration file,

1. Open the configuration file that you want to use as your new default.
2. From the Start Menu, select **Programs**, click **IBM Communications Server**, then click **SNA Node Configuration**.
3. The SNA Node Configuration window appears. Click **File**, then click **Open**.
4. Select the file you want to use as the default.
5. Click **File** and then click **Save**.
6. A message will ask you to confirm that you want to use the new file as the default. Click **Yes**.

Use SNA Node Operations to apply your new configuration and ensure that the relevant part of the product runs as you have configured it.

If you have errors in configuration reflected at run time, you can get error messages at this time. Refer to the help for the error message for more information.

SNA Node Operations

SNA Node Operations enables you to display information about Communications Server resources and to manage these resources. The following tasks are supported:

- Starting and stopping resources
- Deleting resources
- Displaying resource information
- Changing session limits
- Adding and modifying select resources

Using the tree view on the SNA Node Operations panel, you can select to manage or display information on the following resources:

- Relational View

  Provides an alternate view of your configuration that shows the hierarchical relationship between sessions, connections, LUs, devices, and data link controls.
- Devices and DLCs

Data link controls (DLCs)
Shows how data is formatted for transmission on the physical connection.

Devices
Shows the workstation hardware, such as adapters, that is used to transmit and receive data.

- Connections

Downstream Connections
Shows connections to downstream nodes

Host Connections
Shows connections to the host

Peer Connections
Shows link stations to the adjacent nodes.

- Host resources

DLUR PUs
Shows dependent logical unit requester (DLUR) physical units (PUs), which are PUs in an APPN end node that own dependent LUs, but request that a dependent LU server provide the SSCP services for those dependent LUs.

Host Pools
Displays the host pools that are currently defined.

Local LU 0 to 3
Shows local logical units (LUs) type 0, 1, 2, or 3, which are dependent LUs on the workstation that provide services for 3270 terminal and printer emulation applications.

PU2.0/DLUR Gateway
Displays information about SNA downstream workstations and the connections to them. Also shows information about the dependent LU requester services.

- TN3270E server

TN3270E Summary
Displays a summary of settings and client connections for the TN3270E server, including the number of active and inactive connections.

TN3270E Sessions
Displays and enables you to stop TN3270E server client connections.

TN3270E Filter Settings
Displays information about IP filters that are configured for the TN3270E server.

- TN5250 server

  TN5250 Ports
  Displays the IP ports used by the TN5250 server and the AS/400s associated with each port.

  TN5250 Summary
  Displays a summary of settings and client connections for the TN5250 server, including the number of active and inactive connections.

  TN5250 Sessions
  Displays and enables you to stop TN5250 server client connections.

  TN5250 Filter Settings
  Displays information about IP filters that are configured for the TN5250 server.

- CPI-C and APPC

  Partner LU 6.2
  Shows remote computers that communicate through an APPC session with local LU 6.2s.

  Local LU 6.2
  Shows local logical units (LUs) type 6.2, which are independent or dependent LUs that provide APPC services.

  LU 6.2 Sessions
  Shows sessions that transport data between two partner LU 6.2s. Conversations between transaction programs use LU 6.2 sessions.

  Modes
  Displays names used by the initiator of a session to designate the characteristics desired for the session, such as traffic pacing values, message-length limits, sync point and cryptography options, and the class of service (COS) within the transport network.

  Transaction Programs
  Shows programs that process transactions in an SNA network. There are two kinds of TPs: application transaction programs and service transaction programs.

  CPI-C Side Information
  Shows a set of parameters that are associated with a specified symbolic destination name.

- APPN options

  Connection Networks
  Shows APPN nodes in a LAN that have direct links with each other without requiring logical link definitions at each node.

Focal Points
Shows systems that provide centralized network management services.

Intermediate Sessions
Shows APPN network nodes that can pass information, but whose end points are elsewhere.

Directory Entry
Shows information on each LU known at the network node, including local LUs, as well as LUs discovered by CP-to-CP sessions to end nodes.

Topology
Shows the topology of the SNA network when the network is configured as a network node. Information is provided on all network nodes and links in the network.

- Hot standby

Critical Servers
Displays definitions and status information for configured critical servers.

Backup Servers
Displays definitions for backup servers.

- AnyNet

AnyNet Sockets Statistics
Displays statistics associated with the AnyNet Gateway function.

AnyNet Sockets Devices
Shows the currently defined sockets devices on a system.

AnyNet Sockets Connections
Shows information about Sockets over SNA access node sockets and gateway connections.

AnyNet IP to LU Mapping
The IP Address to LU Mapping resource shows attributes used to map an IP address to an LU name.

AnyNet Sockets Routes
Shows the AnyNet routes through the network.

Using the Menu Bar

From the menu bar, select one of the following:

Operations
Starts or stops an SNA node. To start a node, you must also specify the configuration file you want to use.

Sets or changes session limits (CNOS). Click the appropriate item to manage the session limits on a mode between the local LU and a partner LU.

Applies an additional configuration file to the active node. Select the configuration file you want to use.

Server Connects to a remote Communications Server. TCP/IP or NetBIOS needs to be running and configured so that the client and server can access TCP/IP for using sockets. The TCP/IP hostname, IP address, or machine name of the server is used to establish the connection with the server. You can connect to several servers at the same time.

You need a user ID and password to connect to the remote server. The user ID must be a member of the IBMCSADMIN user group to be authorized to administer the server. The user ID you logged on with is used initially to log on to the remote server. If this ID is not authorized, Communications Server prompts you to enter an ID and password.

To connect to a remote Communications Server, do *one* of the following:

- Select **Other** on the Server menu and enter the name of the server to which you want to connect, or
- Select **Other** on the Server menu and click the **Discover** button to discover Communication Servers. The discovered servers will be in a dialog box. You can select one of the servers in the list if you want to connect to it, or
- Choose the multiple node view from the toolbar. All discovered servers are displayed in the left side of the split screen.

To connect to the local Communications Server, choose the **Local** option on the menu.

Launch

Launches other Communications Server programs, such as Log Viewer, Trace Facility, or SNA Node Configuration. For more information on Log Viewer, see “Viewing Communications Server Logs” on page 95. For more information on Trace Facility, see “Obtaining Trace Data on the Server” on page 95. For more information on SNA Node Configuration, see “Chapter 4. Configuring Communications Server” on page 49.

View Turns off or on the tool bar or status bar of your Communications Server window

Refreshes the display of resources.

Specifies the view displayed: single node, multiple node, or custom group.

Window

Manages the multiple windows within the Node Operations main window.

To open a new window, either choose New Window from this menu or click on the right icon on the tool bar.

Displaying a Resource

To display a resource, select a resource from the hierarchical view on the left side of the split screen. The data is displayed on the right side of the split screen.

Starting a Resource

To start a resource:

1. Select a resource from the hierarchical view on the left side of the split screen.
2. Click the right mouse button on the resource icon on the right side of the split screen to display the action shortcut menu.
3. Click **Start** to start the resource. A started (active) resource can be stopped, but not deleted.

Stopping a Resource

To stop a resource:

1. Select a resource from the hierarchical view on the left side of the split screen.
2. Click the right mouse button on the resource's icon to display the action shortcut menu.
3. Click **Stop** to suspend the resource. If a resource is stopped (inactive), it can be deleted or redefined.

Modifying a Resource

To delete a resource:

1. Select a resource from the hierarchical view on the left side of the split screen.
2. Click the right mouse button on the resource's icon to display the action shortcut menu.
3. Click **Modify** to bring up the configuration window for the resource.

Deleting a Resource

To delete a resource:

1. Select a resource from the hierarchical view on the left side of the split screen.
2. Click the right mouse button on the resource's icon to display the action shortcut menu.
3. Click **Delete** to delete the resource.

A resource to be redefined need not be deleted, but it should be stopped (inactive).

Updating SNA Resources Dynamically

It is not necessary to delete an SNA resource before redefining it. A resource must be inactive, however, when you redefine it. To redefine resources, use the Apply New Configuration selection under the SNA Node Operations **Operations** menu.

If a redefinition is rejected for a reason other than that the resource is active, check the message log for details. Most rejections are due to inconsistencies in the configuration, such as one of the following:

- Attempting to define a link station with the adjacent CP name set to the local CP name.
- Attempting to define two link stations on a non-switched port with the same destination address.

Such rejections occur regardless of whether you are defining a resource for the first time or redefining it.

