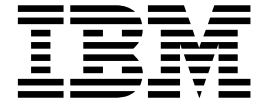
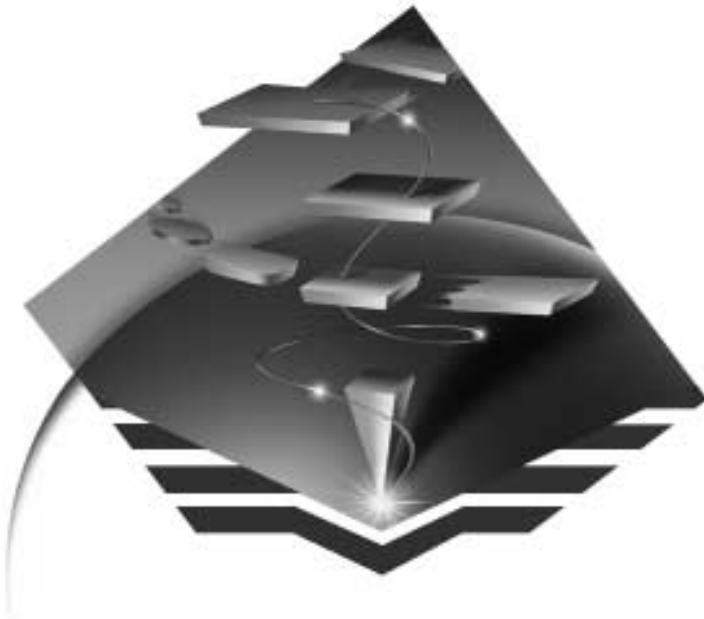


eNetwork Communications Server Version 5.01 for
Windows** NT



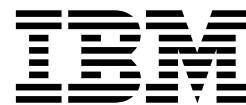
Quick Beginnings

Version 5.01



GC31-8424-01

eNetwork Communications Server Version 5.01 for
Windows** NT



Quick Beginnings

Version 5.01

Note

Before using this information and the product it supports, be sure to read the general information under "Appendix D. Notices" on page 203.

Second Edition (September 1997)

This edition applies to Version 5.01 of Communications Server for Windows NT** and to all subsequent releases and modifications until otherwise indicated in new editions or technical newsletters.

Order publications through your IBM representative or the IBM branch office serving your locality. Publications are not stocked at the address below.

IBM welcomes your comments. A form for readers' comments may be provided at the back of this publication, or you may address your comments to the following address:

International Business Machines Corporation
Department CGMD
P.O. Box 12195
Research Triangle Park, North Carolina
27709-2195

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.

© **Copyright International Business Machines Corporation 1997. All rights reserved.**

Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Contents

Figures	ix
Tables	xi
Welcome to Communications Server	xiii
Road Map	xiii
Conventions	xiv
Double-Byte Character Set Support.	xv

Part 1. The IBM Software Servers . 1

Chapter 1. Introducing IBM's Software Servers	3
IBM Communications Server	4
Directory and Security Server	4
IBM Transaction Series	5
IBM MQSeries	5
Tivoli Management Servers	6
Lotus Go Webserver.	6
IBM DB2 Universal Database.	7
Lotus Domino.	7
Combining Communications Server with other Software Servers	8
Chapter 2. More about IBM Communications Server for Windows NT	9
Features and Functions of Communications Server for Windows NT Version 5.0	11
Features of Communications Server for Windows NT Version 5.01.	12
Description of the Communications Server for Windows NT Features and Functions.	12
Advanced Peer-to-Peer Networking (APPN) Network and End Node Support	13
High-Performance Routing	13
Discovery of Service Providers	14
Dependent LU Requester (DLUR)	14
SNA Gateway Support	14
TN3270E Server	16
SNA API Client Support	18
AnyNet SNA over TCP/IP Access Node and Gateway	20

AnyNet Sockets over SNA Access Node and Gateway	23
Local and Remote Configuration and Administration Support	27
Programming Support	27
Data Security	28
Conformance with SNA	28
Entry-Level Emulator Functions.	30

Part 2. Planning for, Installing, and Configuring Communications Server 33

Chapter 3. Planning for the Installation of Communications Server	35
Before You Start	35
Introduction to Installing Communications Server	35
Prerequisite Software	35
Prerequisite Hardware	36
Startup Drive Requirements during Installation	36
Remote Installation	36
Chapter 4. Installing Communications Server	37
Considerations before Installing	37
Beginning Installation	37
Installing Communications Server for Windows NT	38
Uninstalling Communications Server for Windows NT	39
Reinstalling Communications Server for Windows NT	40
Registering Communications Server for Windows NT	40
License Management	40
Accessing and Installing the SNA API Clients	41
Accessing the Remote Administration Clients	42

Chapter 5. Configuring Communications Server	43	Step 5: Establish a Session.	70
Deciding What to Configure	43	AnyNet SNA over TCP/IP Gateway Configuration	71
SNA Gateway Configuration	44	Before You Begin.	71
Before You Begin.	45	Summary of Steps	71
Summary of Steps	45	Step 1: APPN Network Node Configuration	71
Step 1: Node Setup	46	Step 2: Map the LU Names to TCP/IP Addresses	72
Step 2: Device Configuration	46	Step 3: Start the Node	72
Step 3: Define Host Links and LUs.	48	Step 4: Verify That the Link Is Active	72
Step 4: Define Gateway Clients	50	Step 5: Establish a Session.	72
Step 5: Start the Node	52	AnyNet Sockets over SNA Configuration.	73
Step 6: Verify That the Link Is Active	52	Before You Begin.	73
Step 7: Establish a Session.	52	Summary of Steps	74
TN3270E Server Configuration	52	Step 1: Node Setup	74
Before You Begin.	52	Step 2: Device Configuration	75
Summary of Steps	53	Step 3: Connection Configuration	77
Step 1: Node Setup	53	Step 4: Partner LU 6.2 Configuration	78
Step 2: Device Configuration	54	Step 5: Local TCP/IP Address Configuration	78
Step 3: Define Host Links and LUs.	56	Step 6: Configure the LU Mapping.	79
Step 4: Define TN3270E Server Properties	58	Step 7: Start the Node	79
Step 5: Start the Node	58	Step 8: Start the Session	79
Step 6: Verify That the Link Is Active	59	SNA API Client Configuration for APPC	80
Step 7: Establish a Session.	59	Configuring Communications Server for SNA API Client Support	80
APPN Network Node Configuration	59	Before You Begin.	81
Before You Begin.	59	Configuring Communications Server to Support SNA API Clients Running APPC Applications	82
Summary of Steps	60	Summary of Steps	82
Step 1: Node Configuration	60	Step 1: Administering User IDs	82
Step 2: Device Configuration	61	Step 2: Node Setup	83
Step 3: Connection Configuration	63	Step 3: Device Configuration	84
Step 4: Partner LU 6.2 Configuration	64	Step 4: Connection Configuration	86
Step 5: Connection Network Configuration	65	Step 5: Local LU 6.2 Configuration	87
Step 6: Start the Node	65	Step 6: Partner LU 6.2 Configuration	87
Step 7: Verify That the Link Is Active	65	Step 7: Enable SNA API Client Support	88
Step 8: Establish a Session.	65	Step 8: Transaction Program Configuration	88
DLUR/DLUS Configuration	66	Configuring the SNA API Client to Run APPC Applications	88
Before You Begin.	66	Before You Begin.	89
Summary of Steps	67	Step 1: Configure Global Data	89
DLUR Support for Local LUs Subtask	67	Step 2: Configure Server Location	89
Step 1: DLUR PUs Configuration	67	Step 3: Configure Transaction Program Definition	90
Step 2: Local LU 0 to 3 Configuration	68		
DLUR Support for Downstream LUs Subtask	68		
Step 1: Define a Default DLUS	69		
Step 2: Assign a DLUS to a Client Template	69		
Step 3: Start the Node	70		
Step 4: Verify That the Link Is Active	70		

Step 4: Configure CPI-C Side Information Definition	90	Step 9: Start the Session	109
Testing the Configuration	90	Dependent LU 6.2 Sessions to a Host	110
Step 1: Start the Communications Server Node.	90	Before You Begin.	110
Step 2: Verify That All Configured Links Are Active	91	Summary of Steps	110
Step 3: Establish the Connection from the SNA API Client	91	Step 1: Node Setup	111
SNA API Client Configuration for LUA	91	Step 2: Device Configuration	111
Configuring Communications Server for SNA API Client Support	92	Step 3: Connection Configuration	113
Before You Begin.	92	Step 4: Local LU 6.2 Configuration	115
Summary of Steps	93	Step 5: CPI-C Side Information Configuration	115
Configuring Communications Server to Support SNA API Clients Running 3270 or Other LUA Applications	93	Step 6: Start the Node	116
Step 1: Administering User IDs	93	Step 7: Verify That the Link Is Active	116
Step 2: Node Setup	94	Step 8: Start the Session	116
Step 3: Device Configuration	95	3270 Configuration	117
Step 4: Define Host Links and LUs.	97	Before You Begin.	117
Step 5: Define SNA API Client Access to Host Resources	99	Summary of Steps	117
Configuring the SNA API Client to Run 3270 or Other LUA Applications	99	Step 1: Node Setup	118
Before You Begin.	100	Step 2: Device Configuration	118
Step 1: Configure Global Data	100	Step 3: Connection Configuration	120
Step 2: Create an LUA Definition	100	Step 4: Local LU 0 to 3 Configuration	122
Testing the Configuration	101	Step 5: Start the Node	122
Step 1: Start the Communications Server Node.	101	Step 6: Verify That the Link Is Active	122
Step 2: Verify That All Configured Links Are Active	101	Step 7: Start the Application	122
Step 3: Establish the Connection from the SNA API Client	101	Focal-Point Configuration	123
CPI-C, APPC, or 5250 Emulation Configuration	102	Before You Begin.	123
Before You Begin.	102	Summary of Steps	123
Summary of Steps	103	Step 1: Focal-Point Configuration	124
Step 1: Node Setup	103	Step 2: Start the Node	124
Step 2: Device Configuration	104	Step 3: Verify That the Link Is Active	124
Step 3: Connection Configuration	106	Step 4: Establish a Session.	124
Step 4: Transaction Program Configuration	107		
Step 5: Partner LU 6.2 Configuration	108		
Step 6: CPI-C Side Information Configuration	108		
Step 7: Start the Node	109		
Step 8: Verify That the Link Is Active	109		

Part 3. Using Communications Server 125

Chapter 6. Using Communications Server 127

Starting Communications Server	127
Stopping Communications Server	127
Replacing the Default Configuration	128
SNA Node Operations	129
Using the Menu Bar.	131
Displaying a Resource	133
Starting a Resource	133
Stopping a Resource	133
Deleting a Resource	134
Changing an HPR Path Switch	134
Updating SNA Resources Dynamically	134
Remote Operations	135

Performing Administrative Tasks on the Communications Server	135	Host and Communications Server (DLUR)	164
Command Line Utilities	136	NPSI and Communications Server (X.25)	166
Chapter 7. Problem Determination and Reporting	139	NPSI Connections over X.25	167
Problem Determination (PD)	139	VTAM/NCP and Communications Server (X.25)	168
Symptoms	139	APPC over X.25	170
Environment	139	AS/400 Host Line Definitions	172
Problem Type	140	AS/400 Host Controller Definitions	172
Problem Area	140	AS/400 Host Device Definitions.	174
Problem Re-Creation	140	AS/400 Host Line Description and Communications Server	175
Problem-Source Identification (PSI)	140	AS/400 Host Controller Description and Communications Server	176
Viewing Communications Server Logs	141	AS/400 Twinaxial Descriptions	176
Obtaining Trace Data	142	AS/400 and Communications Server (X.25 PVC)	177
Problem Reporting (PR)	143		
Submitting Problem Determination Information and Receiving Fixes		Appendix B. More Information About Configuring AnyNet SNA over TCP/IP	179
Electronically	143	Mapping SNA Resources to IP Addresses	179
Information Bundler	143	Defining Domain Names and IP Addresses	181
Problem Determination Sender	144	SNA over TCP/IP Gateway Considerations	181
Get Fix	144	Defining Unique CP Names and Connection Network Names	182
World Wide Web Access	144	Using the Wildcard Entry to Reduce Domain Name Server Definitions	183
Contacting IBM	145	SNA over TCP/IP Access Node Function Considerations	185
		How to Route SNA Sessions over AnyNet SNA over TCP/IP	185
Chapter 8. Obtaining Additional Information	147	AnyNet SNA over TCP/IP Configuration Examples	186
		Example 1. Running APPC or CPI-C Applications over a TCP/IP Network	187
Appendix A. Mapping Parameters Between Communications Server and an SNA Host	149	Steps	187
Introduction	149	Example 2. 3270 Emulation via DLUR over a TCP/IP Network	188
NCP Token Ring (NTRI) with VTAM and Communications Server	149	Steps	188
Token Ring with VTAM Switched Network and Communications Server	150	Example 3. Using an SNA Gateway to Enable 3270 Emulation Between SNA and TCP/IP Networks	189
9370 IBM Token-Ring Network Adapter and Communications Server	152	Steps	189
3174 Controller and Communications Server	152	Example 4. Using an SNA Gateway for 3270 Emulation over a TCP/IP Network	190
3174 Controller VTAM PU and Communications Server	153	Steps	190
Ethernet with VTAM Switched Network and Communications Server	155	Example 5. 3270 Emulation from Two Windows NT Workstations on Different IP Networks	191
VTAM/NCP and Communications Server (SDLC)	157		
VTAM and Communications Server (APPC).	161		
ES/9000 and Communications Server (SDLC)	162		

Steps	192	How an IP Address Is Mapped to an LU Name	198
Appendix C. More Information About Sockets over SNA	193	How the Sockets over SNA Gateway Routes and Maps Data	199
How Does Sockets over SNA Work?	193	Defining Sockets over SNA Modes	201
Generating an LU 6.2 Call from a Socket Call	195	Changing the Idle-Timeout Interval	201
Mapping an IP Address to an SNA Network-Qualified Name	195	Appendix D. Notices	203
Routing and Mapping Data over SNA and IP Networks	195	Appendix E. Trademarks	205
Application Program Support Provided by Sockets over SNA	195	Glossary	207
Planning for Sockets over SNA	196	Index	231
Routing and Mapping Overview	196	Readers' Comments — We'd Like to Hear from You	235
Internet Addressing	196		
IP Routing Table	198		
SNA Network ID Used by Sockets over SNA	198		

Figures

1. Example of SNA Gateway Configuration	15	10. Formats of the Domain Names That SNA over TCP/IP Builds	180
2. TN3270E Server with Wide Area TCP/IP Network	17	11. Defining a CP Name and a Connection Network Name	183
3. TCP/IP- or IPX-Attached SNA API Clients	19	12. Domain Name Server Definitions for a Single Gateway Connected to an SNA Network with Two Network IDs	184
4. Running APPC or CPI-C Applications over a TCP/IP Network.	21	13. Domain Name Server Definitions for Parallel Gateways Connected to an SNA Network with Two Network IDs	185
5. Using AnyNet to Connect SNA Applications on Different Platforms	22	14. Structure of a Windows NT Node Running Sockets over SNA.	194
6. 3270 Emulation via an SNA Gateway over a TCP/IP Network.	23	15. Example of an IP Routing Panel	199
7. Sockets Applications Communicating over an SNA Network	24	16. Example of a Network Using the Sockets over SNA Route Discovery Function	200
8. Socket Applications Communicating through Multiple Sockets Gateways	25		
9. Socket Applications on Multiple Operating Systems Communicating over an SNA Network	26		

Tables

1. Road Map for Getting Started	xiii	15. VTAM Communications Server DLUR Parameter Matching Connection from Host to Workstation	165
2. SNA Gateway Summary	16	16. Host/PC Parameter Cross-Reference: NPSI Connections over X.25	167
3. Command Equivalents	18	17. Host/PC Parameters Cross-Reference: X.25 (VTAM/NCP)	168
4. Communications Server for Windows NT Library	147	18. Host/PC Parameters Cross-Reference: APPC on an IBM Token-Ring Network Using X.25 to a Host	170
5. Host/PC Parameters Cross-Reference: IBM Token-Ring Network NTRI Definition	149	19. AS/400 Communications Server Parameters Cross-Reference: OS/400 Host Program Line Definition	172
6. Host/PC Parameters Cross-Reference: IBM Token-Ring Network VTAM Switched Net	150	20. AS/400 Communications Server Parameters Cross-Reference: Controller Parameters	173
7. Host/PC Parameters Cross-Reference: IBM Token-Ring Network 9370 VTAM LAN	152	21. AS/400 Communications Server Parameters Cross-Reference: Device Parameters	175
8. Parameter Matching between a 3174 Token-Ring and Communications Server.	152	22. Host/PC Parameters Cross-Reference: Line Description	175
9. Host/PC Parameters Cross-Reference: IBM Token-Ring Network 3174 Controller VTAM PU and Communications Server	153	23. Host/PC Parameters Cross-Reference: Controller Description	176
10. Host/PC Parameters Cross-Reference: Ethernet Network VTAM Switched Network	155	24. Host/PC Parameters Cross-Reference: Controller Description	176
11. Host/PC Parameters Cross-Reference: SDLC	157	25. AS/400 Communications Server Parameters Cross-Reference: X.25 PVC Connection	177
12. Host/PC Parameters Cross-Reference: APPC	161	26. AS/400 Communications Manager Parameter Cross-Reference: Controller Description	178
13. Host/PC Parameters Cross-Reference: 9370 Information System via SDLC	162	27. IP Address Masks Supported by Sockets over SNA	197
14. VTAM Communications Server Parameter Cross-Reference: Using DLUR.	164		

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. The applicable versions of Windows NT are V3.51 and V4.0.

Part 1 reviews the IBM Software Servers and includes an overview of Communications Server.

Part 2 provides planning, installing, and configuring information for Communications Server.

Part 3 explains how to use Communications Server.

Part 4 provides related information for Communications Server.

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 2. More about IBM Communications Server for Windows NT" on page 9
Install the Communications Server.	"Chapter 4. Installing Communications Server" on page 37
Configure the Communications Server.	"Chapter 5. Configuring Communications Server" on page 43
Start using Communications Server.	"Chapter 6. Using Communications Server" on page 127
Display diagnostic information.	"Chapter 7. Problem Determination and Reporting" on page 139
View or print online documentation.	"Chapter 8. Obtaining Additional Information" on page 147

Table 1. Road Map for Getting Started (continued)

If you want to...	Refer to...
Contact IBM.	"Contacting IBM" on page 145

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 that you supply a value for
 - Book titles
 - A letter that is being used as a letter or a work 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 rightmost 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.

Double-Byte Character Set Support

Communications Server supports double-byte character sets (DBCS), in which each character is represented by 2 bytes. Languages such as Japanese, Chinese, and Korean, which contain more symbols than can be represented by 256 code points, require double-byte character sets. Because each character requires 2 bytes, the typing, displaying, and printing of DBCS characters require hardware and programs that support DBCS.

Where information applies specifically to DBCS, it is noted in this manual.

ASCII refers to PC single-byte code in this book. ASCII should be considered as JISCII in Japan.

Part 1. The IBM Software Servers

Chapter 1. Introducing IBM's Software Servers

When you choose the newest version of IBM Communications Server for Windows NT, you'll be putting your business on the fast path to client/server and network computing.

This powerful new server and client software, part of a family of IBM*, Lotus**, and Tivoli** products, is one of the best network enhancements you can make. They comprise middleware plus administration and end user tools. Since they run on hardware servers and are designed to support state-of-the-art applications, we refer to them as **application servers**. IBM Software Servers are packaged to help you to quickly install and run a family of multifunctional, compatible application servers. IBM Software Servers were designed to work together. They are *modular*, which means they'll work individually, in pairs, or in many other configurations. You can add function at any time by simply adding new Software Servers. You can build a high-function, reliable environment for decision support, messaging and groupware, transaction processing, and other client/server functions vital to today's business. And with new Web functions, you can exploit new technologies and move into the world of network computing.

This family of products provides:

- New Web functions and improved integration, now available in Version 5.0
- Popular software chosen by application providers to run their applications
- Greatest depth and breadth of application servers—providing unequalled depth in each server, as well as the widest breadth of application servers—making it easy to grow from the smallest departmental servers to the largest systems of a modern enterprise
- Open solutions available on multiple platforms—popular clients (such as Windows, Windows 95, Windows NT**, Macintosh**, OS/2*, UNIX** and popular browsers used on the Internet or in intranets) and servers (such as OS/2, Windows NT, NetWare**, OS/400*, MVS, AIX* and other UNIX systems)—and in conformance with all key industry-standard interfaces
- Support for existing investments, since IBM Software Servers work with your existing systems, are thoroughly tested, and work together
- Growth paths for future needs, allowing you to add new servers when needed, move applications to more powerful platforms as demand grows, and extend your existing systems with new technologies in the move to collaborative and network computing

Introducing IBM's Software Servers

- Ease of installation and simple administration, with common packaging and documentation

The IBM Software Servers family includes several servers, designed to meet your needs.

IBM Communications Server

IBM Communications Server will meet your requirements for interconnecting diverse networks and prove to be a winner for your business. With Communications Server, workstation users and applications can communicate with other workstations and central computer applications, regardless of the networking protocols used in each system. Communications Server has full-function gateways to clients on SNA and TCP/IP networks plus support of a broad range of industry-standard networking protocols. Communications Server will help you to get users communicating with each other in networks of all sizes, from small workgroups, to large corporate headquarters.

Communications Server provides businesses with a variety of opportunities to:

- Expand the use of applications, while protecting current network investments
- Reduce operation and management costs by connecting networks without impacting existing applications
- Increase productivity and convenience by giving employees access to applications while at work, home or when travelling
- Reduce costs of central computer and peer-to-peer connectivity by sharing communication resources
- Gain efficiency in response times by assigning priority to short, interactive data transmissions rather than to batch-oriented bulk data traffic

Directory and Security Server

With IBM Directory and Security Server, you can simplify the effort involved in having increased control over complex networks, multivendor systems, and multiple platforms, while maintaining security within your network. With Directory and Security Server you can generate and manage secure, distributed applications that are interoperable and portable. Directory services make it easy to combine multiple directories, even across WANs, into a simple, single view. Plus, it can be done without deleting users and resources with the same names. You get a single integrated view of all available resources, including printers, files, and applications—no matter where they are located.

Directory and Security Server gives systems administrators a single logical view of all LAN and WAN resources—regardless of installed platforms and vendors. And users get convenient single sign-on, providing transparent access to any authorized enterprise resource, which can include the IBM Software Servers.

The security services are based on the Kerberos security model, which uses a third-party authentication server. This server authenticates both the client and server, making impersonation virtually impossible. Another security measure allows only authentication tickets to flow over the network, so thieves can't steal passwords. Data encryption standard (DES) and commercial data masking facility (CDMF) data encryption technologies are also available for total data privacy.

IBM Transaction Series

IBM Transaction Series lets you make flexible and strategic use of new technology, while continuing to meet your business needs using established technology. Transaction Series coordinates and integrates the functions of multiple application servers, locally or throughout your enterprise. This helps you to produce and manage very high performance applications. It also enables organizations to get and use the operational data needed on customer transactions and stay a jump ahead of the competition.

Transaction Series provides the ideal environment for applications to run anywhere, any time, no matter where they reside in the network. No matter how demanding your applications and requirements are, Transaction Series gives you the safety, security, and integrity you need for your business.

Transaction Series offers two flexible programming styles. The CICS* API is available for those who want to leverage existing CICS applications. Encina supports those who want to exploit an open, standards-based API.

IBM MQSeries

In an open-systems environment, communications coding is complex and difficult to manage. IBM MQSeries simplifies things, giving you time to develop the solutions that deliver your business mission. IBM MQSeries simplifies the task of connecting your applications across unlike environments. Programs communicate using the IBM MQSeries API, an easy-to-use, high-level program interface that shields your programmers from the

Introducing IBM's Software Servers

complexities of different operating systems and underlying networks. You focus on the business logic, while IBM MQSeries manages your connections to the computer systems.

IBM MQSeries also provides an immensely flexible infrastructure, on which you can build mobile communications, multimedia applications, transaction-based systems, and a whole new generation of network applications.

Tivoli Management Servers

Managing today's network computing enterprise is not merely harder, it is fundamentally different from managing the corporate computing environments of the past. Managing your business-critical applications, your systems, and your network now requires new tools based on a new computing model. It requires an open, highly scalable, cross-platform solution.

Tivoli answers this challenge with TME 10 (Tivoli Management Environment), a suite of management applications that gives you the power to manage your entire network computing enterprise: your data center, your distributed system, even your laptops. TME 10 Servers unite these disparate environments and enable you to manage them together as a single business unit, treating each as a strategic component of your complete enterprise.

TME 10 Servers enable you to manage software distributions, system resource monitoring, events, network devices, security, and user access, all from a central view. And TME 10 Servers protect your current investment, providing cross-platform support of all major versions of UNIX, Windows NT, Windows 95, OS/2, NetWare, and OS/390.

TME 10 Servers are the overwhelming choice of companies seeking to gain control over their network computing enterprise. Tivoli customers are some of the world's leading companies in financial services, telecommunications, transportation, manufacturing, electronics and computers, healthcare, retail, service industries, and utilities.

Lotus Go Webserver

With Lotus Go Webserver, you can host and manage Hypertext Markup Language (HTML) pages and other online documents, and create your own corporate Web site.

From the corporate home page, your company can:

- Distribute up-to-date information to the world using text, high-quality graphics, audio, and video
- Create information that customers and suppliers can access through electronic forms or e-mail
- Publish product descriptions and price lists with electronic order forms, so customers can purchase your products and services with a credit card—right from their own computers
- Track how customers, suppliers, and personnel use your published information, so you can tell when you are reaching your target audience
- Gain a competitive edge by creating a worldwide presence for your company

IBM DB2 Universal Database

IBM DB2* Universal Database gives you the foundation for reliable data management, offering complete integrity, high availability, and fast performance. DB2 Universal Database makes it easy to create multimedia applications to present your data through video, audio, and image techniques. Local and remote users can store, retrieve, manipulate, manage, and share data—easily and reliably, using the newest and best-tested technology in the relational database industry.

With the IBM DB2 family of products, you can access data on multiple platforms. Access to IBM and non-IBM relational and nonrelational data is available through optional components of the DB2 family.

Lotus Domino

Lotus Domino transforms Lotus Notes into an interactive Web application server, allowing any Web client to participate in Notes applications securely. Domino bridges the open networking environment of Internet standards and protocols with the powerful application development facilities of Notes. You get a solution that combines messaging, groupware, and the Internet, all built-in.

With Domino, you can rapidly develop a broad range of business applications for the Internet and intranet. Plus, you get support for many popular operating systems for both clients and servers, as well as Web browsers. Domino can be your central access point for finding and sharing the information you need—whether it's centrally located in an e-mail message, a relational database, a host-based system, in your favorite desktop application,

Introducing IBM's Software Servers

or on the World Wide Web. How? You can combine with Lotus Domino any of the other Software Servers, plus other vendors' application servers and applications.

Combining Communications Server with other Software Servers

When you combine Communications Server with other software servers in this family, you get an integrated software environment that will support your applications today and lay the foundation for the future. Other software suppliers have expressed interest in or have already built integrated solutions using members of this IBM software family.

This document describes IBM Communications Server for Windows NT, which provides flexible, reliable communications for your network. Take advantage of your easy-to-use OS/2-, and Windows-based workstations as you access existing applications on S/390* and AS/400* hosts. Plus, an extensive set of application programming interfaces makes it ideal for client/server computing.

Communications Server can be installed with currently supported releases of Windows NT. (See "Prerequisite Software" on page 35 for a complete list of software requirements.)

To learn how to install Communications Server, refer to "Chapter 4. Installing Communications Server" on page 37.

Chapter 2. More 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), including SDLC, twinaxial, X.25, LAN (Token-Ring and Ethernet), channel, switched lines, nonswitched lines, and TCP/IP. 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 a compatibility of 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

More about Communications Server

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 Software Developers 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 your multiprotocol challenges with its AnyNet, SNA API clients, 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.

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.

Features and Functions of Communications Server for Windows NT Version 5.0

The Communications Server Version 5.0 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)
- Discovery of service providers
- Dependent LU Requester (DLUR)
- SNA gateway
- TN3270E Server
- SNA API 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
- 32-bit application programming interfaces (APIs)
 - CPI-C
 - APPC
 - LUA RUI
 - Management Services API
 - Common Services API
 - Node Operations API

More about Communications Server

- Data security
- LAN support
- Local and wide area connectivity 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.

Features of Communications Server for Windows NT Version 5.01

This release includes the following features:

- IPX support for Win32 API clients
Clients can now use IPX to communicate with the server.
- LUA SLI API on the server
You can now use LUA SLI verbs in your applications. Refer to the online *Client/Server Programming Reference* for more information about these verbs.
- 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 improvementsSNA data compression is compatible with the S/390 and AS/400 implementations and can be used with all LU types.
- TN3270E IP address filtering
You can specify at the server the clients, based on IP address, 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.

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 LAN, SDLC, and X.25 connections.

HPR routing requires VTAM V4R3 for host connections. However, you can use HPR in non-host-oriented networks.

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.

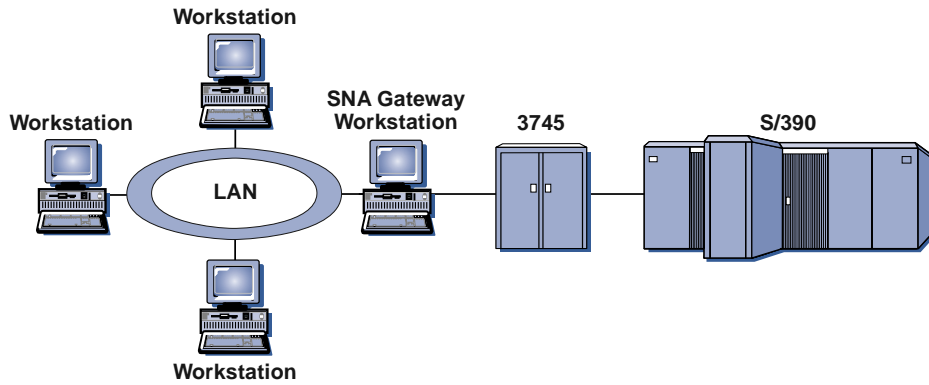


Figure 1. Example of SNA Gateway Configuration

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 2.0 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.

More about Communications Server

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 (third-party adapter support) channel (upstream only)
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 17.

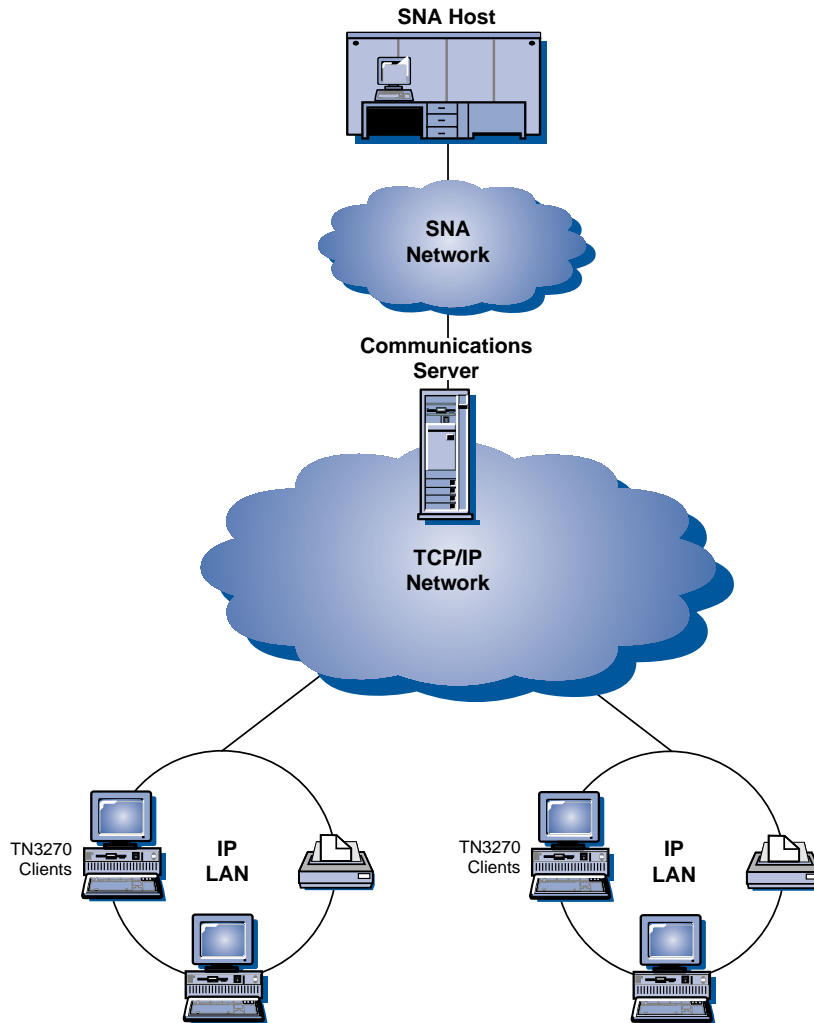


Figure 2. TN3270E Server with Wide Area TCP/IP Network

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 or in their TCP/IP network, using LU 1 and LU 3 print sessions.

More about Communications Server

TN3270E Server implements the protocols outlined in 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.

- IP Address Filtering

TN3270E Server enables the user to specify at the server the clients, based on IP address, 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.

- Response handling

TN3270E-enabled clients can send both positive and negative responses, which TN3270E Server sends on to the host. TN3270E Server generates request 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	ATTN	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.

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.x, and OS/2 as illustrated by Figure 3.

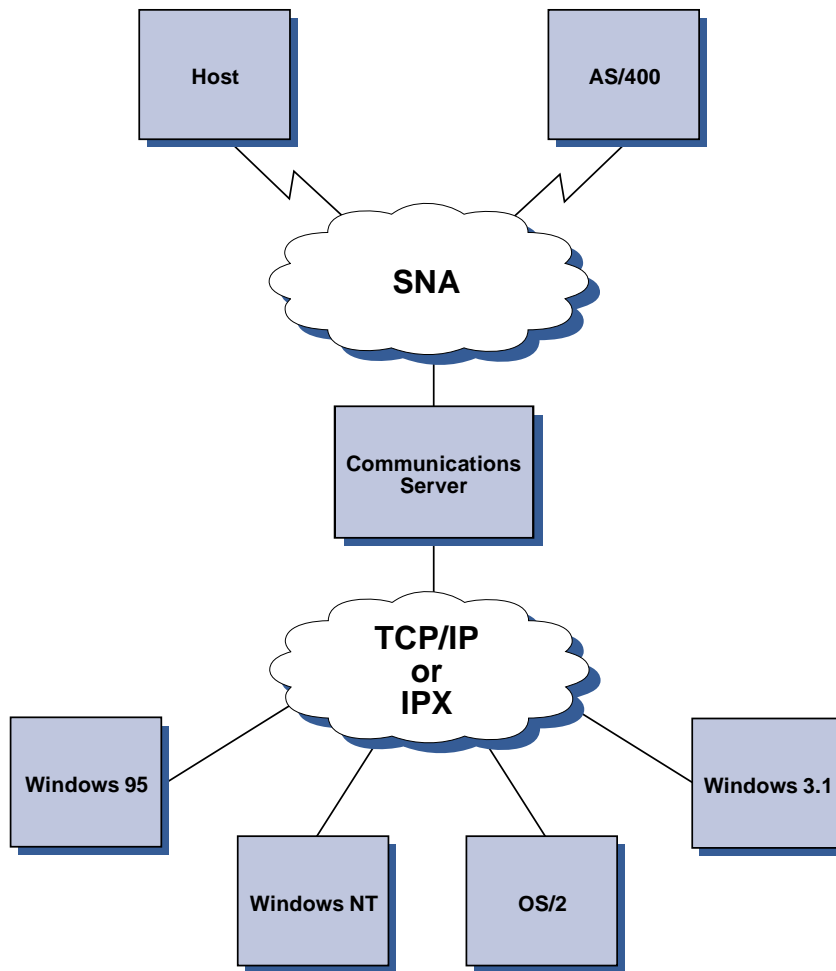


Figure 3. TCP/IP- or IPX-Attached SNA API Clients

The SNA clients provide support for CPI-C APPC, EHNAPPC, and LUA RUI 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 27 for more information about the programming support available and the Software Developers Kit.

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 “Appendix B. More Information About Configuring AnyNet SNA over TCP/IP” on page 179.

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 4 on page 21 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 “Example 1. Running

APPC or CPI-C Applications over a TCP/IP Network” on page 187 for configuration instructions.

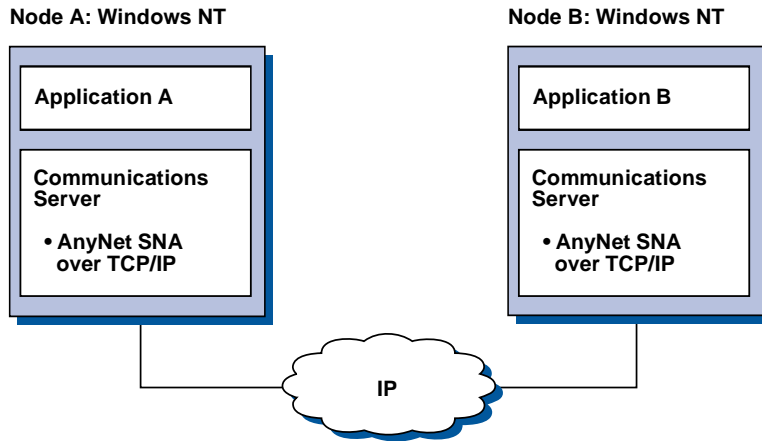


Figure 4. Running APPC or CPI-C Applications over a TCP/IP Network

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

Figure 5 on page 22 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.

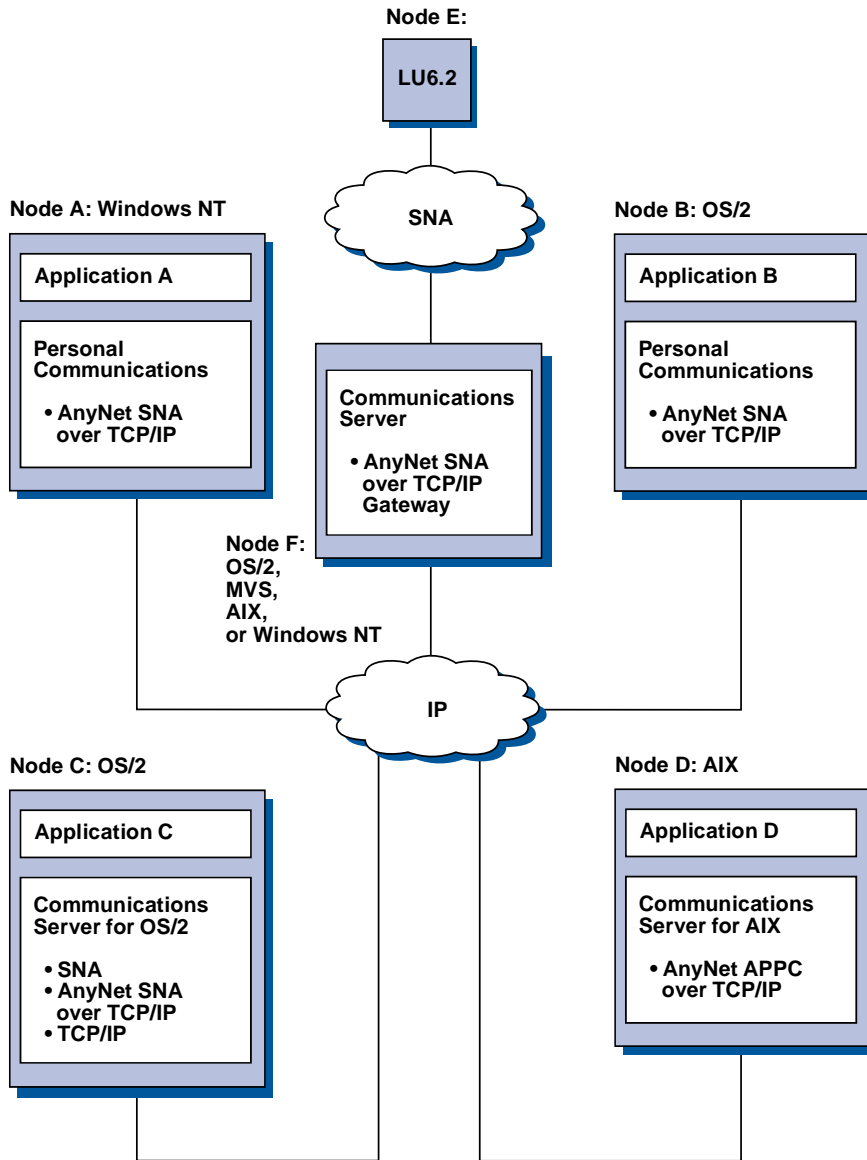


Figure 5. Using AnyNet to Connect SNA Applications on Different Platforms

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

Figure 6 on page 23 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 “Example 4. Using an SNA Gateway for 3270 Emulation over a TCP/IP Network” on page 190 for configuration instructions.

