



TN3270 DESIGN AND IMPLEMENTATION GUIDE

VOLUME 5 IN THE CISCO IBM INTERNETWORKING DESIGN GUIDE SERIES

Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems Europe s.a.r.l.
Parc Evolic, Batiment L1/L2
16 Avenue du Quebec
Villebon, BP 706
91961 Courtaboeuf Cedex
France
<http://www-europe.cisco.com>
Tel: 33 1 6918 61 00
Fax: 33 1 6928 83 26

**Americas
Headquarters**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-7660
Fax: 408 527-0883

Asia Headquarters

Nihon Cisco Systems K.K.
Fuji Building, 9th Floor
3-2-3 Marunouchi
Chiyoda-ku, Tokyo 100
Japan
<http://www.cisco.com>
Tel: 81 3 5219 6250
Fax: 81 3 5219 6001

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the

Cisco Connection Online Web site at <http://www.cisco.com>.

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China (PRC) • Colombia • Costa Rica • Czech Republic • Denmark • England
• France • Germany • Greece • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The
Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Russia • Saudi Arabia • Scotland • Singapore
South Africa • Spain • Sweden • Switzerland • Taiwan, ROC • Thailand • Turkey • United Arab Emirates • United States • Venezuela

	About this Guide	xiii
	Intended Audience	xiii
	Document Structure	xiv
	Cisco's Data Center Solutions	xiv
	Evolution of the Data Center	xiv
	Credits	xvi
	Cisco Connection Online	xvi
Chapter 1	Introduction to Telnet 3270	1-1
	Why use Telnet 3270?	1-1
	Background	1-2
	What is a 3270 Data Stream?	1-2
	What is SNA 3270?	1-2
	What is TN3270?	1-2
	What is TN3270E?	1-3
	Cisco Product Offerings	1-4
	TN3270 Server on a CIP or CPA	1-4
Chapter 2	TN3270 Server Implementation	2-1
	TN3270 Server on the CIP/CPA	2-1
	Hardware and Software Requirements	2-2
	Planning for Implementation	2-2
	Where to Place the TN3270 Server and How Many Servers You Need	2-3
	Implementing TN3270 Server on a CIP/CPA	2-3
	Defining PUs	2-4
	Defining LUs	2-5
	Addressing LAN Printing Requirements	2-14
	Addressing SNA Routing in Multi-Domain Environments	2-15
	Addressing End User Service Level Requirements	2-18
	Addressing Availability Requirements (Redundancy/Load Balancing)	2-18
	Satisfying Expanding Network Address Requirements	2-20
	TN3270 Configuration	2-21
	TN3270 Server Configuration Modes	2-21
	Configuring the TN3270 Server	2-23
	Monitoring the TN3270 Server	2-30

Chapter 3	TN3270 Client Implementation	3-1
	How TN3270 Clients Work	3-1
	Types of TN3270 Clients	3-2
	TN3270 Client of OC://WebConnect Pro	3-3
	Cisco WebClient	3-6
Chapter 4	Migration Scenarios	4-1
	PU and LU Definitions	4-1
	XCA Major Node	4-2
	LUGROUP Major Node	4-2
	Scenario 1: TN3270 Server with Static LUs	4-5
	Design Considerations	4-5
	Router Configuration	4-6
	Host Configuration	4-9
	Scenario 2: TN3270 Server with Dynamic LUs	4-10
	Design Considerations	4-10
	Router Configuration	4-11
	Host Configuration	4-14
	Scenario 3: TN3270 Server Using LU Nailing	4-16
	Design Considerations	4-16
	Router Configuration	4-16
	Host Configuration	4-19
	Scenario 4: TN3270 Server Using LU Nailing with Static LUs	4-21
	Router Configuration	4-21
	Host Configuration	4-24
	Scenario 5: TN3270 Server Using Nailing for Printer LUs	4-26
	Design Considerations	4-26
	Router Configuration	4-27
	Host Configuration	4-29
	Scenario 6: Using a Remote TN3270 Server	4-30
	Design Considerations	4-30
	Router Configuration	4-31
	Host Configuration	4-34
	Scenario 7: TN3270 Server with LocalDirector	4-35
	Design Considerations	4-35
	LocalDirector Configuration	4-36
	Router Configuration	4-39
	Host Configuration	4-43
	Scenario 8: TN3270 Server Using DistributedDirector	4-44
	Design Considerations	4-45
	DistributedDirector Configuration	4-46