Keep in mind the following when redefining resources:

- You may not change the ls_role of a port that has link stations defined on it. The link stations must be deleted before the port role can be changed (because a link station may default to the port ls_role).
- You may not change the type of a named DLC. The DLC definition must be deleted before the same name can be reused for a DLC of a different type.

Remote Operations

By default, the administration tools (Node Operations, Node Configuration, Configuration Verification, and Log Viewer) run locally on the Communications Server machine that is being administered. However, you may use the tools to administer Communications Servers running on remote machines. You can administer remote Communications Servers either from a machine that has Communications Server installed or from a machine that has only the Administration Client installed.

Use the Server menu in Node Operations and Node Configuration to select and connect to a remote Communications Server machine. This remote connection uses the TCP/IP or NetBIOS protocol. All the queries and actions you select are performed against the remote machine.

The remaining administration tools (Configuration Verification and Log Viewer) are not enabled to directly connect to a remote machine. These applications all operate on files, so you need access to the appropriate files on the remote server. You can get access to the configuration files and log files by using the file server capabilities of Windows NT to share the Communications Server installation directory, then mapping a drive to this shared directory from the administration machine. This enables you to view or update files directly.

An alternative way to administer Communications Server remotely is to use the Web Administration facility. Most of the Node Operations functions are available through a Web browser. This facility can be installed from the Communications Server CD-ROM.

Performing Administrative Tasks on the Communications Server

Some administrative tasks for Communications Server can only be completed by a person with a user ID that is contained in the IBMCSADMIN user group. Your user ID must be in IBMCSADMIN if you want to:

- Remotely configure and manage the server
- Delete SNA resources through SNA Node Operations
- Stop SNA resources through SNA Node Operations.

During the installation procedure, the IBMCSADMIN group is established and one user ID is placed in this group. Use the Windows NT User Manager to add additional user IDs to this group as needed. Refer to the Windows NT documentation for more information on the User Manager.

Command Line Utilities

You can use the following Communications Server commands:

`CSDISPLAY resource [object_id] [/D#]`

Displays information about Communications Server resources, where:

resource

Is one of the following:

AIL	AnyNet IP to LU mapping
ASC	AnyNet Sockets IP connections
ASD	AnyNet Sockets devices
ASR	AnyNet Sockets routes
AST	AnyNet Sockets statistics
BSV	Hot Standby backup servers
CNT	Connection networks
CON	Connections
CPS	CPI-C side information
CRL	Critical server connections
CRS	Host Standby Critical servers
DCN	Downstream connections
DLC	Data link controls
DEV	Devices
DIR	Directory services
DPU	DLUR PUs
FPT	Focal points
HCN	Host connections
INT	Intermediate sessions
LU0	Local LU 0 to 3
L62	Local LU 6.2
L6S	LU 6.2 sessions
MOD	Modes
NNS	Network node statistics
NOD	Nodes
PCN	Peer connections
PLU	Partner LU 6.2
PDG	PU 2.0/DLUR gateways
RTP	RTP connections
TOP	Topology
TRP	Transaction programs

3FS TN3270E filter settings

3SS TN3270E sessions

3SY TN3270E summary

5FS TN5250 filter settings

5PT TN5250 ports

5SS TN5250 sessions

5SY TN5250 summary

object_id
Specifies a case-sensitive value (for example, LU001 or LINK001) to search for. Only objects whose first attribute matches this value are displayed.

/D# Specifies the level of detail to display. The # is a number between 1 and 3, where 1 is the lowest level of detail and 3 shows all information. 2 is the default.

`CSLIC [ number ]`
Enables you to update the number of concurrent licenses that you have purchased. If `number` is not supplied as a parameter, the following information is displayed:

- Number of licenses purchased
- Number of licenses in use
- Highest number of licenses ever used

`CSMODIFY resource object_id action`
Enables you to control Communications Server resources, where:

resource
Is one of the following:

BSV Hot Standby backup servers. You can start or stop monitoring this resource.

CON Connections. You can start, stop, or delete this resource.

CPS CPI-C side information. You can delete this resource.

CRL Hot Standby critical server connections. You can start or stop monitoring this resource.

CRS Hot Standby critical servers. You can start or stop monitoring this resource.

DLC Data link controls. You can start, stop, or delete this resource.

DEV Devices. You can start, stop, or delete this resource.

DPU DLUR DPUs. You can start or stop this resource.

LU0 Local LU 0 to 3. You can delete this resource unless the LU is in use.

L62 Local LU 6.2. You can delete this resource.

L6S LU 6.2 sessions. You can stop this resource unless a CP-CP session is active.

PDG PU 2.0/DLUR gateway. You can delete this resource, unless a downstream LU is in use.

RTP RTP connections. You can switch the path of this resource.

3SS TN3270E Sessions. You can stop this resource normally.

5SS TN5250 Sessions. You can stop this resource normally.

object_id
Specifies a case-sensitive value (for example, LU001 or LINK001) to search for. Only objects whose first attribute matches this value are displayed.

action One of the following:

SN	Normal stop
SI	Immediate stop
ST	Start
DL	Delete
PS	Path switch
TH	Start Hot Standby monitor
PH	Stop Hot Standby monitor

`CSQUERY [ -p | -q ]`
Queries the status of the Communications Server. If the **-p** flag is used, all messages are shown in a message box. Messages are written to the standard output device (usually the screen) by default. The **-q** flag suppresses all output. Along with the running or stopped status, the default and active configuration file names are shown. If the server is running, CSQUERY returns zero, otherwise a non-zero value is returned.

`CSSTART [-p | -q ] [-a | -m | -d] [cfgfile]`
Starts Communications Server with a specified configuration.

CSSTART has a user exit capability that enables you to start other processes when the node is started. If there is a batch file named csntstart.bat in the Communications Server directory (usually C:/IBMCS), it is run after the node is started. You can put any command in this batch file, such as a command to start the NNLINKS program.

If the **-p** flag is used, all messages are shown in a message box. Messages are written to the standard output device (usually the screen) by default. The **-q** flag suppresses all output.

The **-a** flag enables automatic start up after rebooting the machine. The **-m** flag disables automatic start up. The **-d** flag makes the configuration file name specified in **cfgfile** the default.

The **cfgfile** parameter is the full path name of the configuration file you want to use to start the product. If no path is specified, the path is assumed to be in the Communications Server installation directory under the private subdirectory (C:\ibmcs\private for example). If no file extension is specified, .acg is assumed. If no **cfgfile** parameter is specified, the default configuration file is used. If no default configuration file has been set, an error is reported. If the server is successfully started, CSSTART returns zero; otherwise a non-zero value is returned.

CSSTOP [-p | -q]

Stops Communications Server. If the **-p** flag is used, all messages are shown in a message box popup. Messages are written to the standard output device (usually the screen) by default. The **-q** flag suppresses all output. If the server is successfully stopped, CSSTOP returns zero; otherwise a non-zero value is returned.

Chapter 6. Problem Determination and Reporting

This chapter describes the information that will help you to solve a problem, to recognize a problem accurately before reporting it to your system administrator, or to report a problem to IBM.

These are the processes that you should follow:

1. Problem determination (PD)
2. Problem-source identification (PSI)
3. Viewing message logs
4. Obtaining trace data
5. Problem reporting (PR)

Problem Determination (PD)

Problem determination (PD) is the first stage in solving your problem.

Symptoms

You recognize there are differences between what you expect to see and what you do see.

Environment

Identify the environment in which the problem occurs:

- Communications Server configuration
  - Communications Server version and CSD level
  - The name of the SNA Node configuration file
- Workstation configuration
  - The machine type and model, the system memory, the video adapter
  - The communication adapter you are using
  - Other adapters (especially communication adapters) installed
  - Other devices installed, such as sound cards, modems, or fax machines
- Software configuration
  - Windows NT version, level, and fix packs (if any)
  - Communication device-driver version and level
  - Other communication programs (such as Novell NetWare, Microsoft SNA Server, or Microsoft Data Link Control) that are running and using resources

Problem Type

Categorize your problem into one of the following types:

1. **Installation Problem**. Note the error message and take the appropriate action as described in the online help.
2. **Configuration or Setup Problem**. If Communications Server did not connect to the remote node, verify that your hardware, software, and Communications Server configurations are correctly set up for your environment. To help you to isolate what is wrong, look up any error messages in the online help. Refer to other sources, such as the online *Network Administration Guide*, for detailed information.
3. **Operational Problem**. Although you were able to connect to the remote node, you might have difficulty doing some operations or using a certain Communications Server function. Look up any error messages in the online help, and study this manual to see how the operation should be performed.