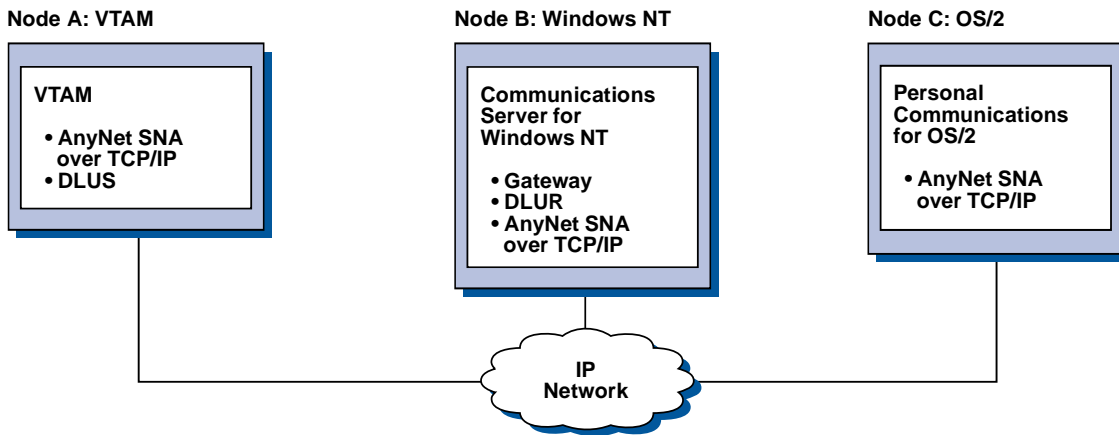


Figure 6. 3270 Emulation via an SNA Gateway over a TCP/IP Network

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 7 on page 24 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.

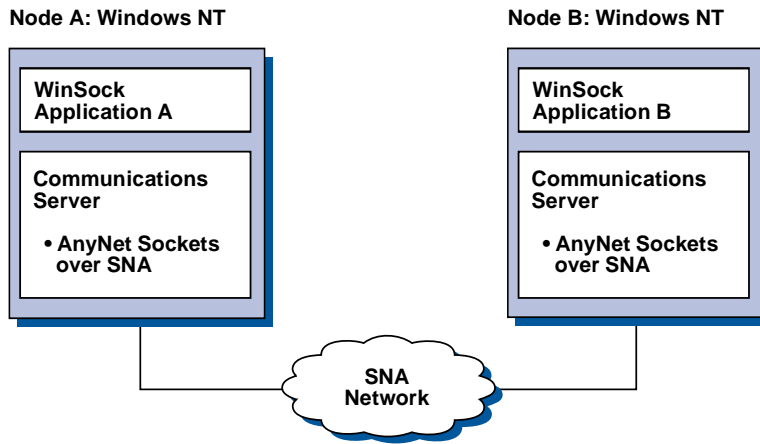


Figure 7. Sockets Applications Communicating over an SNA Network

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 8 on page 25, 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.

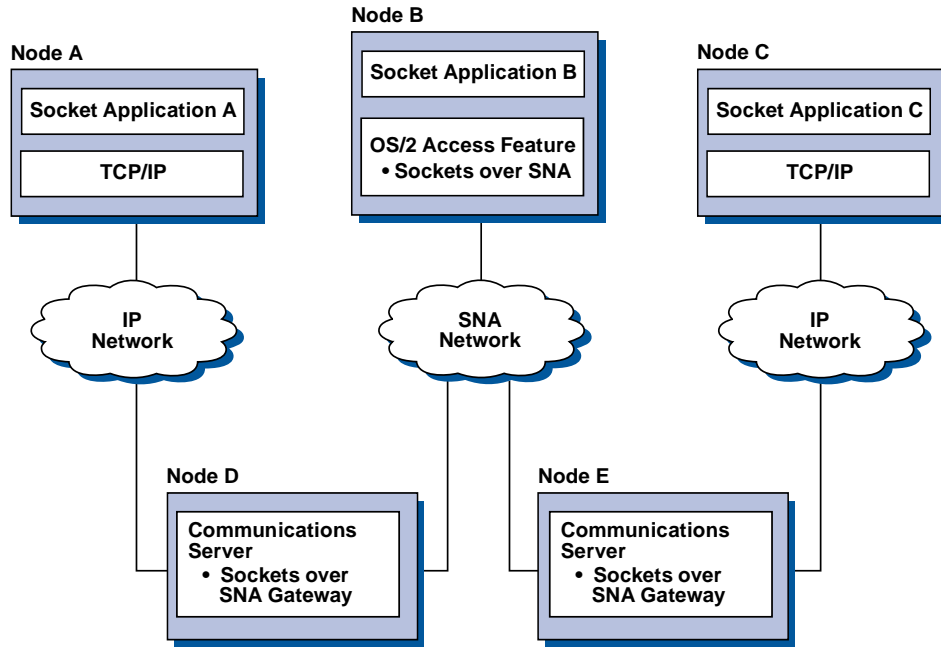


Figure 8. Socket Applications Communicating through Multiple Sockets Gateways

Connecting Sockets over SNA Access Nodes on Different Operating Systems

Figure 9 on page 26 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.

More about Communications Server

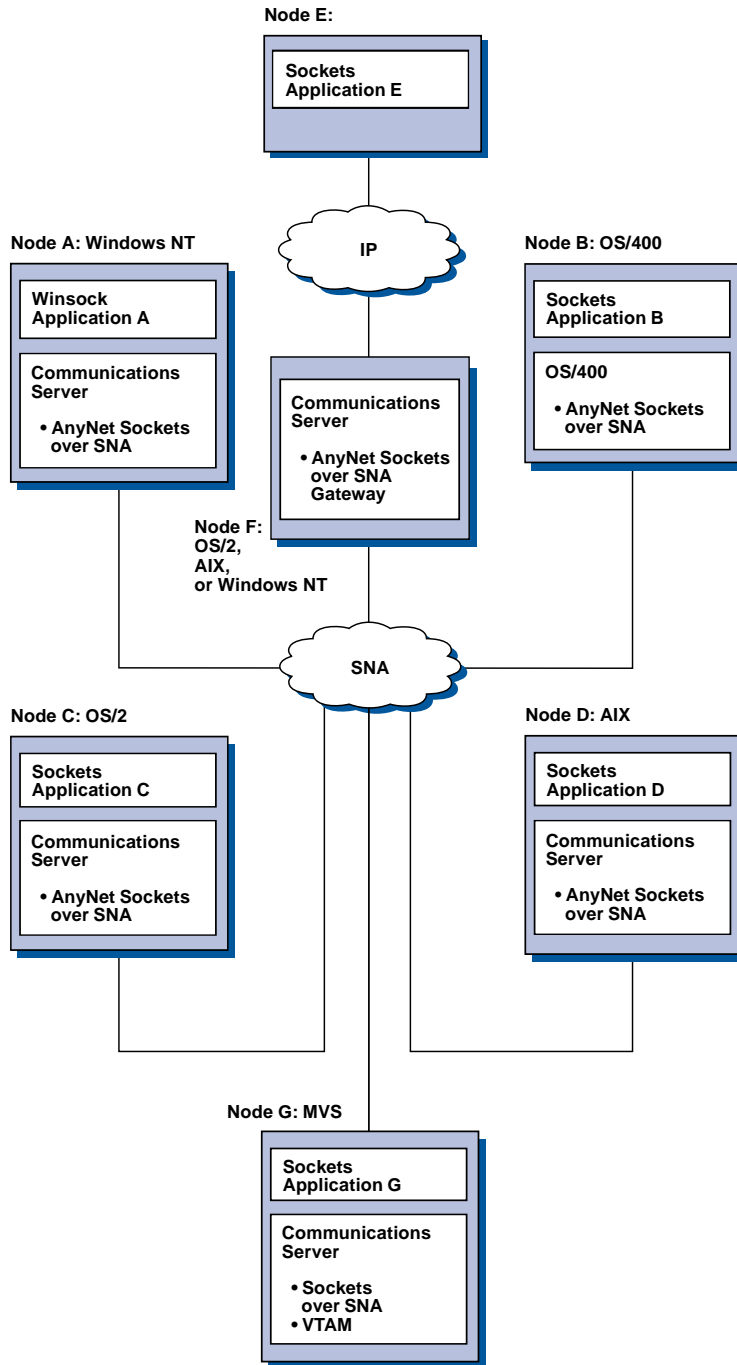


Figure 9. Socket Applications on Multiple Operating Systems Communicating over an SNA Network

Refer to “Appendix C. More Information About Sockets over SNA” on page 193 for more information about Sockets over SNA.

Local and Remote Configuration and Administration Support

A configuration GUI provides a user interface for entering configuration data. Local configuration is supported at both the client and server level. Remote configuration of the server is supported from Windows NT 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 clients. This support allows Node Operations to connect to and manage remote Communications Servers.

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
- WinSock
- Network Operator Facility
- Management Services
- Common Services

On the clients, the 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.

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, X.25, twinaxial (for upstream communication), and SNA over TCP/IP.

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.

The following Communications Server functions support a wide range of LU types:

- ***SNA Gateway Feature***

The SNA gateway enables an S/390 host to support LAN-attached workstations that implement LU 0, 1, 2, 3, or dependent LU 6.2. These LUs can be routed to multiple hosts.

The SNA gateway also supports LU 0, 1, 2, or 3 to AS/400 host computers. The AS/400 host passes the data through to an S/390 host.

- ***Conventional LU Application (LUA)***

The LUA consists of system software that supplies service routines to support LUs 0, 1, 2, and 3. These LUs can be routed to multiple hosts.

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.

More about Communications Server

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

The SNA Node Operations Facility 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 7. Problem Determination and Reporting” on page 139.

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

More about Communications Server

purposes. This emulator provides basic 5250 and 3270 support, and provides 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.

Part 2. Planning for, Installing, and Configuring Communications Server

Chapter 3. 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 start to install Communications Server, you should:

- 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 Version 5.0” on page 11 .
- Obtain access to the installation media (either a CD-ROM or the appropriate LAN environment).
- Prepare to use an administrator user ID with local authority when installing Communications Server.

Introduction to Installing Communications Server

Communications Server provides an interactive interface for installing the product.

Prerequisite Software

The minimum software requirements for Communication Server is Microsoft Windows NT Server 3.51 or 4.0. Consult the Windows NT documentation to determine the memory and hard disk storage requirements for your operating system.

TCP/IP is required for SNA API clients and Remote Administration clients to communicate with Communications Server.

Many 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.

Planning for Installing Communications Server

Communications Server will not install successfully on a machine that has Microsoft SNA Server** installed.

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

Prerequisite Hardware

Communications Server for Windows NT, Version 5.0 can be used on all Intel**-based systems that are supported by the Windows NT Server, Version 3.51 or Version 4.0 releases. An Intel Pentium machine, 100 MHz CPU with 32 MB of RAM, is the recommended server hardware.

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

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

Startup Drive Requirements during Installation

Communications Server requires 10 MB 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.

Remote Installation

For information on installing Communications Server remotely, refer to the Communications Server for Windows NT Web page:

<http://www.networking.ibm.com/cms/csnabt.html>

or refer to the product README file for more information.

Chapter 4. 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. As part of the Communications Server installation, the clients for SNA API client services and the clients for remote administration and configuration will be installed on the server.

In addition to the product files, the following features can be selectively installed from the CD, but the Communication Server product should be installed first.

- Clients for SNA API client services
 - OS/2
 - Windows 3.x
 - Windows 95
 - Windows NT
- Remote administration and configuration clients
- IBM Host On-Demand (a Web-based emulator)
- IBM Web Administration for Communications Server for Windows NT
- Entry-Level Personal Communications Emulator (install only after the Communications Server product)

Note: The IBM Host On-Demand and the Web Administration products are available in English only and require a Web server.

Considerations before Installing

Communications Server should be installed on an Intel-based computer running either Windows NT Server 3.51 or 4.0. To install the Communications Server, you must have a Windows NT administrator user ID with local authority.

Beginning Installation

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

Installing Communications Server

Communications Server 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.

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 in the interface provided.



Windows NT Version 3.51 does not automatically launch the interface. If you are installing on a machine running this version, you must 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. Online help is available throughout the installation procedure by clicking the **Help** button.

2. Click **Setup** to begin the installation of the InstallShield** Wizard. Once installed, the wizard will guide you through the rest of 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.
3. Choose the drive and directory for the installation of Communications Server. The default is **C:\IBMCS**, which will appear in the Destination Directory box. 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 to the Select Program Folder window.
4. 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 provided. 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.
5. 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**.

6. The Number of Concurrent Licenses window appears. Type the number of concurrent user licenses that you have purchased and click **Next**.
7. 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.
8. 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.

9. Once all product files have been copied, the Installing NT Services window appears.
10. 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**.

If you select **Yes** to install the IBM LLC2 protocol, the install program will launch a network control window with instructions for configuring IBM LLC2 to operate over your LAN adapters.

11. 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. Once you have created icons in the appropriate folder, you will need to associate these files with the Adobe Acrobat reader. See the README.TXT file for more information.

Uninstalling Communications Server for Windows NT

If you would like to uninstall the Communications Server product, do as follows:

Installing Communications Server

1. For Windows NT 3.51, click the **uninstall** icon from the IBM Communications Server folder and follow the procedures provided.
2. For Windows NT 4.0, click the **Control Panel** icon. Click the **Add/Remove Programs** icon. In the list box provided, click on whatever you called your folder, and then click the **Remove** button.
3. If you have the IBM LLC2 protocol interface installed, a help panel will help you uninstall the LLC2 protocol.



It is recommended 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.

Reinstalling Communications Server for Windows NT

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

Registering Communications Server for Windows NT

The IBM Software Servers offer a common method for registering the server products. The Axtive Registration Tool is used for this purpose. You can use this tool to register the Communications Server that you have purchased. 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 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 (CSNT50.LIC in the \csnt directory of the licensed product CD-ROM) to the directory where you installed Communications Server (normally 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.

Another alternative is to uninstall 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.

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. The SNA API clients are for the following operating systems:

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

Installing Communications Server

The client installation packages are located in the following directories under your Communications Server installation directory:

- clients\winNT
- clients\win95
- clients\win31
- 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 all of the other clients.

Another possibility is to install the SNA API clients directly from the CD-ROM onto a client machine instead of from a server. Follow the steps provided on the Communications Server CD-ROM.

Accessing the Remote Administration Clients

Remote administration and configuration clients are clients (for Windows NT only) used to remotely administer and configure the server. The remote administration clients are located in the following directory under your Communications Server installation directory:

- 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.

Another possibility is to install the remote administration clients directly from the CD-ROM onto a client machine instead of from a server. Follow the steps provided on the Communications Server CD-ROM.



It is not necessary to put the remote administration and configuration clients on the same machine as your server because they are already available on that machine.

Chapter 5. 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.



It is recommended 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.

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 44
Use Communications Server as a TN3270E server	“TN3270E Server Configuration” on page 52
Define an APPN network node (with HPR and connection networks)	“APPN Network Node Configuration” on page 59

Configuration Type	Refer To:
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 66
Define an AnyNet SNA over TCP/IP gateway	“AnyNet SNA over TCP/IP Gateway Configuration” on page 71
Define AnyNet Sockets over SNA	“AnyNet Sockets over SNA Configuration” on page 73
Configure Communications Server to support SNA API clients running APPC applications	“SNA API Client Configuration for APPC” on page 80
Configure Communications Server to support SNA API clients running 3270 or other LUA applications	“SNA API Client Configuration for LUA” on page 91
Run APPC or CPI-C applications or 5250 emulation to an AS/400 system	“CPI-C, APPC, or 5250 Emulation Configuration” on page 102
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 110
Access host applications using a 3270 emulator	“3270 Configuration” on page 117
Define a focal point	“Focal-Point Configuration” on page 123

SNA Gateway Configuration

This section describes the steps to take to configure Communications Server as a 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 “Step 1: Node Setup” on page 46, 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:

- 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 “Mapping SNA Resources to IP Addresses” on page 179 for more information.

Summary of Steps

- Step 1: Node Setup
- Step 2: Device Configuration
- Step 3: Define Host Links and LUs
- Step 4: Define Gateway Clients
- Step 5: Start the Node
- Step 6: Verify That the Link Is Active
- Step 7: Establish a Session

Step 1: Node Setup

Use the following procedure to name the local node and the network in which it operates:

1. Open the SNA Node Operations application by clicking the **SNA Node Operations** icon in the Communications Server folder. On the toolbar, click **Node Configuration** to launch the configuration application.
2. From the **File** menu, select **New**. Then from the **Scenarios** menu, select **SNA Gateway**.
3. From the SNA Node Configuration window, click **Configure Node**, then click **New**. The Define the Node window appears. Click the **Basic** tab and enter the following required information:

Control Point (CP)

Specify a fully qualified, unique CP name, which identifies the node within the network environment. It consists of two parts: the network name and the CP name.



If you do not know your CP name, as an example of a unique name, you can use the first 8 characters of the node's TCP/IP host name, which is found by entering **hostname** as a Windows NT command.

Local Node ID

Specify the node ID (XID) corresponding to the host PU. The local node ID consists of two parts: the block ID and the physical unit ID.

4. Click **OK** to continue.

Step 2: Device Configuration

Use this step to define supported communications devices on the machine, over which SNA links can be established to other nodes in the network.

From the SNA Node Configuration window, click **Configure Devices** and click one of the data link control (DLC) types listed below. Then click **New**. The following DLC types are available:

- **LAN**: There are three property pages for configuring a LAN device: Basic, Activation, and Performance. The only parameter you need to specify is the adapter number. If you have more than one LAN communications card (for example, token ring or Ethernet) installed, select the adapter number for the card you wish to use. You should accept all other defaults. Click **OK** to create the LAN device definition.



If no adapter information appears, you have chosen not to install the IBM LLC2 DLC interface during Communication Server installation, or you have failed to reboot after installing IBM LLC2. To install IBM LLC2, refer to the SETUP2.HLP help file, which is located in the Communications Server installation directory.

- **COM Port:** There are three property pages for configuring a COM port device: Basic, Incoming Call, and Performance. Typically, you will be using a modem to communicate over a COM port to a telephone network. Click on **Configure modem...** and follow the instructions for selecting and configuring a modem. Make sure that **Accept incoming calls** is checked if you want downstream clients to dial in. When you are finished, click **OK** to create the COM port device definition.
- **SDLC-MPA:** Define this type of device if you are using an MPA communications adapter for accessing a telephone network. There are four property pages for configuring an SDLC-MPA device: Basic, Adapter, Incoming Call, and Performance. Specify the communication port of the MPA card you will be using and make sure that **Accept incoming calls** is checked. When you are finished, click **OK** to create the SDLC-MPA device definition.



If your MPA card does not function properly when you start communications, a common cause is an incorrect IRQ setting. Return to this Adapter page and adjust the IRQ setting value.

- **SDLC-WAC:** Define this type of device if you are using a WAC communications adapter to access a telephone network. There are four property pages for configuring an SDLC-WAC device: Basic, Adapter, Incoming Call, and Performance. Specify the adapter number of the WAC card you will be using and make sure that **Accept incoming calls** is checked. Specify the port level (upper or lower) you will use. If you have an ISA adapter, be sure to also specify a shared RAM address that matches the shared RAM address of the card. When you are finished, click **OK** to create the SDLC-WAC device definition.
- **X.25-COM Port:** There are four property pages for configuring an X.25 COM port device: Basic, Network Parameters, Incoming Calls, and Frame Values. Typically, you will be using a modem to communicate over a COM port to an X.25 cloud. Specify the modem you will be using. Click **Configure modem...** and follow the instructions for selecting and configuring a modem. On the Network Parameters page, make sure that **Accept incoming call** is selected. When you are finished, click **OK** to create the X.25-COM port device definition.
- **X.25-WAC:** Define this type of device if you are using a WAC communications adapter for accessing an X.25 cloud. There are four property pages for configuring an X.25-WAC device: Basic, Network

SNA Gateway Configuration

Parameters, Incoming Calls, and Frame Values. Specify the adapter number and the port level (upper or lower) you will use. If you have an ISA adapter, be sure to also specify a shared RAM address that matches the shared RAM address of the card. On the Network Parameters page, make sure that **Accept incoming calls** is selected. When you are finished, click **OK** to create the X.25 WAC device definition.

- **Twinaxial:** Define this type of device if you are using an adapter which supports communications over a twinaxial cable. There is one property page for configuring this device: Basic. On this page, identify the supported twinaxial communications adapter type that you have installed. When you are finished, click **OK** to create the twinaxial device definition.
- **AnyNet SNA Over TCP/IP:** Define this type of device if you want to route your sessions over TCP/IP to another AnyNet SNA over TCP/IP node that is configured as a SNA gateway or client. There are three property pages for configuring this device: Basic, Routing Preferences, and Performance. On the Basic page, the SNA domain name should be the same name that you collected in “Before You Begin” on page 45. On the Routing Preferences page, specify **native first** as the default routing preference. When you are finished, click **OK** to create the AnyNet SNA over TCP/IP device.
- **OEM Adapters:** Communications Server provides configuration support for various OEM communication adapters. The configuration requirements are adapter-specific. Refer to the documentation provided with the adapter in order to complete this device configuration.

However, there are common parameters, which are located under the Basic tab, that you must specify for all OEM adapters. When you select the OEM Page tab, you must specify the port name. You should also select **APPN support** and **HPR support**.

Step 3: Define Host Links and LUs

This step configures the resources that are available on the host, in terms of LU addresses and the link used to access them. To define host links:

1. From the list of configuration options, select **Configure Gateway**, then click **View/Add/Change**.
2. From the Gateway Configuration window, click the **Host Links** tab. The Host Links property page appears, showing a list box containing all currently defined host links, that is, those that support SSCP-to-PU sessions.
3. Click **Create** to define a new link. The Host Link Type window appears.
4. Select the type of link you want to define by specifying the DLC type, then click **OK** to continue.



All connection definitions have a link station name associated with them. This is the name by which you will identify the connection when it is started by node operations. A default host link name is provided for you which you may change.

- **LAN:** There are three property pages for configuring a LAN connection: Basic, Advanced, and Security. For a LAN connection to a host, specify on the Basic page the link address of the host's communication controller, or an SNA gateway, to which you will be connecting. Also, on the Advanced page, specify the local node ID obtained in "Before You Begin" on page 45. Click **OK** to create the LAN connection definition.
- **COM Port, SDLC-MPA, and SDLC-WAC:** There are three property pages for configuring this connection: Basic, Link Information, and Performance. On the Basic page, specify the phone number to be used to dial into the host or the SNA gateway to the host. Be sure that the appropriate communication port is selected for the device that you configured in Step 2 above. On the Link Information page, specify that the link station address matches the address that is provided to you by the host's PU definition. (If you are using a switched line to a host, a local node ID (XID) should be used instead.) When you are finished, click **OK** to create the connection definition.
- **X.25-COM Port, X.25-WAC:** There are three property pages for configuring this connection: Basic, Link Information, and SVC Advanced Optional Facilities. On the Basic page, specify the communication port you plan to use as defined in Step 2 above. Also, select whether this link will be over a switched virtual circuit (SVC) or private virtual circuit (PVC). If it is an SVC link, specify the DTE addresses and extensions for establishing the link. If it is a PVC link, specify the PVC connection logical channel number. When you are finished, click **OK** to create the connection definition.
- **Twinaxial:** There are two property pages for configuring this connection: Basic and Security. On the Basic page, specify the TDLC station address of the host's communications controller. Also, provide the local node ID (XID) corresponding to the host's PU. When you are finished, click **OK** to create the connection definition.
- **AnyNet SNA over TCP/IP:** There is one property page for configuring this connection: Basic. On this page, specify the fully qualified CP name in the Adjacent Node Identifier box. If you are connecting to the host through an SNA gateway, specify the CP name of the SNA gateway connecting to the host. Otherwise, use the host's CP name. Click **OK** to create the connection definition.



The CP name you specified must be mapped to a TCP/IP address in order for AnyNet to determine where to route your SNA session over TCP/IP. To map the CP name to a TCP/IP address, refer to “Mapping SNA Resources to IP Addresses” on page 179.

- **OEM Adapters:** Communications Server provides configuration support for various OEM communication adapters. The configuration requirements are adapter-specific. Refer to the documentation provided with the adapter in order to complete this device configuration.

However, there are common parameters that you must specify for all OEM adapters. On the Link Information page, specify that this link supports SSCP sessions. Also, specify the local node ID (XID) provided by the host’s PU.

5. Respond **Yes** when asked if you want to create LUs on this new link.
6. The Define LUs window appears. With this window, you can define either a single LU or a range of LUs on the specified host link that reside on the host to which the link connects. Since you typically set up a host link with a range of available LUs, you will create a range of LUs instead of a single LU.
 - a. With **Range LU definition** selected, specify a base name for all LUs created for this range (for example, HOST). Each LU created in the range will begin with this base name followed by the LU’s address. The base name can be up to 5 characters long.
 - b. Specify the starting LU address and the number of consecutive addresses to create for the range.
 - c. By default, all LUs created are added to a pool (usually PUBLIC).
 - d. Click **OK** to define the range of LUs, then click **OK** again to close the Assigned LUs window.

Step 4: Define Gateway Clients

Use this step to define attributes for the downstream SNA client workstations that will be connecting into this gateway. To make the configuration as simple as possible, you will define the gateway to support implicit workstations, meaning that whenever a client establishes a link into the gateway, it will be assigned an LU resource from a default pool of resources, regardless of that client’s identity.

1. On the Gateway Configuration property sheet, click the **Implicit Clients** tab. The Implicit Clients page appears, showing a list of defined devices on the left-hand side (as defined in Step 2 above) and a tree diagram of implicit client templates on the right. At this point, there are no client templates displayed. A client template defines a range of client LU addresses and to which host LU pool they will be associated. This template is meant to be applied to a particular communications device.

Any client establishing a link to the gateway using that device will be issued an available resource from that template.



A template can use more than one pool, and a pool can be used in more than one template.

- a. To create a new client template, click **Create...** beneath the list box of currently defined client templates. The Implicit Template Definition window appears.
- b. Specify a name for the template, such as CLIENT.
- c. Specify the starting and ending address for the range of available addresses for clients to use. Clients must request an LU (NAU - network addressable unit) address you have defined.
- d. Select the pool from the pool name pull-down. The pool of host resources to which you are dedicating these client LUs should be the same pool name referenced by the Host LU Definition window in “Step 3: Define Host Links and LUs” on page 48.
- e. Click **OK** to create the client template.



- You can specify more than one range of addresses for a template, although you can only assign each address within a pool once. To add another range to a defined template, select a template and click **Add Range...** The Defined Templates window appears. Specify the starting and ending address and select a pool name. Then click **OK**.
 - To change the name of a template, select the template and click **Change...** The Implicit Template Definition window appears. Specify the new name and click **OK**. The name is changed dynamically wherever the template is used.
 - To change a range within a template, select the range and click **Change...** The Implicit Template Definition window appears. Specify the new range and click **OK**.
2. With the client template you just created highlighted on the right, select the communications port over which clients will establish links with this gateway.
 - a. Click **<<Assign to Port** to associate the template with the specified port.
 - b. Your SNA gateway configuration is complete. Click **OK** at the bottom of the Gateway property sheet to complete the gateway configuration.

SNA Gateway Configuration

You are done with the configuration aspect of this task. Save your configuration, giving it a name you can easily identify. After saving the configuration, exit the Node Configuration application and return to the SNA Node Operations application.

Step 5: Start the Node

Click **Start** 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.

Step 6: 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. To verify that the link you configured in Step 3 is active, click **Connections** on the SNA Node Operations toolbar. It may take a few moments for the link to be established.

Step 7: Establish a Session

You are now ready to have your clients attempt to 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.

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 “Step 1: Node Setup” on page 53, 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:

- 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

- Step 1: Node Setup
- Step 2: Device Configuration
- Step 3: Define Host Links and LUs
- Step 4: Define TN3270E Server Properties
- Step 5: Start the Node
- Step 6: Verify That the Link Is Active
- Step 7: Establish a Session

Step 1: Node Setup

Use the following procedure to name the local node and the network in which it operates:

1. Open the SNA Node Operations application by clicking the **SNA Node Operations** icon in the Communications Server folder. On the toolbar, click **Node Configuration** to launch the configuration application.
2. From the **File** menu, select **New**. Then, from the **Scenarios** menu, select **TN3270E Server**.
3. From the SNA Node Configuration window, click **Configure Node**, then click **New**. The Define the Node window appears. Click the **Basic** tab and enter the following required information:

Control Point (CP)

Specify a fully qualified, unique CP name, which identifies the node within the network environment. It consists of two parts: the network name and the CP name.



If you do not know your CP name, as an example of a unique name, you can use the first 8 characters of the node's TCP/IP host name, which is found by entering **hostname** as a Windows NT command.

Local Node ID

Specify the node ID (XID) corresponding to the host PU. The local node ID consists of two parts: the block ID and the physical unit ID.

4. Click **OK** to continue.

Step 2: Device Configuration

Use this step to define supported communications devices on the machine, over which SNA links can be established to other nodes in the network.

From the SNA Node Configuration window, click **Configure Devices** and then click one of the data link control (DLC) types. Then click **New**. The following DLC types are available:

- **LAN:** There are three property pages for configuring a LAN device: Basic, Activation, and Performance. The only parameter you need to specify is the device number. If you have more than one LAN communications card (for example, token ring or Ethernet) installed, select the adapter number for the card you wish to use. You should accept all other defaults. Click **OK** to create the LAN device definition.



If no adapter information appears, you have chosen not to install the IBM LLC2 DLC interface during Communication Server installation, or you have failed to reboot after installing IBM LLC2. To install IBM LLC2, refer to the SETUP2.HLP help file, which is located in the Communications Server installation directory.

- **COM Port:** There are three property pages for configuring a COM port device: Basic, Incoming Call, and Performance. Typically, you will be using a modem to communicate over a COM port to a telephone network. Click on **Configure modem...** and follow the instructions for selecting and configuring a modem. Make sure that **Accept incoming calls** is checked if you expect workstations to dial into this server. When you are finished, click **OK** to create the COM port device definition.
- **SDLC-MPA:** Define this type of device if you are using an MPA communication port for accessing a telephone network. There are four property pages for configuring an SDLC-MPA device: Basic, Adapter, Incoming Call, and Performance. Specify the communication port of the MPA card you will be using and make sure that **Accept incoming calls** is checked if you expect workstations to dial into this server. When you are finished, click **OK** to create the SDLC-MPA device definition.



If your MPA card does not function properly when you start communications, you may need to return to this Adapter page and adjust the IRQ setting value.

- **SDLC-WAC:** Define this type of device if you are using a WAC communications adapter to access a telephone network. There are four property pages for configuring an SDLC-WAC device: Basic, Adapter, Incoming Call, and Performance. Specify the adapter number and the port level (upper or lower) you will use. If you have an ISA adapter, be sure to also specify a shared RAM address. Finally, make sure that **Accept incoming calls** is checked if you expect workstations to dial into this server. When you are finished, click **OK** to create the SDLC-WAC device definition.
- **X.25-COM Port:** There are four property pages for configuring an X.25 COM port device: Basic, Network Parameters, Incoming Calls, and Frame Values. Typically, you will be using a modem to communicate over a COM port to an X.25 cloud. The only value you need to specify is the modem you will be using. Click **Configure modem...** and follow the instructions for selecting and configuring a modem. On the Network Parameters page, make sure that **Accept incoming calls** is checked if you expect workstations to dial into this server. When you are finished, click **OK** to create the X.25-COM port device definition.
- **X.25-WAC:** Define this type of device if you are using a WAC communications adapter for accessing an X.25 cloud. There are four property pages for configuring an X.25-WAC device: Basic, Network Parameters, Incoming Calls, and Frame Values. Specify the adapter number and the port level (upper or lower) you will use. If you have an ISA adapter, be sure to also specify a shared RAM address. On the Network Parameters page, make sure that **Accept incoming calls** is checked if you expect workstations to dial into this server. When you are finished, click **OK** to create the X.25 WAC device definition.
- **Twinaxial:** Define this type of device if you are using an adapter which supports communications over a twinaxial cable. There is one property page for configuring this device: Basic. On this page, identify the supported twinaxial communications adapter type that you have installed. When you are finished, click **OK** to create the twinaxial device definition.
- **AnyNet SNA Over TCP/IP:** Define this type of device if you want to route your 3270 session over TCP/IP to another AnyNet SNA over TCP/IP node that is configured as a SNA gateway or client. There are three property pages for configuring this device: Basic, Routing Preferences, and Performance. On the Basic page, the SNA domain name should be the same name as you collected in “Before You Begin” on page 52. On the Routing Preferences page, specify **native first** as the default routing preference. When you are finished, click **OK** to create the AnyNet SNA over TCP/IP device.
- **OEM Adapters:** Communications Server provides configuration support for various OEM communication adapters. The configuration requirements are

adapter-specific. Refer to the documentation provided with the adapter in order to complete this device configuration.

However, there are common parameters, which are located under the Basic tab, that you must specify for all OEM adapters. When you select the OEM Page tab, you must specify the port name. You should also select **APPN support** and **HPR support**.

Step 3: Define Host Links and LUs

This step configures the resources that are available on the host, in terms of LU addresses and the link used to access them. To define host links:

1. From the list of configuration options, select **Configure Gateway**, then click **View/Add/Change**.
2. From the Gateway Configuration window, click the **Host Links** tab. The Host Links property page appears, showing a list box containing all currently defined host links.
3. Click **Create** to define a new link. The Host Link Type window appears.
4. Select the type of link you want to define by specifying the DLC type, then click **OK** to continue.



All connection definitions have a link station name associated with them. This is the name by which you will identify the connection when it is started by node operations. A default name is provided for you which you may change.

- **LAN:** There are three property pages for configuring a LAN connection: Basic, Advanced, and Security. For a LAN connection to a host, specify on the Basic page the destination address of the host's communication controller, or an SNA gateway, to which you will be connecting, or click **Discover network address**. Also, on the Advanced page, specify the local node ID obtained in "Before You Begin" on page 52. Click **OK** to create the LAN connection definition.
- **COM Port, SDLC-MPA, and SDLC-WAC:** There are three property pages for configuring this connection: Basic, Link Information, and Performance. On the Basic page, specify the phone number to be used to dial into the host or the SNA gateway to the host. Be sure that the appropriate adapter or port number is selected for the device that you configured in Step 2 above. On the Link Information page, specify that the link station address matches that address that is provided to you by the host's PU definition. (If you are using a switched line to a host, a local node ID (XID) should be used instead.) When you are finished, click **OK** to create the connection definition.
- **X.25-COM Port, X.25-WAC:** There are three property pages for configuring this connection: Basic, Link Information, and SVC Advanced

Optional Facilities. On the Basic page, specify the communication port you plan to use as defined in Step 2 above. Also, select whether this link will be over a switched virtual circuit (SVC) or private virtual circuit (PVC). If it is an SVC link, specify the DTE addresses and extensions for establishing the link. If it is a PVC link, specify the PVC number for the link. On the Link Information page, specify that this link supports SSCP sessions. When you are finished, click **OK** to create the connection definition.

- **Twinaxial:** There are two property pages for configuring this connection: Basic and Security. On the Basic page, specify the TDLC station address of the host's communications controller. Also, provide the local node ID (XID) corresponding to the host's PU. When you are finished, click **OK** to create the connection definition.
- **AnyNet SNA over TCP/IP:** If you are connected to a host via DLUS/DLUR, you do not need to define an AnyNet SNA over TCP/IP connection. If you are connected to a host through an SNA gateway, there is only one property page for configuring this connection: Basic. On this page, specify the adjacent CP name for the SNA gateway which you will be connecting. If you are connecting to the host through an SNA gateway, specify the CP name of the SNA gateway connecting to the host. Otherwise, use the host's CP name. Click **OK** to create the connection definition.



The CP name you specify must be mapped to a TCP/IP address in order for AnyNet to determine where to route your SNA session over TCP/IP. To map the CP name to a TCP/IP address, refer to "Mapping SNA Resources to IP Addresses" on page 179.

- **OEM Adapters:** Communications Server provides configuration support for various OEM communication adapters. The configuration requirements are adapter-specific. Refer to the documentation provided with the adapter in order to complete this device configuration. However, there are common parameters that you must specify for all OEM adapters. On the Link Information page, specify that this link supports SSCP sessions. Also, specify the local node ID (XID) provided by the host's PU.
5. Respond **Yes** when asked if you want to create LUs on this new link.
 6. The Define LUs window appears. With this window, you can define either a single LU or a range of LUs on the specified host link that reside on the host to which the link connects. Since you typically set up a host link with a range of available LUs, you will create a range of LUs instead of a single LU.
 - a. With **Range LU definition** selected, specify a base name for all LUs created for this range (for example, HOST). Each LU created in the

TN3270E Server Configuration

range will begin with this base name followed by the LU's address. The base name can be up to 5 characters long.

- b. Specify the starting LU address and the number of consecutive addresses to create for the range.
- c. By default, all LUs created are added to a pool (usually PUBLIC).



Make sure that the LU model is for a 3270-2 display.

- d. Click **OK** to define the range of LUs, then click **OK** again to close the Assigned LUs window.

Step 4: Define TN3270E Server Properties

Use this step to define attributes for the host LUs to make them usable by TCP/IP clients. TCP/IP clients will use their TN3270E (or TN3270) applications to telnet into the gateway and establish emulator sessions with an SNA host using LUs you defined in Step 3 above.

1. On the Gateway Configuration property sheet, click the **TN3270E** tab. The TN3270E page appears, showing a field for specifying the default TN3270E pool, as well as any pools and/or single LUs you have defined in the list control below. You need to define only a default pool from which all incoming TN3270E (or TN3270) session requests will obtain an upstream host LU to use.
2. From the drop-down list, select **PUBLIC** as your default pool.



If you need to associate a printer to a particular workstation LU for use by a TCP/IP client, you will have to define a printer LU on your host link. On the TN3270E page, associate this printer to a particular LU in the PUBLIC pool.

Your TN3270E server configuration is complete. Click **OK** at the bottom of the property sheet to complete the server configuration.

You are done with the configuration aspect of this task. Save your configuration, giving it a name you can easily identify. After saving the configuration, exit the Node Configuration application and return to the SNA Node Operations application.

Step 5: Start the Node

Click **Start** on the SNA Node Operations toolbar to start the local node. Select the file you have just finished configuring and click **Open**. It may take a moment for the node to start and to establish all the defined links.

Step 6: 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. To verify that the link you configured in Step 3 is active, on the SNA Node Operations toolbar, click **Connections**.