Problem Area

You also need to identify where the problem is:

- Installation and configuration
- Node Operations
- API
- Other Communications Server functional area

Problem Re-Creation

As the final step of the problem determination process, try to re-create the problem. The problem re-creation procedure and the probability of the recurrence of the problem are key factors in isolating it. If the problem is intermittent, any factor that you think is related to it becomes important information.

Problem-Source Identification (PSI)

The second stage is to try to identify the real cause of the problem; this depends largely on the problem area:

1. **Installation and configuration**. Make sure that your workstation hardware and software are configured correctly. You might also need to contact your system administrator to verify that your Communications Server setup values are correct for your system.
2. **Node operations**. Identify the operation you are having a problem with:
   - Starting resources

- Stopping resources
- Displaying resources
- Using the Log Viewer
- Using the Trace Facility

3. **API**. The cause could be in an application that uses an API, or the problem could be in Communications Server. Identify which of these is causing the problem. The API trace might also help you to identify the source of the problem.
4. **Other Communications Server functional area**. Make sure that you can explain why you think that the source of the problem is in Communications Server.

Viewing Communications Server Logs

The Communications Server Log Viewer utility enables you to view information contained in a Communications Server log. You can use the viewer during problem determination to view the messages in the message log. The default name of the message log output file is PCSMSG; its file extension must be .MLG.

To view messages in a message log:

1. From the SNA Node Operations window, click **Log Viewer**.
2. From the list of logged messages, double-click on a message number to display message help.

Note: The Windows NT Application Event Log will indicate if there was a problem logged for Communications Server. Start there to determine if the problem lies with Communications Server or another product.

Obtaining Trace Data on the Server

The Communications Server trace facility enables you to log trace information for certain Communications Server functions, which can be useful in identifying the source of problems. After formatting, the trace data is saved to a file. You can view this file with your own editor, then send it to IBM.

To start a trace, follow these steps:

1. From the SNA Node Operations window, click **Trace Facility**. The trace status on the title bar displays the current state:

   Active Trace data is being collected by the trace facility.

Inactive
No trace data is being collected. The trace facility is not ready to collect data.

2. From the Trace Facility window that appears, select the type of data you want to trace from the Function Name, Component Name, and Trace Options lists. You can trace multiple functions and components, as well as multiple trace options for the various components.

   Function Name
   A specific set of Communications Server features, such as User Services.

   Component Name
   The name of a specific part of a function, such as Node Initialization (for the User Services function).

   Trace Options
   The options associated with a particular component, such as API trace (for the Node Initialization component).
3. Start tracing data by clicking **Start**, or apply changes to the trace options by clicking **Apply**.
4. Run the operation that you want to trace.
5. Optionally, stop the trace by clicking **Stop**.
6. Save the trace data to your hard disk by clicking **Save**.
7. Click **Format** to specify a formatted trace file name and to format the trace data. Click **OK**.
8. Click **Clear** to clear the trace buffer where you save a trace.

Obtaining Trace Data on the SNA API Client

The Communications Server trace facility enables you to log trace information for certain Communications Server functions, which can be useful in identifying the source of problems. After formatting, the trace data is saved to a file. You can view this file with your own editor, then send it to IBM.

To start a trace on the Windows 95, Windows NT, or OS/2 client, follow these steps:

1. Double-click the trace icon in the client folder.
2. Click **Start** to turn on tracing with the current settings. Tracing begins immediately.
3. Once you have captured the information you want, click **Stop** to end the trace.
4. If you want to format the trace, click **Format**.

To start a trace on the Windows 3.1 client, follow these steps:

1. Use the configuration tool to change the trace setting.
2. Changes to the configuration settings take place only when the client is restarted. Either restart Windows, or stop all applications that might be using the client, including the configuration tool, attach manager, any other applications provided with the client, and any emulators and applications that communicate using the client code.

Problem Reporting (PR)

If your problem still persists even at this stage, and if you think that the source is in Communications Server, report the problem to IBM.

When you do this, you need to provide the information you obtained through the problem determination (PD) and problem-source identification (PSI) processes:

1. PD information includes:
   - Symptoms
   - Environment
   - Type of problem
   - Problem area
   - Problem re-creatability and re-creation procedure
2. PSI information includes:
   - Error messages (if any)
   - Key factors related to the problem
   - Output from Trace facility
   - Message log
   - Data in the **\PRIVATE** subdirectory, such as .ACG files.

Submitting Problem Determination Information and Receiving Fixes Electronically

Communications Server provides you with utilities for sending problem determination information to a specified destination, as well as receiving fixes electronically from IBM. These utilities include the following:

- Information Bundler
- Problem Determination Sender
- Get Fix / Apply Fix
- World Wide Web Access

Information Bundler

This utility gathers system files and specific trace and log files, as well as registry information such as the software installed or running on a machine.

1. From the RAS folder in the Communications Server program group, double-click the **Information Bundler** icon.
2. A **.ZIP** file containing system and Communications Server PSI is created in the Communications Server directory.

Problem Determination Sender

This utility enables you to send a compacted file that contains the system and diagnostic data collected by the Information Bundler to an FTP server. Double-click on the **Problem Determination Sender** icon in the Communications Server program group. Follow the instructions for locating the service file in your system and establish a connection to a specified anonymous FTP site. The default site is the IBM service site for Communications Server for Windows NT.

Get Fix

Using this utility, you can retrieve fix packages from an FTP server, either on the local network or over the Internet at the IBM service site. Double-click on the **Get Fix** icon in the Communications Server program group. The application will attempt to locate a Web browser installed on your system. If one cannot be found, you can specify the location of a specific browser. Click **OK** to launch the browser and point to the Communications Server anonymous FTP service site. Optionally, you can specify a different FTP server from which to obtain fix packages.

When it is retrieved, the fix package should be extracted into a temporary directory. Follow the instructions provided in the README file contained in the fix package to apply the fix to the system.

World Wide Web Access

You can access Communications Server’s product and service pages on the World Wide Web by double-clicking on the **Service Page** icon in the Communications Server program group. The application will attempt to locate a Web browser installed on your system. If one cannot be found, you may specify the location of a specific browser. Click **OK** to launch the browser and point it to the Communications Server product pages on the World Wide Web.

You can also access Communications Server’s online documentation by double-clicking **Online Documentation** in the Communications Server program group. The application will attempt to locate a Web browser installed on your system. If one cannot be found, you may specify the location of a specific browser. By default, the application will specify the URL for the online documentation available on the World Wide Web. If you have installed this documentation elsewhere, you can specify an alternate location. Click **OK** to launch the browser and point it to the specified URL.

Contacting IBM

This section lists a number of ways you can reach IBM for various reasons. Depending on the nature of your problem or concern, we will ask you to be prepared to provide us with information to allow us to serve you better.

If you have a technical problem, please take the time to review and carry out the actions suggested here. Use your local support personnel before contacting IBM. Only persons with in-depth knowledge of the problem should contact IBM; therefore, support personnel should act as the interface with IBM.

If you determine that you need to contact IBM, you can do any of the following:

- Consult the **Customer Service and Support Guide**, which is a card contained in the product package.
- Access the Communications Server for Windows NT Web page at:

  `http://www.software.ibm.com/enetwork/commserver`
- Access the IBM Personal Software Services Web page, which links to the IBM Software Support Handbook at:

  `http://ps.software.ibm.com/`
- Access the Communications Server for Windows NT customer bulletin board:
  - Dial 919-254-6231 or 919-254-6306 (use country code 001 from outside the U.S.A.).
  - Use protocol N81.
  - Follow the instructions. Entering your first and last names registers you the first time you use the facility.

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Chapter 7. Obtaining Additional Information

This chapter describes the sources of information that can be useful when you are using Communications Server or related products.

Communications Server Library

The following documents are provided as Adobe** Acrobat Portable Document Format (PDF) files and as HTML files on the Communications Server CD-ROM:

Table 4. Communications Server for Windows NT Library

Order Number	Title	Description
GC31-8424	*Quick Beginnings*	Provides an overview of Communications Server and the access features and emulator provided with it. Also gives installation and configuration information.
SC31-8425	*Client/Server Communications Programming*	Describes the advanced program-to-program communications (APPC) application programming interface (API) support provided by Communications Server.
SC31-8655	*Configuration File Reference*	Describes how to use an ASCII editor to copy or change configuration files. This book lists all of the configuration file keywords and their valid values.
SC31-8656	*Network Administration Guide*	Provides information for the Network Administrator’s use in planning and maintaining networks that use Communications Server.
SC31-8426	*System Management Programming*	Describes the usage of the Node Operator Facility (NOF) API messages for developing programs using Communications Server.

For information about ordering publications listed in this document, contact your IBM authorized dealer or marketing representative. In the United States, you can also order publications by dialing **1-800-879-2755**. In Canada, you can also order publications by dialing **1-800-IBM-4YOU** (**426-4968**).

You can view the books directly from the CD-ROM in either format. The .PDF files are located as follows:

csnt\sdk\pubs\cscsp.pdf
Client/Server Communications Programming

csnt\pubs\cscfr.pdf
Configuration File Reference

csnt\pubs\csnag.pdf
Network Administration Guide

csnt\pubs\csqkb.pdf
Quick Beginnings

csnt\sdk\pubs\cssmp.pdf
System Management Programming

The HTML files are located as follows:

csnt\sdk\pubs\cscsp\clsvr.htm
Client/Server Communications Programming

csnt\pubs\cscfr\cscfr.htm
Configuration File Reference

csnt\pubs\csnag\csnag.htm
Network Administration Guide

csnt\pubs\csqkb\quick.htm
Quick Beginnings

csnt\sdk\pubs\cssmp\cssmp.htm
System Management Programming

Related Information

Additional information is contained in the following related publications:

- *Common Programming Interface Communications Reference* SC26–4399

  Describes CPI Communications. It is intended for programmers who want to write applications that use communications products supporting CPI Communications. Available on the Communications Server CD-ROM in HTML and PDF formats.
- *IBM Software Glossary*

Defines technical terms used in the documentation for IBM products. Available on the Web at http://www.networking.ibm.com/nsg/nsgmain.htm.

- *Novell Netware for SAA 3270 Client Interface Guide and Reference* P/N 100–002018–001

  For application programmers writing QEL/MU client software.
- *Systems Network Architecture Formats* GA27–3136

  Describes SNA formats used between subarea nodes and peripheral nodes, and between nodes implementing APPN or low-entry networking (LEN) protocols. Available on the Communications Server CD-ROM in PDF format.
- *Systems Network Management Services Reference* GC31–8302

  Describes SNA Management Services formats used between nodes in subarea networks, and between nodes implementing APPN or low-entry networking (LEN) protocols, or both. Available on the Communications Server CD-ROM in PDF format.

You can also get information from the following Web pages:

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

Appendix A. Directory Exploitation

You can configure multiple clients from a central location using the Lightweight Directory Access Protocol (LDAP) to simplify the configuration process. This section provides conceptual information helpful in planning for LDAP.

Client Configuration Concepts

There is an LDAP object type, the server list, to help you configure certain client applications.

The server list object represents a list of servers that can be associated with APPC or 3270 sessions. The name of a server list object can be specified when configuring APPC or 3270 LU data for users, organizational units, or organizations. You can create any number of server list objects.

To minimize duplication of information, most configuration information can be inherited from a higher level. For example, the configuration for a specific user is inherited from the ***container***, the hierarchy of the organizational units and organization that comprises a user's distinguished name, in which the user is located. Specific values can be overridden at the user level. Containers inherit from their containers.

Inherited parameters are displayed automatically when the object details are displayed. They can be accepted or overridden at that time.

The SNA API-specific data consists of:

- The APPC configuration attributes for user or container objects, which are used to store client configuration data associated with LU 6.2 applications.
- The 3270/LUA configuration attribute for user or container objects, which is used to store client configuration data associated with 3270/LUA applications.
- The AS/400 configuration attribute for user or container objects, which is used to store client configuration data associated with EHNAPPC applications.
- The server list object, which represents a server discovery method to be used by LU 6.2 and 3270/LUA applications. A server list consists of one of the following:
  - A list of explicit servers
  - An implicit list of TCP/IP servers within a scope

  - An implicit list of TCP/IP servers that are not within a scope (they are unscoped)
  - Any server (server name is *)

  The name of a server list object can be specified when configuring LU 6.2 and 3270/LUA data for user, group, or container objects.

Planning for Client Configuration

Before you configure your clients, consider:

- Where to locate each piece of information in the directory tree in order to take advantage of inheritance.
- How LUs should be planned in order to maximize reusing the information. If wildcard values and nondedicated LUs are used, less information needs to be configured at the user level. You should weigh this advantage against the needs of the network.

Before configuring client information, gather the following information:

- An explicit list of up to four servers and their corresponding transport protocols (IP or IPX).
- A scope name. A TCP/IP connection will be established with a Communications Server within the specified scope.
- A single item list with a server name of * (asterisk) and a corresponding protocol (IP or IPX). A connection will be established with any Communications Server in the network that can satisfy the request.

  When you configure a server list, specify the SPX name or IP host name or Internet address of the Communications Server that you want to connect to.
- The types of applications the SNA API client will run: APPC and CPI-C, LUA, or EHNAPPC.
- The address of the system where Communications Server resides.
- The protocol to be used (IP or SPX).
- If you are configuring APPC and CPI-C applications, you might also need the following:
  - If transaction programs on the SNA API client will need to be run by remote SNA nodes, then you must create a transaction program definition.
  - If you will be running an APPC application program locally, check to see what session information it requires. You may need to specify a partner LU 6.2 name and mode name as parameters, for example. You may also need to configure CPI-C side information.

- If you are configuring the SNA API client to run LUA applications and require a specific LU address, you need the LU name of an LU configured on Communications Server.
- If you are configuring the SNA API client to run EHNAPPC applications, you need the list of AS/400s that the EHNAPPC applications will access and a list of user IDs and passwords authorized to access these AS/400s.

Appendix B. Using Web Administration

You can use Web Administration to manage your communications server over an intranet. Using a Web browser, an administrator can query node status, obtain information about resources, modify resources, display configuration files, display message logs, and perform other administrative tasks.

Security

Web Administration restricts the use of its functions through user authentication based on Windows NT security. A Windows NT user ID and a valid password are required. Optionally, you can enter the Windows NT domain in which the user ID is defined. During Communications Server installation, an existing user ID is added to the IBMCSADMIN group; to determine which user ID was added, log on to Windows NT as an administrator and use the Windows NT User Manager to view group settings. Unless a secure browser and secure server are used, the user ID and password will be transmitted in an encoded, but not encrypted, form over the network. While this is probably not a concern for an administrator using an internal intranet, unsecured usage over the open Internet could pose risks. For more information about secure browser/server software, visit: `http://www.ics.raleigh.ibm.com/ics/icfgive.htm`.

For authentication to function properly, your Web server must be run as a system service or under the context of a Windows NT user ID with the ″Act as part of the operating system″ privilege set. This is described in the customization sections below.

Web Administration does not use Web server protection or authorization for authentication. This means that the user ID and password are only passed once instead of with every request as is the case with Web server authentication. Reauthentication is required for each new browser session or when the browser has been active for at least one day.

Installation

Web Administration is installed in a subdirectory of the path you select for Communications Server installation. By default this is C:\IBMCS\WEBADMIN. No additional installation is required on the client side once the Web browser has been successfully installed, but several configuration changes are required on the server side after your Web server has been installed. Before making these changes, be certain that you can access your Web server from your Web browser. For most servers, you can display Web server information by using your browser to open the page `http://hostname`, where hostname is the TCP/IP name of the system running your Web and communication servers.

Type `hostname` in a console window to find the hostname. An IP address can be used instead of a hostname.

Once you have verified that your Web browser can access your Web server, you need to customize your Web server.

Customizing IBM Internet Connection Server

The IBM Internet Connection Server (ICS) must be installed to run as a system service. Refer to your ICS installation instructions for details.

If you chose the Automatic Configuration option during the Web Administration installation, ICS was configured for you. Otherwise, you must edit the HTTPD.CNF Web server configuration file with a text editor. HTTPD.CNF is found under directories WINNT, WINNT35, or the directory specified by the ETC environment variable. Assuming that C:\IBMCS is your install directory, add the lines:

```
Pass                    /csc/*                  C:\IBMCS\webadmin\html\*
Pass                    /csc-html/*             C:\IBMCS\webadmin\html\*
Exec                    /csc-bin/*              C:\IBMCS\webadmin\bin\*
```

If the statement `Pass * somepath` exists in your HTTPD.CNF file, these lines must precede it.