Step 7: Establish a Session

Your TCP/IP clients may now attempt to establish a session through the TN3270E server to the host. From the client, start a TN3270E or TN3270 session, using the server's TCP/IP address or hostname as the destination. The server should then route that session to the host and provide an emulator session to the client.

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 “Step 1: Node Configuration” on page 60, 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 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 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

APPN Network Node Configuration

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 to do this. See “Step 3: Connection Configuration” on page 63 for details.

- 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 “Mapping SNA Resources to IP Addresses” on page 179 for more information.

Summary of Steps

- Step 1: Node Configuration
- Step 2: Device Configuration
- Step 3: Connection Configuration
- Step 4: Partner LU 6.2 Configuration
- Step 5: Connection Network Configuration
- Step 6: Start the Node
- Step 7: Verify That the Link Is Active
- Step 8: Establish a Session

Step 1: Node Configuration

To define a new node:

- Open the SNA Node Operations application by clicking the **SNA Node Operations** icon in the Communications Server folder. On the toolbar, click **Node Configuration** to launch the configuration application.
- From the **File** menu, select **New**. Then, from the **Scenarios** menu, select **APPN Network Node**.
- From the SNA Node Configuration window, click **Configure Node**, then click **New**. The Define the Node window appears, which contains the Basic property page.

Enter the following required information:

Control Point (CP)

Specify a fully qualified, unique CP name, which identifies the node within the network environment. It consists of two parts: the network name and the CP name.



If you do not know your CP name, as an example of a unique name, you can use the first 8 characters of the node's TCP/IP host name, which is found by entering **hostname** as a Windows NT command.

Node Type

Specify that the node is to be configured as a network node.

Step 2: Device Configuration

Use this step to define supported communications devices on the machine, over which SNA links can be established to other nodes in the network.

From the SNA Node Configuration window, click **Configure Devices** and then click one of the data link control (DLC) types listed below. Then click **New**. The following DLC types are available:

- **LAN:** There are three property pages for configuring a LAN device: Basic, Activation, and Performance. The only parameter you need to specify is the device number. If you have more than one LAN communications card (for example, token ring or Ethernet) installed, select the adapter number for the card you wish to use. You should accept all other defaults. Click **OK** to create the LAN device definition.



If no adapter information appears, you have chosen not to install the IBM LLC2 DLC interface during Communication Server installation, or you have failed to reboot after installing IBM LLC2. To install IBM LLC2, refer to the SETUP2.HLP help file, which is located in the Communications Server installation directory.

- **COM Port:** There are three property pages for configuring a COM port device: Basic, Incoming Call, and Performance. Typically, you will be using a modem to communicate over a COM port to a telephone network. Click on **Configure modem...** and follow the instructions for selecting and configuring a modem. Make sure that **Accept incoming calls** is checked if you expect workstations to dial into this server. When you are finished, click **OK** to create the COM port device definition.
- **SDLC-MPA:** Define this type of device if you are using an MPA communications adapter for accessing a telephone network. There are four property pages for configuring an SDLC-MPA device: Basic, Adapter, Incoming Call, and Performance. Specify the communication port of the

APPN Network Node Configuration

MPA card you will be using and make sure that **Accept incoming calls** is checked if you expect workstations to dial into this server. When you are finished, click **OK** to create the SDLC-MPA device definition.



If your MPA card does not function properly when you start communications, you may need to return to this Adapter page and adjust the IRQ setting value.

- **SDLC-WAC:** Define this type of device if you are using a WAC communications adapter to access a telephone network. There are four property pages for configuring an SDLC-WAC device: Basic, Adapter, Incoming Call, and Performance. Specify the adapter number and the port level (upper or lower) you will use. If you have an ISA adapter, be sure to also specify a shared RAM address. Finally, make sure that **Accept incoming calls** is checked if you expect workstations to dial into this server. When you are finished, click **OK** to create the SDLC-WAC device definition.
- **X.25-COM Port:** There are four property pages for configuring an X.25 COM port device: Basic, Network Parameters, Incoming Calls, and Frame Values. Typically, you will be using a modem to communicate over a COM port to an X.25 cloud. The only value you need to specify is the modem you will be using. Click **Configure modem...** and follow the instructions for selecting and configuring a modem. On the Network Parameters page, make sure that **Accept incoming calls** is checked if you expect workstations to dial into this server. When you are finished, click **OK** to create the X.25-COM port device definition.
- **X.25-WAC:** Define this type of device if you are using a WAC communications adapter for accessing an X.25 cloud. There are four property pages for configuring an X.25-WAC device: Basic, Network Parameters, Incoming Calls, and Frame Values. Specify the adapter number and the port level (upper or lower) you will use. If you have an ISA adapter, be sure to also specify a shared RAM address. On the Network Parameters page, make sure that **Accept incoming calls** is checked if you expect workstations to dial into this server. When you are finished, click **OK** to create the X.25 WAC device definition.
- **Twinaxial:** Define this type of device if you are using an adapter which supports communications over a twinaxial cable. There is one property page for configuring this device: Basic. On this page, identify the supported twinaxial communications adapter type that you have installed. When you are finished, click **OK** to create the twinaxial device definition.
- **AnyNet SNA over TCP/IP:** Define this device if you want to route your sessions over TCP/IP to another AnyNet SNA over TCP/IP node. There are three property pages for configuring this device: Basic, Routing Preferences, and Performance. On the Basic page, the SNA domain name should be the same name as you collected in “Before You Begin” on page 59. On the

Routing Preferences page, specify **non-native first** as the default routing preference. When you are finished, click **OK** to create the AnyNet SNA over TCP/IP device.

- **OEM Adapters:** Communications Server provides configuration support for various OEM communication adapters. The configuration requirements are adapter-specific. Refer to the documentation provided with the adapter in order to complete this device configuration.

However, there are common parameters, which are located under the Basic tab, that you must specify for all OEM adapters. When you select the OEM Page tab, you must specify the port name. You should also select **APPN support** and **HPR support**.

Step 3: Connection Configuration

You need to configure a connection only if the network node will establish links to other nodes in the network. Typically, network nodes all establish one link to another network node, while end nodes establish links into their network node servers.

Use this step to define links to other nodes in the SNA network over devices defined in Step 2. Applications will use these links in order to establish conversations with remote applications.



All connection definitions have a link station name associated with them. This is the name by which you identify the connection when it is started by node operations. A default name is provided for you, which you can change.

- From the SNA Node Configuration window, click **Configure Connection**. The following DLCs are available:
 - **LAN:** There are three property pages for configuring a LAN connection: Basic, Advanced, and Security. For a LAN connection, on the Basic page, specify the link address of the remote node to which you will be connecting. If you configured the node with a discovery server name, such as IROUTSNA, click **Discover Network Address...** to get a list of APPN network nodes to which you can connect.



Under Node Setup, you can also configure a unique group name that other end nodes can use to find this node.

Also, on the Advanced page, specify HPR support. Click **OK** to create the LAN connection definition.

- **COM Port, SDLC-MPA, and SDLC-WAC:** There are three property pages for configuring this connection: Basic, Link Information, and Performance. On the Basic page, specify the phone number to be used to

APPN Network Node Configuration

dial into the remote node. Be sure that the appropriate adapter or port number is selected for the device which you configured in Step 2 above. Also, on the Link Information page, specify HPR support. When you are finished, click **OK** to create the connection definition.

- **X.25-COM Port, X.25-WAC:** There are three property pages for configuring this connection: Basic, Link Information, and SVC Advanced Optional Facilities. On the Basic page, specify the communication port you plan to use as defined in Step 2 above. Also, specify whether this link will be over a switched virtual circuit (SVC) or private virtual circuit (PVC). If it is a SVC link, specify the DTE addresses and extensions for establishing the link. If it is a PVC link, specify the PVC number for the link. Also, on the Link Information page, specify HPR support. When you are finished, click **OK** to create the connection definition.
- **AnyNet SNA Over TCP/IP:** For independent LU 6.2 sessions, you do not need to specify an AnyNet SNA over TCP/IP connection. Setting the routing preference to route over TCP/IP will cause sessions initiated from this node to be routed to TCP/IP (see “How to Route SNA Sessions over AnyNet SNA over TCP/IP” on page 185).
- **OEM Adapters:** Communications Server provides configuration support for various OEM communication adapters. The configuration requirements are adapter-specific. Refer to the documentation provided with the adapter in order to complete this device configuration.
However, there are common parameters that you must specify for all OEM adapters. On the Link Information page, select **APPN support** and **HPR support**.

Step 4: Partner LU 6.2 Configuration

If the network node will be connecting to adjacent LEN nodes, you must configure all LUs that these LEN nodes own. These LUs will be made available to other nodes in the APPN network as if the LUs resided on end nodes. To accomplish this, you must define these partner LUs and their locations in terms of the owning LEN node’s control point name.

1. From the SNA Node Configuration window, click **Configure Partner LU 6.2**, then click **New**.
2. On the Basic property page, specify the LEN node’s LU name as the fully qualified (network name plus LU name) partner LU name. Also, specify the LEN node’s fully qualified control point (CP) name.
3. Click **OK** to continue.

Step 5: Connection Network Configuration

If you know that the network node will participate in a connection network, you must configure a connection network definition for each connection network in which this network node will participate.

1. From the SNA Node Configuration window, click **Configure Connection Networks**, then click **New**.
2. On the Basic property page, specify the fully qualified (network name plus CP name) connection network name that represents the connection network. Also, check each LAN device over which this connection network is to be accessed.
3. Click **OK** to create the connection network definition.

You have completed the configuration aspect of this task. Save your configuration, giving it a name you can easily identify. After saving the configuration, exit the Node Configuration application and return to the SNA Node Operations application.

Step 6: Start the Node

Click **Start** on the SNA Node Operations toolbar to start the local node. Specify the configuration you have just finished configuring, then click **Open**. It may take a moment for the node to start and to establish all the defined links.

Step 7: Verify That the Link Is Active

When the node has started, you will see a view of the active node with the control point name displayed that you specified in Step 1. To verify that the link you configured in Step 3 is active, click **Connections** on the SNA Node Operations toolbar and make sure that the link is on the list and is active. It may take a few moments for the link to be established.

Step 8: Establish a Session

The network node is now ready to route independent LU 6.2 (APPC) sessions. Make sure that each end node or LEN node is connected to the network node and that any other network nodes that should be linked with this node have done so. 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.

APPN Network Node Configuration



Make sure that the APINGD application is installed and that a TP definition for the application is configured on the remote system.

DLUR/DLUS Configuration

This task shows you how 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 both 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 59). You may also use this task to configure the local node as an APPN end node; to do this, on the Node Configuration step, select **End node** as the node type, and disregard the Partner LU 6.2 Configuration step.



Before proceeding with “Step 1: DLUR PUs Configuration” on page 67, 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 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 "Mapping SNA Resources to IP Addresses" on page 179 for more information.



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

Summary of Steps

Subtask: DLUR Support for Local LUs

- Step 1: DLUR PUs Configuration
- Step 2: Local LU 0 to 3 Configuration

Subtask: DLUR Support for Downstream LUs

- Step 1: Define a Default DLUS
- Step 2: Assign a DLUS to a Client Template
- Step 3: Start the Node
- Step 4: Verify That the Link Is Active
- Step 5: Establish a Session

DLUR Support for Local LUs Subtask

Step 1: DLUR PUs Configuration

You must configure an internal DLUR PU which will serve as the PU for the dependent LUs, managing sessions between these LUs and the host DLUS.

1. From the SNA Node Configuration window, click **Configure DLUR PUs**, then click **New**.
2. On the Basic property page, specify a PU name to which the local LU 0 to 3 LUs will be associated. Also, specify the local node ID (XID)

corresponding to the host's PU, as well as the DLUS name. Specify a backup DLUS name if you have one (to specify your own values, uncheck **Use global defaults**).



You can specify a default DLUS and a backup DLUS when defining the node. By checking **Use Global Defaults**, you are choosing to use these default values.

3. Click **OK** to create the DLUR PU definition.

Step 2: Local LU 0 to 3 Configuration

Use this step to define the local LU which will serve your application (for example, a 3270 emulator) by establishing an SNA session with a host's LU.

1. From the SNA Node Configuration window, click **Configure Local LU 0 to 3**, then click **New**.
2. On the Basic property page, define the following parameters:
 - **LU name:** Specify a name up to 8 characters long that identifies this LU for your application. For example, use a portion of your last name.
 - **NAU address:** Specify an available LU address on the host's PU.
 - **PU name:** This name is the same as the DLUR PU name you specified in Step 1. This name should already be included in the pull-down list.
3. Click **OK** to create the LU definition.

This step also applies to the configuration of Dependent LU 6.2 Sessions to a Host. See "Dependent LU 6.2 Sessions to a Host" on page 110 for more information.

You have finished with the configuration aspect of this task. Save your configuration, providing it with a name that you can easily identify. After saving the configuration, exit the Node Configuration application and return to the SNA Node Operations application.

Continue with "Step 3: Start the Node" on page 70.

DLUR Support for Downstream LUs Subtask

When using DLUR/DLUS to support downstream LUs, you do not configure direct links to the host. Instead, you assign a DLUS and backup DLUS-name pair to implicit client template definitions. The APPN network will be responsible for routing dependent LU session requests from the clients to the DLUS in the network.

Step 1: Define a Default DLUS

1. From the list of configuration options, click **Configure Node**, then click **View/Change/Add** to modify the existing node definition.
2. On the DLU Requester tab, specify the name of your primary DLUS. Also, specify the backup DLUS, if you have one. These names correspond to the default dependent LU servers for this node.
3. Click **OK** to save your changes.

Step 2: Assign a DLUS to a Client Template

By creating an implicit client template and associating it to the default DLUS and a communications device, you are specifying that all clients calling into this gateway on this device are to have their session requests routed to the specified DLUS. Note that you haven't defined any local LU 0 to 3 LUs or host links. As a gateway, the local node has no knowledge of which LUs are available on the host; it is passing that responsibility to the downstream DLUR client.

To establish PU connections, you create a template with an NAU address range and a host pool defined. Then, you associate the template with a defined port. Each port can have a single template associated with it, but you can associate the same template with several ports.

1. From the list of configuration options, click **Configure Gateway**, then click **View/Change/Add** to invoke the gateway configuration property sheet.
2. On the Gateway Configuration property sheet, click the **Implicit Clients** tab. The Implicit Clients page appears, showing a list of defined devices on the left-hand side and a list of client templates on the right. At this point, there are no client templates displayed. A client template defines a range of client LU addresses and to which DLUS, in this case, they will be associated. This template is meant to be applied to a particular communications device. Any client establishing a link to the gateway using that device will be issued an available resource from that template.
 - a. To create a new client template, click **Create...** beneath the list box of currently defined client templates. The Implicit Template Definition window appears.
 - b. Specify a name for the template, such as CLIENT.
 - c. Select the port name you want to use and then select the template you want to associate with it. Then click **<<Assign to Port**.
 - d. Check **Provide DLUR services for the downstream PU**.
 - e. Click **OK** to create the client template.

You have completed the configuration aspect of this task. Save your configuration, giving it a name that you can easily identify. After saving the configuration, exit the Node Configuration application and return to the SNA Node Operations application.

Step 3: Start the Node

Click **Start** 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.

Step 4: 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. To verify that the link you configured to the APPN network is active, click **Connections** on the SNA Node Operations toolbar.

Step 5: Establish a Session

The local node is now ready for communicating to the DLUS.

Start a 3270 Session (for DLUR Support for Local LUs Subtask)

You are now ready to start your 3270 display, printer session application, or emulator.



If you have problems, verify that the LU address you chose is active with a session to the host by displaying active LU 0 to 3 sessions. If no application (emulator) is currently active, an SSCP-LU session will be active with the LU address. Otherwise an LU-LU session will be active, which indicates that your application is in conversation with the host. Also, verify that you have a session using the DLUR mode name **CPSVRMGR**.

Establish a Session Through the Gateway (for DLUR Support for Downstream LUs Subtask)

You are now ready to have your clients attempt to 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.

AnyNet SNA over TCP/IP Gateway Configuration

This section describes how 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 wish to route dependent LU sessions from downstream AnyNet SNA over TCP/IP workstations to upstream hosts, you must use the SNA Gateway function along with AnyNet SNA over TCP/IP. See “SNA Gateway Configuration” on page 44 to set up the local node for this function.



Do not proceed with Step 1 until you can answer all questions and locate all required 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

- Step 1: APPN Network Node Configuration
- Step 2: Map the LU Names to TCP/IP Addresses
- Step 3: Start the Node
- Step 4: Verify That the Link Is Active
- Step 5: Establish a Session

Step 1: APPN Network Node Configuration

Complete Steps 1 through 5 of “APPN Network Node Configuration” on page 59 as appropriate. When you define the AnyNet SNA over TCP/IP

AnyNet SNA over TCP/IP Gateway Configuration

device, be sure to specify gateway support, not access node support. When you specify gateway support, APPN searches AnyNet SNA over TCP/IP for SNA resources in the IP network.

Step 2: Map the LU Names to TCP/IP Addresses

In order for the AnyNet SNA over TCP/IP gateway to route session traffic to other AnyNet SNA over TCP/IP nodes, fully qualified LU names must be mapped to the TCP/IP address of the remote AnyNet SNA over TCP/IP node through which the gateway gains access to the LU. This information is stored in the HOSTS file in your TCP/IP configuration. See “Appendix B. More Information About Configuring AnyNet SNA over TCP/IP” on page 179 for details on how to perform this mapping.

Step 3: Start the Node

Click **Start** on the SNA Node Operations toolbar to start the local node. Select the file you have just finished configuring and click **Open**. It may take a moment for the node to start and to establish all the defined links.

Step 4: 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. To verify that links you have configured to other APPN or LEN nodes are active, on the SNA Node Operations toolbar, click **Connections**.

Step 5: Establish a Session

The AnyNet SNA over TCP/IP gateway is now ready to route SNA traffic between SNA nodes and AnyNet SNA over TCP/IP nodes.

For APPC sessions, you can use the Check Connection (APING) application from the Communications Server program group on the desktop to verify that an AnyNet SNA over TCP/IP node is reachable. When you invoke the application, specify the fully qualified control point name (NetworkID.CPName) of the remote AnyNet SNA over TCP/IP node as the partner LU name. Click **OK** to continue. The application will send test packets of data to the remote node’s APINGD application. These packets will then be returned to the local application.



Make sure that the APINGD application is installed on the remote system.

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 Step 1, answer all questions and 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:

- 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.

AnyNet Sockets over SNA Configuration

- 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), then 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

- Step 1: Node Setup
- Step 2: Device Configuration
- Step 3: Connection Configuration
- Step 4: Partner LU 6.2 Configuration
- Step 5: Local TCP/IP Address Configuration
- Step 6: Configure the LU Mapping
- Step 7: Start the Node
- Step 8: Start the Session

Step 1: Node Setup

Use the following procedure to name the local node and the network in which it operates.

1. Open the SNA Node Operations application by clicking the **SNA Node Operations** icon in the Communications Server folder. On the toolbar, click **Node Configuration** to launch the configuration application.
2. From the **File** menu, select **New**. Then, from the **Scenarios** menu, select **AnyNet Sockets over SNA**.
3. From the SNA Node Configuration window, click **Configure Node**, then click **New**. The Define the Node window appears, which contains the Basic property page.

Enter the following required information:

Control Point (CP)

Specify a fully qualified, unique CP name, which identifies the node within the network environment. It consists of two parts: the network name and the CP name.



If you do not know your CP name, as an example of a unique name, you can use the first 8 characters of the node's TCP/IP host name, which is found by entering **hostname** as a Windows NT command.

Node Type

Specify whether the node is to be configured as an end node or network node. The default setting is end node.

4. Click **OK** to continue.

Step 2: Device Configuration

Use this step to define supported communications devices on the machine, over which SNA links can be established to other nodes in the network.

From the SNA Node Configuration window, click **Configure Devices** and then click one of the data link control (DLC) types listed below. Then click **New**. The following DLC types are available:

- **LAN:** There are three property pages for configuring a LAN device: Basic, Advanced, and Performance. The only parameter you need to specify is the device number. If you have more than one LAN communications card (for example, token ring or Ethernet) installed, select the adapter number for the card you wish to use. You should accept all other defaults. Click **OK** to create the LAN device definition.



If no adapter information appears, you have chosen not to install the IBM LLC2 DLC interface during Communication Server installation, or you have failed to reboot after installing IBM LLC2. To install IBM LLC2, refer to the SETUP2.HLP help file, which is located in the Communications Server installation directory.

- **COM Port:** There are three property pages for configuring a COM port device: Basic, Incoming Call, and Performance. Typically, you will be using a modem to communicate over a COM port to a telephone network. Click on **Configure modem...** and follow the instructions for selecting and configuring a modem. Make sure that **Accept incoming calls** is checked if you expect workstations to dial into this server. When you are finished, click **OK** to create the COM port device definition.
- **SDLC-MPA:** Define this type of device if you are using an MPA communications adapter for accessing a telephone network. There are four property pages for configuring an SDLC-MPA device: Basic, Adapter, Incoming Call, and Performance. Specify the adapter number of the MPA card you will be using and make sure that **Accept incoming calls** is checked if you expect workstations to dial into this server. When you are finished, click **OK** to create the SDLC-MPA device definition.



If your MPA card does not function properly when you start communications, you may need to return to the Adapter page and adjust the IRQ setting value.

- **SDLC-WAC:** Define this type of device if you are using a WAC communications adapter to access a telephone network. There are four property pages for configuring an SDLC-WAC device: Basic, Adapter, Incoming Call, and Performance. Specify the adapter number and the port level (upper or lower) you will use. If you have an ISA adapter, be sure to also specify a shared RAM address. Finally, make sure that **Accept incoming calls** is checked if you expect workstations to dial into this server. When you are finished, click **OK** to create the SDLC-WAC device definition.
- **X.25-COM Port:** There are four property pages for configuring an X.25 COM port device: Basic, Network Parameters, Incoming Calls, and Frame Values. Typically, you will be using a modem to communicate over a COM port to an X.25 network. The only value you need to specify is the modem you will be using. Click **Configure modem...** and follow the instructions for selecting and configuring a modem. On the Network Parameters page, make sure that **Accept incoming calls** is checked if you expect workstations to dial into this server. When you are finished, click **OK** to create the X.25-COM port device definition.
- **X.25-WAC:** Define this type of device if you are using a WAC communications adapter for accessing an X.25 cloud. There are four property pages for configuring an X.25-WAC device: Basic, Network Parameters, Incoming Calls, and Frame Values. Specify the adapter number and the WAC port (upper or lower) you will use. If you have an ISA adapter, be sure to also specify a shared RAM address. On the Network Parameters page, make sure that **Accept incoming calls** is checked if you expect workstations to dial into this server. When you are finished, click **OK** to create the X.25 WAC device definition.
- **Twinaxial:** Define this type of device if you are using an adapter which supports communications over a twinaxial cable. There is one property page for configuring this device: Basic. On this page, identify the supported twinaxial communications adapter type that you have installed. When you are finished, click **OK** to create the twinaxial device definition.
- **OEM Adapters:** Communications Server provides configuration support for various OEM communication adapters. The configuration requirements are adapter-specific. Refer to the documentation provided with the adapter in order to complete this device configuration.

However, there are common parameters, which are located under the Basic tab, that you must specify for all OEM adapters. When you select the OEM Page tab, you must specify the port name. You should also select **APPN support** and **HPR support**.

Step 3: Connection Configuration

Use this step to define links to other nodes in the SNA network over devices defined in Step 2. Sockets over SNA will use these links in order to establish conversations with remote Sockets over SNA nodes.



All connection definitions have a link station name associated with them. This is the name by which you identify the connection when it is started by node operations. A default name is provided for you, which you can change.

- From the SNA Node Configuration window, click **Configure Connections**. The following DLCs are available:
 - **LAN**: There are three property pages for configuring a LAN connection: Basic, Advanced, and Security. For a LAN connection, on the Basic page, specify the link address of the remote node to which you will be connecting. If you configured the node with a discovery server name, such as IROUTSNA, click **Discover Network Address...** to discover an appropriate LAN address for your network node server. Also, on the Advanced page, specify HPR support. Click **OK** to create the LAN connection definition.



Under Node Setup, you can also configure a unique group name that other end nodes can use to find this node.

- **COM Port, SDLC-MPA, and SDLC-WAC**: There are three property pages for configuring this connection: Basic, Link Information, and Performance. On the Basic page, specify the phone number to be used to dial into the remote node. Be sure that the appropriate adapter or port number is selected for the device which you configured in Step 2 above. Also, on the Link Information page, specify HPR support. When you are finished, click **OK** to create the connection definition.
- **X.25-COM Port, X.25-WAC**: There are three property pages for configuring this connection: Basic, Link Information, and SVC Advanced Optional Facilities. On the Basic page, specify the communications adapter you plan to use as defined in Step 2 above. Also, specify whether this link will be over a switched virtual circuit (SVC) or private virtual circuit (PVC). If it is a SVC link, specify the DTE addresses and extensions for establishing the link. If it is a PVC link, specify the PVC number for the link. Also, on the Link Information page, specify HPR support. When you are finished, click **OK** to create the connection definition.
- **OEM Adapters**: Communications Server provides configuration support for various OEM communication adapters. The configuration requirements are adapter-specific. Refer to the documentation provided with the adapter in order to complete this device configuration.

AnyNet Sockets over SNA Configuration

However, there are common parameters that you must specify for all OEM adapters. On the Link Information page, select **APPN support** and **HPR support**.

Step 4: Partner LU 6.2 Configuration

You only need to configure a Partner LU 6.2 definition if you are not connecting into an APPN network via a network node. This definition allows you to specify the location of the partner LU in terms of its owning control point name (the control point name is unique per node in the entire network). The APPN network would normally locate the LU for you. Using this definition can expedite the search for an APPN resource, or be used to allow the local node to determine the route to the LU itself, in which case the owning control point is assumed to be an adjacent node in the network (LEN level connection). See “How an IP Address Is Mapped to an LU Name” on page 198 for more information.

1. From the SNA Node Configuration window, click **Configure Partner LU 6.2**, then click **New**.
2. On the Basic property page, specify the fully qualified partner LU name (network name plus LU name) to which you wish to connect. Also, specify the fully qualified owning control point name.
3. Click **OK** to continue.

Step 5: Local TCP/IP Address Configuration

Here you will assign a TCP/IP address to the AnyNet Sockets over SNA node. This IP address will be used by remote sockets applications elsewhere in the network when accessing sockets applications through the AnyNet Sockets over SNA access node. If this node will act as a Sockets over SNA gateway, this IP address is the gateway address specified in routes on other Sockets over SNA nodes.

1. From the SNA Node Configuration window, click **Configure AnyNet Sockets over SNA**, then click **New**.
2. On the Local page, select **sna0 interface** and click **Change....**
3. In the resulting dialog, specify the TCP/IP address which will represent this Sockets over SNA node. Also specify the associated subnet mask. If you do not specify a subnet mask, a default will be assigned for you.
4. Click **OK** to save the IP address.
5. When you return to the Local page, make sure that **Yes** is selected for using this configuration on the local node. Do *not* click **OK** at the bottom of the property sheet yet.

Step 6: Configure the LU Mapping

You can either explicitly associate an LU name to a TCP/IP address, or have AnyNet generate the LU name based upon the TCP/IP address. It is recommended that you generate LU names based on a template and mask and that you use the same template and mask on every Sockets over SNA node in the network. Since the algorithms for generating the names are the same on every AnyNet node, you do not need to be aware of new nodes being added to the network. All you need to know is their AnyNet Sockets over SNA IP address.

1. From the AnyNet Sockets over SNA property sheet, select the LUs tab.
2. On the LUs page, click **New...** to specify a new mapping.
3. On the resulting panel, leaving **Generate LU names** selected, specify the address mask and LU template. The template will be used to prefix all generated LU names, the rest of the name being filled in based upon the destination IP address at runtime. Use the online help for more information about LU name generation.
4. Click **OK** to save the LU mapping. The other tabs on the AnyNet Sockets over SNA property sheet are for more advanced features and are not necessary for getting your configuration up and running.
5. Click **OK** at the bottom of the AnyNet Sockets over SNA property sheet to commit your changes. You will be immediately taken into a panel for the installation of the AnyNet gateway device driver information. Follow the instructions on that panel carefully in order to get the device installed properly on your system. For detailed instructions, click **Help**. This device is necessary for allowing the local system to act as an AnyNet Sockets over SNA gateway as well as an access node.

You are finished with the configuration aspect of this task. Save your configuration, giving it a name you can easily identify. After saving the configuration, exit the Node Configuration application and return to the SNA Node Operations application. Shut down and restart your workstation.

Step 7: Start the Node

Click **Start** 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**.

Step 8: Start the Session

Once a link between you and the APPN network or partner node is active, you are ready to try your TCP/IP application.

AnyNet Sockets over SNA Configuration

Try using 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 that you configured in Step 5 above.

SNA API Client Configuration for APPC

This section describes the steps necessary for configuring 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 91. 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 Step 1, locate **all** required information listed in "Before You Begin" on page 81. 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 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.

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, you can make up a fictitious name, if you do not know what the value should be.

- 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), then 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, then 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

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

- Step 1: Administering User IDs
- Step 2: Node Setup
- Step 3: Device Configuration
- Step 4: Connection Configuration
- Step 5: Local LU 6.2 Configuration
- Step 6: Partner LU 6.2 Configuration
- Step 7: Enable SNA API Client Support
- Step 8: Transaction Program Configuration

Configuring the SNA API client to run APPC applications:

- Step 1: Configure Global Data
- Step 2: Configure Server Location
- Step 3: Configure Transaction Program Definition
- Step 4: Configure CPI-C Side Information Definition

Testing the configuration:

- Step 1: Start the Communications Server Node
- Step 2: Verify That All Configured Links Are Active
- Step 3: Establish the Connection from the SNA API Client

Step 1: 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 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 under Start, Programs, Administrative Tools, or for Windows NT 3.51 under Main, Administrative Tools.
2. If user IDs for the SNA API client end users do not already exist, create them with the User Manager. From the File pull-down, create a new user.

Specify a user ID and password for this user. You can use the full name and description to describe the particular SNA API client that will use this ID, such as “Bob’s machine”.

3. 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 that you want to give access to, if they are not listed.



Ambiguous user IDs that are replicated across domains (local and trusted) can cause logon access to be denied. Communications Server resolves the ID by using only the first occurrence of it, starting with:

- a. The local server running Communications Server
- b. The local domain controller that the server is associated with
- c. Any trusted domain that the local domain controller has trusted relationships with.

To ensure that the user is able to attach to the server, follow these steps. If the user ID specified during the login process is defined:

- Locally on the server system
Include this local ID in the local IBMCSAPI or IBMCSADMIN group, or both, on that server either explicitly or through a local or global group.
- Both locally and on one or more domains
Add the local ID (or a local/global group that it is a member of) to the local IBMCSAPI or IBMCSADMIN groups, or both, to represent the other instances of that ID on the domain controller. Otherwise, you must use an alternative ID that is not defined on the local system.
- On one or more domains
Ensure that it is defined on the local domain controller associated with the Communications Server system and add that ID (or a local/global group that it is a member of) to the IBMCSAPI or IBMCSADMIN group, or both.

4. Exit the User Manager application.

Step 2: Node Setup

Use the following procedure to name the local node and the network in which it operates.

1. Open the SNA Node Operations application by clicking the **SNA Node Operations** icon in the Communications Server folder. On the toolbar, click **Node Configuration** to launch the configuration application.

SNA API Client Configuration for APPC

2. From the **File** menu, select **New**. Then, from the **Scenarios** menu, select **SNA API Clients running APPC applications**.
3. From the SNA Node Configuration window, click **Configure Node**, then click **New**. The Define the Node window appears.
4. Enter the following required information:

Control Point (CP)

Specify a fully qualified, unique CP name, which identifies the node within the network environment. It consists of two parts: the network name and the CP name.

Node Type

Specify whether the node is to be configured as an end node or network node. The default setting is end node.

5. Click **OK** to continue.

Step 3: Device Configuration

Use this step to define supported communications devices on the machine, over which SNA links can be established to other nodes in the network.

From the SNA Node Configuration window, click **Configure Devices** and select one of the data link control (DLC) types listed below. Then click **New**. The following DLC types are available:

- **LAN:** There are three property pages for configuring a LAN device: Basic, Activation, and Performance. The only parameter you need to specify is the device number. If you have more than one LAN communications card (for example, token ring or Ethernet) installed, select the adapter number for the card you wish to use. You should accept all other defaults. Click **OK** to create the LAN device definition.



If no adapter information appears, you have chosen not to install the IBM LLC2 DLC interface during Communication Server installation, or you have failed to reboot after installing IBM LLC2. To install IBM LLC2, refer to the SETUP2.HLP help file, which is located in the Communications Server installation directory.

- **COM Port:** There are three property pages for configuring a COM port device: Basic, Incoming Call, and Performance. Typically, you will be using a modem to communicate over a COM port to a telephone network. Click on **Configure modem...** and follow the instructions for selecting and configuring a modem. Make sure that **Accept incoming calls** is checked if you expect workstations to dial into this server. When you are finished, click **OK** to create the COM port device definition.
- **SDLC-MPA:** Define this type of device if you are using an MPA communications adapter for accessing a telephone network. There are four

property pages for configuring an SDLC-MPA device: Basic, Adapter, Incoming Call, and Performance. Specify the adapter number of the MPA card you will be using and make sure that **Accept incoming calls** is checked. When you are finished, click **OK** to create the SDLC-MPA device definition.



If your MPA card does not function properly when you start communications, you may need to return to this Adapter page and adjust the IRQ setting value.

- **SDLC-WAC:** Define this type of device if you are using a WAC communications adapter to access a telephone network. There are four property pages for configuring an SDLC-WAC device: Basic, Adapter, Incoming Call, and Performance. Specify the adapter number and the port level (upper or lower) you will use. If you have an ISA adapter, be sure to also specify a shared RAM address. Finally, make sure that **Accept incoming calls** is checked if you expect workstations to dial into this server. When you are finished, click **OK** to create the SDLC-WAC device definition.
- **X.25-COM Port:** There are four property pages for configuring an X.25 COM port device: Basic, Network Parameters, Incoming Calls, and Frame Values. Typically, you will be using a modem to communicate over a COM port to an X.25 cloud. The only value you need to specify is the modem you will be using. Click **Configure modem...** and follow the instructions for selecting and configuring a modem. On the Network Parameters page, make sure that **Accept incoming calls** is checked if you expect workstations to dial into this server. When you are finished, click **OK** to create the X.25-COM port device definition.
- **X.25-WAC:** Define this type of device if you are using a WAC communications adapter for accessing an X.25 cloud. There are four property pages for configuring an X.25-WAC device: Basic, Network Parameters, Incoming Calls, and Frame Values. Specify the adapter number and the port level (upper or lower) you will use. If you have an ISA adapter, be sure to also specify a shared RAM address. On the Network Parameters page, make sure that **Accept incoming calls** is checked if you expect workstations to dial into this server. When you are finished, click **OK** to create the X.25 WAC device definition.
- **Twinaxial:** Define this type of device if you are using an adapter which supports communications over a twinaxial cable. There is one property page for configuring this device: Basic. On this page, identify the supported twinaxial communications adapter type that you have installed. When you are finished, click **OK** to create the twinaxial device definition.
- **AnyNet SNA over TCP/IP:** Define this device if you want to route your session over TCP/IP to another AnyNet SNA over TCP/IP node. There are three property pages for configuring this device: Basic, Routing Preferences, and Performance. On the Basic page, the SNA domain name should be the

same name as you collected in “Before You Begin” on page 81. On the Routing Preferences page, specify **non-native first** as the default routing preference. When you are finished, click **OK** to create the AnyNet SNA over TCP/IP device.

- **OEM Adapters:** Communications Server provides configuration support for various OEM communication adapters. The configuration requirements are adapter-specific. Refer to the documentation provided with the adapter in order to complete this device configuration.

However, there are common parameters, which are located under the Basic tab, that you must specify for all OEM adapters. When you select the OEM Page tab, you must specify the port name. You should also select **APPN support** and **HPR support**.

Step 4: Connection Configuration

Use this step to define links to other nodes in the SNA network over devices defined in Step 2. Applications will use these links in order to establish conversations with remote applications.



All connection definitions have a link station name associated with them. This is the name by which you identify the connection when it is started by node operations. A default name is provided for you, which you can change.

- From the SNA Node Configuration window, click **Configure Connections** and select one of the data link control (DLC) types listed below. Then click **New**. The following DLC types are available:
 - **LAN:** There are three property pages for configuring a LAN connection: Basic, Advanced, and Security. For a LAN connection, on the Basic page, specify the link address of the remote node to which you will be connecting. If you configured the node with a discovery server name, such as IROUTSNA, click **Discover Network Address...** to discover an appropriate LAN address for your network node server. Also, on the Advanced page, specify HPR support. Click **OK** to create the LAN connection definition.
 - **COM Port, SDLC-MPA, and SDLC-WAC:** There are three property pages for configuring this connection: Basic, Link Information, and Performance. On the Basic page, specify the phone number to be used to dial into the remote node. Be sure that the appropriate adapter or port number is selected for the device which you configured in Step 2 above. Also, on the Link Information page, specify HPR support. When you are finished, click **OK** to create the connection definition.
 - **X.25-COM Port, X.25-WAC:** There are three property pages for configuring this connection: Basic, Link Information, and SVC Advanced Optional Facilities. On the Basic page, specify the communications

adapter you plan to use as defined in Step 2 above. Also, specify whether this link will be over a switched virtual circuit (SVC) or private virtual circuit (PVC). If it is a SVC link, specify the DTE addresses and extensions for establishing the link. If it is a PVC link, specify the PVC number for the link. Also, on the Link Information page, specify HPR support. When you are finished, click **OK** to create the connection definition.

- **AnyNet SNA Over TCP/IP:** For independent LU 6.2 sessions, you do not need to specify an AnyNet SNA over TCP/IP connection. Setting either the default routing preference for all LUs or for particular LUs to **non-native first** or **non-native only** on the AnyNet SNA over TCP/IP device will cause the session to be routed over TCP/IP.
- **OEM Adapters:** Communications Server provides configuration support for various OEM communication adapters. The configuration requirements are adapter-specific. Refer to the documentation provided with the adapter in order to complete this device configuration.
However, there are common parameters that you must specify for all OEM adapters. On the Link Information page, select **APPN support** and **HPR support**.

Step 5: Local LU 6.2 Configuration

You must explicitly define local LUs on Communications Server for use by SNA API clients. The local LUs will manage the local side of the APPC session for the SNA API client.

1. From the SNA Node Configuration window, click **Configure Local LU 6.2**, then click **New**.
2. On the Basic property page, specify the local LU name that the SNA API client will use for establishing its APPC sessions, both inbound and outbound. You will need to use this name when configuring the SNA API client. Also, specify that a session using this LU is to be routed to an SNA API client.
3. Click **OK** to continue.

Step 6: Partner LU 6.2 Configuration

You only need to configure a Partner LU 6.2 definition if you are not connecting into an APPN network via a network node. This definition allows you to specify the location of the partner LU in terms of its owning control point name (the control point name is unique per node in the entire network). The APPN network would normally locate the LU for you. Using this definition can expedite the search for an APPN resource, or be used to allow

SNA API Client Configuration for APPC

the local node to determine the route to the LU itself, in which case the owning control point is assumed to be an adjacent node in the network (LEN level connection).

1. From the SNA Node Configuration window, click **Configure Partner LU 6.2**, then click **New**.
2. On the Basic property page, specify the fully qualified partner LU name (network name plus LU name) to which you wish to connect. Also, specify the fully qualified owning control point name.
3. Click **OK** to continue.

Step 7: Enable SNA API Client Support

To enable SNA API clients:

1. From the SNA Node Configuration window, click **Configure Gateway**, then click **View/Change/Add**.
2. On the SNA Client tab, make sure that **Enable SNA API Client Services** is checked.
3. Click **OK** to continue.

Step 8: Transaction Program Configuration

If you need to configure the client with an application for other nodes to access using APPC, you may need to create a Transaction Program definition for that application.