Customizing Lotus Domino

To customize the Lotus Domino Web server, follow these steps:

1. If you do not already have a Domino Web Server Configuration database, create one using the Domino Web Server Configuration template (domcfg.ntf). The database must be named domcfg.nsf. To create a database:
   a. From the Lotus Notes menu, select **File**, select **Database**, and then select **New**.
   b. Enter `Domino Server Configuration` as the title.
   c. Enter `DOMCFG.NSF` as the file name.

d. Select **Domino Server Configuration** and click **OK**.

e. Press the escape key to exit.

2. If you chose the Automatic Configuration option during installation, your Web server was configured automatically and you can skip this step. Otherwise, open the Domino Configuration database and choose **Create -> Mapping URL -> Directory**.

   In the panel that appears, add each of the following mappings for the Web Administration directories in the MAPPING section. Since each mapping is effectively a unique record in the configuration database, you must save and close each record before creating the next one.

URL path	Directory	Access
/csc	c:\ibmcs\webadmin\html	Read
/csc-html	c:\ibmcs\webadmin\html	Read
/csc-bin	c:\ibmcs\webadmin\bin	Execute

   After saving the last record, close the database.

3. Give the Windows NT log in user account ″Act as part of operating system″ rights:

   a. Decide which Windows NT user account (Administrator, for example) that you will use to log in to your system when running Domino, since it does not run as a service.

   b. Open **User Manager** from the **Administrative Tools** folder and then select the ID (Administrator, for example) that you want to use.

   c. Select **Policies -> User Rights** and click the **Show Advanced User Rights** check box.

   d. From the **Right** pull-down menu, select **Act as part of operating system**.

   e. Click **Add**.

   f. Click **Show users** and then select the user ID (Administrator, for example) that you want to use. Then click **Add**.

   g. Click **Ok**.

   h. Click **Ok** on the User Rights Policy window.

   i. Exit User Manager and reboot your system.

   j. When the system reboots, log in using the ID you chose previously (Administrator, for example) and restart Domino.

Customizing Lotus GO Web Server

The Lotus GO Web Server must be installed to run as a system service. Refer to your Lotus GO installation information for details.

If you chose the Automatic Configuration option during the Web Administration installation, Lotus GO was configured for you. Otherwise, you must edit the HTTPD.CNF Web server configuration file with a text editor. HTTPD.CNF is found under directories WINNT, WINNT35, or the directory specified by the ETC environment variable. Assuming that C:\IBMCS is your install directory, add the lines:

```
Pass                      /csc/*                    C:\IBMCS\webadmin\html\*
Pass                      /csc-html/*               C:\IBMCS\webadmin\html\*
Exec                      /csc-bin/*                C:\IBMCS\webadmin\bin\*
```

If the statement `Pass * somepath` exists in your HTTPD.CNF file, these lines must precede it.

Customizing Microsoft Internet Information Server

To customize Microsoft Internet Information Server, follow these steps:

1. If you chose the Automatic Configuration option during the Web Administration installation, your Web server was configured automatically and you can skip this step. Otherwise, use the Internet Service manager to map URL requests to file locations:
   a. Find and start the Internet Service Manager (on Windows NT 4.0, select **Start->Programs->Microsoft Internet Server->Internet Service Manager**).
   b. Select the local Web server (WWW service) and select **Service Properties...** from the **Properties** pull-down menu.
   c. Click the **Directories** tab and press **Add**.
   d. Assuming that C:\IBMCS is your install directory, enter the following data:

Directory	**Virtual Directory Alias**	**Access**
C:\IBMCS\webadmin\html	/csc	Read
C:\IBMCS\webadmin\html	/csc-html	Read
C:\IBMCS\webadmin\bin	/csc-bin	Execute

   e. Click **Apply**.
2. Give the IIS user account ″Act as part of operating system″ rights:
   a. Select the Web services entry in the Internet Service Manager.
   b. Click the properties menu.
   c. Choose service properties.
   d. Write down the user ID in the ″Anonymous Logon″ field. It is IUSR_machine by default (where ″machine″ is the name of the server) and press **OK**.

e. Exit the Internet Services Manager.

f. Open the **User Manager** tool in the **Administrative Tools** folder.

g. Select IUSR_machine (user ID from the ″Anonymous Logon″ field above).

h. Select **Policies -> User Rights**.

i. Click the **Show Advanced User Rights** check box.

j. From the **Right** pull-down menu, select **Act as part of operating system**.

k. Press **ADD**.

l. Press **SHOW USERS**.

m. Select **IUSR_machine**.

n. Press **ADD**.

o. Press **OK**.

p. Press **OK** on the User Rights Policy panel.

q. Exit User Manager and reboot your system for changes to take effect.

Using Other Web Servers

Other Web servers may support Web Administration. First follow the installation instructions above. Then modify the server configuration files (as described in your server documentation) to map virtual file requests to actual file directories, based on the customization instructions above. Your server must run as a system service or under the context of a Windows NT user ID with the ″Act as part of the operating system″ privilege set. Sometimes a server can be run as a system service and also have a user ID associated with it, like Microsoft IIS above. As in the Micrsoft IIS case, be certain that the user ID has ″Act as part of operating system″ rights. Follow the procedures for Domino and IIS for modifying user rights.

Starting Web Administration

Once you have installed and configured Web Administration and the required Web software, you can begin managing your communications server from the Web. Use your browser to open the page: `http://hostname/csc/main.html`, where *hostname* is the TCP/IP name of the system running your Web and communication servers.

Type `hostname` in a console window to find the hostname. An IP address can be used instead of a hostname.

Before performing any operation, you will be asked to log on with a Windows NT user ID and password. Optionally, you can enter the Windows NT domain in which the user ID is defined. This user ID must be a member of the IBMCSADMIN group. After receiving authentication, you can use Web administration without logging on again for up to one day, or until your browser is restarted.

Navigation Within Web Administration

While using Web Administration, navigation is accomplished by using the navigation tree located on the left side of your browser's display area. Since real-time information is being sent to your browser, avoid using the browser's **Forward** and **Backward** buttons. Use the navigation tree.

Appendix C. Remote Installation and Uninstallation

This chapter describes how to remotely install and uninstall Communications Server for NT using the Microsoft Systems Management Server (SMS) product. The information in this chapter can be used with other management applications such as Tivoli Software Distribution.

Refer to the online *Network Administration Guide* for information about using the Tivoli Plus module for Communications Server. Remote installation and uninstallation is available through this module.

This chapter also includes information about using other software distribution products and performing simple installs and uninstalls without using any software distribution product.

Remote installation and uninstallation can be performed in a normal (attended) or silent (unattended) mode.

Remote Installation of the Server

You can install with or without SMS. Choose the task you want from the following table:

If you want to:	**Start with:**	**And then:**
Install the server silently	"Create a Response File"	Follow the instructions for SMS or non-SMS installation.
Use SMS to install the server	"Install the Server using SMS" on page 117	
Install the server without using SMS	"Install the Server Without Using SMS" on page 119	

Create a Response File

If you plan to perform silent remote installs, you must create a response file, which must be placed in the same directory as the Communications Server installation software. You must copy the software from the CD-ROM into a directory on a local or shared drive.

To copy the installation software onto a local or shared drive and create a response file, follow these steps:

1. Create a directory named CSNT on a local or shared network drive by issuing the following command:

   ```
   MD d2:\CSNT
   ```

   where *d2* is the local or shared network drive where you want to copy the software.
2. Copy the Communications Server installation software from the CD-ROM to the local or shared network drive by issuing the following command:

   ```
   XCOPY d1:\CSNT d2:\CSNT /s
   ```

   where *d1* is the CD-ROM drive letter and *d2* is the drive where you created the directory in the previous step.
3. Create a response file by following these steps:
   a. Change to the directory you created above.
   b. From the directory, issue the following command:

      ```
      SETUP -noinst -r -f1d2:SETUP.ISS
      ```

      where *d2* is the letter of the drive where you copied the installation software.

      Notes:

      1) The –noinst parameter specifies that you want to be prompted for the installation choices and then exit without installing. If you want to install the code and create a response file at the same time, remove this parameter. If you use this parameter, it must be the first parameter.
      2) The –r parameter specifies that you want to create a response file.
      3) The –f1 parameter specifies where you want to create the response file. The default is the directory where you installed Windows NT. The example above creates the file in the directory where the install code resides. Due to an InstallShield problem, the name of this directory must be shorter than 43 characters. If the name of the directory where you want this file is longer than 43 characters, you must use another directory and then copy the file.
      4) If you change the name or location of the response file once it is created, you must specify the –f1 parameter when you invoke the SETUP program to perform silent installations. See “Create an SMS Software Package” on page 117 for more information about these parameters.
   c. Enter the values and responses you want in the dialog.