1. From the SNA Node Configuration window, click **Configure Transaction Program**, then click **New**.
2. On the Basic property page, the only parameters you must specify are the TP name and the complete pathname to the application. The TP name is the 8-character identifier with which the application will be associated on the SNA network. When a remote node needs to invoke this application, it must specify the name you put in this field. You should specify a meaningful name that can be identified with the function provided by the application.
On the Advanced page, specify that this TP is for use by the SNA API client.
3. Click **OK** to continue.

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.



Locate all required information in “Before You Begin” before proceeding to Step 1.

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 NT system where Communications Server resides.
- The TCP/IP address 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, then you must 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? 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, then Step 4 under the APPC configuration subtask is also required.

The following steps assume you have started the SNA API client's configuration utility from the SNA client folder. The configuration options mentioned below are generic in the sense that they do not map to a particular configuration interface.

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.

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 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 an APPC 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 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 to save the Communications Server configuration. 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 now 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 will need to 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 necessary for configuring 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

SNA API Client Configuration for LUA

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 91 . 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 Step 1, 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.

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.

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

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

- Step 1: Administering User IDs
- Step 2: Node Setup
- Step 3: Device Configuration
- Step 4: Define Host Links and LUs
- Step 5: Define SNA API Client Access to Host Resources

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

- Step 1: Configure Global Data
- Step 2: Create an LUA Definition

Testing the configuration:

- Step 1: Start the Communications Server Node
- Step 2: Verify That All Configured Links Are Active
- Step 3: Establish the Connection from the SNA API Client

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

Step 1: 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. It may take a moment for the node to start and to establish all the defined links.

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

1. Invoke the User Manager application for Windows NT 4.0 under Start, Programs, Administrative Tools, or for Windows NT 3.51 under Main, Administrative Tools.
2. If user IDs for the SNA API client end users do not already exist, create them with the User Manager. From the File pull-down, create a new user. Specify a user ID and password for this user. You can use the full name and description to describe the particular SNA API client that will use this ID, such as "Bob's machine".

SNA API Client Configuration for LUA

- 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 that you want to give access to, if they are not listed.



Ambiguous user IDs that are replicated across domains (local and trusted) can cause logon access to be denied. Communications Server resolves the ID by using only the first occurrence of it, starting with:

- The local server running Communications Server
- The local domain controller that the server is associated with
- Any trusted domain that the local domain controller has trusted relationships with.

To ensure that the user is able to attach to the server, follow these steps. If the user ID specified during the login process is defined:

- Locally on the server system
Include this local ID in the local IBMCSAPI or IBMCSADMIN group, or both, on that server either explicitly or through a local or global group.
- Both locally and on one or more domains
Add the local ID (or a local/global group that it is a member of) to the local IBMCSAPI or IBMCSADMIN groups, or both, to represent the other instances of that ID on the domain controller. Otherwise, you must use an alternative ID that is not defined on the local system.
- On one or more domains
Ensure that it is defined on the local domain controller associated with the Communications Server system and add that ID (or a local/global group that it is a member of) to the IBMCSAPI or IBMCSADMIN group, or both.

- Exit the User Manager application.

Step 2: Node Setup

Use the following procedure to name the local node and the network in which it operates:

- Open the SNA Node Operations application by clicking the **SNA Node Operations** icon in the Communications Server folder. On the toolbar, click **Node Configuration** to launch the configuration application.
- From the **File** menu, select **New**. Then, from the **Scenarios** menu, select **SNA API Clients running 3270 or other LUA applications**.

- From the SNA Node Configuration window, click **Configure Node**, then click **New**. The Define the Node window appears. Click the **Basic** tab and enter the following required information:

Control Point (CP)

Specify a fully qualified, unique CP name, which identifies the node within the network environment. It consists of two parts: the network name and the CP name.

Local Node ID

Specify the node ID (XID) corresponding to the host PU. The local node ID consists of two parts: the block ID and the physical unit ID.

- Click **OK** to continue.

Step 3: Device Configuration

Use this step to define supported communications devices on the machine, over which SNA links can be established to other nodes in the network.

From the SNA Node Configuration window, click **Configure Devices** and select one of the data link control (DLC) types listed below. Then click **New**. The following DLC types are available:

- **LAN:** There are three property pages for configuring a LAN device: Basic, Activation, and Performance. The only parameter you need to specify is the device number. If you have more than one LAN communications card (for example, token ring or Ethernet) installed, select the adapter number for the card you wish to use. You should accept all other defaults. Click **OK** to create the LAN device definition.



If no adapter information appears, you have chosen not to install the IBM LLC2 DLC interface during Communication Server installation, or you have failed to reboot after installing IBM LLC2. To install IBM LLC2, refer to the SETUP2.HLP help file, which is located in the Communications Server installation directory.

- **COM Port:** There are three property pages for configuring a COM port device: Basic, Incoming Call, and Performance. Typically, you will be using a modem to communicate over a COM port to a telephone network. Click on **Configure modem...** and follow the instructions for selecting and configuring a modem. Make sure that **Accept incoming calls** is checked if you expect workstations to dial into this server. When you are finished, click **OK** to create the COM port device definition.
- **SDLC-MPA:** Define this type of device if you are using an MPA communications adapter for accessing a telephone network. There are four property pages for configuring an SDLC-MPA device: Basic, Adapter, Incoming Call, and Performance. Specify the adapter number of the MPA

card you will be using and make sure that **Accept incoming calls** is checked if you expect workstations to dial into this server. When you are finished, click **OK** to create the SDLC-MPA device definition.



If your MPA card does not function properly when you start communications, you may need to return to this Adapter page and adjust the IRQ setting value.

- **SDLC-WAC:** Define this type of device if you are using a WAC communications adapter to access a telephone network. There are four property pages for configuring an SDLC-WAC device: Basic, Adapter, Incoming Call, and Performance. Specify the adapter number and the port level (upper or lower) you will use. If you have an ISA adapter, be sure to also specify a shared RAM address. When you are finished, click **OK** to create the SDLC-WAC device definition.
- **X.25-COM Port:** There are four property pages for configuring an X.25 COM port device: Basic, Network Parameters, Incoming Calls, and Frame Values. Typically, you will be using a modem to communicate over a COM port to an X.25 cloud. Specify the modem you will be using. Click **Configure modem...** and follow the instructions for selecting and configuring a modem. On the Network Parameters page, make sure that **Accept incoming call** is selected if you expect workstations to dial into this server. When you are finished, click **OK** to create the X.25-COM port device definition.
- **X.25-WAC:** Define this type of device if you are using a WAC communications adapter for accessing an X.25 cloud. There are four property pages for configuring an X.25-WAC device: Basic, Network Parameters, Incoming Calls, and Frame Values. Specify the adapter number and the port level (upper or lower) you will use. If you have an ISA adapter, be sure to also specify a shared RAM address. On the Network Parameters page, make sure that **Accept incoming calls** is selected if you expect workstations to dial into this server. When you are finished, click **OK** to create the X.25 WAC device definition.
- **Twinaxial:** Define this type of device if you are using an adapter which supports communications over a twinaxial cable. There is one property page for configuring this device: Basic. On this page, identify the supported twinaxial communications adapter type that you have installed. When you are finished, click **OK** to create the twinaxial device definition.
- **AnyNet SNA Over TCP/IP:** Define this type of device if you want to route your sessions over TCP/IP to another AnyNet SNA over TCP/IP node. There are three property pages for configuring this device: Basic, Routing Preferences, and Performance. On the Basic page, the SNA domain name should be the same name as you collected in “Before You Begin” on page 92

. On the Routing Preferences page, specify **non-native first** as the default routing preference. When you are finished, click **OK** to create the AnyNet SNA over TCP/IP device.

- **OEM Adapters:** Communications Server provides configuration support for various OEM communication adapters. The configuration requirements are adapter-specific. Refer to the documentation provided with the adapter in order to complete this device configuration.

However, there are common parameters, which are located under the Basic tab, that you must specify for all OEM adapters. When you select the OEM Page tab, you must specify the port name. You should also select **APPN support** and **HPR support**.

Step 4: Define Host Links and LUs

This step configures the resources that are available on the host, in terms of LU addresses and the link used to access them. To define host links:

1. From the list of configuration options, select **Configure Gateway**, then click **View/Change/Add**.
2. From the Gateway Configuration window, click the **Host Links** tab. The Host Links property page appears, showing a list box containing all currently defined host links.
3. Click **Create** to define a new link. The Host Link Type window appears.
4. Select the type of link you want to define by specifying the DLC type, then click **OK** to continue.



All connection definitions have a link station name associated with them. This is the name by which you will identify the connection when it is started by node operations. A default name is provided for you which you may change.

- **LAN:** There are three property pages for configuring a LAN connection: Basic, Advanced, and Security. For a LAN connection to a host, specify on the Basic page the link address of the host's communication controller, or an SNA gateway, to which you will be connecting. Also, on the Advanced page, specify the local node ID obtained in "Before You Begin" on page 92. Click **OK** to create the LAN connection definition.
- **COM Port, SDLC-MPA, and SDLC-WAC:** There are three property pages for configuring this connection: Basic, Link Information, and Performance. On the Basic page, specify the phone number to be used to dial into the host or the SNA gateway to the host. Be sure that the appropriate adapter or port number is selected for the device that you configured in Step 2 above. On the Link Information page, specify that the link station address matches that address that is provided to you by

the host's PU definition. (If you are using a switched line to a host, a local node ID (XID) should be used instead.) When you are finished, click **OK** to create the connection definition.

- **X.25-COM Port, X.25-WAC:** There are three property pages for configuring this connection: Basic, Link Information, and SVC Advanced Optional Facilities. On the Basic page, specify the communications adapter you plan to use as defined in Step 2 above. Also, select whether this link will be over a switched virtual circuit (SVC) or private virtual circuit (PVC). If it is an SVC link, specify the DTE addresses and extensions for establishing the link. If it is a PVC link, specify the PVC number for the link. When you are finished, click **OK** to create the connection definition.
- **Twinaxial:** There are two property pages for configuring this connection: Basic and Security. On the Basic page, specify the TDLC station address of the host's communications controller. Also, provide the local node ID (XID) corresponding to the host's PU. When you are finished, click **OK** to create the connection definition.
- **AnyNet SNA over TCP/IP:** If your host connectivity is through DLUS/DLUR, you do not need to specify an AnyNet SNA over TCP/IP connection. Setting the default routing preference for all LUs or for particular LUs to **non-native first** or **non-native only** on the AnyNet SNA over TCP/IP device will cause the session to be routed over TCP/IP. If your host connectivity is to another SNA gateway, there is one property page for configuring this connection: Basic. On this page, specify the adjacent CP name for the host to which you will connect. If you are connecting to the host through an SNA gateway, specify the CP name of the SNA gateway connecting to the host. Otherwise, use the host's CP name. Click **OK** to create the connection definition.



The CP name you specified must be mapped to a TCP/IP address in order for AnyNet to determine where to route your SNA session over TCP/IP. To map the CP name to a TCP/IP address, refer to "Mapping SNA Resources to IP Addresses" on page 179.

- **OEM Adapters:** Communications Server provides configuration support for various OEM communication adapters. The configuration requirements are adapter-specific. Refer to the documentation provided with the adapter in order to complete this device configuration.

However, there are common parameters that you must specify for all OEM adapters. On the Link Information page, specify that this link supports SSCP sessions. Also, specify the local node ID (XID) provided by the host's PU.

5. When asked is you want to create LUs on this new link, respond **Yes**.

6. The Define LUs window appears. With this window, you can define either a single LU or a range of LUs on the specified host link that reside on the host to which the link connects. Since you typically set up a host link with a range of available LUs, you will create a range of LUs instead of a single LU.
 - a. With **Range LU definition** selected, specify a base name for all LUs created for this range (for example, HOST). Each LU created in the range will begin with this base name followed by the LU's address. The base name can be up to 5 characters long.
 - b. Specify the starting LU address and the number of consecutive addresses to create for the range.
 - c. By default, all LUs created are added to a pool (usually PUBLIC).
 - d. Click **OK** to define the range of LUs, then click **OK** again to close the Assigned LUs window.

Step 5: Define SNA API Client Access to Host Resources

In Step 4 you configured host LUs for access by SNA API clients. You also configured all of the LUs to be contained in the PUBLIC LU pool. You will now define the PUBLIC pool as the default pool for use by SNA API clients. SNA API clients may either request any available LU from the pool or a specific LU (by LU name) for use in a new session.

On the Gateway Configuration property sheet, click the SNA Clients tab. The SNA Clients page appears, which shows that SNA API Client Services is supported. Specify the PUBLIC pool as the default pool for SNA API Client Services. Click **OK** at the bottom of the Gateway property sheet when done.

You are finished with the configuration aspect of this task for Communications Server. All that is left is to configure the SNA API Client, then attach the two. Save your configuration, giving it a name you can easily identify. After saving the configuration, exit the Node Configuration application and return to the SNA Node Operations application.

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.



Locate all required information in “Before You Begin” on page 100 before proceeding with Step 1.

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 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.

The following steps assume you have started the SNA API client's configuration utility from the SNA client folder. The configuration options mentioned below are generic in the sense that they do not map to a particular configuration interface.

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.

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 wish 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, you must 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 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 to save the Communications Server configuration.

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 now 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 will need to start the Attach Manager application. Attach Manager automatically starts transaction programs configured to start with Attach Manager.

CPI-C, APPC, or 5250 Emulation Configuration

This section describes the steps to take 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), then 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 “Mapping SNA Resources to IP Addresses” on page 179 for more information.

Summary of Steps

- Step 1: Node Setup
- Step 2: Device Configuration
- Step 3: Connection Configuration
- Step 4: Transaction Program Configuration
- Step 5: Partner LU 6.2 Configuration
- Step 6: CPI-C Side Information Configuration
- Step 7: Start the Node
- Step 8: Verify That the Link Is Active
- Step 9: Start the Session

Step 1: Node Setup

Use the following procedure to name the local node and the network in which it operates.

1. Open the SNA Node Operations application by clicking the **SNA Node Operations** icon in the Communications Server folder. On the toolbar, click **Node Configuration** to launch the configuration application.
2. From the **File** menu, select **New**. Then, from the **Scenarios** menu, select **CPI-C, APPC, or 5250 Emulation**.
3. From the SNA Node Configuration window, click **Configure Node**, then click **New**. The Define the Node window appears, which contains the Basic property page:
 - Basic
Enter the following required information:

Control Point (CP)

Specify a fully qualified, unique CP name, which identifies the node within the network environment. It consists of two parts: the network name and the CP name.



If you do not know your CP name, as an example of a unique name, you can use the first 8 characters of the node's TCP/IP host name, which is found by entering **hostname** as a Windows NT command.

Node Type

Specify whether the node is to be configured as an end node or network node. The default setting is end node.

4. Click **OK** to continue.

Step 2: Device Configuration

Use this step to define supported communications devices on the machine, over which SNA links can be established to other nodes in the network.

From the SNA Node Configuration window, click **Configure Devices** and select a data link control (DLC) type from the list. Then click **New**. The following DLC types are available:

- **LAN:** There are three property pages for configuring a LAN device: Basic, Activation, and Performance. The only parameter you need to specify is the adapter number. If you have more than one LAN communications card (for example, token ring or Ethernet) installed, select the adapter number for the card you wish to use. You should accept all other defaults. Click **OK** to create the LAN device definition.



If no adapter information appears, you have chosen not to install the IBM LLC2 DLC interface during Communication Server installation, or you have failed to reboot after installing IBM LLC2. To install IBM LLC2, refer to the SETUP2.HLP help file, which is located in the Communications Server installation directory.

- **COM Port:** There are three property pages for configuring a COM port device: Basic, Incoming Call, and Performance. Typically, you will be using a modem to communicate over a COM port to a telephone network. Click on **Configure modem...** and follow the instructions for selecting and configuring a modem. Make sure that **Accept incoming calls** is checked if you expect workstations to dial into this server. When you are finished, click **OK** to create the COM port device definition.
- **SDLC-MPA:** Define this type of device if you are using an MPA communications adapter for accessing a telephone network. There are four property pages for configuring an SDLC-MPA device: Basic, Adapter,

Incoming Call, and Performance. Select the communication port of the MPA card you will be using. When you are finished, click **OK** to create the SDLC-MPA device definition.



If your MPA card does not function properly when you start communications, you may need to return to this Adapter page and adjust the IRQ setting value.

- **SDLC-WAC:** Define this type of device if you are using a WAC communications adapter to access a telephone network. There are four property pages for configuring an SDLC-WAC device: Basic, Adapter, Incoming Call, and Performance. Specify the adapter number and the WAC port (upper or lower) you will use. If you have an ISA adapter, be sure to also specify a shared RAM address. Finally, make sure that **Accept incoming calls** is checked if you expect workstations to dial into this server. When you are finished, click **OK** to create the SDLC-WAC device definition.
- **X.25-COM Port:** There are four property pages for configuring an X.25 COM port device: Basic, Network Parameters, Incoming Calls, and Frame Values. Typically, you will be using a modem to communicate over a COM port to an X.25 cloud. The only value you need to specify is the modem you will be using. Click **Configure modem...** and follow the instructions for selecting and configuring a modem. On the Network Parameters page, make sure that **Accept incoming calls** is checked. When you are finished, click **OK** to create the X.25-COM port device definition.
- **X.25-WAC:** Define this type of device if you are using a WAC communications adapter for accessing an X.25 cloud. There are four property pages for configuring an X.25-WAC device: Basic, Network Parameters, Incoming Calls, and Frame Values. Specify the adapter number and the port level (upper or lower) you will use. If you have an ISA adapter, be sure to also specify a shared RAM address. On the Network Parameters page, make sure that **Accept incoming calls** is checked. When you are finished, click **OK** to create the X.25 WAC device definition.
- **Twinaxial:** Define this type of device if you are using an adapter which supports communications over a twinaxial cable. There is one property page for configuring this device: Basic. On this page, identify the supported twinaxial communications adapter type that you have installed. When you are finished, click **OK** to create the twinaxial device definition.
- **AnyNet SNA over TCP/IP:** Define this device if you want to route your session over a TCP/IP connection to another AnyNet SNA over TCP/IP access node or gateway. There are three property pages for configuring this device: Basic, Routing Preferences, and Performance. On the Basic page, the SNA domain name should be the same name that you collected in “Before You Begin” on page 102. On the Routing Preferences page, specify **non-native first** as the default routing preference. When you are finished,

click **OK** to create the AnyNet SNA over TCP/IP device. See “Mapping SNA Resources to IP Addresses” on page 179 for more information.

- **OEM Adapters:** Communications Server provides configuration support for various OEM communication adapters. The configuration requirements are adapter-specific. Refer to the documentation provided with the adapter in order to complete this device configuration.

However, there are common parameters, which are located under the Basic tab, that you must specify for all OEM adapters. When you select the OEM Page tab, you must specify the port name. You should also select **APPN support** and **HPR support**.

Step 3: Connection Configuration

Use this step to define links to other nodes in the SNA network over devices defined in Step 2. Applications will use these links in order to establish conversations with remote applications.



All connection definitions have a link station name associated with them. This is the name by which you identify the connection when it is started by node operations. A default name is provided for you, which you can change.

- From the SNA Node Configuration window, click **Configure Connections** and select a data link control (DLC) type. Then click **New**. The following DLC types are available:
 - **LAN:** There are three property pages for configuring a LAN connection: Basic, Advanced, and Security. For a LAN connection, on the Basic page, specify the destination address of the remote node to which you will be connecting. If you configured the node with a discovery server name, such as IROUTSNA, click **Discover Network Address...** to discover an appropriate LAN address for your network node server. Also, on the Advanced page, specify HPR support. Click **OK** to create the LAN connection definition.
 - **COM Port, SDLC-MPA, and SDLC-WAC:** There are three property pages for configuring this connection: Basic, Link Information, and Performance. On the Basic page, specify the phone number to be used to dial into the remote node. Be sure that the appropriate communication port number is selected for the device which you configured in Step 2 above. Also, on the Link Information page, specify HPR support. When you are finished, click **OK** to create the connection definition.
 - **X.25-COM Port, X.25-WAC:** There are three property pages for configuring this connection: Basic, Link Information, and SVC Advanced Optional Facilities. On the Basic page, specify the communications port you plan to use as defined in Step 2 above. Also, specify whether this link will be over a switched virtual circuit (SVC) or private virtual circuit

(PVC). If it is a SVC link, specify the DTE addresses and extensions for establishing the link. If it is a PVC link, specify the PVC connection logical channel number. Also, on the Link Information page, specify HPR support. When you are finished, click **OK** to create the connection definition.

- **AnyNet SNA Over TCP/IP:** For independent LU 6.2 sessions, you do not need to define an AnyNet SNA over TCP/IP connection. Setting the default routing preference for all LUs or for particular LUs on the AnyNet SNA over TCP/IP device will cause the sessions to be routed over TCP/IP.
- **OEM Adapters:** Communications Server provides configuration support for various OEM communication adapters. The configuration requirements are adapter-specific. Refer to the documentation provided with the adapter in order to complete this device configuration.

However, there are common parameters that you must specify for all OEM adapters. On the Link Information page, select **APPN support** and **HPR support**.

Step 4: Transaction Program Configuration

If you need to configure the local node with an application for other nodes to access using APPC, you may need to create a Transaction Program definition for that application.

1. From the SNA Node Configuration window, click **Configure Transaction Program**, then click **New**.
2. On the Basic property page, the only parameters you must specify are the TP name and the complete pathname to the application. The TP name is the 8-character identifier with which the application will be associated on the SNA network. When a remote node needs to invoke this application, it must specify the name you put in this field. You should specify a meaningful name that can be identified with the function provided by the application.

The complete pathname specifies the disk, directory, and executable name for the application (for example, D:\MYFILES\MYTP.EXE). The executable name may or may not be the same as the TP name. If any command line parameters are necessary for invoking this application, specify them on the Basic page as well.

If you do not create a Transaction Program definition, the name specified in the incoming allocation request will be appended with **.exe** and used as the definition.

3. Click **OK** to continue.

Step 5: Partner LU 6.2 Configuration

This definition allows you to specify the location of the partner LU in terms of its owning control point name (the control point name is unique for each node in the entire network). The APPN network can normally locate the LU for you. Using this definition can expedite the search for an APPN resource, or be used to allow the local node to determine the route to the LU itself, in which case the owning control point is assumed to be an adjacent node in the network (LEN level connection).

1. From the SNA Node Configuration window, click **Configure Partner LU 6.2**, then click **New**.
2. On the Basic property page, specify the fully qualified partner LU name (network name plus LU name) to which you wish to connect. Also, specify the fully qualified owning control point name.
3. Click **OK** to continue.

Step 6: CPI-C Side Information Configuration

If you are running a CPI-C application locally and it requires that you specify a CPI-C Side Information definition as a parameter, you must create this definition.

1. From the SNA Node Configuration window, click **Configure CPI-C Side Information**, then click **New**.
2. On the Basic property page, define the following:
 - **Symbolic destination name:** Specify the name that the application will use to establish a session with the remote LU specified in this definition.
 - **Partner LU name:** Specify the fully qualified partner LU name (network name plus LU name) of the partner LU with which this definition will be used to establish a session.
 - **Mode name:** Use one of the default IBM-architected modes for specifying session parameters by selecting one from the pull-down. The #INTER mode is most often used for user applications. If one of these modes is not appropriate, or if you must define a different mode name, you must create a mode definition.
 - **TP name:** Specify the remote TP name which will be invoked as a result of running a local application using this side information. If your application does not specify the remote TP to execute and requires you to do so, specify the TP name of that application here.
3. Click **OK** to continue.

You are finished with the configuration aspect of this task. Save your configuration, giving it a name you can easily identify. After saving the configuration, exit the Node Configuration application and return to the SNA Node Operations application.

Step 7: Start the Node

Click **Start** 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.

Step 8: Verify That the Link Is Active



This step is not necessary for AnyNet SNA over TCP/IP connections.

When 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. To verify that the link you configured in Step 3 is active, on the SNA Node Operations toolbar, click **Connections** and verify that the link you configured in Step 3 shows up on the list and that it is active. It may take a few seconds for the link to establish.

If you did not configure a link, a remote node must establish a link with the local node. Ensure that the remote node's link has been started and verify that it becomes active with the local node.

Step 9: Start the Session

Once a link between you and the APPN network or partner node is active, you are ready to try your APPC application.

You can use the Check Connection (APING) application from the Communications Server program group on the desktop to verify that the partner LU is reachable. When you invoke the application, specify either the fully qualified partner LU or the symbolic destination name of the CPI-C Side Information definition you created in Step 6 above. Click **OK** to continue. The application will send test packets of data to the remote node's APINGD application which will in turn be returned to the local application.



Be sure that the APINGD application is installed and configured on the remote system.

Dependent LU 6.2 Sessions to a Host

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



Before proceeding with "Step 1: Node Setup" on page 111, 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:

- 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 "Mapping SNA Resources to IP Addresses" on page 179 for more information.

Summary of Steps

- Step 1: Node Setup
- Step 2: Device Configuration
- Step 3: Connection Configuration
- Step 4: Local LU 6.2 Configuration
- Step 5: CPI-C Side Information Configuration
- Step 6: Start the Node

- Step 7: Verify That the Link Is Active
- Step 8: Start the Session

Step 1: Node Setup

Use the following procedure to name the local node and the network in which it operates:

1. Open the SNA Node Operations application by clicking the **SNA Node Operations** icon in the Communications Server folder. On the toolbar, click **Node Configuration** to launch the configuration application.
2. From the **File** menu, select **New**. Then from the **Scenarios** menu, select **Dependent LU 6.2 Sessions to a Host**.
3. From the SNA Node Configuration window, click **Configure Node**, then click **New**. The Define the Node window appears. Click the **Basic** tab and enter the following required information:

Control Point (CP)

Specify a fully qualified, unique CP name, which identifies the node within the network environment. It consists of two parts: the network name and the CP name.

Local Node ID

Specify the SNA network in which this local node operates. The local node ID consists of two parts: the block ID and the physical unit ID.

4. Click **OK** to continue.

Step 2: Device Configuration

Use this step to define supported communications devices on the machine, over which SNA links can be established to other nodes in the network.

From the SNA Node Configuration window, click **Configure Devices** and then click one of the data link control (DLC) types listed below. Then click **New**. The following DLC types are available:

- **LAN**: There are three property pages for configuring a LAN device: Basic, Activation, and Performance. The only parameter you need to specify is the device number. If you have more than one LAN communications card (for example, token ring or Ethernet) installed, select the adapter number for the card you wish to use. You should accept all other defaults. Click **OK** to create the LAN device definition.



If no adapter information appears, you have chosen not to install the IBM LLC2 DLC interface during Communication Server installation, or you have failed to reboot after installing IBM LLC2. To install IBM LLC2, refer to the SETUP2.HLP help file, which is located in the Communications Server installation directory.

- **COM Port:** There are three property pages for configuring a COM port device: Basic, Incoming Call, and Performance. Typically, you will be using a modem to communicate over a COM port to a telephone network. Click on **Configure modem...** and follow the instructions for selecting and configuring a modem. Make sure that **Accept incoming calls** is checked if you expect workstations to dial into this server. When you are finished, click **OK** to create the COM port device definition.
- **SDLC-MPA:** Define this type of device if you are using an MPA communications adapter for accessing a telephone network. There are four property pages for configuring an SDLC-MPA device: Basic, Adapter, Incoming Call, and Performance. Specify the communication port of the MPA card you will be using and make sure that **Accept incoming calls** is checked. When you are finished, click **OK** to create the SDLC-MPA device definition.



If your MPA card does not function properly when you start communications, you may need to return to this Adapter page and adjust the IRQ setting value.

- **SDLC-WAC:** Define this type of device if you are using a WAC communications adapter to access a telephone network. There are four property pages for configuring an SDLC-WAC device: Basic, Adapter, Incoming Call, and Performance. Specify the adapter number and the port level (upper or lower) you will use. If you have an ISA adapter, be sure to also specify a shared RAM address. Finally, make sure that **Accept incoming calls** is checked if you expect workstations to dial into this server. When you are finished, click **OK** to create the SDLC-WAC device definition.
- **X.25-COM Port:** There are four property pages for configuring an X.25 COM port device: Basic, Network Parameters, Incoming Calls, and Frame Values. Typically, you will be using a modem to communicate over a COM port to an X.25 cloud. The only value you need to specify is the modem you will be using. Click **Configure modem...** and follow the instructions for selecting and configuring a modem. On the Network Parameters page, make sure that **Accept incoming calls** is checked if you expect workstations to dial into this server. When you are finished, click **OK** to create the X.25-COM port device definition.
- **X.25-WAC:** Define this type of device if you are using a WAC communications adapter for accessing an X.25 cloud. There are four property pages for configuring an X.25-WAC device: Basic, Network

Parameters, Incoming Calls, and Frame Values. Specify the adapter number and the port level (upper or lower) you will use. If you have an ISA adapter, be sure to also specify a shared RAM address. On the Network Parameters page, make sure that **Accept incoming calls** is checked if you expect workstations to dial into this server. When you are finished, click **OK** to create the X.25 WAC device definition.

- **Twinaxial:** Define this type of device if you are using an adapter which supports communications over a twinaxial cable. There is one property page for configuring this device: Basic. On this page, identify the supported twinaxial communications adapter type that you have installed. When you are finished, click **OK** to create the twinaxial device definition.
- **AnyNet SNA Over TCP/IP:** Define this type of device if you want to route your session over TCP/IP to another AnyNet SNA over TCP/IP node. There are three property pages for configuring this device: Basic, Routing Preferences, and Performance. On the Basic page, the SNA domain name should be the same name as you collected in “Before You Begin” on page 110 . On the Routing Preferences page, specify **native first** as the default routing preference. When you are finished, click **OK** to create the AnyNet over TCP/IP device.
- **OEM Adapters:** Communications Server provides configuration support for various OEM communication adapters. The configuration requirements are adapter-specific. Refer to the documentation provided with the adapter in order to complete this device configuration.

However, there are common parameters, which are located under the Basic tab, that you must specify for all OEM adapters. When you select the OEM Page tab, you must specify the port name. You should also select **APPN support** and **HPR support**.

Step 3: Connection Configuration

Use this step to define links to other nodes in the SNA network over devices defined in Step 2. Applications will use these links to establish conversations with remote applications.



All connection definitions have a link station name associated with them. This is the name that identifies the connection when it is started by node operations. A default name is provided; you may change this name if you wish.

From the SNA Node Configuration window, click **Configure Connections** and select a data link control (DLC) type. Then click **New**. The following DLC types are available:

- **LAN:** There are three property pages for configuring a LAN connection: Basic, Advanced, and Security. For a LAN connection to a host, specify on

Dependent LU 6.2 Sessions to a Host

the Basic page the link address of the host's communication controller, or an SNA Gateway, to which you will be connecting. On the Advanced page, specify that this link supports SSCP sessions. Also, specify the local node id (XID) corresponding to the host's PU. Also, on the Advanced page, specify the local node ID obtained in "Before You Begin" on page 110. When you are finished, click **OK** to create the LAN connection definition.

- **COM Port, SDLC-MPA, and SDLC-WAC:** There are three property pages for configuring this connection: Basic, Link Information, and Performance. On the Basic page, specify the telephone number to be used to dial into the host or the SNA Gateway to the host. Be sure that the appropriate communication port is selected for the device that you configured in Step 2 above. On the Link Information page, specify that the link should support SSCP sessions and make sure that the link station address matches the address that is provided to you by the host's PU definition. (If you are using a switched line to a host, then a local node ID (XID) should be used instead.) When you are finished, click **OK** to create the connection definition.
- **X.25-COM Port, X.25-WAC:** There are three property pages for configuring this connection: Basic, Link Information, and SVC Advanced Optional Facilities. On the Basic page, specify the communication port you plan to use as defined in Step 2 above. Also, select whether this link will be over a switched virtual circuit (SVC) or a private virtual circuit (PVC). If it is a SVC link, specify the DTE addresses and extensions for establishing the link. If it is a PVC link, specify the PVC number for the link. On the Link Information page, specify that the link should support SSCP sessions. When you are finished, click **OK** to create the connection definition.
- **Twinaxial:** There are two property pages for configuring this connection: Basic and Security. On the Basic page, specify the TDLC station address of the host's communications controller. Also, specify that SSCP sessions are supported and provide local node ID (XID) corresponding to the host's PU. When you are finished, click **OK** to create the connection definition.
- **AnyNet SNA Over TCP/IP:** There is one property page for configuring this connection: Basic. On this page, you need to specify the adjacent CP name for the SNA gateway to which you will connect. If you are connecting to the host through an SNA gateway, specify the CP name of the SNA gateway connecting to the host. Otherwise, use the host's CP name. Click **OK** to create the connection definition.



The CP name you specified must be mapped to a TCP/IP address in order for AnyNet to determine where to route your SNA session over TCP/IP. To map the CP name to a TCP/IP address, refer to "Mapping SNA Resources to IP Addresses" on page 179.

- **OEM Adapters:** Communications Server provides configuration support for various OEM communication adapters. The configuration requirements are adapter-specific. Refer to the documentation provided with the adapter in order to complete this device configuration.

However, there are common parameters that you must specify for all OEM adapters. On the Link Information page, specify that this link supports SSCP sessions. Also, specify the local node ID (XID) provided by the host's PU.

Step 4: Local LU 6.2 Configuration

You must configure the local LU with which to establish your dependent LU 6.2 session. Most APPC applications use the local control point as the local LU for independent LU 6.2 sessions, but since the control point cannot also function as a dependent LU, you must define your own LU 6.2 LU.

To define a new local LU 6.2:

1. From the SNA Node Configuration window, click **Configure Local LU 6.2**, then click **New**.
2. On the Basic property page, specify the following:
 - **Local LU name:** The LU with which to establish your dependent LU 6.2 session. This name must match the application definition on the host.
 - Check **Dependent LU**.
 - **PU name:** Specify the PU name of the connection you configured to the host in Step 3 above. Usually, this name is the same as the link station name. It should appear in the PU name drop-down list.
 - **NAU address:** The available address on the host's PU to which you will establish a session.
3. Click **OK** to continue.

Step 5: CPI-C Side Information Configuration

To define new CPI-C side information:

1. From the SNA Node Configuration window, click **Configure CPI-C Side Information**, then click **New**.
2. On the Basic property page, define the following:
 - **Symbolic destination name:** Specify the name that the application will use to establish a session with the remote node specified in this definition.
 - **Partner LU name:** Specify the fully qualified partner LU name (network ID plus the LU name) of the partner LU with which this definition will be used to establish a session.

Dependent LU 6.2 Sessions to a Host

- **Mode name:** Use one of the default IBM-architected modes for specifying session parameters by selecting one from the pull-down. The #INTER mode is most often used for user applications. If one of these modes is not appropriate, or if you must define a different mode name, then you must create a mode definition.
- **TP name:** Specify the remote TP name which will be invoked as a result of running a local application using this side information. If your application does not specify the remote TP to execute and requires you to do so, then specify the TP name of that application here.

3. Click **OK** to continue.

You are done with the configuration aspect of this task. Save your configuration, giving it a name you can easily identify. After saving the configuration, exit the Node Configuration application and return to the SNA Node Operations application.

Step 6: Start the Node

Click **Start** 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 finished configuring and click **Open**. It may take a moment for the node to start and to establish all the defined links.

Step 7: Verify That the Link Is Active

When the node has started, you should see a view of the active node with the control point name display that you specified in Step 1. To verify that the link you configured in Step 3 is active, on the SNA Node Operations toolbar, click **Connections** and verify that the link you configured in Step 3 shows up on the list and that it is active. It may take a few seconds for the link to be established.

Step 8: Start the Session

You are now ready to start your application. Verify that the LU address you chose is active with a session to the host by displaying LU 6.2 sessions. If no application is currently active, an SSCP-LU session will be active with the LU address. Otherwise, an LU-LU session is active, which indicates that your application is in conversation with the host.

3270 Configuration

This section describes the steps to take to configure Communications Server for a 3270 session with a host. For APPC3270 configuration, go to “CPI-C, APPC, or 5250 Emulation Configuration” on page 102.



Before proceeding with “Step 1: Node Setup” on page 118, 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:

- 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 “Mapping SNA Resources to IP Addresses” on page 179 for more information.

Summary of Steps

- Step 1: Node Setup
- Step 2: Device Configuration
- Step 3: Connection Configuration
- Step 4: Local LU 0 to 3 Configuration
- Step 5: Start the Node
- Step 6: Verify That the Link Is Active
- Step 7: Start the Application

Step 1: Node Setup

Use the following procedure to name the local node and the network in which it operates:

1. Open the SNA Node Operations application by clicking the **SNA Node Operations** icon in the Communications Server folder. On the toolbar, click **Node Configuration** to launch the configuration application.
2. From the **File** menu, select **New**. Then, from the **Scenarios** menu, select **3270/LUA Applications**.
3. From the SNA Node Configuration window, click **Configure Node**, then click **New**. The Define the Node window appears. Click the **Basic** tab and enter the following required information:

Control Point (CP)

Specify a fully qualified, unique CP name, which identifies the node within the network environment. It consists of two parts: the network name and the CP name.



If you do not know your CP name, as an example of a unique name, you can use the first 8 characters of the node's TCP/IP host name, which is found by entering **hostname** as a Windows NT command.

Local Node ID

Specify the node ID (XID) corresponding to the host PU. The local node ID consists of two parts: the block ID and the physical unit ID.

4. Click **OK** to continue.

Step 2: Device Configuration

Use this step to define supported communications devices on the machine, over which SNA links can be established to other nodes in the network.

From the SNA Node Configuration window, click **Configure Devices** and click one of the data link control (DLC) types listed below. Then click **New**. The following DLC types are available:

- **LAN:** There are three property pages for configuring a LAN device: Basic, Activation, and Performance. The only parameter you need to specify is the device number. If you have more than one LAN communications card (for example, token ring or Ethernet) installed, select the adapter number for the card you wish to use. You should accept all other defaults. Click **OK** to create the LAN device definition.



If no adapter information appears, you have chosen not to install the IBM LLC2 DLC interface during Communication Server installation, or you have failed to reboot after installing IBM LLC2. To install IBM LLC2, refer to the SETUP2.HLP help file, which is located in the Communications Server installation directory.

- **COM Port:** There are three property pages for configuring a COM port device: Basic, Incoming Call, and Performance. Typically, you will be using a modem to communicate over a COM port to a telephone network. Click on **Configure modem...** and follow the instructions for selecting and configuring a modem. When you are finished, click **OK** to create the COM port device definition.
- **SDLC-MPA:** Define this type of device if you are using an MPA communications adapter for accessing a telephone network. There are four property pages for configuring an SDLC-MPA device: Basic, Adapter, Incoming Call, and Performance. Specify the communication port of the MPA card you will be using. When you are finished, click **OK** to create the SDLC-MPA device definition.



If your MPA card does not function properly when you start communications, you may need to return to this Adapter page and adjust the IRQ setting value.

- **SDLC-WAC:** Define this type of device if you are using a WAC communications adapter to access a telephone network. There are four property pages for configuring an SDLC-WAC device: Basic, Adapter, Incoming Call, and Performance. Specify the adapter number of the WAC card you will be using. Specify the port level (upper or lower) you will use. If you have an ISA adapter, be sure to also specify a shared RAM address. When you are finished, click **OK** to create the SDLC-WAC device definition.
- **X.25-COM Port:** There are four property pages for configuring an X.25 COM port device: Basic, Network Parameters, Incoming Calls, and Frame Values. Typically, you will be using a modem to communicate over a COM port to an X.25 cloud. The only value you need to specify is the modem you will be using. Click **Configure modem...** and follow the instructions for selecting and configuring a modem. When you are finished, click **OK** to create the X.25-COM port device definition.
- **X.25-WAC:** Define this type of device if you are using a WAC communications adapter for accessing an X.25 cloud. There are four property pages for configuring an X.25-WAC device: Basic, Network Parameters, Incoming Calls, and Frame Values. Specify the adapter number and the port level (upper or lower) you will use. If you have an ISA adapter, be sure to also specify a shared RAM address. When you are finished, click **OK** to create the X.25 WAC device definition.