4. Customize the response file (if necessary). There are several variables that you can safely change using an ASCII text editor. If you change any other lines in the response file, your installation may not work. The variables are:

   szDir=
   The directory where you want the code installed on the target workstation.

   szFolder=
   Folder on the target workstation that will contain the Communications Server icons.

   szText=
   First occurrence in the file: Name of an existing user ID on the target workstation. This ID will be added to the IBMCSADMIN group, which enables users to configure and administer Communications Server remotely.

   szText=
   Second occurrence in the file: Number of Communications Server licenses purchased.

Install the Server using SMS

To install Communications Server remotely using SMS, you need to create a software package that contains the Communications Server installation software and then create an SMS job to distribute and install the software package. Refer to the Microsoft Systems Management Server documentation for more detailed information on how to create a software package and a job.

Create an SMS Software Package

To create a package, follow these steps:

1. From the Microsoft SMS Administrator application, open the Packages folder and then create a new package.
2. In the Package Properties window, click on the Import button to create the software package by importing a package definition file (PDF).
3. The File Browser window appears. Select the drive where the Communications Server CD-ROM is located and then select the CSNT subdirectory, which contains the package definition file CSNT.PDF. If you are performing a silent install, you can also find this file in the local or network drive where you copied the installation software.
4. Select the CSNT.PDF file and click OK.
5. Click Workstation.

   In the Source Directory field, specify the fully-qualified path name to the CSNT directory that contains the Communications Server installation software. If you are performing an attended install, this directory is on the CD-ROM. If you are performing a silent install, this directory is on the local or network drive you specified when you created the response file.

If you are performing a silent install and have changed the name or location of the response file since you created it, you must change the command line syntax. To do this, select the Silent Installation command and click on the Properties button. Append the following text to the end of the command in the Command Line entry field:

```
-f1d:\path\responsefile
```

where *d:\path\responsefile* is the fully-qualified path and filename of the response file.

6. Click Close to close the Workstation Properties window.

   If you specified a local path in the Source Directory entry field, you will get a pop-up window that warns you that the local path you specified may not be accessible to SMS components running on another machine. Click OK to continue.

7. Click OK to close the Package Properties window.

   If a pop-up window appears, indicating that SMS will update the software package at all sites, click OK to continue.

The software package can now be installed by creating an SMS job.

Create an SMS Job

Refer to the Microsoft Systems Management Server documentation for detailed instructions about creating and running a job.

When you create the SMS Job, be sure to select **Normal Installation** or **Silent Installation** from the drop-down list in the Run Phase section of the Job Details panel.

The user logged on to the target machine must have administrator authority to install Communications Server.

At the end of the installation:

- Normal Installation

  If you reply **No** when you are asked whether you want to install the IBM LLC2 Protocol Interface, a panel will appear that asks whether you want to reboot the machine so that changes made during installation can take effect. You must reply **No**, since SMS will not allow the machine to reboot while it is running. Once you reply **No**, you can reboot the machine manually before starting Communications Server.

If you reply **Yes** when you are asked whether you want to install the IBM LLC2 Protocol Interface, LLC2 will be installed. After LLC2 is installed, a panel will appear that asks whether you want to reboot the machine so that changes made during installation can take effect. You must reply **No**, since SMS will not allow the machine to reboot while it is running. Once you reply **No**, you can reboot the machine manually before starting Communications Server.

- Silent Installation

  You must manually reboot the machine before starting Communications Server.

- A warning panel with the title ISSET_SE may appear at the end of the installation using SMS. This is a known InstallShield problem and does not affect the installation. Click on **OK** to close the panel.

Install the Server Without Using SMS

To install Communications Server remotely without using SMS, you can create a command file that includes the command for normal or silent installation. The target machine must have local or shared access to the drive that contains either the CD-ROM or the copied installation software. If you want to use other installation packages, refer to the documentation that came with the package for details about using command files or InstallShield commands.

- Normal installation

  The syntax of the InstallShield program for normal installation is

  ```
  SETUP -SMS
  ```

  You could create a command file that includes a net use to the directory that contains the installation software and executes the InstallShield program. For example, if the installation software were in the CODESERV\CSNT directory:

  ```
  NET USE X:\\CODESERV\CSNT
  X:
  SETUP -SMS
  C:
  NET USE X:/DELETE
  ```

  At the end of a normal installation you are asked whether you want to install the IBM LLC2 Protocol Interface. If you want to install LLC2, answer **Yes**. If you do not want to install LLC2, answer **No**. The installation program will ask whether you want to reboot the machine. If you reply **No**, you must manually reboot the machine before you start Communications Server.

- Silent installation

  The syntax of the InstallShield program for silent installation is

  ```
  SETUP -s -f1d2:\CSNT\SETUP.ISS -SMS
  ```

where *d2* is the local or shared network drive letter where you copied the Communications Server installation software. The -f1 parameter specifies the fully-qualified path and filename of the response file. Do not leave a space between the parameter and the drive letter. If you changed the name or location of the response file SETUP.ISS, then specify the new name or location.

You could create a command file that includes a net use to the directory that contains the installation software and executes the InstallShield program. For example, if the installation software were in the CODESERV\CSNT directory:

```
NET USE X:\\CODESERV\CSNT
X:
SETUP -s -f1X:\SETUP.ISS -SMS
C:
NET USE X:/DELETE
```

At the end of a silent installation, you must manually reboot the machine before you start Communications Server.

Remote Uninstallation

You can remove Communications Server remotely with or without SMS. The InstallShield program uninstalls Communications Server, but it does not remove the IBM LLC2 Protocol Interface. Refer to "Uninstalling LLC2" on page 122 for instructions on manually removing LLC2.

If you want to:	**Start with:**	**And then:**
Use SMS to uninstall	"Removing Communications Server Using SMS"	Follow the instructions in "Uninstalling LLC2" on page 122
Uninstall without using SMS	"Removing Communications Server Without SMS" on page 122	Follow the instructions in "Uninstalling LLC2" on page 122

Removing Communications Server Using SMS

To uninstall Communications Server using SMS, you must modify the SMS package used to install Communications Server and then create a Job. If the package has been deleted, follow the instructions in "Install the Server using SMS" on page 117 to recreate it. You do not need to create a response file to silently uninstall Communications Server.

Modify the SMS Package

To modify the SMS Package, follow these steps:

1. Open the Packages folder in the Microsoft SMS Administrator application. Select the Communications Server SMS software package and double-click on it to open it.
2. Click Workstation.
3. Select **Normal Uninstall** or **Silent Uninstall** from the Setup Package for Workstations window and then click Properties.
4. On the Command Line Properties window, check the command line field. If Communications Server is installed in a directory other than C:\IBMCS, then you need to change the directory location in two places in the command. Click **OK**.
5. Click **Close** on the Setup Package for Workstations window. If you get a warning that the local path you specified may not be accessible to SMS components running on another machine, click **OK**.
6. Click **OK** to close the Package Properties window. If you get a message saying that SMS will update the software package at all sites, click **OK** to close that window.

You can now use the software package to remove Communications Server by creating an SMS Job.

Create an SMS Job

Refer to the SMS documentation for detailed instructions on creating Jobs. When you create the Job, be sure to select **Normal Uninstall** or **Silent Uninstall** from the drop-down list in the Run Phase section of the Job Details window.

The user logged on to the target machine must have administrator authority to install Communications Server.

At the end of the uninstall:

- Normal uninstall

  The Network application will be started for you to install LLC2. Follow the instructions in “Uninstalling LLC2” on page 122, including rebooting the machine.

- Silent Installation

  You must open the control panel folder and start the Network application. Follow the instructions in “Uninstalling LLC2” on page 122, including rebooting the machine.

If you do not want to install the IBM LLC2 Protocol Interface, you must manually reboot the machine before starting Communications Server.

- A warning panel with the title ISSET_SE may appear at the end of the installation using SMS. This is a known InstallShield problem and does not affect the installation. Click **OK** to close the panel.

Removing Communications Server Without SMS

To uninstall Communications Server remotely without using SMS, you can create a command file that includes the command for normal or silent removal. The target machine must have local or shared access to the drive that contains either the CD-ROM or the copied installation software. If you want to use other installation packages, refer to the documentation that came with the package for details about using command files or InstallShield commands.

The syntax of the InstallShield program for removal is

```
UNINST.EXE -a -fd2:\xxxx\DeIsL1.isu -cd2:\xxxx\UNINST.DLL
```

where:

- **-**a indicates a silent removal. You can remove this parameter if you choose.
- *d2* is the drive on the target workstation where you installed Communications Server.
- *xxxx* is the directory on the target workstation where you installed Communications Server.

At the end of a normal removal, the network control application is automatically invoked so that you can remove the IBM LLC2 Protocol Interface. Instructions for removing the interface also appear.

At the end of a silent removal, you must manually bring up the network control application (in the Settings folder) and follow the instructions in “Uninstalling LLC2” to remove LLC2. You must reboot the machine for the removal to complete.

Uninstalling LLC2

The InstallShield program does not remove the IBM LLC2 protocol interface. You need to manually uninstall it using the Network settings application in the Windows NT Control Panel folder:

1. Open the Network application in the Control Panel folder.
2. Select the **Protocols** tab.
3. Select **IBM LLC2 Protocol** and click **Remove**.
4. A window appears, asking whether you want to continue. Click **Yes**.

5. Click **Close** to close the Network application.
6. Click **Yes** on the Network Settings Change window to restart the computer.

Remote Installation of the SNA API Clients

You can install with or without SMS. Choose the task you want from the following table:

If you want to:	**Start with:**	**And then:**
Install the SNA API client silently	"Create a Response File for the SNA API Client"	Follow the instructions for SMS or non-SMS installation.
Use SMS to install the SNA API client	"Install the SNA API Client using SMS" on page 125	
Install the SNA API client without using SMS	"Install the SNA API Clients Without Using SMS" on page 127	

Create a Response File for the SNA API Client

If you plan to perform silent remote installs, you must create a response file, which must be placed in the same directory as the Communications Server installation software. You must copy the software from the CD-ROM into a directory on a local or shared drive.

Windows Clients

To copy the installation software onto a local or shared drive and create a response file, follow these steps:

1. Create a directory named CLIENTS\WIN32 on a local or shared network drive by issuing the following commands:

   ```
   MD d2:\CLIENTS
   MD d2:\CLIENTS\WIN32
   ```

   where *d2* is the local or shared network drive where you want to copy the software.
2. Copy the SNA API client installation software from the CD-ROM to the local or shared network drive by issuing the following command:

   ```
   XCOPY d1:\CLIENTS\WIN32 d2:\CLIENTS\WIN32 /s
   ```

   where *d1* is the CD-ROM drive letter and *d2* is the drive where you created the directory in the previous step.

3. Create a response file by following these steps:
   a. Change to the directory you created above.
   b. From the directory, issue the following command:

      ```
      SETUP -noinst -r -f1d2:SETUP.ISS
      ```

      where *d2* is the letter of the drive where you copied the installation software.

      Notes:

      1) The –noinst parameter specifies that you want to be prompted for the installation choices and then exit without installing. If you want to install the code and create a response file at the same time, remove this parameter. If you use this parameter, it must be the first parameter.
      2) The –r parameter specifies that you want to create a response file.
      3) The –f1 parameter specifies where you want to create the response file. The default is the directory where you installed Windows NT. The example above creates the file in the directory where the install code resides. Due to an InstallShield problem, the name of this directory must be shorter than 43 characters. If the name of the directory where you want this file is longer than 43 characters, you must use another directory and then copy the file.
      4) If you change the name or location of the response file once it is created, you must specify the –f1 parameter when you invoke the SETUP program to perform silent installations. See "Create an SMS Software Package" on page 125 for more information about these parameters.
   c. Enter the values and responses you want in the dialog.
4. Customize the response file (if necessary). There are two variables that you can safely change using an ASCII text editor. If you change any other lines in the response file, your installation may not work. The variables are:

   szDir=
   The directory where you want the code installed on the target workstation.

   Result=
   Whether you want to reboot the system after installation completes. Set this value to 0 (no) if you will be using SMS. If you will not be using SMS, set this value to 1 (yes).

OS/2 Client

To copy the installation software onto a local or shared drive and modify the provided response file, follow these steps:

1. Create a directory named CLIENTS\OS2 on a local or shared network drive by issuing the following commands:

   ```
   MD d2:\CLIENTS
   MD d2:\CLIENTS\OS2
   ```

   where *d2* is the local or shared network drive where you want to copy the software.
2. Copy the OS/2 SNA API client installation software from the CD-ROM to the local or shared network drive by issuing the following command:

   ```
   XCOPY d1:\CLIENTS\OS2 d2:\CLIENTS\OS2 /s
   ```

   where *d1* is the CD-ROM drive letter and *d2* is the drive where you created the directory in the previous step.
3. Modify the sample response file OS2INST.RSP, which is located in the \CLIENTS\OS2 directory.

   If you change the name or location of the response file once it is created, you must specify the `–f1` parameter when you invoke the SETUP program to perform silent installations. See “Create an SMS Software Package” for more information about these parameters.

   There is one variable that you can safely change using an ASCII text editor. If you change any other lines in the response file, your installation may not work. The variable is:

   FILE= The directory where you want the code installed on the target workstation.

Install the SNA API Client using SMS

To install the SNA API client remotely using SMS, you need to create a software package that contains the installation software and then create an SMS job to distribute and install the software package. Refer to the Microsoft Systems Management Server documentation for more detailed information on how to create a software package and a job.

Create an SMS Software Package

To create a package, follow these steps. Wherever the variable ***xxxx*** exists, substitute one of the following:

Windows NT or Windows 95	WIN32
Windows 3.1	WIN16
OS/2	OS2

1. From the Microsoft SMS Administrator application, open the Packages folder and then create a new package.

2. In the Package Properties window, click on the Import button to create the software package by importing a package definition file (PDF).
3. The File Browser window appears. Select the drive where the Communications Server CD-ROM is located and then select the CLIENTS/xxxx subdirectory.

   This directory contains the package definition file xxxx.PDF. If you are performing a silent install, you can also find this file in the local or network drive where you copied the installation software.
4. Select the xxxx.PDF file and click **OK**.
5. Click **Workstation**.

   In the Source Directory field, specify the fully-qualified path name to the directory that contains the SNA API client installation software. If you are performing an attended install, this directory is on the CD-ROM. If you are performing a silent install, this directory is on the local or network drive you specified when you created the response file.

   If you are performing a silent install and have changed the name or location of the response file since you created it, you must change the command line syntax. To do this, select the Silent Installation command and click **Properties**.

   a. For Windows operating systems, append the following text to the end of the command in the Command Line entry field:

      ```
      -f1d:\path\responsefile
      ```

      where *d:\path\responsefile* is the fully-qualified path and filename of the response file.
   b. For OS/2, change the /R: parameter in the Command Line entry field to specify the fully-qualified name of the response file.
6. Click **Close** to close the Workstation Properties window.

   If you specified a local path in the Source Directory entry field, you will get a pop-up window that warns you that the local path you specified may not be accessible to SMS components running on another machine. Click **OK** to continue.
7. Click **OK** to close the Package Properties window.

   If a pop-up window appears, indicating that SMS will update the software package at all sites, click OK to continue.

The software package can now be installed by creating an SMS job.

Create an SMS Job

Refer to the Microsoft Systems Management Server documentation for detailed instructions about creating and running a job.

When you create the SMS Job, be sure to select **Normal Installation** or **Silent Installation** from the drop-down list in the Run Phase section of the Job Details panel.

At the end of the installation:

- Normal Installation

  A panel will appear that asks whether you want to reboot the machine so that changes made during installation can take effect. You must reply **No**, since SMS will not allow the machine to reboot while it is running. Once you reply **No**, you can reboot the machine manually before starting Communications Server.
- Silent Installation

  You must manually reboot the machine before starting Communications Server.

Install the SNA API Clients Without Using SMS

To install Communications Server remotely without using SMS, you can create a command file that includes the command for normal or silent installation. The target machine must have local or shared access to the drive that contains either the CD-ROM or the copied installation software. If you want to use other installation packages, refer to the documentation that came with the package for details about using command files or InstallShield commands.

Windows Clients

- Normal installation

  The syntax of the InstallShield program for normal installation is

  ```
  SETUP -SMS
  ```

  You could create a command file that includes a net use to the directory that contains the installation software and executes the InstallShield program. For example, if the installation software were in the CODESERV\CLIENTS\WIN32 directory:

  ```
  NET USE X:\\CODESERV\CLIENTS
  X:
  CD WIN32
  SETUP -SMS
  C:
  NET USE X:/DELETE
  ```
- Silent installation

  The syntax of the InstallShield program for silent installation is

  ```
  SETUP -s -f1d2:\CSNT\SETUP.ISS -SMS
  ```

  where *d2* is the local or shared network drive letter where you copied the Communications Server installation software. The -f1 parameter specifies the fully-qualified path and filename of the response file. Do not leave a space between the parameter and the drive letter. If you changed the name or location of the response file SETUP.ISS, then specify the new name or location.