3270 Configuration

- **Twinaxial:** Define this type of device if you are using an adapter which supports communications over a twinaxial cable. There is one property page for configuring this device: Basic. On this page, identify the supported twinaxial communications adapter type that you have installed. When you are finished, click **OK** to create the twinaxial device definition.
- **AnyNet SNA Over TCP/IP:** Define this type of device if you want to route your sessions over TCP/IP to another AnyNet SNA over TCP/IP node with SNA gateway configured. There are three property pages for configuring this device: Basic, Routing Preferences, and Performance. On the Basic page, the SNA domain name should be the same name you collected in “Before You Begin” on page 117. On the Routing Preferences page, specify **native first** as the default routing preference. When you are finished, click **OK** to create the AnyNet SNA over TCP/IP device.
- **OEM Adapters:** Communications Server provides configuration support for various OEM communication adapters. The configuration requirements are adapter-specific. Refer to the documentation provided with the adapter in order to complete this device configuration.

However, there are common parameters, which are located under the Basic tab, that you must specify for all OEM adapters. When you select the OEM Page tab, you must specify the port name. You should also select **APPN support** and **HPR support**.

Step 3: Connection Configuration

Use this step to define links to other nodes in the SNA network over devices defined in Step 2. Applications will use these links to establish conversations with remote applications.



All connection definitions have a link station name associated with them. This is the name that identifies the connection when it is started by node operations. A default name is provided; you may change this name if you wish.

From the SNA Node Configuration window, click **Configure Connections**, then click **New**. The following DLCs are available:

- **LAN:** There are three property pages for configuring a LAN connection: Basic, Advanced, and Security. For a LAN connection to a host, specify on the Basic page the link address of the host’s communication controller, or an SNA Gateway, to which you will be connecting. On the Advanced page, specify that this link supports SSCP sessions. Also, specify the local node id (XID) corresponding to the host’s PU. Also, on the Advanced page, specify the local node ID obtained in “Before You Begin” on page 117. When you are finished, click **OK** to create the LAN connection definition.

- **COM Port, SDLC-MPA, and SDLC-WAC:** There are three property pages for configuring this connection: Basic, Link Information, and Performance. On the Basic page, specify the telephone number to be used to dial into the host or the SNA Gateway to the host. Be sure that the appropriate adapter or port number is selected for the device that you configured in Step 2 above. On the Link Information page, specify that the link should support SSCP sessions and make sure that the link station address matches the address that is provided to you by the host's PU definition. (If you are using a switched line to a host, then a local node ID (XID) should be used instead. You can find the XID field on the Basic page.) When you are finished, click **OK** to create the connection definition.
- **X.25-COM Port, X.25-WAC:** There are three property pages for configuring this connection: Basic, Link Information, and SVC Advanced Optional Facilities. On the Basic page, specify the communication port you plan to use as defined in Step 2 above. Also, select whether this link will be over a switched virtual circuit (SVC) or a private virtual circuit (PVC). If it is a SVC link, specify the DTE addresses and extensions for establishing the link. If it is a PVC link, specify the PVC number for the link. On the Link Information page, specify that the link should support SSCP sessions. When you are finished, click **OK** to create the connection definition.
- **Twinaxial:** There are two property pages for configuring this connection: Basic and Security. On the Basic page, specify the TDLC station address of the host's communications controller. Also, specify that SSCP sessions are supported and provide a local node ID (XID) corresponding to the host's PU. When you are finished, click **OK** to create the connection definition.
- **AnyNet SNA over TCP/IP:** There is only one property page for configuring this connection: Basic. On this page, specify the adjacent CP name for the SNA gateway to which you will be connecting. If you are connecting to the host through an SNA gateway, specify the CP name of the SNA gateway connecting to the host. Otherwise, use the host's CP name. Click **OK** to create the connection definition.



The CP name you specify must be mapped to a TCP/IP address in order for AnyNet to determine where to route your SNA session over TCP/IP. To map the CP name to a TCP/IP address, refer to "Mapping SNA Resources to IP Addresses" on page 179.

- **OEM Adapters:** Communications Server provides configuration support for various OEM communication adapters. The configuration requirements are adapter-specific. Refer to the documentation provided with the adapter in order to complete this device configuration.

However, there are common parameters that you must specify for all OEM adapters. On the Link Information page, specify that this link supports SSCP sessions. Also, specify the local node ID (XID) provided by the host's PU.

Step 4: Local LU 0 to 3 Configuration

Use this step to define the local LU which will serve your 3270 application (emulator) by establishing an SNA session with a host's LU.

1. From the SNA Node Configuration window, click **Configure Local LU 0 to 3**, then click **New**.
2. On the Basic property page, define the following parameters:
 - **LU name:** Specify a name up to 8 characters long that identifies this LU for your application. For example, use a portion of your last name.
 - **NAU address:** Specify an available LU address on the host's PU.
 - **PU name:** Specify the same name as you specified in Step 3 for the link station name. This name should already be listed in the pull-down list.
3. Click **OK** to create the LU definition.

You have finished with the configuration aspect of this task. Save your configuration, providing it with a name that you can easily identify. After saving the configuration, exit the Node Configuration application and return to the SNA Node Operations application.

Step 5: Start the Node

Click **Start** on the SNA Node Operations toolbar to start the local node. Specify the configuration you have just finished configuring, then click **Open**. It may take a moment for the node to start and to establish all the defined links.

Step 6: Verify That the Link Is Active

When the node has started, you will see a view of the active node with the control point name displayed that you specified in Step 1. To verify that the link you configured in Step 3 is active, click **Connections** on the SNA Node Operations toolbar and make sure that the link you configured in Step 4 is on the list and is active. It may take a few seconds for the link to be established.

Step 7: Start the Application

You are now ready to start your 3270 display, printer session application, or emulator.



If you have problems, verify that the LU address you chose is active with a session to the host by displaying active LU 0 to 3 sessions. If no application (emulator) is currently active, an SSCP-LU session will be active with the LU address. Otherwise an LU-LU session will be active, which indicates that your application is in conversation with the host.

If you are using Personal Communications as your emulator, use in your Personal Communications configuration the same LU name as you specified in Step 4 above.

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 59. 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 “Step 1: Focal-Point Configuration” on page 124, 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

- Step 1: Focal-Point Configuration
- Step 2: Start the Node

Focal-Point Configuration

- Step 3: Verify That the Link Is Active
- Step 4: Establish a Session

Step 1: Focal-Point Configuration

To define a new focal point:

1. From the SNA Node Configuration window, click **Configure Focal Points**, then click **New**.
2. On the Basic property page, specify the following information:
 - The management services category for which you want to forward alert information. You can define multiple focal points; each can forward alert data for a different management services category to a different focal point.
 - The application name used to process the alert data on the focal points. This value can be the same for both the primary and backup focal point.
 - The control point name of the primary focal point.
 - The control point name of the backup focal point, if applicable.
3. Click **OK** to create the focal point definition. You can create as many focal points as you need to forward alerts for all applicable management services categories.

You have completed the configuration aspect of this task. Save your configuration, giving it a name that you can easily identify. After saving the configuration, exit the Node Configuration application and return to the SNA Node Operations application.

Step 2: Start the Node

Click **Start** 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.

Step 3: 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. To verify that the link you configured in the APPN Configuration task is active, click **Connections** on the SNA Node Operations toolbar. It may take a few seconds for the link to be established.

Step 4: Establish a Session

Use SNA Node Operations to display the focal point you have configured.

Part 3. Using Communications Server

Chapter 6. Using Communications Server

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

Starting Communications Server

Do the following to start the Communications Server:

1. For Windows NT 3.51, from the Program Manager group, double-click the **IBM Communications Server** icon.

For Windows NT 4.0, from the Start menu, select **Programs**, and then **IBM Communications Server**.

2. Click the **SNA Node Operations** icon.

The Communications Server SNA Node Operations window appears.

From the Communications Server SNA Node Operations window, do either:

- Click **Operations**.
- Click **Start Node**. The Open file dialog window appears.
- Select the appropriate configuration.
- Click **OK** to start the node.

or

- Click the leftmost green icon on the tool bar.
- The Open file dialog window appears.
- Select the appropriate configuration.
- Click **OK** to start the node.

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

Alternatively, you can use the **csstart** command to start Communications Server.

Stopping Communications Server

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

1. For Windows NT 3.51, from the Program Manager group, double-click the **IBM Communications Server** icon.
For Windows NT 4.0, from the Start menu, select **Programs**, and then click **IBM Communications Server**.
2. Click the **SNA Node Operations** icon. The Communications Server SNA Node Operations window appears.
From the SNA Node Operations window, do as follows:
 - Click **Operations**
 - Click **Stop Node**

or

 - On the tool bar, click the second icon from the left (the red one).
3. Click **OK** at the verification prompt.

Alternatively, you can use the **csstop** command to stop Communications Server.

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. Once you have completed a new configuration, you can replace the default configuration with your new one.

To replace a default configuration file,

1. Open the new configuration file that you would like to use as your new default.
2. For Windows NT 3.51, from the Program Manager group, double-click on the **IBM Communications Server** icon.
For Windows NT 4.0, from the Start Menu, select **Programs** and then click **IBM Communications Server**.
3. Click **SNA Node Configuration**. The SNA Node Configuration window appears.
4. Click **File**.
5. Click **Open**.
6. Select the new file you would like to use as the default.
7. Click **File**.

8. Click **Save**.
9. A message will ask you to confirm that you would like 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 any errors in configuration that are reflected at run time, you could get error messages at this time. In this case, refer to the help for the error message.

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
- Initiating path switches

Using the **Select SNA Resources** field on the SNA Node Operations panel, you can select to manage or display information on the following resources:

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 Connections

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

AnyNet Sockets Devices

Shows the currently defined sockets devices on a system.

AnyNet Sockets Routes

Shows the AnyNet routes through the network.

AnyNet Sockets Statistics

Displays statistics associated with the AnyNet Gateway function.

Connections

Shows link stations to the adjacent nodes

Connection Networks

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

CPI-C Side Information

Shows a set of parameters that are associated with a specified symbolic destination name.

Data Link Controls

Shows how data is formatted for transmission on the physical connection.

Devices

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

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.

DLUR PU

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.

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.

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.

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.

Network Node Statistics

Shows statistics for the Communications Server when it is configured as a network node. Statistics are provided for the directory, topology, and management services functions, which can be useful for tuning parameters of the network node.

Node Shows the control point that manages the node and its associated resources. The local node provides APPN services.

Partner LU 6.2

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

PU2.0/DLUR Gateway

Displays information about SNA downstream workstations and the connections to them. Also shows information about the dependent LU requester services.

RTP Connections

In high-performance routing (HPR), shows the rapid transport protocol (RTP) connections that are established between the endpoints of the route to transport session traffic.

TN3270E Sessions

Shows information about the sessions between TN3270 clients and the Communications Server.

TN3270E Summary

Summarizes information about TN3270E connectivity and tells you the number of active and inactive connections.

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.

Transaction Programs

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

Using the Menu Bar

From the menu bar, select one of the following:

Operations

To start or stop an SNA node. To start a node, select the configuration file you want to use.

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

To get and put configuration files and to get log files from a remote Communications Server. A retrieved file is stored in a subdirectory under the path in which Communications Server was installed. The name of the subdirectory is the same as the name of the remote server you are connected to.

To start or stop Attach Manager. When active, the Attach Manager processes inbound TP attachments.

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

Server To connect to a remote Communications Server, TCP/IP needs to be running and configured so that the client and server can access TCP/IP for using sockets. The TCP/IP hostname or IP address of the server is used to establish the connection with the server. You can only connect to one server at a time. Any different choice will disconnect you from the server you are currently viewing.

A user ID and password must be supplied 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.

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

1. Choose the name of the server from the list of recently used servers.
2. Select **Other** on the Server pulldown and enter the name of the server to which you want to connect.
3. Select **Other** on the Server pulldown and then click the **Discover** button to discover Communication Servers through a TCP/IP broadcast. The discovered servers will be in a dialog box. You can select one of the servers in the list if you wish to connect to it.

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

Launch

To launch 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 141. For more information on Trace Facility, see “Obtaining Trace Data” on page 142. For more information on SNA Node Configuration, see “Chapter 5. Configuring Communications Server” on page 43.

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

To refresh the display of resources.

To select resource attributes, which allows you to customize the display of SNA resource attributes.

To view frequently used resources, such as:

- Nodes
- Connections
- Local LU 0 to 3 sessions
- LU 6.2 sessions
- Partner LUs

Window

To manage 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 rightmost icon on the tool bar.

Displaying a Resource

To display a resource, select a resource from the Select SNA Resource pull-down list at the right on the tool bar. The data will be displayed in the window that you selected.

Starting a Resource

To start a resource:

1. Select a resource from the Select SNA Resource pull-down list.
2. Click the right mouse button on the first column of an item to display the action pop-up.
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 Select SNA Resource pull-down list.

2. Click the right mouse button on the first column of an item to display the action pop-up.
3. Click **Stop** to suspend the resource. If a resource is stopped (inactive), it can be deleted or redefined.

Deleting a Resource

To delete a resource:

1. Select a resource from the Select SNA Resource pull-down list.
2. Click the right mouse button on the first column of an item to display the action pop-up.
3. Click **Delete** to delete the resource.

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

Changing an HPR Path Switch

To perform a high performance routing (HPR) path switch:

1. Click **RTP connections** from the Select SNA Resource pull-down list.
2. Click the right mouse button on the first column of an item to display the action pop-up.
3. Click **HPR path switch** to change the path for the data on this RTP connection.

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, a STATE_CHECK return code is returned, as well as a specific secondary return code as listed in the NOF specification. Most rejections are due to inconsistencies in the configuration, such as one of the following:

- Attempting to define an LS 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 an LS 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 clients installed.

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

The remaining administration tools (Node Configuration, Configuration Verification, 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 using either of these methods:

- Use the Get and Put functions under the Operations pull-down menu in Node Operations to retrieve and to store configuration files or to retrieve log files.
- Use the file server capabilities of Windows NT to share the Communications Server installation directory, then map a drive to this shared directory from the administration machine. This allows 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

Four command line programs are available to perform basic operations for Communications Server.

CSSTART [-p | -q] [-a | -m] [cfgfile]

The CSSTART command is used to start the Communications Server with a specified configuration.

If the **-p** flag is used, then all messages are shown in a message box popup. Messages are written to stdout by default. The **-q** flag suppresses all output. The **-a** flag enables automatic startup after rebooting the machine. The **-m** flag disables automatic startup.

The **cfgfile** parameter is the full path name of the configuration file you want to use to start the product. If no **cfgfile** parameter is specified, then the default configuration file is used. If no default configuration file has been set, then an error is reported. If the server is successfully started, then CSSTART returns zero, otherwise a non-zero value is returned.

CSSTOP [-p | -q]

The CSSTOP command is used to stop the Communications Server. The flags have the same meaning as for CSSTART. If the server is successfully stopped then CSSTOP returns zero, otherwise a non-zero value is returned.

CSQUERY [-p | -q]

The CSQUERY command is used to query the status of the Communications Server. The flags have the same meaning as for CSSTART. Along with the running or stopped status, the default and active configuration file names are shown. If the server is running then CSQUERY returns zero, otherwise a non-zero value is returned.

CSLIC [number]

The CSLIC command allows 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

Chapter 7. Problem Determination and Reporting

This chapter describes the information that will help you to solve a problem yourself, 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

Recognize the differences between what you expect to see and what you do see.

Environment

Recognize 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 and level
 - Communication device-driver version and level

- Other communication programs (such as 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 “Appendix A. Mapping Parameters Between Communications Server and an SNA Host” on page 149, 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:

1. Installation and configuration
2. Node Operations
3. API
4. 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. You should start there to determine if the problem lies with Communications Server or another product.

Obtaining Trace Data

The Communications Server trace facility enables you to log trace information for certain Communications Server functions, which could 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, perform the following 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 and 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 list boxes. 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 saved a trace.

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 **.RAM** 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 may 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.

Once 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 some 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.networking.ibm.com/cms/csnabt.html>
- 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.

Chapter 8. Obtaining Additional Information

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

The following documents are provided as Adobe** Acrobat .PDF files on the Communications Server CD-ROM:

Table 4. Communications Server for Windows NT Library

Order Number	Title	Description
GC31-8424	<i>Quick Beginnings</i>	Provides an overview of Communications Server and the access features and emulator provided with it. Also gives installation and configuration information.
SC31-8425	<i>Client/Server Communications Programming</i>	Describes the advanced program-to-program communications (APPC) application programming interface (API) support provided by Communications Server.
SC31-8426	<i>System Management Programming</i>	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)**.

Appendix A. Mapping Parameters Between Communications Server and an SNA Host

This appendix describes the mapping between the configuration parameters you specify during Communications Server configuration and the parameters you specify on System/390 (including System/370) or AS/400 hosts.

Introduction

You can connect workstations running Communications Server to System/390 hosts (including System/370 hosts). Many of the values you specify for Communications Server configuration are also used when you configure the host. This chapter contains tables that list the parameters that can be used to eliminate the common parameters on each macro to be issued between Communications Server and the host.

Many NCP parameters issued from the LINE, PU, and LU macros can be specified in the GROUP macro for readability and ease of coding. This matching of parameters eliminates the need to include common parameters on each subsequent macros and still allows the capability to override when appropriate.

NCP Token Ring (NTRI) with VTAM and Communications Server

Table 5 compares host parameters to Communications Server parameters for IBM Token-Ring Network connections.

Table 5. Host/PC Parameters Cross-Reference: IBM Token-Ring Network NTRI Definition

NTRI/NCP	Communications Server Profile/Parameters	Remarks
GROUP ECLTYPE = PHY	DLC Type: LAN	
LINE LOCADDR	Configure Connections LAN Destination address	The value set for this parameter under Communications Server must be the address of the IBM Token-Ring Network adapter in the host controller.

Token Ring with VTAM Switched Network and Communications Server

Table 6 compares host parameters to Communications Server parameters for IBM Token-Ring Network connections using a VTAM switched network.

Table 6. Host/PC Parameters Cross-Reference: IBM Token-Ring Network VTAM Switched Net

VTAM	Communications Server Profile/Parameters	Remarks
IDBLK=	Configure Node Local node ID Block ID	The host IDBLK must match the first 3 hexadecimal characters of the Local node ID , which defaults to X'05D' for Communications Server. Specify this parameter when using switched lines, or omit this parameter if you use CPNAME=.
IDNUM=	Configure Node Local Node ID Physical Unit ID	The host IDNUM must match the last 5 hexadecimal characters of the Local node ID . Specify this parameter when using switched lines, or omit this parameter if you use CPNAME=.
CPNAME=	Node Definition Configure Node Fully qualified CP name (second field)	Specify this parameter when using switched lines, or omit when using IDBLK= and IDNUM=.

Mapping Communications Server—Host Parameters

Table 6. Host/PC Parameters Cross-Reference: IBM Token-Ring Network
VTAM Switched Net (continued)

VTAM	Communications Server Profile/Parameters	Remarks
LOCADDR	Configure LU 0 to 3 or: Configure Gateway/Host Links Create/Change LUs NAU address	These parameters must have the same value. For independent LUs, VTAM recommends creating a CDRSC definition or using the DYNLU operand instead of coding LOCADDR=0. For more information on coding CDRSC definitions for independent LUs, refer to the <i>VTAM Network Implementation Guide</i> . No host definitions are required for dependent LUs if SDDL or dynamic definition is used for independent LUs on VTAM 3.4 or later.
MAXDATA	Configure LAN Device Maximum PIU size (265–65535)	These values do not have to match.
MAXOUT	Configure LAN Device Receive buffer count (2–64)	The Receive buffer count in Communications Server should be equal to the MAXOUT parameter on the host.

9370 IBM Token-Ring Network Adapter and Communications Server

Table 7 compares 9370 host parameters to Communications Server parameters for IBM Token-Ring Network connections.

Table 7. Host/PC Parameters Cross-Reference: IBM Token-Ring Network 9370 VTAM LAN

VTAM	Communications Server Profile/Parameters	Remarks
VBUILD TYPE = LAN	DLC Type: LAN	
PORT MACADDR=	Configure Connection LAN Destination address	The destination address specified in the Communications Server customization must be the address of the 9370 IBM Token-Ring adapter.
PORT SAPADDR=04	Configure Connection LAN Remote SAP	These values must match.
ADDR=04 (outgoing only)	Configure Connection LAN Local SAP	These values must match.

3174 Controller and Communications Server

Table 8 compares 3174 controller parameters to Communications Server for IBM Token-Ring connections.

Table 8. Parameter Matching between a 3174 Token-Ring and Communications Server

3174	Communications Server Profile/Parameters	Remarks
Upper limit address greater than 104: CUA	DLC Type: LAN	
Token-Ring address for gateway	Configure Connections LAN Destination address	These values must match.

Mapping Communications Server—Host Parameters

Table 8. Parameter Matching between a 3174 Token-Ring and Communications Server (continued)

3174	Communications Server Profile/Parameters	Remarks
Ring transmission definition. W= window max out, F=0, W = 1-7, F=1, W = 1-7, F=2, W = 1-4, F=3, W = 1-2	Configure Devices LAN Receive buffer count (1-8)	The Communications Server receive buffer count should be equal to 3174 W.

3174 Controller VTAM PU and Communications Server

Table 9 compares 3174 controller VTAM PU parameters to Communications Server for IBM Token-Ring connections.

Table 9. Host/PC Parameters Cross-Reference: IBM Token-Ring Network 3174 Controller VTAM PU and Communications Server

VTAM	Communications Server Profile/Parameters	Remarks
CUADDR (local) or ADDR (remote)	(none)	Mapped by 3174 controller to IBM Token-Ring address
MAXDATA (remote only)	Configure Devices LAN Maximum PIU size (99-65535)	The Maximum PIU size value set on the Communications Server workstation must match the value set on the host.
MAXOUT (remote only)	Configure Devices LAN Receive buffer count (2-64)	The Communications Server Receive buffer count should be equal to MAXOUT .

Mapping Communications Server—Host Parameters

Table 9. Host/PC Parameters Cross-Reference: IBM Token-Ring Network 3174 Controller VTAM PU and Communications Server (continued)

VTAM	Communications Server Profile/Parameters	Remarks
LOCADDR	Configure LU 0 to 3 or: Configure Gateway/Host Links Create/Change LUs NAU address	<p data-bbox="932 296 1224 701">These parameters must have the same value. For independent LUs, VTAM recommends creating a CDRSC definition or using the DYNLU operand instead of coding LOCADDR=0. For more information on coding CDRSC definitions for independent LUs, refer to the <i>VTAM Network Implementation Guide</i></p> <p data-bbox="932 730 1224 919">No host definitions are required for dependent LUs if SDDL or dynamic definition is used for independent LUs on VTAM 3.4 or later.</p>

Ethernet with VTAM Switched Network and Communications Server

Table 10 compares host parameters to Communications Server parameters for Ethernet Network connections using a VTAM switched network.

Table 10. Host/PC Parameters Cross-Reference: Ethernet Network VTAM Switched Network

VTAM	Communications Server Profile/Parameters	Remarks
IDBLK=	Configure Node Local node ID Block ID	The host IDBLK must match the first 3 hexadecimal characters of the Local node ID , which defaults to X'05D' for Communications Server. Specify this parameter when using switched lines, or omit this parameter if you use CPNAME=.
IDNUM=	Configure Node Local Node ID Physical Unit ID	The host IDNUM must match the last 5 hexadecimal characters of the Local node ID . Specify this parameter when using switched lines, or omit this parameter if you use CPNAME=.
CPNAME=	Node Definition Configure Node Fully qualified CP name (second field)	Specify this parameter when using switched lines, or omit when using IDBLK= and IDNUM=.

Mapping Communications Server—Host Parameters

Table 10. Host/PC Parameters Cross-Reference: Ethernet Network VTAM Switched Network (continued)

VTAM	Communications Server Profile/Parameters	Remarks
LOCADDR	Configure LU 0 to 3 or: Configure Gateway/Host Links Create/Change LUs NAU address	<p>These parameters must have the same value. For independent LUs, VTAM recommends creating a CDRSC definition or using the DYNLU operand instead of coding LOCADDR=0. For more information on coding CDRSC definitions for independent LUs, refer to the <i>VTAM Network Implementation Guide</i>.</p> <p>No host definitions are required for dependent LUs if SDDL or dynamic definition is used for independent LUs on VTAM 3.4 or later.</p>
MAXDATA	Configure LAN Device Maximum PIU size (265–65535)	These values do not have to match.
MAXOUT	Configure LAN Device Receive buffer count (2–64)	The Receive buffer count in Communications Server should be equal to the MAXOUT parameter on the host.

VTAM/NCP and Communications Server (SDLC)

Table 11 compares VTAM/NCP host parameters to Communications Server parameters for SDLC connections.

Table 11. Host/PC Parameters Cross-Reference: SDLC

VTAM/NCP	Communications Server Profile/Parameters	Remarks
NETID=	Configure Node Fully qualified CP name (first field)	This parameter can be used for both leased and switched lines. This parameter identifies the SNA network you connect to using Communications Server.
NAME PU		Always use a NAME PU. This PU name should be a name that is not the same as the local CP name so you can define an LU for the control point.
IDBLK=	Configure Node Local node ID Block ID	The host IDBLK must match the first 3 hexadecimal characters of the Local node ID , which defaults to X'05D' for Communications Server. Specify this parameter when using switched lines, or omit this parameter if you use CPNAME=.
IDNUM=	Configure Node Local Node ID Physical Unit ID	The host IDNUM must match the last 5 hexadecimal characters of the Local node ID . Specify this parameter when using switched lines, or omit this parameter if you use CPNAME=.

Mapping Communications Server—Host Parameters

Table 11. Host/PC Parameters Cross-Reference: SDLC (continued)

VTAM/NCP	Communications Server Profile/Parameters	Remarks
CPNAME=	Node Definition Configure Node Fully qualified CP name (second field)	Specify this parameter when using switched lines, or omit when using IDBLK= and IDNUM=.
LNCTL=SDLC	DLC Type: SDLC-WAC, SDLC-MPA, COM Port (depends on hardware used)	SDLC must be selected here. This parameter is used for both leased and switched lines.
LOCADDR	Configure LU 0 to 3 or: Configure Gateway/Host Links Create/Change LUs NAU address	<p>These parameters must have the same value. For independent LUs, VTAM recommends creating a CDRSC definition or using the DYNLU operand instead of coding LOCADDR=0. For more information on coding CDRSC definitions for independent LUs, refer to the <i>VTAM Network Implementation Guide</i></p> <p>No host definitions are required for dependent LUs if SDDL or dynamic definition is used for independent LUs on VTAM 3.4 or later.</p>

Mapping Communications Server—Host Parameters

Table 11. Host/PC Parameters Cross-Reference: SDLC (continued)

VTAM/NCP	Communications Server Profile/Parameters	Remarks
NRZI= YES/NO	Configure Connections SDLC-WAC, SDLC-MPA, COM Port NRZI encoding	<p>Communications Server uses NRZ=NO and NRZI=YES.</p> <p>This parameter is found only on PCMs for Modem Type: Synchronous Switched, Synchronous NonSwitched, and AutoSync.</p> <p>The encoding scheme, NRZI or NRZ, must be configured the same way at both ends of a connection. If the encoding schemes do not match, the modems will connect but data transfer will not succeed and the connection will be disconnected by Communications Server after a link-level timeout (typically 40 seconds).</p> <p>We recommend the NRZ encoding scheme when you connect to an X.25 network using an IBM Wide Area Connector.</p>
DUPLEX= FULL/HALF	Configure Connections SDLC-WAC and COM Port only Full-duplex communication	<p>The values set on each side must be consistent with the modem type and configuration. This parameter is used for both leased and switched lines.</p>

Mapping Communications Server—Host Parameters

Table 11. Host/PC Parameters Cross-Reference: SDLC (continued)

VTAM/NCP	Communications Server Profile/Parameters	Remarks
(TRANSFR * BFRS) -47	Configure Devices SDLC-WAC, SDLC-MPA, COM Port Maximum PIU size (265-4105)	The Maximum I-field size value must be less than or equal to the (TRANSFR * BFRS) - 47 indicated on the host. This parameter is used for both leased and switched lines.
MAXDATA=	Configure Devices SDLC-WAC, SDLC-MPA, COM Port Maximum PIU size (265-4105)	These values do not have to match. This parameter is used for both leased and switched lines. The lowest value will be used.
MAXOUT=	Configure Devices SDLC-WAC, SDLC-MPA, COM Port Receive window count (1-30)	The Receive window count in Communications Server should be equal to the MAXOUT parameter on the host. This parameter is used for both leased and switched lines.
ADDR=	Configure Devices SDLC-WAC, SDLC-MPA, COM Port Link station address (01-FE)	These parameters must have the same value. This is coded in hexadecimal for both Communications Server and VTAM/NCP. This parameter is used for both leased and switched lines.

VTAM and Communications Server (APPC)

Table 12 compares VTAM host parameters to Communications Server parameters for APPC connections.

Table 12. Host/PC Parameters Cross-Reference: APPC

VTAM	Communications Server Profile/Parameters	Remarks
LU NAME	Configure Local LU 6.2 Local LU name or: Configure Node Fully qualified CP name (second field)	
LOCADDR	Configure LU 0 to 3 or: Configure Gateway/Host Links Create/Change LUs NAU address	These parameters must have the same value. For independent LUs, VTAM recommends creating a CDRSC definition or using the DYNLU operand instead of coding LOCADDR=0. For more information on coding CDRSC definitions for independent LUs, refer to the <i>VTAM Network Implementation Guide</i> No host definitions are required for dependent LUs if SDDL or dynamic definition is used for independent LUs on VTAM 3.4 or later.
NETID APPL	Configure Partner LU 6.2 Partner LU name	
VTAM Interpret Table	Configure Partner LU 6.2 Partner LU name	This is for dependent LUs only.
LOGMODE Table LOGMODE=	Configure Mode Mode name	These parameters must match.

Mapping Communications Server—Host Parameters

Table 12. Host/PC Parameters Cross-Reference: APPC (continued)

VTAM	Communications Server Profile/Parameters	Remarks
LOGMODE Table RUSIZES=	Configure Mode Maximum RU size (256–32767)	Final values are negotiated.

ES/9000 and Communications Server (SDLC)

Table 13 compares 9370 Information System parameters to Communications Server parameters for SDLC connections.

Table 13. Host/PC Parameters Cross-Reference: 9370 Information System via SDLC

9370/VTAM	Communications Server Profile/Parameters	Remarks
QFI: Non-return -to-zero inverted (microcode configuration)	Configure Connections SDLC-WAC, SDLC-MPA, COM Port NRZI encoding	These parameters must match. This parameter is used for both leased and switched lines. Communications Server uses NRZ=NO and NRZI=YES. This is the synchronous data stream.
QFI: Protocol (microcode configuration) VTAM: GROUP LNCTL = SDLC	DLC Type SDLC-WAC, SDLC-MPA COM Port	The microcode and VTAM parameters must match. This parameter is used for both leased and switched lines.
MAXDATA	Configure Devices SDLC-WAC, SDLC-MPA, COM Port Maximum PIU Size (265–4105)	These values do not have to match. This parameter is used for both leased and switched lines.

Mapping Communications Server—Host Parameters

Table 13. Host/PC Parameters Cross-Reference: 9370 Information System via SDLC (continued)

9370/VTAM	Communications Server Profile/Parameters	Remarks
MAXBFRU * IOBUF size	Configure Devices SDLC-WAC, SDLC-MPA, COM Port Maximum PIU Size (265-4105)	The Maximum I-field size value must be equal to or less than the MAXBFRU times IOBUF size indicated on the host. This parameter is used for both leased and switched lines.
MAXOUT=	Configure Devices Receive window count (1-30)	The Receive window count in Communications Server should be equal to the MAXOUT parameter on the host. This parameter is used for both leased and switched lines.
ADDR=	Configure Devices Link station address (01-FE)	The values set for these parameters must match. This parameter is used for both leased and switched lines.
IDBLK=	Configure Node Local Node ID Block ID	The host IDBLK must match the first 3 hexadecimal characters of the Local node ID , which defaults to X'05D' for Communications Server. Specify this parameter when using switched lines, or omit this parameter if you use CPNAME=.
IDNUM=	Configure Node Local node ID Physical unit ID	The host IDNUM must match the last 5 hexadecimal characters of the Local node ID . Specify this parameter when using switched lines, or omit this parameter if you use CPNAME=.

Mapping Communications Server—Host Parameters

Table 13. Host/PC Parameters Cross-Reference: 9370 Information System via SDLC (continued)

9370/VTAM	Communications Server Profile/Parameters	Remarks
CPNAME=	Configure Node Fully qualified CP name (second field)	Specify this parameter when using switched lines, or omit when using IDBLK= or IDNUM=.
LOCADDR	Configure LU 0 to 3 or: Configure Gateway/Host Links Create/Change LUs NAU address	LOCADDR and NAU parameters must have the same value. For independent LUs, VTAM recommends creating a CDRSC definition or using the DYNLU operand instead of coding LOCADDR=0. For more information on coding CDRSC definitions for independent LUs, refer to the <i>VTAM Network Implementation Guide</i> . This parameter is used for both leased and switched lines.

Host and Communications Server (DLUR)

Table 14 compares host and Communications Server parameters for VTAM connections over DLUR.

Table 14. VTAM Communications Server Parameter Cross-Reference: Using DLUR

VTAM	Communications Server	Remarks
IDBLK=	Configure DLUR PUs Block ID	The IDBLK must match the first 3 hexadecimal characters of the Node ID, that defaults to X'05D' for Communications Server. Specify this parameter when NOT using CPNAME=.

Mapping Communications Server—Host Parameters

Table 14. VTAM Communications Server Parameter Cross-Reference: Using DLUR (continued)

VTAM	Communications Server	Remarks
IDNUM=	Configure DLUR PUs Physical unit ID	The IDBLK must match the last 5 hexadecimal characters of the Node ID. Specify this parameter when NOT using CPNAME=.
CPNAME=	Configure DLUR PUs PU name	The CPNAME must match the local PU name. Specify this parameter when NOT using IDNUM= and IDBLK=.

Table 15 lists the following parameters on the PATH statement that are used when establishing a connection from the host to the workstation.

Table 15. VTAM Communications Server DLUR Parameter Matching Connection from Host to Workstation

VTAM	Communications Server	Remarks
DLURNAME=	Configure Node Fully qualified CP name (second field)	The DLURNAME provides the name of the DLUR node that owns the DLUR PU. For Communications Server, this is the fully qualified CP name.
DLCADDR= (1,C,INTPU)		Required. This parameter tells the DLUR that the connection is for an internal PU.
DLCADDR= (2,X,zzzzzzzz)	Configure DLUR PUs Block ID and Physical unit ID	The zzzzzzzz in DLCADDR=(2,X,zzzzzzzz) must match the Node ID. Specify this parameter when NOT using DLCADDR=(3,C,puname).

Mapping Communications Server—Host Parameters

Table 15. VTAM Communications Server DLUR Parameter Matching Connection from Host to Workstation (continued)

VTAM	Communications Server	Remarks
DLCADDR= (3,C,puname)	Configure DLUR PUs PU name	The PU name in DLCADDR=(3,C,puname) must match Local PU name. Specify this parameter when NOT using DLCADDR=(2,X,zzzzzzzz).

NPSI and Communications Server (X.25)

Communications Server X.25 support enables the transmission of SNA frames across an X.25 network. X.25 treats SNA frames as raw data and transmits them as data-within-data packets. The two network nodes are not directly connected, but both are connected to an intermediary called the packet-switching data network (PSDN). The X.25 network can comprise any of the X.25 connectivities.

The software that interacts with the PSDN and packages the SNA data into packets and extracts it intact is an integral part of Communications Server. On the S/370 host side, the X.25 functions are handled by a separate software product called X.25 Network Control Program Packet Switching Interface (NPSI). The NPSI definitions are generated along with the NCP and the NPSI software runs in harmony with the NCP in the same 3705, 3725, 3720, or 3745 controller.

The majority of the X.25 parameters specifiable in both Communications Server and NPSI take values that are agreed upon by you and the X.25 network provider rather than between the two nodes. For example, with an SDLC connection on a nonswitched line, the host controller (NCP) is configured to poll a particular secondary address. Communications Server is configured to respond to that address on a physical link between the Communications Server workstation and the host.

NPSI Connections over X.25

Table 16 compares host and Communications Server parameters for NPSI connections over X.25.

Table 16. Host/PC Parameter Cross-Reference: NPSI Connections over X.25

NPSI	Communications Server Profile/Parameters	Remarks
X25.LINE TYPE=	DLC Type X.25 COM Port, X.25-WAC	Specify TYPE=P for PVCs and TYPE=S for SVCs for NPSI X.25 line definition.
CALL= (only for type = S)	Configure Devices X.25 COM Port, X.25-WAC Virtual circuit ranges	Virtual circuit ranges must match your X.25 network subscription.
MAXDATA=	Configure Devices X.25 COM Port, X.25-WAC Maximum PIU size (256–4105)	These values do not have to match.
VWINDOW	Configure Devices X.25 COM Port, X.25-WAC Window size (1–7)	The SVC/PVC window size must match the X.25 subscriptions.
MWINDOW	Configure Devices X.25 COM Port, X.25-WAC Frame values Window size (1–7)	

Mapping Communications Server—Host Parameters

Table 16. Host/PC Parameter Cross-Reference: NPSI Connections over X.25 (continued)

NPSI	Communications Server Profile/Parameters	Remarks
FRMLGTH	Configure Devices X.25 COM Port, X.25-WAC Frame sequence Modulo	The host FRMLGTH value must be at least MAXPKT +3 when running Modulo 8 or MAXPKT +4 when running Modulo 128. The host and Communications Server Modulo size and the packet sizes must match your X.25 subscription.
MAXPKTL	Configure Devices X.25 COM Port, X.25-WAC Packet size	The host SVC/PVC packet sizes must match the X.25 subscription value.

VTAM/NCP and Communications Server (X.25)

Table 17 compares host and Communications Server parameters for X.25 (VTAM/NCP).

Table 17. Host/PC Parameters Cross-Reference: X.25 (VTAM/NCP)

VTAM/NCP	Communications Server Profile/Parameters	Remarks
NETID=	Configure Node Fully qualified CP name (first field)	This identifies the SNA network you connect to using Communications Server.
PU NAME		Always use a PU name. This PU name should not be the same as the local CP name so you can define an LU for the control point.

Mapping Communications Server—Host Parameters

Table 17. Host/PC Parameters Cross-Reference: X.25
(VTAM/NCP) (continued)

VTAM/NCP	Communications Server Profile/Parameters	Remarks
IDBLK=	Configure Node Local node ID Block ID	First 3 hex digits of the Local node ID , which defaults to X'05D' for Communications Server. Specify this parameter when using switched lines, or omit this parameter if you use CPNAME=.
IDNUM=	Configure Node Local node ID Physical unit ID	The host IDNUM must match the last 5 hexadecimal characters of the Local node ID . Specify this parameter when using switched lines, or omit this parameter if you use CPNAME=.
CPNAME=	Configure Node Fully qualified CP name (second field)	Specify this parameter when using switched lines, or omit when using IDBLK= and IDNUM=.
(TRANSFR * BFRS) - 47	Configure Devices X.25 COM Port, X.25-WAC Maximum PIU size (265–4105)	The Maximum PIU must be equal to the value set on the host.
MAXDATA=	Configure Devices X.25 COM Port, X.25-WAC Maximum PIU size (265–4105)	These values do not have to match.