You could create a command file that includes a net use to the directory that contains the installation software and executes the InstallShield program. For example, if the installation software were in the CODESERV\CSNT directory:

```
NET USE X:\\CODESERV\CSNT
X:
SETUP -s -f1X:\SETUP.ISS -SMS
C:
NET USE X:/DELETE
```

At the end of a silent installation, you must manually reboot the machine before you start the SNA API client.

OS/2 Clients

IBM Software Installer is used to install the OS/2 SNA API clients.

- Normal installation

  The syntax of the Software Installer program for normal installation is

  ```
  INSTALL
  ```

  You could create a command file that includes a net use to the directory that contains the installation software and executes Software Installer. For example, if the installation software were in the CODESERV\CLIENTS\OS2 directory:

  ```
  NET USE X:\\CODESERV\CLIENTS
  X:
  CD OS2
  INSTALL
  C:
  NET USE X:/DELETE
  ```

  A panel will appear that asks whether you want to reboot the machine so that changes made during installation can take effect. Reply **Yes**. If you reply **No**, you must reboot the machine manually before starting the SNA API client.

- Silent installation

  The syntax of the Software Installer program for silent installation is

  ```
  INSTALL /X /R:d2:\CLIENTS\OS2\OS2INST.RSP
  ```

  where *d2* is the local or shared network drive letter where you copied the Communications Server installation software. The R: parameter specifies the fully-qualified path and filename of the response file. Do not leave a space between the parameter and the drive letter. If you changed the name or location of the response file SETUP.ISS, then specify the new name or location.

You could create a command file that includes a net use to the directory that contains the installation software and executes the InstallShield program. For example, if the installation software were in the CODESERV\CLIENTS\OS2 directory:

```
NET USE X:\\CODESERV\CLIENTS
X:
CD OS2
INSTALL /X /R:X:\OS2\OS2INST.RSP
C:
NET USE X:/DELETE
```

Removing the SNA API Clients Using SMS

To uninstall the SNA API clients using SMS, you must modify the SMS package used to install the clients and then create a Job. If the package has been deleted, follow the instructions in “Install the SNA API Client using SMS” on page 125 to recreate it. You do not need to create a response file to silently uninstall the SNA API clients.

Modify the SMS Package

Windows Clients: To modify the SMS Package, follow these steps:

1. Open the Packages folder in the Microsoft SMS Administrator application. Select the SNA API client SMS software package and double-click on it to open it.
2. Click **Workstation**.
3. Select **Normal Uninstall** or **Silent Uninstall** from the Setup Package for Workstations window and then click **Properties**.
4. On the Command Line Properties window, check the command line field. If the SNA API client is installed in a directory other than C:\CSNTAPI, then you need to change the directory location in two places in the command. Click **OK**.
5. Click **Close** on the Setup Package for Workstations window. If you get a warning that the local path you specified may not be accessible to SMS components running on another machine, click **OK**.
6. Click **OK** to close the Package Properties window. If you get a message saying that SMS will update the software package at all sites, click **OK** to close that window.

You can now use the software package to remove Communications Server by creating an SMS Job.

OS/2 Clients: To modify the SMS Package, follow these steps:

1. Open the Packages folder in the Microsoft SMS Administrator application. Select the OS/2 SNA API client SMS software package and double-click on it to open it.
2. Click **Workstation**.
3. Select **Normal Uninstall** or **Silent Uninstall** from the Setup Package for Workstations window and then click **Properties**.
4. On the Command Line Properties window, check the command line field. If you are performing a silent install, you must modify the Uninstall_Silent parameter. You must also change the path specified on the /R: parameter to reflect the fully-qualified name of the OS2UNIN.RSP file. Click **OK**.
5. Click **Close** on the Setup Package for Workstations window. If you get a warning that the local path you specified may not be accessible to SMS components running on another machine, click **OK**.
6. Click **OK** to close the Package Properties window. If you get a message saying that SMS will update the software package at all sites, click **OK** to close that window.

You can now use the software package to remove Communications Server by creating an SMS Job.

Create an SMS Job

Refer to the SMS documentation for detailed instructions on creating Jobs. When you create the Job, be sure to select **Normal Uninstall** or **Silent Uninstall** from the drop-down list in the Run Phase section of the Job Details window.

At the end of the uninstall:

- Normal uninstall

  A window appears that asks whether you want to reboot the machine for the uninstall to be completed. Reply **No**. SMS will not allow the machine to reboot while it is running. Once you reply **No**, you must reboot your machine manually to complete the uninstall.
- Silent installation

  You must manually reboot the machine to complete the uninstall.

Removing the SNA API Client Without SMS

To uninstall the SNA API client remotely without using SMS, you can create a command file that includes the command for normal or silent removal. The target machine must have local or shared access to the drive that contains either the CD-ROM or the copied installation software. If you want to use other installation packages, refer to the documentation that came with the package for details about using command files or InstallShield commands.

The syntax of the InstallShield program for removal of the Windows 32–bit client is

```
UNINST.EXE -a -fd2:\xxxx\DeIsL1.isu
```

where:

- -a indicates a silent removal. You can remove this parameter if you choose.
- *d2* is the drive on the target workstation where you installed Communications Server.
- *xxxx* is the directory on the target workstation where you installed Communications Server.

The syntax of the InstallShield program for removal of the Windows 3.x client is

```
UNINST16.EXE -a -fd2:\xxxx\DeIsL1.isu
```

where the parameters are the same as those for the 32–bit client.

The syntax of the Software Installer program for removal of the OS/2 client is

```
INSTALL /X /A:D /R:d2:\CLIENTS\OS2\OS2UNIN.RSP
```

where:

- /X indicates a silent uninstall. Remove this parameter if you want a normal uninstall.
- /A:D specifies that the product should be deleted.
- /R: specifies the fully-qualified name of the silent uninstall response file OS2UNIN.RSP. Remove this parameter on a normal uninstall.

At the end of a normal removal, a window appears that asks whether you want to reboot the machine. Reply **Yes**. If you reply **No**, you must reboot the machine manually for the uninstall to complete.

At the end of a silent removal, you must manually reboot the machine for the removal to complete.

Appendix D. Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Department TL3B/062
P.O. Box 12195
Research Triangle Park, NC 27709-2195
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, International Programming License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

Advanced Peer-to-Peer Networking
AIX
AnyNet
APPN
AS/400
DB2
eNetwork
ESCON
Global Network
IBM
IBMLink
IMS
Micro Channel
OS/2
OS/400
Personal System/2
System/370System/390
S/370
S/390
TalkLink
VTAM
WebExplorer

Tivoli, Tivoli Management Environment, and TME 10 are trademarks of Tivoli Corporation, an IBM company.

Other company, product, and service names may be trademarks or service marks of others.

Adobe is a trademark of Adobe Systems, Incorporated.

C-bus is a trademark of Corollary, Inc.

Java and HotJava are trademarks of Sun Microsystems, Inc.

Microsoft, Windows, and the Windows 95 logo are registered trademarks of Microsoft Corporation.

PC Direct is a trademark of Ziff Communications Company and is used by IBM Corporation under license.

ActionMedia, LANDesk, MMX, Pentium, and ProShare are trademarks or registered trademarks of Intel Corporation in the U.S. and other countries.

For a complete list of Intel trademarks see www.intel.com/tradmarx.htm.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Index

Readers' Comments — We'd Like to Hear from You

eNetwork Communications Server
Version 6.0 for
Windows NT
Quick Beginnings
Version 6.0

Publication No. GC31-8424-02

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	□	□	□	□	□

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	□	□	□	□	□
Complete	□	□	□	□	□
Easy to find	□	□	□	□	□
Easy to understand	□	□	□	□	□
Well organized	□	□	□	□	□
Applicable to your tasks	□	□	□	□	□

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? □ Yes □ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name

Address

Company or Organization

Phone No.

Readers' Comments — We'd Like to Hear from You

GC31-8424-02

Cut or Fold
Along Line

Fold and Tape

Please do not staple

Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
Information Development
Department CGMD / Bldg 500
P.O. Box 12195
Research Triangle Park, NC
27709-9990

Fold and Tape

Please do not staple

Fold and Tape

Cut or Fold
Along Line

Part Number: 30L8745

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

30L8745

GC31-8424-02