Mapping Communications Server—Host Parameters

Table 17. Host/PC Parameters Cross-Reference: X.25
(VTAM/NCP) (continued)

VTAM/NCP	Communications Server Profile/Parameters	Remarks
LOCADDR	Configure LU 0 to 3 or: Configure Gateway/Host Links Create/Change LUs NAU address	<p data-bbox="932 296 1224 701">These parameters must have the same value. For independent LUs, VTAM recommends creating a CDRSC definition or using the DYNLU operand instead of coding LOCADDR=0. For more information on coding CDRSC definitions for independent LUs, refer to the <i>VTAM Network Implementation Guide</i></p> <p data-bbox="932 730 1224 919">No host definitions are required for dependent LUs if SDDL or dynamic definition is used for independent LUs on VTAM 3.4 or later.</p>

APPC over X.25

Table 18 matches the parameters for a Communications Server workstation running advanced program-to-program communications (APPC) connecting to a host by way of X.25.

Table 18. Host/PC Parameters Cross-Reference: APPC on an IBM Token-Ring Network Using X.25 to a Host

NCP	Communications Server Profile/Parameters	Remarks
LU NAME	Configure Local LU 6.2 Local LU name or: Configure Node Fully qualified CP name (second field)	

Mapping Communications Server—Host Parameters

Table 18. Host/PC Parameters Cross-Reference: APPC on an IBM Token-Ring Network Using X.25 to a Host (continued)

NCP	Communications Server Profile/Parameters	Remarks
LOCADDR	Configure LU 0 to 3 or: Configure Gateway/Host Links Create/Change LUs NAU address	These parameters <i>must</i> have the same value. For independent LUs, VTAM recommends creating a CDRSC definition or using the DYNLU operand instead of coding LOCADDR=0. For more information on coding CDRSC definitions for independent LUs, refer to the <i>VTAM Network Implementation Guide</i> . No host definitions are required for dependent LUs if SDDL or dynamic definition is used for independent LUs on VTAM 3.4 or later.
NETID APPL	Configure Partner LU 6.2 Partner LU name	
VTAM Interpret Table	Configure Partner LU 6.2 Partner LU name	This is for dependent LUs only.
LOGMODE Table LOGMODE=	Configure Mode Mode name	These parameters <i>must</i> match.
LOGMODE Table RUSIZES=	Configure Mode Maximum RU size (256–32767)	These values must match.

AS/400 Host Line Definitions

AS/400 host line definitions include matching OS/400 host program parameters with Communications Server parameters. Table 19 contains the SDLC line parameters.

Table 19. AS/400 Communications Server Parameters Cross-Reference: OS/400 Host Program Line Definition

OS/400	Communications Server Profile/Parameters	Remarks
NRZI= Data Encoding	Configure Connections SDLC-WAC, SDLC-MPA, COM Port NRZI encoding	Communications Server uses NRZ=NO and NRZI=YES. This parameter is found only on PCMs for Modem Type: Synchronous Switched, Synchronous NonSwitched, and AutoSync.
Modem data rate select	Configure Devices COM Port only Configure modem	The parameters on both systems for modem connection types, asynchronous switched, must match.
Maximum frame size (MAXFRAME)	Configure Devices SDLC-WAC, SDLC-MPA, COM Port Receive window count (1-30)	Asynchronous nonswitched values do not have to match.
Maximum outstanding frames (MAXOUT)	Configure Devices SDLC-WAC, SDLC-MPA, COM Port Receive window count (1-30)	The Receive window count in Communications Server should be equal to the MAXOUT parameter on the AS/400 host.

AS/400 Host Controller Definitions

Defining the AS/400 host controller includes matching OS/400 host program parameters with Communications Server parameters.

Mapping Communications Server—Host Parameters

Table 20 shows the OS/400 host program parameters.

Table 20. AS/400 Communications Server Parameters Cross-Reference:
Controller Parameters

OS/400	Communications Server Profile/Parameters	Remarks
Linktype: *SDLC	DLC Type SDLC-WAC, SDLC-MPA COM Port	Link type on both systems must match. This parameter is on the line description, but include for completeness.
Attached Nonswitched Line	Configure Devices SDLC-WAC, SDLC-MPA, COM Port Switched line	This parameter is for nonswitched connections. This value must match a previously defined host line definition.
Switched Line List	(none)	This parameter is for switched connections. This value must match a previously defined host line definition.
Maximum frame size	Configure Devices SDLC-WAC, SDLC-MPA, COM Port Maximum PIU size (265–4105)	These values do not have to match.
Remote network identifier	Configure Node Fully qualified CP name (first field)	These values must match.
Remote control point name	Configure Node Fully qualified CP name (second field)	These values must match.

Mapping Communications Server—Host Parameters

Table 20. AS/400 Communications Server Parameters Cross-Reference:
Controller Parameters (continued)

OS/400	Communications Server Profile/Parameters	Remarks
Data link role:	Configure Connections SDLC-WAC, SDLC-MPA, COM Port Link station role	The parameters on both systems are complementary. If the host role is primary the Communications Server workstation must be configured as secondary or negotiable. Unless multipoint (*MP) is used, it is best to set the data link role to negotiable (*NEG).
Station address	Configure Devices SDLC-WAC, SDLC-MPA, COM Port Link station address (01-FE)	These values must match.
APPN CP session support: (Yes/No)	Configure Connections SDLC-WAC, SDLC-MPA, COM Port APPN Support	These must match if CP-CP sessions are desired.
APPN node type:	Configure Connections SDLC-WAC, SDLC-MPA, COM Port Adjacent CP type	These values must match.

AS/400 Host Device Definitions

The AS/400 host can create a device definition when Communications Server workstation connects without a previously defined device definition.

Mapping Communications Server—Host Parameters

Table 21 contains the OS/400 host program device parameters.

Table 21. AS/400 Communications Server Parameters Cross-Reference: Device Parameters

OS/400	Communications Server Profile/Parameters	Remarks
Remote location name	Configure Local LU 6.2 Local LU name or: Configure Node Fully qualified CP name (second field)	These values must match.
Attached controller	(none)	This parameter is for nonswitched connections. This value must match a previously defined host line definition.
Local location name		Use the default provided.
Remote network identifier	Configure Node Fully qualified CP name (first field)	Use the default provided.
Mode	Configure Mode Mode name	Use the default provided.

AS/400 Host Line Description and Communications Server

Table 22 contains the AS/400 host program line description.

Table 22. Host/PC Parameters Cross-Reference: Line Description

OS/400	Communications Server Profile/Parameters	Remarks
Local adapter address:	Configure Connections LAN destination address	The two addresses must match to communicate.

AS/400 Host Controller Description and Communications Server

Table 23 contains the OS/400 host program controller description.

Table 23. Host/PC Parameters Cross-Reference: Controller Description

OS/400	Communications Server Profile/Parameters	Remarks
Active switched line	(none)	This parameter is for nonswitched connections. This value must match a previously defined host line definition.
Remote control point	Configure Node Fully qualified CP name (second field)	The names must match.
Remote network identifier	Configure Node Fully qualified CP name (first field)	Use the default or match the parameters if different from the AS/400's Local Network ID.
Model controller description		This parameter must be YES if the AS/400 uses a connection network.
Connection network ID and Connection network CP name	Configure Connection Network Connection network name	These values must match for all nodes participating in a connection network.

AS/400 Twinaxial Descriptions

Table 24 contains the AS/400 twinaxial description.

Table 24. Host/PC Parameters Cross-Reference: Controller Description

AS/400	Communications Server Profile/Parameters	Remarks
Attached nonswitched line	(none)	This parameter is for nonswitched connections. This value must match a previously defined host line definition.

Mapping Communications Server—Host Parameters

Table 24. Host/PC Parameters Cross-Reference: Controller Description (continued)

AS/400	Communications Server Profile/Parameters	Remarks
Remote control point	Configure Node Fully qualified CP name (second field)	The names must match.
Remote network identifier	Configure Node Fully qualified CP name (first field)	Use the default or match the parameters if different from the AS/400's Local Network ID.
Data link role=*SEC:	Configure Connections SDLC-WAC, SDLC-MPA COM Port Link station role	The parameters on both systems are complementary. If the host role is primary, the Communications Server workstation must be configured as secondary or negotiable. Unless multipoint (*MP) is used, it is best to set the data link role to negotiable (*NEG).

AS/400 and Communications Server (X.25 PVC)

Table 25 contains the X.25 line parameters.

Table 25. AS/400 Communications Server Parameters Cross-Reference: X.25 PVC Connection

AS/400	Communications Server Profile/Parameters	Remarks
X.25 logical channel ID	Configure Connections X.25 COM Port, X.25-WAC Connection type	The two parameters must match your X.25 subscription. This AS/400 field can be found in the panel controller description. It has been included for completeness.

Mapping Communications Server—Host Parameters

Table 26. AS/400 Communications Manager Parameter Cross-Reference:
Controller Description

AS/400	Communications Manager Profile/Parameters	Remarks
Remote control point name	Configure Node Fully qualified CP name (second field)	These values must match.
Switched Connection Type		AS/400 will not start link without *DIAL.
Remote network identifier	Configure Node Fully qualified CP name (first field)	Use the default or match the parameters if different from the AS/400's Local Network ID.

Appendix B. More Information About Configuring AnyNet SNA over TCP/IP

This chapter contains more detailed information about the configuration necessary to use AnyNet SNA over TCP/IP.

Mapping SNA Resources to IP Addresses

One of the most crucial steps needed to enable SNA over TCP/IP communication is not done through Communication Server panels. Before SNA sessions or connections can be established, SNA over TCP/IP must determine the IP address of the partner. This is achieved by mapping the SNA identifier of the partner to an IP address using the following steps:

1. SNA over TCP/IP receives the SNA identifier from Communications Server in one of the following formats:
 - For LU names, `netid.luname`
 - For CP names, `netid.cpname`
 - For IDBLK and IDNUM values, configured as adjacent node ID, with two fields: `block ID` and `physical unit ID`.
2. SNA over TCP/IP takes the identifier and generates a domain name:
 - For LU names, `luname.netid.snasuffix`
 - For CP names, `cpname.netid.snasuffix`
 - For IDBLK and IDNUM values, `bbnnnnn.snasuffix`



The default value for `snasuffix` is **SNA.IBM.COM**. For additional information on the SNA domain name suffix, refer to the online help.

Figure 10 on page 180 shows examples of domain names generated by SNA over TCP/IP.

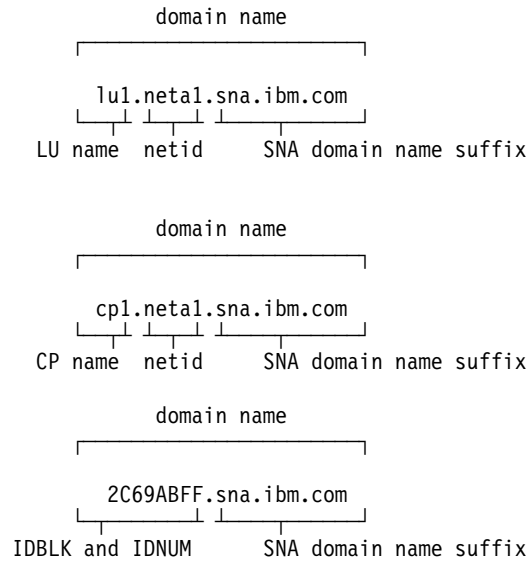


Figure 10. Formats of the Domain Names That SNA over TCP/IP Builds

3. SNA over TCP/IP requests that the domain name be translated into an IP address.
4. TCP/IP uses the HOSTS file or domain name server to translate the domain name into an IP address (for example, 9.67.192.28).

When the IP network includes SNA over TCP/IP gateways, consider the following additional address mapping issues:

- If the partner LU can be reached through a gateway, the domain name of the partner must be mapped to the IP address of the gateway. If there are parallel gateways, the domain name should be mapped to each gateway IP address.
- To minimize the address mapping information needed for AnyNet, consider using a naming convention in which your LU name is the same as the TCP/IP host name. For example, suppose your computer's host name is JANEDOE.ANYNET.OURCORP.COM. If you use the LU name JANEDOE and the netid ANYNET, and then set the SNA domain name suffix to OURCORP.COM, AnyNet will ask TCP/IP to resolve the name JANEDOE.ANYNET.OURCORP.COM. This name should already be in your domain name server.

Defining Domain Names and IP Addresses

This section describes the TCP/IP name resolution function, used by AnyNet to map SNA resources to IP addresses. This function queries both the local HOSTS file and any domain name servers to convert a domain name (for example, lua1.neta1.sna.ibm.com) into an IP address (for example, 10.1.1.1).

HOSTS File

You can use TCP/IP HOSTS files to map domain names to IP addresses for your network. However, as your network becomes larger and maintaining the HOSTS file on each end-user workstation becomes too time-consuming, it is recommended that you use a domain name server.

The HOSTS file (in the drivers\etc subdirectory of your NT system directory) lists:

- IP address
- Domain name
- Other aliases for the domain name

For example, if your IP address is 10.1.1.1, network ID is NETA1, SNA resource name is LUA1, and SNA domain name suffix is the default (sna.ibm.com), enter the following in your HOSTS file:

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

Domain Name Server

Domain names and IP addresses can also be defined in the domain name server database.

Each SNA identifier is mapped to a corresponding IP address by a domain name server. The location of these servers is configured in the Network section of the Control Panel.

For more information on HOSTS files and domain name servers, refer to your TCP/IP documentation. If your workstation is using the TCP/IP support in Windows NT, refer to the online TCP/IP documentation that is included with the Windows NT product.

SNA over TCP/IP Gateway Considerations

The following information pertains to gateways but not to access node functions.

Defining Unique CP Names and Connection Network Names

For configurations that have two or more SNA over TCP/IP gateways connecting an SNA network with two or more IP networks, you must define a unique SNA control point (CP) name and a unique SNA connection network name for each IP network.

All LUs that reside on access nodes in the IP network appear to reside on a node with this CP name.

Use the reverse data file of the domain name server or the HOSTS file to define the CP name and the connection network name for a given IP network. Map the IP address 127.0.0.3 to the CP name and map the IP address 127.0.0.4 to the connection network name.

The following example shows entries in the reverse data file. For an IP network with SNA network ID NETA, CP name MYCPNAME, and connection network name MYCNET, you would define the following entries:

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



A period is required at the end of the name only if the definition is in the DNS reverse data file. No period is used in HOSTS file definitions.



Do not include the SNA domain name suffix.

The AnyNet SNA over TCP/IP function of Communications Server provides a default CP name (\$ANYNET.\$GWCP) and a default connection network name (\$ANYNET.\$GWCNET). In configurations with one IP network, you can use the default by not defining a CP name or a connection network name. In configurations with multiple gateways connecting multiple IP networks, one IP network can use the default. You must, however, define a unique CP name and connection network name for all other IP networks.

Figure 11 on page 183 shows how to define the CP name and the connection network name for a configuration with two IP networks.

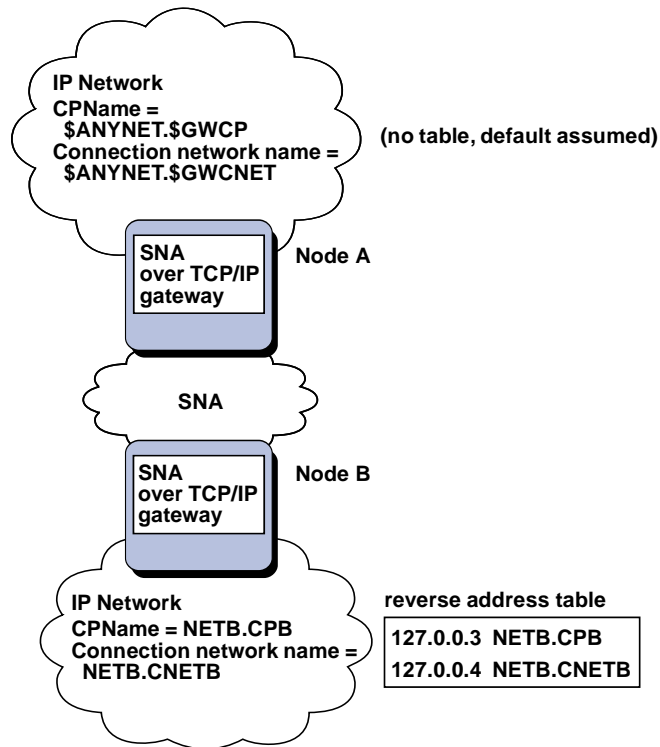


Figure 11. Defining a CP Name and a Connection Network Name

Using the Wildcard Entry to Reduce Domain Name Server Definitions

If you are using the SNA/IP gateway and your configuration meets the following naming restrictions, you can reduce the number of domain name server entries by defining a domain name entry for each SNA network ID that can be accessed through one or more SNA over TCP/IP gateways.

- Each SNA network must have an SNA network ID that is unique among all SNA networks.
- Each IP network must have an SNA network ID that is unique among all IP networks.
- An SNA network and an IP network can have the same SNA network ID.

By coding a single domain name entry for each SNA network ID, you do not have to define a domain name entry for every LU in the SNA network that you want to communicate with over the IP network. You can use a wildcard entry (*) to specify the LU name of all LUs that have the same SNA network

ID. By substituting a wildcard entry for the luname in the entry, you define a single domain name server entry that represents all LUs in that particular network.

Note: If you use the wildcard entry, you must use the full wildcard. Partial wildcards, such as LUA*, are not valid.

The wildcard entry is mapped to the IP address of the first SNA over TCP/IP gateway used to reach the network with that SNA network ID. As shown in Figure 12, logical units SNAAPPL1, APPC1, APPC2, and LU5 reside in network NETB and can only be reached from the IP network through an SNA over TCP/IP gateway with IP address IPgwg. If the SNA domain name suffix is SNA.IBM.COM, you define the following entry in the domain name server:

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

This entry is used for all four logical units.

Note: You have the option of defining each logical unit individually.

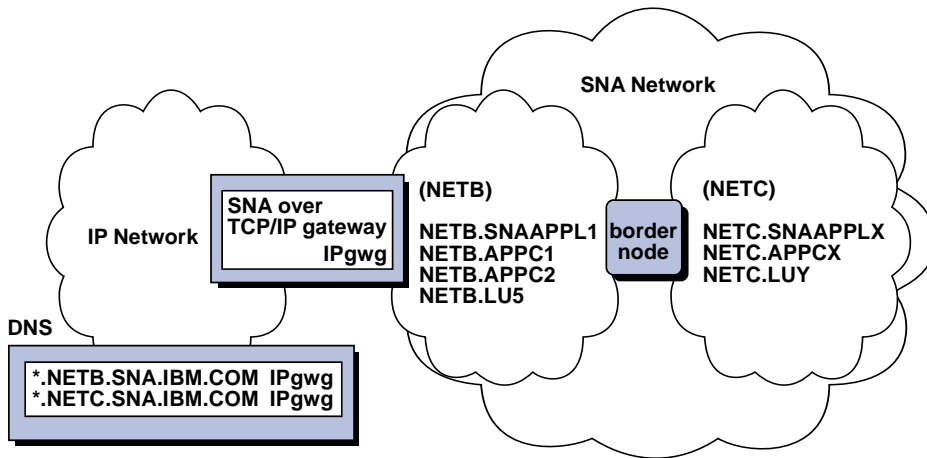


Figure 12. Domain Name Server Definitions for a Single Gateway Connected to an SNA Network with Two Network IDs

Each SNA network must have a unique entry. As shown in Figure 12, if you also have SNAAPPLX, APPCX, and LUY in network NETC, which can only be reached through the SNA over TCP/IP gateway with IP address IPgwg, the domain name server entries are as follows:

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

In addition, each gateway must have a unique entry. If you add a parallel SNA over TCP/IP gateway, as shown in Figure 13, with IP address IPgwh to the preceding example, the domain name server entries are as follows:

```

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

```

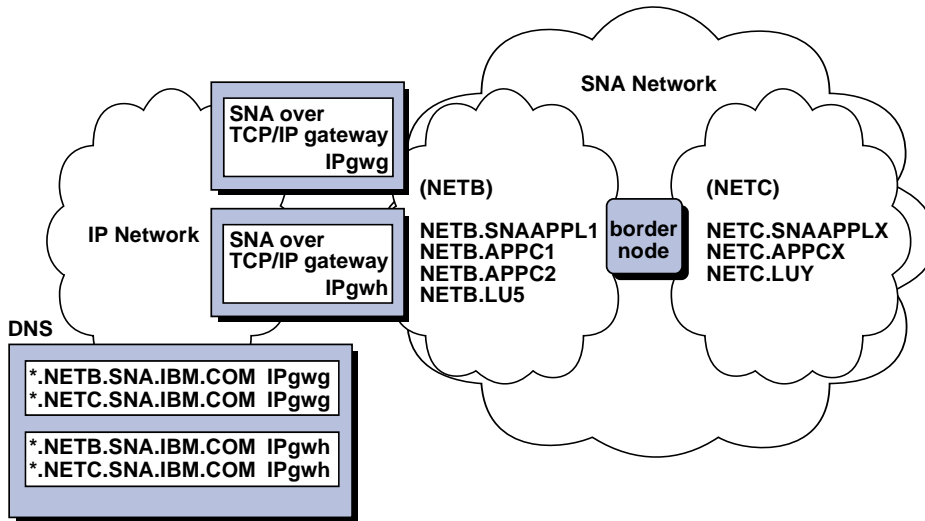


Figure 13. Domain Name Server Definitions for Parallel Gateways Connected to an SNA Network with Two Network IDs

SNA over TCP/IP Access Node Function Considerations

The following information pertains to access nodes only, and not to gateways.

How to Route SNA Sessions over AnyNet SNA over TCP/IP

When an SNA application initiates a session, Communications Server must first determine which transport to use - either SNA, IP, or a combination of the two.

You configure which transport you prefer by setting the routing preference. The routing preference can be set for the whole node via the default routing preference on the AnyNet over TCP/IP device or on a per LU basis when defining partner LUs.

The routing preference table is used only for new sessions. Previously existing sessions use the same transport; they are not brought down and rerouted if the routing preference table is changed.

Note: The routing preference for a node only governs sessions that are initiated from the node (access node sessions). Sessions that go through a node are not affected by the routing preference.

You can set or modify the default routing preference to one of the following:

Native first

Requests are routed over SNA. If no SNA route is available, requests are routed over TCP/IP.

Non-native first

Requests are routed over TCP/IP. If no TCP/IP route is available, requests are routed over SNA.

Native only

Requests are routed only over SNA. If no SNA route is available, the connection will fail.

Non-native only

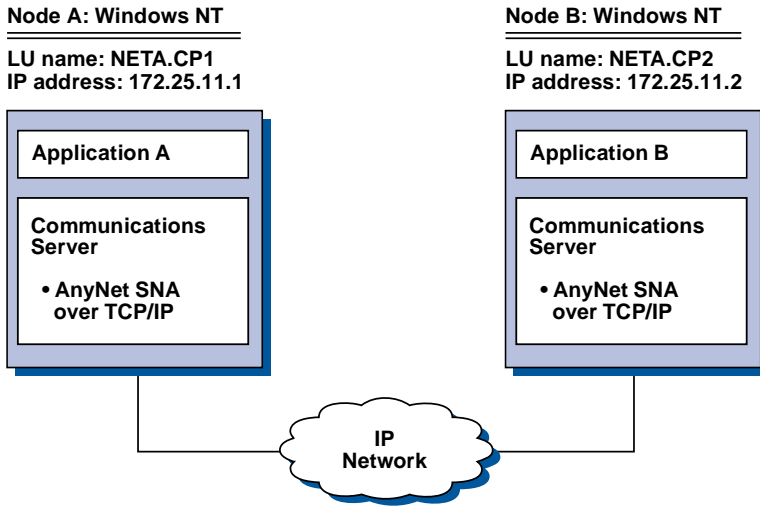
Requests are routed only over TCP/IP. If no TCP/IP route is available, the connection will fail.

AnyNet SNA over TCP/IP Configuration Examples

This section includes examples of AnyNet enabling SNA over IP communication. The following configuration instructions are complete only for the Windows NT operating system. In all examples, the SNA domain name suffix is SNA.IBM.COM.

For more information about configuring AnyNet for any other platforms mentioned in this section (such as VTAM or AS/400), refer to the appropriate product documentation.

Example 1. Running APPC or CPI-C Applications over a TCP/IP Network



Steps

Follow these steps to establish communications between the two Windows NT nodes. Note that in this example, the CP names are used as LU names.

For Windows NT Node A, do as follows:

1. Add the following entry to the local HOSTS file:
172.25.11.2 CP2.NETA.SNA.IBM.COM
2. Use the “CPI-C, APPC, or 5250 Emulation Configuration” on page 102, using **NETA.CP1** as the control point name in the Node Configuration step. Ensure that the routing preference is set to route sessions over TCP/IP.

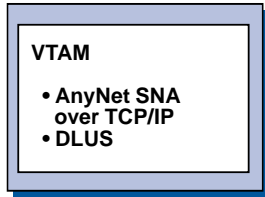
For Windows NT Node B, do as follows:

1. Add the following entry to the local HOSTS file:
172.25.11.1 CP1.NETA.SNA.IBM.COM
2. Use the “CPI-C, APPC, or 5250 Emulation Configuration” on page 102, using **NETA.CP2** as the control point name in the Node Configuration step. Ensure that the routing preference is set to route sessions over TCP/IP.

Example 2. 3270 Emulation via DLUR over a TCP/IP Network

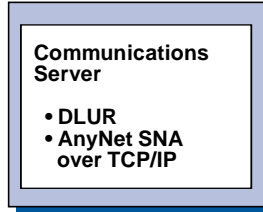
Node A: VTAM

CP name: NETA.CP1
IP address: 192.168.7.8



Node B: Windows NT

CP name: NETA.CP2
IP address: 192.168.7.10
Dependent LU name: NETA.DEPLU1



Steps

Follow these steps to establish communications between the VTAM Host (Node A) and the Windows NT workstation (Node B).

For Windows NT Node B, do as follows:

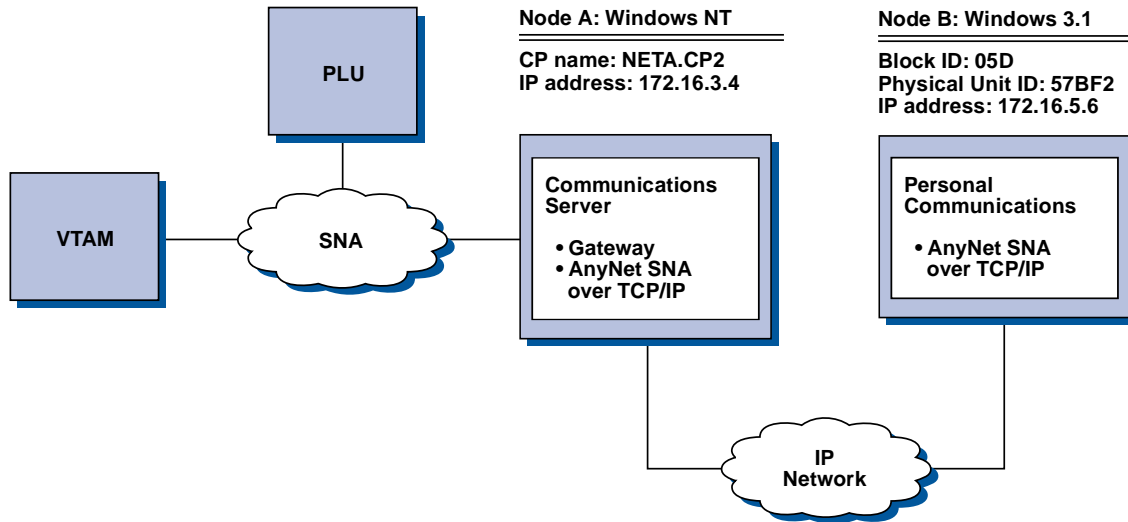
1. Add the following entry to the local HOSTS file:
192.168.7.8 CP1.NETA.SNA.IBM.COM
2. Use the “DLUR Support for Local LUs Subtask” on page 67, using:
 - **NETA.CP2** as the control point name in the Node Configuration step
 - **NETA.CP1** as the DLUS name in the DLUR PU Configuration step.Ensure that the routing preference is set to route sessions over TCP/IP.

For VTAM Node A, add the following entries to the HOSTS file:

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

Note that MVS AnyNet SNA over TCP/IP currently requires DLUS/DLUR for dependent LU communication.

Example 3. Using an SNA Gateway to Enable 3270 Emulation Between SNA and TCP/IP Networks



Steps

Follow these steps to establish communications between the Windows 3.1 workstation (Node B) and the VTAM host.

For Windows NT Node A, do as follows:

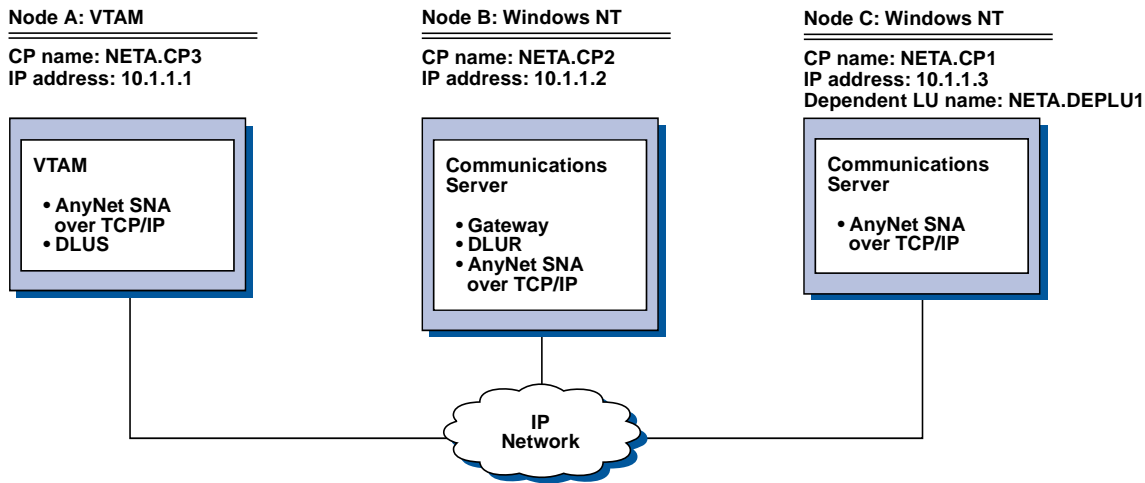
1. Add the following entry to the local HOSTS file:
172.16.5.6 05D57BF2.SNA.IBM.COM
2. Use the “SNA Gateway Configuration” on page 44, using
 - **NETA.CP2** as the control point name in the Node Configuration step
 - ANYNET device to which to assign implicit templates in the Defining Clients step.

For the Windows 3.1 node, add the following to the local HOSTS file:

172.16.3.4 CP2.NETA.SNA.IBM.COM

Note that Windows 3.1 clients are currently the only AnyNet SNA over TCP/IP clients that use Block ID and physical unit ID for AnyNet address mapping. All other clients and servers use the fully qualified CP name for communication with an SNA gateway.

Example 4. Using an SNA Gateway for 3270 Emulation over a TCP/IP Network



Steps

Follow these steps to establish communications between the Windows NT Workstation (Node C) and the VTAM host (Node A).

For Windows NT Node B, do as follows:

1. Add the following entry to the local HOSTS file:
10.1.1.3 CP1.NETA.SNA.IBM.COM
2. Use the “DLUR Support for Downstream LUs Subtask” on page 68, using:
 - **NETA.CP2** as the control point name in the Node Configuration step
 - **NETA.CP1** as the adjacent CP name on the AnyNet SNA over IP Connection definition in the Define Client Links step
 - **NETA.CP3** as the DLUS name in the Assign DLUS to a Client Link stepEnsure that routing preference is set to non-native for NETA.CP3.

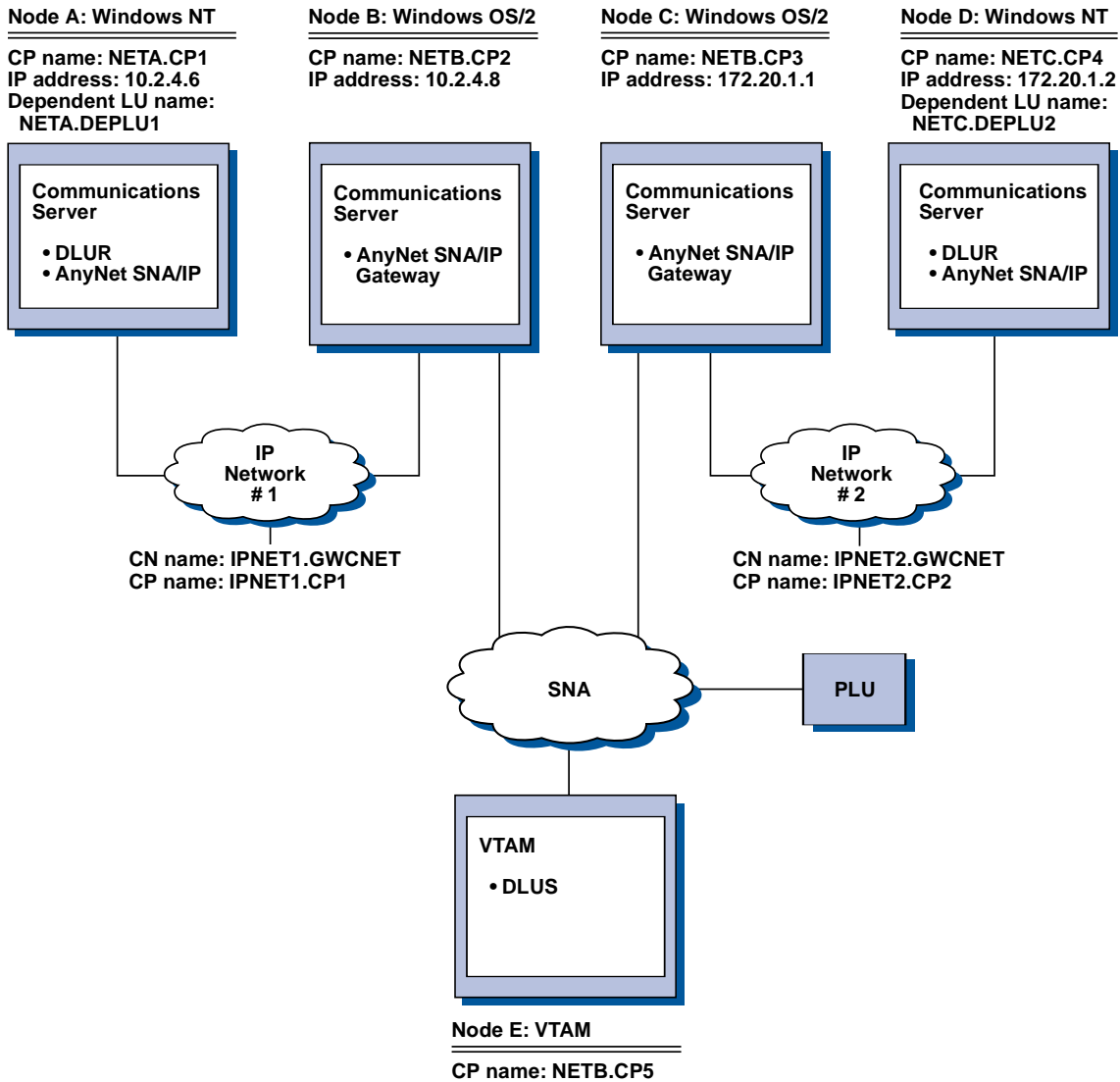
For Windows NT Node C, do as follows:

1. Add the following entry to the HOSTS file:
10.1.1.2 CP2.NETA.SNA.IBM.COM
2. Use the “3270 Configuration” on page 117 using:
 - **NETA.CP1** as the control point name in the node configuration step.
 - **NETA.CP2** as the adjacent CP name on the AnyNet SNA over IP connection definition in the connection configuration step.

For VTAM Node A, add the following entry to the HOSTS file:

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

Example 5. 3270 Emulation from Two Windows NT Workstations on Different IP Networks



Steps

Follow these steps to establish communications from the Windows NT workstation (Nodes A and D) to the VTAM Host (Node E).

For Windows NT Node A, do as follows:

1. Add the following entries to the local HOSTS file:

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

2. Use the “DLUR Support for Local LUs Subtask” on page 67, using:

- **NETA.CP1** as the control point name in the Node Configuration step
- **NETB.CP5** as the DLUS name in the DLUR PU Configuration step
Ensure that the routing preference for NETB.CP5 is set to non-native.

For OS/2 Node B, add the following entries to the HOSTS file:

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

For OS/2 Node C, add the following entries to the HOSTS file:

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

For Windows NT Node D, do as follows:

1. Add the following entry to the local HOSTS file:

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

2. Use “DLUR Support for Local LUs Subtask” on page 67, using

- **NETC.CP4** as the control point name in the Node Configuration step
- **NETB.CP5** as the DLUS name in the DLUR PU Configuration step
Ensure that the routing preference for NETB.CP5 is set to non-native.

Appendix C. More Information About Sockets over SNA

This chapter contains more information about how to configure Sockets over SNA.

The Sockets over SNA access node function of Communications Server enables WinSock compliant applications to communicate over SNA networks. The Sockets over SNA gateway function enables socket applications in SNA and IP networks to communicate.

How Does Sockets over SNA Work?

Figure 14 on page 194 shows the structure of a Windows NT node that is running Sockets over SNA and illustrates how socket application programs and Sockets over SNA operate on a Windows NT node.

More about AnyNet Sockets over SNA

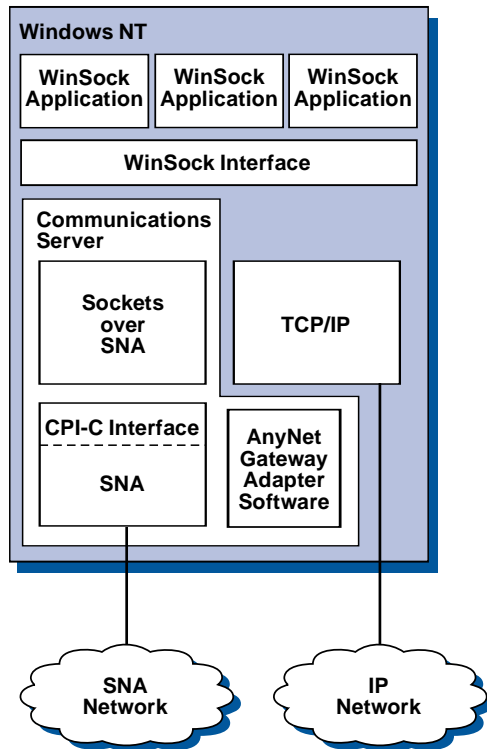


Figure 14. Structure of a Windows NT Node Running Sockets over SNA

WinSock is an API that lets socket applications run in a Windows environment. The TCP/IP stack that came with Windows NT version 3.51 (and with earlier Windows NT versions) implemented version 1.1 of WinSock. Starting with version 4.0, Windows NT supports version 2 of the WinSock API.

Sockets over SNA does not provide a WinSock interface and does not process socket calls. Instead, WinSock applications use the WinSock interface of the native TCP/IP stack. The Sockets over SNA gateway code then allows these applications to communicate across the SNA network.

Sockets over SNA gateway will allow socket applications running in an IP network to communicate with socket applications running on Sockets over SNA nodes. This is accomplished by routing packets between the SNA and IP networks and transforming them between SNA and IP protocols. The AnyNet gateway device driver assists in routing packets between TCP/IP and SNA networks, and the Sockets over SNA code converts between the two protocols.

Generating an LU 6.2 Call from a Socket Call

To enable TCP/IP-formatted information to route over SNA, Sockets over SNA maps IP addresses to SNA network-qualified LU names. When an application program invokes Sockets over SNA to establish a stream connection with another application program, Sockets over SNA establishes two half-duplex LU 6.2 conversations for the stream connection.

Sockets over SNA establishes one LU 6.2 conversation for all datagrams sent to a single destination. Conversations dedicated to datagram traffic are deallocated if they are unused for some specified period of time.

Mapping an IP Address to an SNA Network-Qualified Name

When an application program invokes Sockets over SNA to communicate with another application program, it supplies the IP address of the destination node. Sockets over SNA must map the IP address to an SNA address to issue an appropriate LU 6.2 call. For every IP address that identifies a node, there will be a corresponding SNA network-qualified name.

“Routing and Mapping Overview” on page 196 explains how address mapping works and provides guidelines and requirements for setting up IP-LU address mapping.

Routing and Mapping Data over SNA and IP Networks

Sockets over SNA gateways enable communication between socket application programs in IP and SNA networks by combining the routing function of TCP/IP with the protocol translation and address mapping capabilities of Sockets over SNA.

Protocol translation and address mapping are required when data is routed between nodes that use different transport protocols. The Sockets over SNA gateway automatically performs protocol translation after determining the type of transport associated with the destination IP address. For a summary of the routing and mapping process, see “How the Sockets over SNA Gateway Routes and Maps Data” on page 199.

Application Program Support Provided by Sockets over SNA

Sockets over SNA supports WinSock 1.1 and WinSock 2.0 (Windows NT 4.0 only) applications that use AF_INET sockets.

Sockets over SNA does not support applications that use broadcasting.

More about AnyNet Sockets over SNA

If you intend to use Sockets over SNA gateway to route information to and from an MVS/ESA node configured with the VTAM V3R4.2 Sockets over SNA function, you must first install the route function on the MVS/ESA node. To install the route function on MVS/ESA, install the program temporary fix (PTF) UW03567. You can obtain PTFs through any of the following sources:

- Information Access
- SoftwareXcel Extended
- IBMLink (ServiceLink)

If you do not have access to these sources, contact the IBM Support Center.

Planning for Sockets over SNA

This section describes what the network planner should consider before configuring a network with Sockets over SNA.

Routing and Mapping Overview

This section explains basic concepts of Internet addressing and how those concepts relate to routing and mapping. It includes the following information:

- “Internet Addressing”
- “IP Routing Table” on page 198
- “SNA Network ID Used by Sockets over SNA” on page 198
- “How an IP Address Is Mapped to an LU Name” on page 198
- “How the Sockets over SNA Gateway Routes and Maps Data” on page 199

Internet Addressing

Every host is assigned at least one unique Internet Protocol (IP) address, which is used to route data through the network.

Note: In the IP suite of protocols, *host* refers to an end system and can be any workstation; it does not have to be a mainframe.

The IP address assigned to the host does not define a host on the network; it defines a network interface on that host to a network. For example, the address of the SNA network interface identifies a node’s connection to the SNA network.

More about AnyNet Sockets over SNA

A gateway host has a unique IP address for each network interface. Because Sockets over SNA gateway routes SNA and TCP/IP data, you must set up unique IP addresses for the TCP/IP and SNA interfaces.

The following section describe the IP address format, address classes, and network masks. For more detailed information, see your TCP/IP documentation.

IP Address Format and Classes

An IP address consists of a 2-part, 32-bit address field:

- The first part of the address field contains the network address; the second part contains the host address.
- The number of bits used for the network and host portions of an IP address are variable, depending on the address class of the IP address.
- A network mask enables you to use part of the host portion of the IP address as a subnetwork address.

Default network masks are shown in Table 27.

Table 27. IP Address Masks Supported by Sockets over SNA

For a dotted decimal IP address in the form <i>a.b.c.d</i> , the range of values for <i>a</i> is:	Default Network Mask
1–127	255.0.0.0
128–191	255.255.0.0
192–223	255.255.255.0

Masks Used by Sockets over SNA

Sockets over SNA uses two types of masks:

- **Subnet mask**

The subnet mask is used in routing and is specified during the configuration of the local node and routes. You can accept the default subnet mask or specify a value other than the default to define subnetwork addresses.

- **Address mask**

The address mask is used for generated IP-LU address mapping and is specified during configuration.

IP Routing Table

Each host has an IP routing table that stores information about possible destinations and how to reach them. Route entries are added when:

- The local IP address is defined. For more information, see the online help.
- Route statements are defined from the SNA Node Configuration window. Click **Configure AnyNet Sockets** and then click **Routes**. For more information, see the online help.
- A route with fewer hops is found. This occurs when Sockets over SNA gateway receives an ICMP redirect or RIP message. For more information, see “Route Discovery Function” on page 200.

For a routing table example, see Figure 15 on page 199.

SNA Network ID Used by Sockets over SNA

For each route you define through the SNA interface (sna0), there must be a corresponding SNA network ID to which the IP network address is mapped. The number of SNA network IDs you define depends on how you want to map the IP network to the SNA network.

For example, if the socket applications using SNA are configured to use IP subnetworks 9.67.0.0 and 9.77.0.0, you can define an SNA network ID that corresponds to each IP subnetwork, or you can define one SNA network ID that corresponds to both subnetworks. Sockets over SNA does not require a unique one-to-one mapping between an IP network address and an SNA network ID.

How an IP Address Is Mapped to an LU Name

You can use either explicit or generated mapping to map IP addresses to SNA LU names:

- In explicit mapping, all LU names are defined, and you assign each IP host address to a specific SNA LU name during configuration.
- In generated mapping, LU names are automatically generated for you. During configuration, you specify a network IP address, address mask, network ID, and LU template value.

Sockets over SNA uses the address mask to map the network portion of the IP address to the SNA network ID and the host portion to the SNA LU name. The LU template value is used to determine the characters and the positions of characters used in the LU name.

You can display the generated LU name for a given IP address using the **sxmap** command line utility. The syntax for this utility is:

sixmap convert <IP address> <address mask> <LU template>

How the Sockets over SNA Gateway Routes and Maps Data

The following steps briefly describe how Sockets over SNA Gateway determines whether to route data over SNA or TCP/IP, and how address mapping is handled:

1. Sockets over SNA searches its own routing table to find a route that enables data to reach the destination IP address. If Sockets over SNA does not find any matching routes, the connection request is forwarded to the native TCP/IP stack.
2. If Sockets over SNA finds a matching route, the route entry indicates how the destination can be reached:
 - a. If the router address is the address of a local network interface, such as `sna0`, the destination network, subnetwork, or host address can be reached directly.
 - b. If the router address is the address of a gateway or router, the destination can only be reached through that intermediate gateway or router.

Figure 15 shows an example of an IP routing table.

Destination IP Address	Destination Mask	Gateway IP Address	Use Count
1.2.3.4	255.255.255.255	199.245.253.1	10
10.0.0.0	255.0.0.0	199.245.253.2	0
10.11.0.0	255.255.0.0	199.245.253.113	37
127.0.0.1	255.255.255.255	127.0.0.1	8
128.1.0.0	255.255.0.0	199.245.253.3	0
199.245.253.0	255.255.255.0	199.245.253.113	368

Figure 15. Example of an IP Routing Panel

3. If no route is found in the Sockets over SNA routing table, then Sockets over SNA assumes that the TCP/IP destination can be reached through a native IP network. Refer to your TCP/IP documentation for more information on how TCP/IP routes data.
4. If the chosen route indicates that data should go over the SNA interface (`sna0`), Sockets over SNA looks up the next-hop address in the IP-LU mapping table:
 - a. If Sockets over SNA finds a matching entry, an LU 6.2 connection is established.

More about AnyNet Sockets over SNA

- b. If Sockets over SNA does not find a matching entry, the connection attempt fails and Sockets over SNA returns completion error code WSAEHOSTUNREACH.
 - c. Sockets over SNA passes the destination address and data to Communications Server.
5. All routes defined to Sockets over SNA are mirrored to the native TCP/IP stack so that packets from IP can be routed over SNA.

Route Discovery Function

The route discovery function provided by Sockets over SNA gateway can help you route TCP/IP traffic more efficiently and reduce the number of explicitly defined route statements in your network. You do not have to select or configure this function.

One of the problems with large networks is how to discover that new networks or subnetworks have been added and what router to use to get to the new network or subnetwork. Sockets over SNA solves this problem by having all nodes initially use a default router that notifies other nodes when a more direct route is discovered. This is more efficient than using the typical TCP/IP solution of broadcasting routing information.

Note: To effectively use this function, algorithmic mapping of IP addresses to LU names and an APPN backbone network should be used. Otherwise, nodes must explicitly define LU names and IP addresses for all remote nodes with which they communicate.

Figure 16 shows a configuration example.

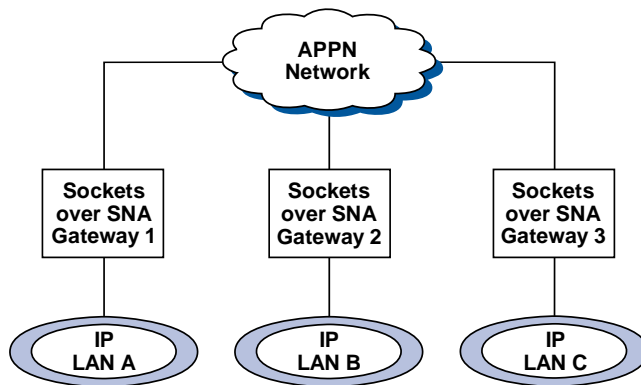


Figure 16. Example of a Network Using the Sockets over SNA Route Discovery Function

In this scenario:

- Gateways 1, 2, and 3 are Sockets over SNA gateways connected to IP LANs. These gateways connect the IP LANs to an APPN backbone network.
- Gateway 1 is the only gateway where you maintain a complete, permanent routing table.

Gateways 2 and 3 define Gateway 1 as their default router. If a remote network or subnetwork is known to Gateway 1, Gateways 2 and 3 do not have to explicitly define these routes.

- When Gateways 2 and 3 route data to undefined networks or subnetworks, these requests are sent to their default router, Gateway 1.

If the network or subnetwork is known to Gateway 1 and a more direct path is available, Gateway 1 sends an ICMP redirect message back to the requester indicating the path to take in the future. This ICMP redirect message updates the requester's routing table. Therefore, Gateways 2 and 3 dynamically build their routing tables for remote networks and subnetworks as needed.

- If new gateways are added, update the permanent routing table of Gateway 1. No explicit route statements are needed for Gateways 2 and 3.

Defining Sockets over SNA Modes

Sockets over SNA uses LU 6.2 conversations to enable communication between socket application programs. When an LU 6.2 conversation is established, Sockets over SNA defines the mode and associated session characteristics of the connection. Communications Server uses the mode name to identify characteristics of the connection between the two Sockets over SNA nodes.

The default Sockets over SNA mode is BLANK. You can use the default mode for Sockets over SNA or define your own. To change the default Sockets over SNA mode, from the SNA Node Configuration window, click **Configure AnyNet Sockets Over SNA** and then click **Modes**. You can define another default mode for all TCP/IP traffic and assign a specific mode to a specific TCP/IP port.

If you specify an alternative mode that is not defined by Communications Server, you must define the session characteristics associated with that mode to Communications Server.

Changing the Idle-Timeout Interval

The Idle Timeout start option allows you to adjust the number of idle seconds before Sockets over SNA deallocates a datagram conversation. This interval enables you to balance between using system resources to maintain an

More about AnyNet Sockets over SNA

existing datagram conversation and taking longer to reestablish a new datagram conversation. For example, if you set this value low, unused datagram conversations end faster, but it takes longer to send the next datagram. The default idle-timeout interval is 90 seconds.

To modify the start option, from the SNA Node Configuration window, click **Configure AnyNet Sockets over SNA**, then click **View/Change/Add**, click the **Advanced** tab and select a new value for this option.

Appendix D. Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make them available in all countries in which IBM operates. 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. Subject to IBM's valid intellectual property or other legally protectable rights, any functionally equivalent product, program, or service may be used instead of the IBM product, program, or service. The evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, are the responsibility of the user.

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
USA

For license inquiries regarding double-byte character set (DBCS) information, contact:

IBM World Trade Asia Corporation Commercial Relations
IBM Kamiya-cho Building, 4-3-9 Toranomom, Minato-ku
Tokyo, Japan

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:

Site Counsel
IBM Corporation
P.O. Box 12195
3039 Cornwallis Road
Research Triangle Park, NC 27709-2195
USA

Notices

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 document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement.

This document is not intended for production use and is furnished as is without any warranty of any kind, and all warranties are hereby disclaimed including the warranties of merchantability and fitness for a particular purpose.

Appendix E. Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

Advanced Peer-to-Peer Networking	Micro Channel
AIX	NetView
AnyNet	OS/2
APPNAS/400	OS/400
AT	Personal System/2
BookManager	Portmaster
CICS	Presentation Manager
DB2/2	PS/2
eNetwork	System/370
Enterprise System/9000	System/390
ES/9000	SystemView
FFST/2	S/370
First Failure Support Technology/2	S/390
Global Network	TalkLink
IBM	VTAM
IBMLink	WebExplorer
IMS	

Adobe is a trademark of Adobe Systems, Incorporated.

PC Direct is a trademark of Ziff Communications Company and is used by IBM Corporation under license.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

C-bus is a trademark of Corollary, Inc.

Microsoft, Windows, and the Windows 95 logo are trademarks or registered trademarks of Microsoft Corporation.

Java and HotJava are trademarks of Sun Microsystems, Inc.

Other company, product, and service names, which may be denoted by a double asterisk (**), may be trademarks or service marks of others.

Glossary

This glossary includes terms and definitions from:

- The *American National Standard Dictionary for Information Systems*, ANSI X3.172-1990, copyright 1990 by the American National Standards Institute (ANSI). Copies may be purchased from the American National Standards Institute, 11 West 42nd Street, New York, New York 10036. Definitions are identified by the symbol (A) after the definition.
- The ANSI/EIA Standard—440-A, *Fiber Optic Terminology* Copies may be purchased from the Electronic Industries Association, 2001 Pennsylvania Avenue, N.W., Washington, DC 20006. Definitions are identified by the symbol (E) after the definition.
- The *Information Technology Vocabulary* developed by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC1/SC1). Definitions of published parts of this vocabulary are identified by the symbol (I) after the definition; definitions taken from draft international standards, committee drafts, and working papers being developed by ISO/IEC JTC1/SC1 are identified by the symbol (T) after the definition, indicating that final agreement has not yet been reached among the participating National Bodies of SC1.
- The *IBM Dictionary of Computing*, New York: McGraw-Hill, 1994.
- Internet Request for Comments: 1208, *Glossary of Networking Terms*

- Internet Request for Comments: 1392, *Internet Users' Glossary*
- The *Object-Oriented Interface Design: IBM Common User Access Guidelines*, Carmel, Indiana: Que, 1992.

The following cross-references are used in this glossary:

Contrast with:

This refers to a term that has an opposed or substantively different meaning.

Synonym for:

This indicates that the term has the same meaning as a preferred term, which is defined in its proper place in the glossary.

Synonymous with:

This is a backward reference from a defined term to all other terms that have the same meaning.

See: This refers the reader to multiple-word terms that have the same last word.

See also:

This refers the reader to terms that have a related, but not synonymous, meaning.

Deprecated term for:

This indicates that the term should not be used. It refers to a preferred term, which is defined in its proper place in the glossary.

A

activate. To make a resource ready to perform its function. Contrast with *deactivate*.

active. (1) Operational. (2) Pertaining to a node or device that is connected or is available for connection to another node or device.

adapter. (1) A hardware component that must be installed in the personal computer to connect to the SDLC, LAN, asynchronous, DFT, or other communication attachment (possibly connecting through a modem). (2) A part that electrically or physically connects a device to a computer or to another device.

Advanced Peer-to-Peer Networking (APPN).

An extension to SNA featuring (a) greater distributed network control that avoids critical hierarchical dependencies, thereby isolating the effects of single points of failure; (b) dynamic exchange of network topology information to foster ease of connection, reconfiguration, and adaptive route selection; (c) dynamic definition of network resources; and (d) automated resource registration and directory lookup. APPN extends the LU 6.2 peer orientation for end-user services to network control and supports multiple LU types, including LU 2, LU 3, and LU 6.2.

Advanced Peer-to-Peer Networking (APPN) end node.

A node that provides a broad range of end-user services and supports sessions between its local control point (CP) and the CP in an adjacent network node. It uses these sessions to dynamically register its resources with the adjacent CP (its network node server), to send and receive directory search requests, and to obtain management services. An APPN end node can also attach to other end nodes.

Advanced Peer-to-Peer Networking (APPN) network.

A collection of interconnected network nodes and their client end nodes.

Advanced Peer-to-Peer Networking (APPN)

network node. A node that offers a broad range of end-user services and that can provide the following:

- Distributed directory services, including registration of its domain resources to a central directory server
- Topology database exchanges with other APPN network nodes, enabling network nodes throughout the network to select optimal routes for LU-LU sessions based on requested classes of service
- Session services for its local LUs and client end nodes
- Intermediate routing services within an APPN network

Advanced Peer-to-Peer Networking (APPN)

node. An APPN network node or an APPN end node.

advanced program-to-program communication

(APPC). (1) (2) An LU 6.2 logical unit protocol implementation of SNA that lets interconnected systems share programming tasks. The general facility characterizing the LU 6.2 architecture and its various implementations in products. (3) Sometimes used to refer to the LU 6.2 architecture and its product implementations as a whole, or to an LU 6.2 product feature in particular, such as an APPC application programming interface.

alert. (1) A message sent to a management services focal point in a network to identify a problem or an impending problem. (2) In SNA management services (SNA/MS), a high priority event that warrants immediate attention.

allocate. (1) An LU 6.2 application programming interface (API) verb used to assign a session to a conversation for the conversation's use. (2) Contrast with *deallocate*.

American National Standards Institute (ANSI).

An organization consisting of producers, consumers, and general interest groups, that establishes the procedures by which accredited

organizations create and maintain voluntary industry standards in the United States. (A)

ANR. Automatic network routing.

ANSI. American National Standards Institute.

AnyNet product family. A group of IBM products that implement the multiprotocol transport networking (MPTN) architecture, thus enabling application programs to communicate independently of the underlying network transport protocol.

APAR. Authorized program analysis report.

API. Application programming interface.

APPC. Advanced program-to-program communication.

application programming interface (API). (1) (2) A defined programming language interface between an IBM system control program or an IBM-licensed program and the program user. The set of programming language constructs or statements that can be coded in an application program to obtain the specific functions and services provided by an underlying operating system or service program. (3) In VTAM, the language structure used in control blocks so that application programs can reference them and be identified to VTAM.

APPN. Advanced Peer-to-Peer Networking.

APPN end node. See *Advanced Peer-to-Peer Networking (APPN) end node*.

APPN network. See *Advanced Peer-to-Peer Networking (APPN) network*.

ASCII (American National Standard Code for Information Interchange). The standard code, using a coded character set consisting of 7-bit coded characters (8 bits including parity check), that is used for information interchange among data processing systems, data communication systems, and associated equipment. The ASCII set consists of control characters and graphic characters. (A)

ASYNCR. Asynchronous.

asynchronous (ASYNCR). (1) Pertaining to two or more processes that do not depend upon the occurrence of specific events such as common timing signals. (T) (2) Without regular time relationship; unexpected or unpredictable with respect to the execution of program instructions.

attach. (1) In programming, to create a task that can be executed asynchronously with the execution of the mainline code. (2) To connect a device logically to a ring network.

authorized program analysis report (APAR). A report of a problem caused by a suspected defect in a current unaltered release of a program.

automatic network routing (ANR). In High-Performance Routing (HPR), a highly efficient routing protocol that minimizes cycles and storage requirements for routing network layer packets through intermediate nodes on the route.

B

Basic Input/Output System (BIOS). Code that controls basic hardware operations, such as interactions with diskette drives, hard disk drives, and the keyboard.

batch. (1) An accumulation of data to be processed. (2) A group of records or data processing jobs brought together for processing or transmission. (3) Pertaining to activity involving little or no user action. Contrast with *interactive*. (4) In SNA, a request to activate a session between two logical units (LUs). See also *session activation request*. Contrast with *UNBIND*.

BIOS. (1) Basic Input/Output System. (2) See also *NetBIOS*.

bps. Bits per second.

C

call. (1) The action of bringing a computer program, a routine, or a subroutine into effect,

usually by specifying the entry conditions and jumping to an entry point. (I) (A) (2) In data communication, the actions necessary to make a connection between two stations on a switched line. (3) In communications, a conversation between two users. (4) To transfer control to a procedure, program, routine, or subroutine. (5) To attempt to contact a user, regardless of whether the attempt is successful.

calling. (1) The process of transmitting selection signals in order to establish a connection between data stations. (I) (A) (2) In X.25 communications, pertaining to the location or user that makes a call.

Cancel. A push button that removes a window without applying any changes made in that window.

CD. Compact disc.

CD-ROM. High-capacity read-only memory in the form of an optically read compact disc.

client. (1) A functional unit that receives shared services from a server. (T) (2) A user.

client/server. In communications, the model of interaction in distributed data processing in which a program at one site sends a request to a program at another site and awaits a response. The requesting program is called a client; the answering program is called a server.

clipboard. An area of storage provided by the system to hold data temporarily.

cluster. A station that consists of a control unit (a cluster controller) and the terminals attached to it.

code page. (1) A table that defines a coded character set by assignment of a character meaning to each code point in the table for a language or a country. (2) A mapping between characters and their internal binary representation. (3) An assignment of graphic characters and control function meanings to all code points; for example, assignment of characters and meanings to 256 code points for

an 8-bit code, assignment of characters and meanings to 128 code points for a 7-bit code. (4) In the Print Management Facility, a font library member that associates code points and character identifiers. A code page also identifies invalid code points. (5) A particular assignment of hexadecimal identifiers to graphic characters. (6) In AFP support, a font file that associates code points and graphic character identifiers.

COM. See *ACDI port*.

command. (1) A request from a terminal for the performance of an operation or the execution of a particular program. (2) In SNA, any field set in the transmission header (TH), request header (RH), and sometimes portions of a request unit (RU), that initiates an action or that begins a protocol; for example: (a) Bind Session (session-control request unit), a command that activates an LU-LU session, (b) the change-direction indicator in the RH of the last RU of a chain, (c) the virtual route reset window indicator in an FID4 transmission header.

command area. In Basic CUA architecture, the area on a panel that contains the command entry field.

command line. (1) On a display screen, a display line usually at the bottom of the screen, in which only commands can be entered. (2) In CUA architecture, deprecated term for *command area*.

command line interface (CLI). A type of computer interface in which the input command is a string of text. Contrast with *graphical user interface (GUI)*.

command name. The first term in a command, usually followed by operands.

common operations services (COS). The portion of SNA management services that pertains to the major vectors for limited remote operations control.

Common Programming Interface for Communications (CPI-C). An evolving application programming interface (API),

embracing functions to meet the growing demands from different application environments and to achieve openness as an industry standard for communications programming. CPI-C provides access to interprogram services such as (a) sending and receiving data, (b) synchronizing processing between programs, and (c) notifying a partner of errors in the communication.

communication adapter. (1) A circuit card with associated software that enables a processor, controller, or other device to be connected to a network. (2) A mechanism that enables communication facilities to be attached to host processors..

compact disc (CD). (1) A disc, usually 4.75 inches in diameter, from which data is read optically by means of a laser. (2) A disc with information stored in the form of pits along a spiral track. The information is decoded by a compact-disc player and interpreted as digital audio data, which most computers can process.

compile. (1) To translate all or part of a program expressed in a high-level language into a computer program expressed in an intermediate language, an assembly language, or a machine language. (T) (2) To prepare a machine language program from a computer program written in another programming language by making use of the overall logic structure of the program, or generating more than one computer instruction for each symbolic statement, or both, as well as performing the function of an assembler. (A) (3) To translate a source program into an executable program (an object program). (4) To translate a program written in a high-level programming language into a machine language program.

configuration. (1) The manner in which the hardware and software of an information processing system are organized and interconnected. (T) (2) The devices and programs that make up a system, subsystem, or network. (3) In Personal Communications, the arrangement of personal computers connected to

one or more host systems by one or more attachment types. Examples are: SDLC, LAN, ASYNCH, X.25, or DFT.

configuration file. A file that specifies the characteristics of a system device or network.

configuration services. One of the types of network services in a control point (SSCP, NNCP, or ENCP). Configuration services activates, deactivates, and records the status of physical units, links, and link stations.

configure. To describe to a system the devices, optional features, and programs installed on the system.

control point (CP). (1) A component of an APPN or LEN node that manages the resources of that node. In an APPN node, the CP is capable of engaging in CP-CP sessions with other APPN nodes. In an APPN network node, the CP also provides services to adjacent end nodes in the APPN network. (2) A component of a node that manages resources of that node and optionally provides services to other nodes in the network. Examples are a system services control point (SSCP) in a type 5 subarea node, a network node control point (NNCP) in an APPN network node, and an end node control point (ENCP) in an APPN or LEN end node. An SSCP and an NNCP can provide services to other nodes.

Control Program (CP). In VM/ESA, a component that manages the resources of a single computer so multiple computing systems appear to exist. Each of these apparent systems, or virtual machines, is the functional equivalent of an IBM System/370, 370-XA, or ESA computer.

conversation. A logical connection between two transaction programs using an LU 6.2 session. Conversations are delimited by brackets to gain exclusive use of a session.

CP. (1) Control point. (2) In VM, Control Program.

CPI-C. Common Programming Interface for Communications.

CP name. A network-qualified name of a control point (CP), consisting of a network ID qualifier identifying the network (or name space) to which the CP's node belongs, and a unique name within the scope of that network ID identifying the CP. Each APPN or LEN node has one CP name, assigned to it at system-definition time.

customization. The process of configuring one or more personal computers connected to a host system by the SDLC, LAN, ASYNCH, X.25, DFT, or other attachment. Customization precedes Personal Communications installation and includes the definition of the sessions to be carried out by Personal Communications.

D

data link. In SNA, synonym for *link*.

data link control (DLC). A set of rules used by nodes on a data link (such as an SDLC link or a token ring) to accomplish an orderly exchange of information.

data link control (DLC) layer. In SNA, the layer that consists of the link stations that schedule data transfer over a link between two nodes and perform error control for the link. Examples of data link control are SDLC for serial-by-bit link connection and data link control for the System/370 channel.

Note: The DLC layer is usually independent of the physical transport mechanism and ensures the integrity of data that reaches the higher layers.

DBCS. Double-byte character set.

deactivate. To take a resource of a node out of service, rendering it inoperable, or to place it in a state in which it cannot perform the functions for which it was designed. Contrast with *activate*.

deallocate. An LU 6.2 application programming interface (API) verb that terminates a conversation, thereby freeing the session for a future conversation. Contrast with *allocate*.

default. Pertaining to an attribute, condition, value, or option that is assumed when none is explicitly specified. (I)

Delete. A choice that removes a selected object. The space it occupied is usually filled by the remaining object or objects in the window.

dependent LU. See *SSCP-dependent LU*.

dependent LU requester (DLUR). An APPN end node or an APPN network node that owns dependent LUs, but requests that a dependent LU server provide the SSCP services for those dependent LUs..

dependent LU server (DLUS). An APPN network node that provides SSCP services for a dependent LU in its own or another APPN network. Contrast with *dependent LU requester*..

device driver. (1) A file that contains the code needed to use an attached device. (2) A program that enables a computer to communicate with a specific peripheral device; for example, a printer, a videodisc player, or a CD drive. (3) A collection of subroutines that control the interface between I/O device adapters and the processor.

dialog. (1) The interaction between a user and a computer. (2) In an interactive system, a series of related inquiries and responses similar to a conversation between two people.

directory. (1) A table of identifiers and references to the corresponding items of data. (I) (A) (2) A named hierarchical grouping of files in a file system. (3) A database in an APPN node that lists names of resources (in particular, logical units) and records the CP name of the node where each resource is located. See *distributed directory database* and *local directory database*.

directory services (DS). A control point component of an APPN node that maintains knowledge of the location of network resources.

distributed directory database. The complete listing of all the resources in the network as maintained in the individual directories scattered

throughout an APPN network. Each node has a piece of the complete directory, but it is not necessary for any one node to have the entire list. Entries are created, modified, and deleted through system definition, operator action, automatic registration, and ongoing network search procedures. Synonymous with *distributed network directory* and *network directory database*.

distributed network directory. Synonym for *distributed directory database*.

distributed processing. Processing that takes place across two or more linked systems.

DLC. Data link control.

DLUR. Dependent LU requester.

domain operator. In a multiple-domain network, the person or program that controls operation of resources controlled by one system services control point (SSCP). See also *network operator*.

DOS. Disk Operating System. See *IBM Disk Operating System*.

double-byte character set (DBCS). A set of characters in which each character is represented by 2 bytes. Languages such as Japanese, Chinese, and Korean, which contain more symbols than can be represented by 256 code points, require double-byte character sets. Because each character requires 2 bytes, the typing, display, and printing of DBCS characters requires hardware and programs that support DBCS. Contrast with *single-byte character set (SBCS)*.

double-click. To press and release a button on a pointing device twice while a pointer is within the limits that the user has specified for the operating environment.

download. (1) To transfer programs or data from a computer to a connected device, typically a personal computer. (T) (2) To transfer data from a computer to a connected device, such as a workstation or microcomputer. Contrast with *upload*.

downstream. In the direction of data flow from the host to the user. Contrast with *upstream*.

drive. A peripheral device, especially one that has addressed storage media.

DS. Directory services.

DTE. Data terminal equipment. (A)

DTR. Data terminal ready.

duplex. Pertaining to communication in which data can be sent and received at the same time. Synonymous with *full-duplex*. Contrast with *half-duplex*.

dynamic. (1) In programming languages, pertaining to properties that can only be established during the execution of a program; for example, the length of a variable-length data object is dynamic. (I) (2) Pertaining to an operation that occurs at the time it is needed rather than at a predetermined or fixed time. (3) Contrast with *static*.

E

EBCDIC. Extended binary-coded decimal interchange code. A coded character set of 256 8-bit characters.

EGA. Enhanced graphics adapter.

EHLAPI. Emulator High-Level Language Application Programming Interface.

element. (1) A field in the network address. (2) In SNA, the particular resource within a subarea that is identified by an element address. See also *subarea*.

emulator. A program that allows a device to operate as if it were a different type of device. Personal Communications, for example, allows supported personal computers and printers to operate as if they were 3270-series workstations.

Emulator High-Level Language Application Programming Interface (EHLAPI). In Communications Manager/2, an application

programming interface that provides programming access to the area in computer memory that corresponds to the user's screen image (this area in memory is known as the "presentation space").

end node (EN). (1) See *Advanced Peer-to-Peer Networking (APPN) end node* and *low-entry networking (LEN) end node*. (2) In communications, a node that is frequently attached to a single data link and cannot perform intermediate routing functions.

entry field. An area into which a user types or places text. Its boundaries are usually indicated.

environment variable. A variable that specifies (a) how an operating system or another program will run or (b) the devices that the operating system will recognize.

ER. Explicit route.

error. A discrepancy between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition. (I) (A)

Ethernet. A 10-Mbps baseband local area network that allows multiple stations to access the transmission medium at will without prior coordination, avoids contention by using carrier sense and deference, and resolves contention by using collision detection and delayed retransmission. Ethernet uses carrier sense multiple access with collision detection (CSMA/CD).

event. An occurrence of significance to a task; for example, an SNMP trap, the opening of a window or a submap, or the completion of an asynchronous operation.

exception. An abnormal condition such as an I/O error encountered in processing a data set or a file.

explicit route (ER). In SNA, a series of one or more transmission groups that connect two subarea nodes. An explicit route is identified by an origin subarea address, a destination subarea

address, an explicit route number, and a reverse explicit route number. Contrast with *virtual route (VR)*.

extended binary-coded decimal interchange code (EBCDIC). The standard code, using a character set consisting of 8-bit coded characters, used by Personal Communications for information interchange between personal computers and a host system. See also *American National Standard Code for Information Interchange*.

E1. See *T1*.

F

feature. A part of an IBM product that may be ordered separately by the customer.

file transfer. The transfer of one or more files from one system to another over a data link.

File Transfer Protocol (FTP). In the Internet suite of protocols, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

focal point (FP). See *management services focal point (MSFP)*.

folder. A container used to organize objects.

FP. Focal point.

frame. (1) In Open Systems Interconnection architecture, a data structure pertaining to a particular area of knowledge and consisting of slots that can accept the values of specific attributes and from which inferences can be drawn by appropriate procedural attachments. (T) (2) The unit of transmission in some local area networks, including the IBM Token-Ring Network. It includes delimiters, control characters, information, and checking characters. (3) In SDLC, the vehicle for every command, every response, and all information that is transmitted using SDLC procedures. (4) A data structure (data frame) composed of fields meeting the field specifications of a type of communication protocol. Frames are used to

control data transfer across a data link. (5) In SDLC, a sequence of bits delimited by an opening and closing flag. In X.25 packet switching data networks, frames are composed of 8-bit byte sequences delimited by beginning and ending flags; the frames in X.25 control various functions, data transfer, and transmission checking.

FTP. File Transfer Protocol.

full-duplex (FDX). Synonym for *duplex*.

G

gateway. (1) A functional unit that interconnects two computer networks with different network architectures. A gateway connects networks or systems of different architectures. A bridge interconnects networks or systems with the same or similar architectures. (T) (2) The combination of machines and programs that provide address translation, name translation, and system services control point (SSCP) rerouting between independent SNA networks to allow those networks to communicate. A gateway consists of one gateway NCP and at least one gateway VTAM. (3) In the IBM Token-Ring Network, a device and its associated software that connect a local area network to another local area network or a host that uses different logical link protocols. (4) In the AIX operating system, an entity that operates above the link layer and translates, when required, the interface and protocol used by one network into those used by another distinct network. (5) In TCP/IP, synonym for *router*.. (6) A station in a local area network through which a connection to a host system or a separate network is established.

generic unbind. Synonym for *session deactivation request*.

GMT. Greenwich mean time.

graphical user interface (GUI). (1) A type of computer interface consisting of a visual metaphor of a real-world scene, often of a desktop. Within that scene are icons, representing

actual objects, that the user can access and manipulate with a pointing device. (2) Contrast with *command line interface (CLI)*.

H

half-duplex (HD, HDX). In data communication, pertaining to transmission in only one direction at a time. Contrast with *duplex*.

hard disk. A rigid-magnetic disk such as the internal disks used in the system units of personal computers and in external hard disk drives (also known as fixed disks).

HD. Half-duplex.

header. (1) System-defined control information that precedes user data. (2) The portion of a message that contains control information for the message such as one or more destination fields, name of the originating station, input sequence number, character string indicating the type of message, and priority level for the message.

high-level language application programming interface (HLLAPI). (1) A software product that supports interaction between a host program and an application program running on a personal computer in terminal emulation (usually 3270 terminal emulation). (2) A programming interface that usually operates in conjunction with an emulator, such as 3270 emulation, and allows interaction using 3270 data stream between a host and a remote application program.

High-Performance Routing (HPR). An addition to APPN that enhances data-routing performance and session reliability..

High-Performance Routing (HPR) node. An APPN end node or network node that includes High-Performance Routing support.

host. (1) In the Internet suite of protocols, an end system. The end system can be any workstation; it does not have to be a mainframe. (2) See *host processor*.

host code page. The character code page used by the host system to which a gateway connects.

host ID. In the Internet suite of protocols, that part of the IP address that defines the host system on the network. The length of the host ID depends on the type of network or network class (A, B, or C).

host print. A printer session on a local personal computer directed by the host system.

host processor. (1) A processor that controls all or part of a user application network. (T) (2) In a network, the processing unit in which the data communication access method resides.

host session. A logical connection that enables a personal computer to communicate with a host system. A session can be identified by LU address, LT number, or session ID. See *DOS session*. See also *logical terminal*.

HPR. High-Performance Routing..

I

IBM Disk Operating System (DOS). A disk operating system based on MS-DOS that operates with all IBM personal computers.

icon. A graphical representation of an object, consisting of an image, image background, and a label.

ID. (1) Identifier. (2) Identification.

IEEE. Institute of Electrical and Electronics Engineers.

IEEE 802.2. An IEEE standard describing how data is formatted into frames for LAN transmission. See also *Type 1 frame* and *Type 2 frame*.

inbound. In communications, data that is received from the network.

installation. (1) In Personal Communications, the process of loading microcode from the Personal Communications diskettes. (2) In system

development, preparing and placing a functional unit in position for use. (T) (3) A particular computing system, including the work it does and the people who manage it, operate it, apply it to problems, service it, and use the results it produces.

interface. (1) A shared boundary between two functional units, defined by functional characteristics, signal characteristics, or other characteristics, as appropriate. The concept includes the specification of the connection of two devices having different functions. (T) (2) Hardware, software, or both, that links systems, programs, or devices.

intermediate node. A node that is at the end of more than one branch. (T)

internet. A collection of networks interconnected by a set of routers that allow them to function as a single, large network. See also *Internet*.

Internet. The internet administered by the Internet Architecture Board (IAB), consisting of large national backbone networks and many regional and campus networks all over the world. The Internet uses the Internet suite of protocols.

Internet Protocol (IP). A connectionless protocol that routes data through a network or interconnected networks. IP acts as an intermediary between the higher protocol layers and the physical network. However, this protocol does not provide error recovery and flow control and does not guarantee the reliability of the physical network.

Internetwork Packet Exchange (IPX). The network protocol used to connect Novell's servers, or any workstation or router that implements IPX, with other workstations. Although similar to the Internet Protocol (IP), IPX uses different packet formats and terminology.

I/O. Input/output.

IP. Internet Protocol..

IPX. Internetwork Packet Exchange.

ISO. International Organization for Standardization.

K

kanji. A Japanese ideographic alphabet. In kanji, each character is represented by 2 bytes. See also *hiragana* and *katakana*.

katakana. One of the two common Japanese phonetic alphabets (the other is hiragana). In katakana, each character is represented by 1 byte. Katakana is primarily used to write foreign words phonetically. See also *kanji*.

kbps. Kilobits per second.

kernel. The part of an operating system that performs basic functions such as allocating hardware resources.

keyboard template. An overlay placed on a keyboard to explain the function of each key.

keyword. (1) In programming languages, a lexical unit that, in certain contexts, characterizes some language construct; for example, in some contexts, IF characterizes an if-statement. A keyword normally has the form of an identifier. (I) (2) One of the predefined words of an artificial language. (A) (3) A significant and informative word in a title or document that describes the content of that document.

L

LAN. Local area network.

link. (1) The combination of the link connection (the transmission medium) and two link stations, one at each end of the link connection. A link connection can be shared among multiple links in a multipoint or token-ring configuration. (2) To interconnect items of data or portions of one or more computer programs: for example, the linking of object programs by a linkage editor, linking of data items by pointers. (T) (3) In SNA, synonymous with *data link*.

link-attached. (1) Pertaining to devices that are connected to a controlling unit by a data link. (2) Contrast with *channel-attached*. (3) Synonymous with *remote*.

link connection. (1) The physical equipment providing two-way communication between one link station and one or more other link stations; for example, a telecommunication line and data circuit-terminating equipment (DCE). (2) In SNA, synonymous with *data circuit*.

link connection segment. A portion of the configuration that is located between two resources listed consecutively in the service point command service (SPCS) query link configuration request list.

link protocol. (1) The rules for sending and receiving data at the link level. (2) Synonymous with *line control discipline* and *line discipline*.

link station. (1) The hardware and software components within a node representing a connection to an adjacent node over a specific link. For example, if node A is the primary end of a multipoint line that connects to three adjacent nodes, node A will have three link stations representing the connections to the adjacent nodes. (2) In VTAM, a named resource within an APPN or a subarea node that represents the connection to another APPN or subarea node that is attached by an APPN or a subarea link. In the resource hierarchy in a subarea network, the link station is subordinate to the subarea link. (3) See also *adjacent link station (ALS)*.

link status (LS). Information maintained by local and remote modems.

load. (1) To bring all or part of a computer program into memory from auxiliary storage so that the computer can run the program. (2) To place a diskette into a diskette drive.

local. (1) Pertaining to a device accessed directly without use of a telecommunication line. (2) Contrast with *remote*. (3) Synonym for *channel-attached*.

local area network (LAN). (1) A computer network located on a user's premises within a limited geographical area. Communication within a local area network is not subject to external regulations; however, communication across the LAN boundary may be subject to some form of regulation. (T) (2) A network in which a set of devices are connected to one another for communication and that can be connected to a larger network. (3) See also *Ethernet* and *token ring*. (4) Contrast with *metropolitan area network (MAN)* and *wide area network (WAN)*.

local directory database. That set of resources (LUs) in the network known at a particular node. The resources included are all those in the node's domain as well as any cache entries.

local LU. A logical unit not distributed over the LAN, but controlled by a gateway personal computer. This is normally a physical device such as a workstation, printer, or terminal.

Locate. Synonym for *Locate/CD-Initiate*.

Locate/CD-Initiate. (1) An abbreviated term for a message exchanged between APPN nodes that contains one of the following sets of general data stream (GDS) variables:

- A Locate, a Find Resource, and a Cross-Domain Initiate GDS variable used for a network search request
- A Locate, a Found Resource, and a Cross-Domain Initiate GDS variable used for a search reply when a network resource has been located

These message structures correspond to the CP components that perform the search of the distributed network directory and establish the session. The Locate GDS variable contains information used to control the delivery of the search messages in the network. The Find and Found GDS variables contain information used in the directories: origin cache data (control point information) and search arguments (destination LU name), and located resource information, respectively. The Cross-Domain Initiate GDS variable contains endpoint TG vector information

to be used in selecting the route for the session. The length of the Locate/CD-Initiate message is limited to 1024 bytes. (2) Synonymous with *Locate* and *Locate search message*.

Locate search message. Synonym for *Locate/CD-Initiate*.

lock. (1) The means by which integrity of data is ensured by preventing more than one user from accessing or changing the same data or object at the same time. (2) In Communications Manager/2, a password-protection system that can be used to prevent access to some advanced functions. See also *keylock*.

logical link. (1) A pair of link stations, one in each of two adjacent nodes, and their underlying link connection, providing a single link-layer connection between the two nodes. Multiple logical links can be distinguished while they share the use of the same physical media connecting two nodes. Examples are 802.2 logical links used on local area network (LAN) facilities and LAP E logical links on the same point-to-point physical link between two nodes. The term logical link also includes the multiple X.25 logical channels that share the use of the access link from a DTE to an X.25 network. (2) In APPNTAM, the unidirectional representation in a node of a link..

logical record. A set of related data or words considered to be a record from a logical viewpoint. (T)

logical terminal. (1) A destination with a name that is related to one or more physical terminals. (2) The definition of a specific 3270 or 5250 emulation session.

logical unit (LU). A type of network accessible unit that enables users to gain access to network resources and communicate with each other.

low-entry networking (LEN) end node. A LEN node receiving network services from an adjacent APPN network node.

LS. Link status.

LU. Logical unit.

LU-LU session. A logical connection between two logical units (LUs) in an SNA network that typically provides communication between two users.

LUS. Logical unit services.

LU type. The classification of an LU in terms of the specific subset of SNA protocols and options it supports for a given session, namely:

- The mandatory and optional values allowed in the session activation request
- The usage of data stream controls, function management headers (FMHs), request unit parameters, and sense data values
- Presentation services protocols such as those associated with FMH usage

LU types 0, 1, 2, 3, 4, 6.1, 6.2, and 7 are defined.

LU 2. A type of LU for an application program that communicates with a single display workstation in an interactive environment, using the SNA 3270 data stream.

LU 3. A type of LU for an application program that communicates with a single printer, using the SNA 3270 data stream.

LU 6.2. (1) A type of logical unit that supports general communication between programs in a distributed processing environment. LU 6.2 is characterized by (a) a peer relationship between session partners, (b) efficient utilization of a session for multiple transactions, (c) comprehensive end-to-end error processing, and (d) a generic application programming interface (API) consisting of structured verbs that are mapped into a product implementation. (2) A type of LU that supports sessions between two applications in a distributed data processing environment using the SNA general data stream, which is a structured-field data stream, or a user-defined data stream.

LU 6.2 verb. A syntactical unit in the LU 6.2 application programming interface representing an operation.

M

management services (MS). (1) One of the types of network services in control points (CPs) and physical units (PUs). Management services are the services provided to assist in the management of SNA networks, such as problem management, performance and accounting management, configuration management, and change management. (2) Services that assist in the management of systems and networks in areas such as problem management, performance management, business management, operations management, configuration management, and change management.

management services focal point (MSFP). For any given management services discipline (for example, problem determination or response time monitoring), the control point that is responsible for that type of network management data for a sphere of control. This responsibility may include collecting, storing, or displaying the data, or all of these. (For example, a problem determination focal point is a control point that collects, and that may store or display, problem determination data.)

mapping. The process of converting data that is transmitted in one format by the sender into the data format that can be accepted by the receiver.

MB. Megabyte.

megabyte (MB). (1) For processor storage, real and virtual storage, and channel volume, 220 or 1 048 576 bytes. (2) For disk storage capacity and communications volume, 1 000 000 bytes.

memory. All of the addressable storage space in a processing unit and other internal storages that is used to execute instructions. (T)

menu bar. The area near the top of a window, below the title bar and above the rest of the window, that contains choices that provide access to other menus.

migration. The installation of a new version or release of a program to replace an earlier version or release.

mode. See *mode name*.

modem (modulator/demodulator). (1) A functional unit that modulates and demodulates signals. One of the functions of a modem is to enable digital data to be transmitted over analog transmission facilities. (T) (A) (2) A device that converts digital data from a computer to an analog signal that can be transmitted on a telecommunication line, and converts the analog signal received to data for the computer.

mode name. The name 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 within the transport network.

module. A program unit that is discrete and identifiable with respect to compiling, combining with other units, and loading; for example, the input to or output from an assembler, compiler, linkage editor, or executive routine. (A)

monitor. (1) A device that observes and records selected activities within a data processing system for analysis. Possible uses are to indicate significant departure from the norm, or to determine levels of utilization of particular functional units. (T) (2) Software or hardware that observes, supervises, controls, or verifies operations of a system. (A) (3) The function required to initiate the transmission of a token on the ring and to provide soft-error recovery in case of lost tokens, circulating frames, or other difficulties. The capability is present in all ring stations. (4) In the NetView Graphic Monitor Facility, to open a view that can receive status changes from the NetView program. Problem determination and correction can be performed directly from the view. Contrast with *browse*.

MS. Management services.

MSFP. Management services focal point.

Multiple Virtual Storage (MVS). See *MVS*.

MVS. Multiple Virtual Storage. Implies MVS/390, MVS/XA, and MVS/ESA.

N

national language support (NLS). The modification or conversion of a United States English product to conform to the requirements of another language or country. This can include the enabling or retrofitting of a product and the translation of nomenclature, machine-readable information (MRI), or documentation of a product. NLS is also known as "internationalization."

negative response (NR). In SNA, a response indicating that a request did not arrive successfully or was not processed successfully by the receiver. Contrast with *positive response*.

NetBIOS. (1) Network Basic Input/Output System. A standard interface to networks, IBM personal computers (PCs), and compatible PCs, that is used on LANs to provide message, print-server, and file-server functions. Application programs that use NetBIOS do not need to handle the details of LAN data link control (DLC) protocols. (2) See also *BIOS*.

network. (1) An arrangement of nodes and connecting branches. (T) (2) A configuration of data processing devices and software connected for information interchange. (3) A group of nodes and the links interconnecting them.

network directory database. Synonym for *distributed directory database*.

network management. The process of planning, organizing, and controlling a communication-oriented data processing or information system.

network management vector transport (NMVT). A management services request/response unit (RU) that flows over an

active session between physical unit management services and control point management services (SSCP-PU session).

network node (NN). See *Advanced Peer-to-Peer Networking (APPN) network node*.

network node server. An APPN network node that provides network services for its local LUs and client end nodes.

NLS. National language support.

NMVT. Network management vector transport.

NN. Network node.

node. (1) In a network, a point at which one or more functional units connect channels or data circuits. (I) (2) Any device, attached to a network, that transmits and receives data. (3) An endpoint of a link or a junction common to two or more links in a network. Nodes can be processors, communication controllers, cluster controllers, or terminals. Nodes can vary in routing and other functional capabilities.

O

object. (1) In object-oriented design or programming, an abstraction consisting of data and the operations associated with that data. See also *class*. (2) An item that a user can manipulate as a single unit to perform a task. An object can appear as text, an icon, or both.

Off. A choice that appears in the cascaded menu from the Refresh choice. It sets the refresh function to off.

offline. (1) Pertaining to the operation of a functional unit that takes place either independently of, or in parallel with, the main operation of a computer. (T) (2) Neither controlled by, nor communicating with, a computer. Contrast with *online*.

OIA. Operator information area.

operating system (OS). Software that controls the execution of programs and that may provide

services such as resource allocation, scheduling, input/output control, and data management. Although operating systems are predominantly software, partial hardware implementations are possible. (T)

operator. (1) In a language statement, the lexical entity that indicates the action to be performed on operands. See also *definition statement*. (2) A person or program responsible for managing activities controlled by a given piece of software such as MVS, the NetView program, or IMS. (3) A person who operates a device. (4) A person who keeps a system running. (5) See also *autotask*, *logged-on operator*, *network operator*, and *operator station task*.

operator information area (OIA). The area near the bottom of the display area where terminal or system status information is displayed.

operator station task (OST). The NetView task that establishes and maintains the online session with the network operator. There is one operator station task for each network operator who logs on to the NetView program. See *NetView-NetView task*.

origin. An external logical unit (LU) or application program from which a message or other data originates. See also *destination*.

OS. Operating system.

P

padding. (1) A technique by which a receiving component controls the rate of transmission of a sending component to prevent overrun or congestion. (2) See *receive pacing*, *send pacing*, *session-level pacing*, and *virtual route (VR) pacing*. (3) See also *flow control*.

pacing group. Synonym for *pacing window*.

pacing window. (1) The path information units (PIUs) that can be transmitted on a virtual route before a virtual-route pacing response is received, indicating that the virtual route receiver is ready to receive more PIUs on the route. (2)

The requests that can be transmitted on the normal flow in one direction on a session before a session-level pacing response is received, indicating that the receiver is ready to accept the next group of requests. (3) Synonymous with *pacing group*.

packet. (1) In data communication, a sequence of binary digits, including data and control signals, that is transmitted and switched as a composite whole. The data, control signals, and, possibly, error control information are arranged in a specific format. (I) (2) A discrete unit of information including addressing and sequence information that can be sent interleaved with other packets of the same and other transmission sequences. Data sent by packet switching protocols, such as the X.25 protocol, do not always arrive in the order sent or even by the same routing on a PSDN.

parallel sessions. Two or more concurrently active sessions between the same two network accessible units (NAUs) using different pairs of network addresses or local-form session identifiers. Each session can have independent session parameters.

page. (1) In a virtual storage system, a fixed-length block that has a virtual address and is transferred as a unit between real storage and auxiliary storage. (I) (A) (2) The information displayed at the same time on the screen of a display device. (3) To replace the information displayed on the screen with prior or subsequent information from the same file.

parameter. (1) A variable that is given a constant value for a specified application and that may denote the application. (I) (A) (2) In Basic CUA architecture, a variable used in conjunction with a command to affect its result. (3) An item in a menu for which the user specifies a value or for which the system provides a value when the menu is interpreted. (4) Data passed to a program or procedure by a user or another program, namely as an operand in a language statement, as an item in a menu, or as a shared data structure.

password. A unique string of characters known to a computer system and to a user, who must specify the character string to gain access to a system and to the information stored within it.

path. (1) In a network, any route between any two nodes. A path may include more than one branch. (T) (2) The series of transport network components (path control and data link control) that are traversed by the information exchanged between two network accessible units. See also *explicit route (ER)*, *route extension (REX)*, and *virtual route (VR)*.

path control (PC). The function that routes message units between network accessible units in the network and provides the paths between them. It converts the basic information units (BIUs) from transmission control (possibly segmenting them) into path information units (PIUs) and exchanges basic transmission units containing one or more PIUs with data link control. Path control differs by node type: some nodes (APPN nodes, for example) use locally generated session identifiers for routing, and others (subarea nodes) use network addresses for routing.

path control network. Synonym for *transport network*.

peripheral LU. In SNA, a logical unit in a peripheral node. Contrast with *subarea LU*.

peripheral node. A node that uses local addresses for routing and therefore is not affected by changes in network addresses. A peripheral node requires boundary-function assistance from an adjacent subarea node. A peripheral node can be a type 1, 2.0, or 2.1 node connected to a subarea boundary node.

peripheral PU. In SNA, a physical unit in a peripheral node. Contrast with *subarea PU*.

physical circuit. A circuit established without multiplexing. See also *data circuit*. Contrast with *virtual circuit*.

physical connection. (1) A connection that establishes an electrical circuit. (2) A

point-to-point or multipoint connection. (3)
Synonymous with *connection*.

physical unit (PU). (1) The component that manages and monitors the resources (such as attached links and adjacent link stations) associated with a node, as requested by an SSCP via an SSCP-PU session. An SSCP activates a session with the physical unit in order to indirectly manage, through the PU, resources of the node such as attached links. This term applies to type 2.0, type 4, and type 5 nodes only. (2) See also *peripheral PU* and *subarea PU*.

physical unit (PU) services. In SNA, the components within a physical unit (PU) that provide configuration services and maintenance services for SSCP-PU sessions.

port. (1) An access point for data entry or exit. (2) A connector on a device to which cables for other devices such as display stations and printers are attached. (3) The representation of a physical connection to the link hardware. A port is sometimes referred to as an adapter; however, there can be more than one port on an adapter. There may be one or more ports controlled by a single DLC process. (4) In the Internet suite of protocols, a 16-bit number used to communicate between TCP or the User Datagram Protocol (UDP) and a higher-level protocol or application. Some protocols, such as File Transfer Protocol (FTP) and Simple Mail Transfer Protocol (SMTP), use the same well-known port number in all TCP/IP implementations. (5) An abstraction used by transport protocols to distinguish among multiple destinations within a host machine. (6) Synonymous with *socket*.

positive response. In SNA, a response indicating that a request was received and processed. Contrast with *negative response*.

primitive. Synonym for *service primitive*. (T)

problem determination. The process of determining the source of a problem; for example, a program component, machine failure, telecommunication facilities, user or

contractor-installed programs or equipment, environmental failure such as a power loss, or user error.

procedure. (1) In a programming language, a block, with or without formal parameters, whose execution is invoked by means of a procedure call. (I) (2) The description of the course of action taken for the solution of a problem. (A)

product-set identification (PSID). (1) In SNA, a technique for identifying the hardware and software products that implement a network component. (2) A management services common subvector that transports the information described in definition (1).

profile. Data that describes the significant characteristics of a user, a group of users, or one or more computer resources.

program temporary fix (PTF). A temporary solution or bypass of a problem diagnosed by IBM in a current unaltered release of the program.

protocol. (1) A set of semantic and syntactic rules that determine the behavior of functional units in achieving communication. (I) (2) In Open Systems Interconnection architecture, a set of semantic and syntactic rules that determine the behavior of entities in the same layer in performing communication functions. (T) (3) In SNA, the meanings of, and the sequencing rules for, requests and responses used for managing the network, transferring data, and synchronizing the states of network components. Synonymous with *line control discipline* and *line discipline*. See *bracket protocol* and *link protocol*.

PTF. Program temporary fix.

PU. Physical unit.

R

radio button. A circle with text beside it. Radio buttons are combined to show a user a fixed set

of choices from which the user can select one. The circle becomes partially filled when a choice is selected.

Rapid Transport Protocol (RTP). A connection-oriented, full-duplex transport protocol for carrying session traffic over High-Performance Routing (HPR) routes. See also *automatic network routing (ANR)* and *Rapid Transport Protocol (RTP) connection*.

Rapid Transport Protocol (RTP) connection. A connection between two High-Performance Routing (HPR) nodes that may traverse one or more intermediate HPR nodes and links. The connection endpoints provide error recovery and adaptive rate-based flow control for the connection traffic, and nondisruptive switching of the underlying physical path in the case of route outage. The intermediate HPR nodes minimize their routing overhead using automatic network routing (ANR) protocols, which rely on header information to permit efficient source routing and prioritized transmission along the RTP connection.

read-only memory (ROM). Memory in which stored data cannot be modified by the user except under special conditions.

received line signal detector (RLSD). In the EIA 232 standard, a signal that indicates to the data terminal equipment (DTE) that it is receiving a signal from the remote data circuit-terminating equipment (DCE). Synonymous with *carrier detect* and *data carrier detect (DCD)*.

receive pacing. In SNA, the pacing of message units that a component is receiving. Contrast with *send pacing*.

release. (1) A distribution of a new product or new function and APAR fixes for an existing product. Normally, programming support for the prior release is discontinued after some specified period of time following availability of a new release. The first version of a product is announced as Release 1, Modification Level 0. (2) In VTAM, to relinquish control of resources

(communication controllers or physical units). See also *resource takeover*. Contrast with *acquire*.

remote. (1) Pertaining to a system, program, or device that is accessed through a telecommunication line. (2) Synonym for *link-attached*. (3) Contrast with *local*.

requester. A computer that accesses shared network resources through a server. Synonym for *client*.

resource. Any facility of a computing system or operating system required by a job or task, and including main storage, input/output devices, the processing unit, data sets, and control or processing programs.

resource registration. The process of identifying names of resources, such as LUs, to a network node server or a central directory server.

resource takeover. In VTAM, an action initiated by a network operator to transfer control of resources from one domain to another without breaking the connections or disrupting existing LU-LU sessions on the connection. See also *acquire* and *release*.

resource types. In the NetView program, a concept to describe the organization of panels. Resource types are defined as central processing unit, channel, control unit, and I/O device for one category; and communication controller, adapter, link, cluster controller, and terminal for another category. Resource types are combined with data types and display types to describe display organization. See also *data types* and *display types*.

response. (1) In data communication, a reply represented in the control field of a response frame. It advises the primary or combined station of the action taken by the secondary or other combined station to one or more commands. (2) See also *command*.

return code. (1) A code used to influence the execution of succeeding instructions. (A) (2) A

value returned to a program to indicate the results of an operation requested by that program.

REX. Route extension.

ring. See *ring network*.

ring network. A network configuration in which devices are connected by unidirectional transmission links to form a closed path.

ROM. Read-only memory. (A)

route. (1) An ordered sequence of nodes and transmission groups (TGs) that represent a path from an origin node to a destination node traversed by the traffic exchanged between them. (2) The path that network traffic uses to get from source to destination.

route extension (REX). In SNA, the path control network components, including a peripheral link, that make up the portion of a path between a subarea node and a network addressable unit (NAU) in an adjacent peripheral node. See also *explicit route (ER)*, *path*, and *virtual route (VR)*.

router. (1) A computer that determines the path of network traffic flow. The path selection is made from several paths based on information obtained from specific protocols, algorithms that attempt to identify the shortest or best path, and other criteria such as metrics or protocol-specific destination addresses. (2) An attaching device that connects two LAN segments, which use similar or different architectures, at the reference model network layer. (3) In OSI terminology, a function that determines a path by which an entity can be reached. (4) In TCP/IP, synonymous with *gateway*.. (5) Contrast with *bridge*.

RTP. Rapid Transport Protocol..

RTP connection. See *Rapid Transport Protocol (RTP) connection*..

RU chain. In SNA, a set of related request/response units (RUs) that are consecutively transmitted on a particular normal

or expedited data flow. The request RU chain is the unit of recovery: if one of the RUs in the chain cannot be processed, the entire chain is discarded. Each RU belongs to only one chain, which has a beginning and an end indicated by means of control bits in request/response headers within the RU chain. Each RU can be designated as first-in-chain (FIC), last-in-chain (LIC), middle-in-chain (MIC), or only-in-chain (OIC). Response units and expedited-flow request units are always sent as only-in-chain.

S

SAP. (1) Service access point. (2) Service Advertising Protocol.

SBCS. Single-byte character set.

scroll. To move a display image vertically or horizontally to view data that otherwise cannot be observed within the boundaries of the display screen.

scroll bar. A window component that shows a user that more information is available in a particular direction and can be scrolled into view. Scroll bars can be either horizontal or vertical.

SCS. SNA character string.

SDLC. Synchronous Data Link Control.

segment. In Internet communications, the unit of transfer between TCP functions in different machines. Each segment contains control and data fields; the current byte-stream position and actual data bytes are identified along with a checksum to validate received data.

send pacing. In SNA, the pacing of message units that a component is sending. Contrast with *receive pacing*.

serial. (1) Pertaining to a process in which all events occur one after the other; for example, serial transmission of the bits of a character according to V24 CCITT protocol. (T) (2) Pertaining to the sequential or consecutive occurrence of two or more related activities in a

single device or channel. (A) (3) Pertaining to the sequential processing of the individual parts of a whole, such as the bits of a character or the characters of a word, using the same facilities for successive parts. (A) (4) Contrast with *parallel*.

server. (1) A functional unit that provides shared services to workstations over a network; for example, a file server, a print server, a mail server. (T) (2) In a network, a data station that provides facilities to other stations; for example, a file server, a print server, a mail server. (A)

Server-Requester Programming Interface (SRPI). An IBM application programming interface (API) used by requester and server programs to communicate with the personal computer or host routers.

service access point (SAP). (1) In Open Systems Interconnection (OSI) architecture, the point at which the services of a layer are provided by an entity of that layer to an entity of the next higher layer. (T) (2) A logical point made available by an adapter where information can be received and transmitted. A single service access point can have many links terminating in it. (3) The gateway address of the controller. A SAP provides a point to link the controller to the host system.

Service Advertising Protocol (SAP). In Internetwork Packet Exchange (IPX), a protocol that provides the following:

- A mechanism that allows IPX servers on an internet to advertise their services by name and type. Servers using this protocol have their name, service type, and IP address recorded in all file servers running NetWare.
- A mechanism that allows a workstation to broadcast a query to discover the identities of all servers of all types, all servers of a specific type, or the nearest server of a specific type.
- A mechanism that allows a workstation to query any file server running NetWare to discover the names and addresses of all servers of a specific type.

service point (SP). An entry point that supports applications that provide network management for resources not under the direct control of itself as an entry point. Each resource is either under the direct control of another entry point or not under the direct control of any entry point. A service point accessing these resources is not required to use SNA sessions (unlike a focal point). A service point is needed when entry point support is not yet available for some network management function.

Service Point Application (SPA) Router. In Communications Server, a program that receives commands issued from the NetView program and sends the commands to an application program to be processed on an OS/2 workstation.

session. (1) In network architecture, for the purpose of data communication between functional units, all the activities which take place during the establishment, maintenance, and release of the connection. (T) (2) A logical connection between two network accessible units (NAUs) that can be activated, tailored to provide various protocols, and deactivated, as requested. Each session is uniquely identified in a transmission header (TH) accompanying any transmissions exchanged during the session. (3) A logical connection between a server and a requester that was initiated by a successful request for a shared resource. See also *host session* and *DOS session*.

session activation request. In SNA, a request that activates a session between two network accessible units (NAUs) and specifies session parameters that control various protocols during session activity; for example, BIND and ACTPU. Contrast with *session deactivation request*.

session control (SC). In SNA, either of the following:

- One of the components of transmission control. Session control is used to purge data flowing in a session after an unrecoverable error occurs, to resynchronize the data flow after such an error, and to perform cryptographic verification.

- A request unit (RU) category used for requests and responses exchanged between the session control components of a session and for session activation and deactivation requests and responses.

session data. Data about a session, collected by the NetView program, that consists of session awareness data, session trace data, and session response time data.

session deactivation request. In SNA, a request that deactivates a session between two network accessible units (NAUs); for example, UNBIND and DACTPU. Synonymous with *generic unbind*. Contrast with *session activation request*.

session ID. An alphabetic ID (a through h) assigned by Personal Communications to each session or screen. This applies to all types of host sessions and is used in file transfers. See also *short name*.

session-level pacing. (1) A flow control technique that permits a receiving half-session or session connector to control the data transfer rate (the rate at which it receives request units) on the normal flow. It is used to prevent overloading a receiver with unprocessed requests when the sender can generate requests faster than the receiver can process them. (2) See also *adaptive session-level pacing*, *fixed session-level pacing*, and *virtual route (VR) pacing*.

session parameters. In SNA, the parameters that specify or constrain the protocols (such as bracket protocol and pacing) for a session between two network accessible units. See also *logon mode*.

session services (SS). One of the types of network services in the control point (CP) and in the logical unit (LU). These services provide facilities for an LU or a network operator to request that a control point (an ENCP, NNCP, or SSCP) assist with initiating or terminating sessions between logical units. Assistance with session termination is needed only by SSCP-dependent LUs. See *configuration services*, *maintenance services*, and *management services*.

single-byte character set (SBCS). A character set in which each character is represented by a one-byte code. Contrast with *double-byte character set (DBCS)*.

SNA. Systems Network Architecture.

SNA character string (SCS). In SNA, a character string composed of EBCDIC controls, optionally intermixed with end-user data, that is carried within a request/response unit.

SNA network. The part of a user-application network that conforms to the formats and protocols of Systems Network Architecture. It enables reliable transfer of data among users and provides protocols for controlling the resources of various network configurations. The SNA network consists of network accessible units (NAUs), boundary function, gateway function, and intermediate session routing function components; and the transport network.

SO. The shift-out character. (I) (A)

socket. An endpoint for communication between processes or application programs.

SP. Service point.

SS. Session services.

SSCP. System services control point.

SSCP-dependent LU. An LU that requires assistance from a system services control point (SSCP) in order to initiate an LU-LU session. It requires an SSCP-LU session.

SSCP-LU session. In SNA, a session between a system services control point (SSCP) and a logical unit (LU). The session enables the LU to request the SSCP to help initiate LU-LU sessions.

stage. A program that processes messages in a NetView pipeline. Stages send messages to each other serially.

static. (1) In programming languages, pertaining to properties that can be established before execution of a program; for example, the length

of a fixed length variable is static. (I) (2) Pertaining to an operation that occurs at a predetermined or fixed time. (3) Contrast with *dynamic*.

stream. (1) To send data from one device to another. (2) See *data stream*.

subarea. A portion of the SNA network consisting of a subarea node, attached peripheral nodes, and associated resources. Within a subarea node, all network accessible units (NAUs), links, and adjacent link stations (in attached peripheral or subarea nodes) that are addressable within the subarea share a common subarea address and have distinct element addresses.

subarea LU. In SNA, a logical unit in a subarea node. Contrast with *peripheral LU*.

subarea node (SN). A node that uses network addresses for routing and maintains routing tables that reflect the configuration of the network. Subarea nodes can provide gateway function to connect multiple subarea networks, intermediate routing function, and boundary function support for peripheral nodes. Type 4 and type 5 nodes can be subarea nodes.

subarea PU. In SNA, a physical unit in a subarea node. Contrast with *peripheral PU*.

subdirectory. A directory contained within another directory in a file system hierarchy.

subsystem. A secondary or subordinate system, usually capable of operating independently of, or asynchronously with, a controlling system. (T)

subsystem management. In Communications Manager/2, a group of advanced functions for diagnosis and problem resolution. These functions are typically used by system administrators and application programmers.

synchronization point. Synonym for *sync point*.

synchronous. (1) Pertaining to two or more processes that depend upon the occurrence of specific events such as common timing

signals. (T) (2) Occurring with a regular or predictable time relationship.

Synchronous Data Link Control (SDLC). A discipline conforming to subsets of the Advanced Data Communication Control Procedures (ADCCP) of the American National Standards Institute (ANSI) and High-level Data Link Control (HDLC) of the International Organization for Standardization, for managing synchronous, code-transparent, serial-by-bit information transfer over a link connection. Transmission exchanges may be duplex or half-duplex over switched or nonswitched links. The configuration of the link connection may be point-to-point, multipoint, or loop. (I)

sync point. An intermediate or end point during processing of a transaction at which an update or modification to one or more of the transaction's protected resources is logically complete and error free. Synonymous with *synchronization point*.

system. In data processing, a collection of people, machines, and methods organized to accomplish a set of specific functions. (I) (A)

system services control point (SSCP). A component within a subarea network for managing the configuration, coordinating network operator and problem determination requests, and providing directory services and other session services for users of the network. Multiple SSCPs, cooperating as peers with one another, can divide the network into domains of control, with each SSCP having a hierarchical control relationship to the physical units and logical units within its own domain.

system services control point (SSCP) domain. The system services control point, the physical units (PUs), the logical units (LUs), the links, the link stations, and all the resources that the SSCP has the ability to control by means of activation and deactivation requests.

Systems Network Architecture (SNA). The description of the logical structure, formats, protocols, and operational sequences for

transmitting information units through, and controlling the configuration and operation of, networks. The layered structure of SNA allows the ultimate origins and destinations of information, that is, the users, to be independent of and unaffected by the specific SNA network services and facilities used for information exchange.

T

TCP. Transmission Control Protocol..

TCP/IP. Transmission Control Protocol/Internet Protocol.

template. See *keyboard template*.

token. (1) In a local area network, the symbol of authority passed successively from one data station to another to indicate the station temporarily in control of the transmission medium. Each data station has an opportunity to acquire and use the token to control the medium. A token is a particular message or bit pattern that signifies permission to transmit. (T) (2) In LANs, a sequence of bits passed from one device to another along the transmission medium. When the token has data appended to it, it becomes a frame.

token ring. (1) According to IEEE 802.5, network technology that controls media access by passing a token (special packet or frame) between media-attached stations. (2) A FDDI or IEEE 802.5 network with a ring topology that passes tokens from one attaching ring station (node) to another. (3) See also *local area network (LAN)*.

transaction program (TP). A program that processes transactions in an SNA network. There are two kinds of transaction programs: application transaction programs and service transaction programs. See also *conversation*.

translation table. A table used to replace one or more characters with alternative characters; for example, to translate characters representing a virtual address to those representing a real

address, characters representing an event to those representing a procedure call, characters of a national character set to those of another national language, or characters representing a relocated address to those representing an absolute address.

Transmission Control Protocol (TCP). A communications protocol used in the Internet and in any network that follows the U.S. Department of Defense standards for internetwork protocol. TCP provides a reliable host-to-host protocol between hosts in packet-switched communications networks and in interconnected systems of such networks. It uses the Internet Protocol (IP) as the underlying protocol..

Transmission Control Protocol/Internet Protocol (TCP/IP). A set of communications protocols that support peer-to-peer connectivity functions for both local and wide area networks.

U

UNBIND. In SNA, a request to deactivate a session between two logical units (LUs). See also *session deactivation request*. Contrast with *BIND*.

upstream. In the direction of data flow from the user to the host. Contrast with *downstream*.

user. (1) Any person or any thing that may issue or receive commands and messages to or from the information processing system. (T) (2) Anyone who requires the services of a computing system.

V

verb. See *LU 6.2 verb*.

version. A separately licensed program that usually has significant new code or new functions.

VGA. Video graphics adapter.

video graphics adapter (VGA). A computer adapter that provides high-resolution graphics and a total of 256 colors. See also *enhanced graphics adapter (EGA)*.

virtual circuit. (1) In packet switching, the facilities provided by a network that give the appearance to the user of an actual connection. (T) See also *data circuit*. Contrast with *physical circuit*. (2) A logical connection established between two DTEs.

virtual route (VR). (1) In SNA, either (a) a logical connection between two subarea nodes that is physically realized as a particular explicit route or (b) a logical connection that is contained wholly within a subarea node for intranode sessions. A virtual route between distinct subarea nodes imposes a transmission priority on the underlying explicit route, provides flow control through virtual route pacing, and provides data integrity through sequence numbering of path information units (PIUs). (2) Contrast with *explicit route (ER)*. See also *path* and *route extension (REX)*.

Virtual Telecommunications Access Method (VTAM). An IBM licensed program that controls communication and the flow of data in an SNA network. It provides single-domain, multiple-domain, and interconnected network capability.

VR. Virtual route.

VTAM. (1) Virtual Telecommunications Access Method. (2) Synonymous with *ACF/VTAM*.

V.25. In data communication, a specification of the CCITT that defines the automatic answering equipment and parallel automatic calling equipment on the General Switched Telephone Network, including procedures for disabling of echo controlled devices for both manually and automatically established calls.

W

WAN. Wide area network.

weight. For route selection purposes, the degree to which resources (such as nodes and transmission groups) meet the criteria specified by a particular class of service. In APPN route selection, routes of minimum weight are chosen..

wide area network (WAN). (1) A network that provides communication services to a geographic area larger than that served by a local area network or a metropolitan area network, and that may use or provide public communication facilities. (T) (2) A data communication network designed to serve an area of hundreds or thousands of miles; for example, public and private packet-switching networks, and national telephone networks. (3) Contrast with *local area network (LAN)* and *metropolitan area network (MAN)*.

WinSock application programming interface (API). A socket-style transport interface developed for the Windows family of operating systems.

Index

Numerics

- 3174 Controller
 - Communications Server host parameters 152
 - VTAM PU host parameters 153
- 802.2 35
- 9370
 - Communications Server host parameters 152
 - SDLC host parameters 162

A

- access node
 - SNA over TCP/IP 23
 - Sockets over SNA 23
- administration of SNA networks 10
- administrative tasks
 - setting up the IBMCSADMIN account 135
- Advanced Peer-to-Peer Networking 13
- Advanced Program-to-Program Communications 28
- AnyNet
 - AnyNet examples 186
 - defining unique CP names and connection network names 181
 - mapping SNA resources to IP address 179
 - routing SNA sessions over AnyNet SNA over TCP/IP 185
 - running APPC or CPI-C applications over TCP/IP 21
 - used to connect SNA applications on different platforms 21
- AnyNet configurations 20
- APPC
 - overview 28
 - performance, enhanced 13
 - VTAM host parameters 161
 - X.25 host parameters 170
- APPN
 - description 13
 - functions 13
 - overview 13
 - replacing the default 128

- AS/400
 - host controller (Communications Server) host parameters 176
 - host controller host parameters 172
 - host device host parameters 174
 - host line (Communications Server) host parameters 175
 - host line host parameters 172
 - twinaxial host parameters 176
 - X.25 PVC host parameters 177
- Automatic Network Routing (ANR) 13
- automatically starting Communications Server 136

B

- bibliography 147

C

- CD-ROM contents for Communications Server 37
- Common Programming Interface for Communications 28
- communications protocols 9
- Communications Server 10
 - administration of SNA networks 10
 - application programming interfaces 9
 - emulator products 11
 - flexibility 9
 - introducing 9
 - protecting your investment 11
 - software requirements 35
 - using 127
- Communications Server CD-ROM package 37
- configuration
 - host parameters 149
- configuring Communications Server 43
 - deciding what to configure 43
- connecting remote TCP/IP networks 24
- contacting IBM 145, 139
- CPI-C
 - overview 28

- CPI-C (*continued*)
 - performance, enhanced 13
- CSLIC 136
- CSQUERY 136
- CSSTART 136
- CSSTOP 136

D

- deciding what to configure 43
- default configuration, replacing 128
- dependent LU requester 14
- dependent LU server 14
- diagnostic tools 30
- discovery of service providers 14
- disk space 36
- DLUR
 - description 14
 - host parameters 164
- DLUS 14
- documentation 147

E

- emulator products 11
- entry-level emulator 30
- error log 30
- ES/9000 host connection parameters 162
- Ethernet (VTAM) host parameters 155

G

- gateway
 - SNA over TCP/IP 23
 - Sockets over SNA 23
- gateway support
 - applications on a subarea network 15
 - as a protocol converter 15
 - description 14
 - introduction 10
 - LAN Network Manager 15
 - NetView commands 15
 - summary of features 16
 - table of features 16
 - transmission of NMVTs 15

H

- high-performance routing 13
- host connection parameters 149
- HPR 13

- I**
- IBMCSADMIN 135
- IEEE 802.2 35
- information
 - ordering publications 147
 - printing 147
 - viewing 147
- installation
 - planning 35
 - remote 36
 - SNA client services 42
 - split stack clients 41
- introducing Communications Server 9
- L**
- LAN Network Manager 15
- licensing agreement 204
- local area network (LAN)
 - Communications Manager requirements 35
- log
 - error 30
 - message 30
- log viewer utility 141
- LU pools 15
- LU support 29
- M**
- management services 29
- message
 - viewing 141
- message log 30
- monitoring resources 30
- MPTS, Communications Server requirements for 35
- N**
- NCP (NTRI)
 - Communications Server host parameters 149
- NDIS 35
- network administrator 10
- network management vector transports (NMVTs) 15
- NMVTs 15
- node operations 129
- NPSI host parameters 167
- O**
- ordering publications 147
- P**
- parameters
 - host connection 149
- PD/PSI 30
- planning for
 - installation 35
- problem determination (PD)
 - aids 30
 - environment 139
 - problem area 140
 - problem re-creation 140
 - problem source identification (PSI) 140
 - problem type 140
 - symptom 139
- problem reporting (PR) 143
- programming support 27
- protocol converter 15
- protocols, communication 9
- publications 147
- R**
- Rapid Transport Protocol (RTP) 13
- README file 35
- remote installation 36
- replacing the default configuration 128
- resource monitoring 30
- route discovery function 200
- S**
- SDDLU support host parameters 164
- SDLC host connection
 - 9370 162
 - VTAM/NCP 157
- security
 - conversation 28
 - overview 28
 - session 28
- SNA
 - Advanced Peer-to-Peer Networking 13
 - APPN overview 13
 - Communications Server conformance 28
 - gateways 10, 14
 - LU support 29
 - management services 29
- SNA client services 42
- SNA gateway support
 - description 14
 - introduction 10
 - using for 3270 Emulation over a TCP/IP network 22
- SNA Node Operations 129, 30
- SNA over TCP/IP
 - access node and gateway support
- SNA over TCP/IP (*continued*) 23
- SNA over TCP/IP configurations 20
- sockets over SNA
 - communicating over an SNA network 23
- Sockets over SNA
 - description 23
- sockets over SNA
 - route discovery function 200
 - using sockets over SNA gateway 23
- software requirements
 - Communications Server 35
- startup drive, requirements for 36
- subarea network applications 15
- Systems Network Architecture (SNA) 10
- T**
- technical assistance 145
- Telnet 3270 standard extensions 16
- TN3270E Server 16
- Token-Ring (VTAM) host parameters 150
- Token-Ring host connection
 - 9370 network adapter 152
 - NCP with VTAM 149
 - VTAM switched network 150
- tools
 - diagnostic 30
 - network management 30
- tracing data 142
- trademarks 205
- troubleshooting 139
- twinaxial host parameters 176
- U**
- Uninstalling Communications Server 39
- V**
- VTAM (APPC) host parameters 161
- VTAM/NCP
 - NTRI host parameters 149
 - SDLC host parameters 157
 - X.25 host parameters 168
- VTAM switched network host connection
 - Ethernet 155
 - Token-Ring 150
- W**
- WinSock 193, 194

X

X.25

APPC host connection

parameters 170

AS/400 host parameters 177

NPSI host connection parameters
166

VTAM/NCP host connection

parameters 168

Readers' Comments — We'd Like to Hear from You

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Complete	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Easy to find	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Easy to understand	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Well organized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applicable to your tasks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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
GC31-8424-01



Cut or Fold
Along Line

Fold and Tape

Please do not staple

Fold and Tape



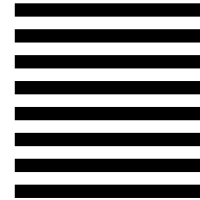
NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

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

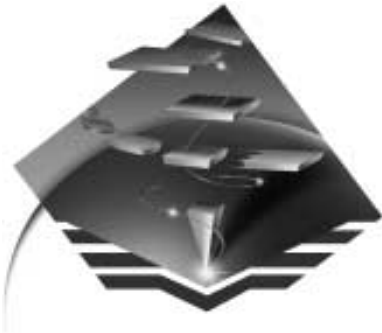
Fold and Tape

GC31-8424-01

Cut or Fold
Along Line



Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.



GC31-8424-01