Host Configuration	4-50
Scenario 9: TN3270 Server Using a Direct PU and INCLUD0E	4-51
Design Considerations	4-51
Router Configuration	4-52
Host Configuration	4-54
Scenario 10: TN3270 Server with Session Switching	4-55
Design Considerations	4-55
Router Configuration	4-56
Host Configuration	4-57
Chapter 5 Network Management	5-1
Overview of Network Management Products.	5-1
Workstation-based Network Management Products.	5-2
Mainframe-based Network Management Products	5-3
TN3270 Management Feature Matrix	5-4
Enabling Management of Cisco Routers	5-4
Managing from the Workstation	5-4
Managing from the Mainframe.	5-5
Viewing TN3270 Server Configuration and Statistics	5-6
Managing from the Router	5-6
Managing from the Workstation	5-7
Managing from the Mainframe.	5-16
Monitoring TN3270 Server Availability	5-28
Managing from the Workstation	5-28
Managing from the Mainframe	5-43
ISM	5-43
Diagnosing Problems	5-46
Gathering Information	5-47
Determining the Nature of the Problem	5-47
Determining Which IP Addresses, PUs, and LUs Correspond to the TN3270 Servers	5-47
Diagnosing Configuration Problems.	5-48
Diagnosing Connectivity Problems	5-48
Monitoring TN3270 Response Time	5-51
Managing from the Workstation	5-51
Managing from the Mainframe.	5-58
Monitoring TN3270 Server Performance.	5-59
Managing from the Workstation	5-59
Managing from the Mainframe.	5-60

Appendix A	Glossary	A-1
Appendix B	References	B-1
	Compliant RFCs	B-1
	Cisco Documentation	B-1

Figure i	Sample SNA Network	xiv
Figure ii	Evolution of IBM Networks	xv
Figure 1-1	Diagram of a TN3270 Session	1-3
Figure 2-1	TN3270 Session Overview	2-2
Figure 2-2	Allocation PUs	2-5
Figure 2-3	LU Selection Algorithm	2-13
Figure 2-4	Control of a Printing Environment	2-14
Figure 2-5	How Session Switching Works	2-17
Figure 3-1	Three-tier TN3270 Web Client Solution	3-3
Figure 3-2	Two-tier TN3270 Web Client Solution	3-3
Figure 3-3	OC://WebConnect Pro TN3270 Window	3-4
Figure 3-4	OpenVista Screen Consolidation	3-5
Figure 3-5	Cisco WebClient Window	3-6
Figure 4-1	LUGROUP Major Node Definition	4-2
Figure 4-2	TN3270 Server with Static LUs	4-5
Figure 4-3	Scenario 1: Switched Major Node	4-9
Figure 4-4	TN3270 Server with Dynamic LUs	4-10
Figure 4-5	Scenario 2: Switched Major Node	4-14
Figure 4-6	TN3270 Server Using LU Nailing	4-16
Figure 4-7	Scenario 3: Switched Major Node	4-20
Figure 4-8	TN3270 Server Using LU Nailing with Static LUs	4-21
Figure 4-9	Scenario 4: Switched Major Node	4-24
Figure 4-10	TN3270 Server Using Nailing for Printer LUs	4-26
Figure 4-11	Scenario 5: Switched Major Node	4-29

Figure 4-12	Using a Remote TN3270 Server	4-30
Figure 4-13	Scenario 6: Switched Major Node	4-34
Figure 4-14	TN3270 Server with LocalDirector.	4-35
Figure 4-15	Scenario 7: Switched Major Node	4-43
Figure 4-16	TN3270 Server Using DistributedDirector	4-45
Figure 4-17	Scenario 8: Switched Major Node	4-50
Figure 4-18	TN3270 Server Using a Direct PU and INCLUD0E	4-51
Figure 4-19	Scenario 9: Switched Major Node	4-54
Figure 4-20	TN3270 Server with Session Switching	4-55
Figure 4-21	Scenario 10: XCA Major Node	4-57
Figure 4-22	Scenario 10: Switched Major Node for TN3270 Server.	4-58
Figure 4-23	Scenario 10: LU Group Member.	4-58
Figure 4-24	Switched Major Node for DLUR Links	4-59
Figure 4-25	Scenario 10: XCA Major Node	4-60
Figure 4-26	Scenario 10: Switched Major Node for the VTAM-VTAM CP-CP Session	4-60
Figure 5-1	TN3270 Monitor—Global Statistics	5-9
Figure 5-2	PU List Window	5-11
Figure 5-3	PU Detail Window	5-11
Figure 5-4	LU List Window	5-12
Figure 5-5	LU Detail Window	5-13
Figure 5-6	Events Window	5-16
Figure 5-7	ISM Main Menu	5-17
Figure 5-8	ISM Status Summary Panel.	5-18
Figure 5-9	Cisco Mainframe Channel Connections Panel	5-19
Figure 5-10	CMCC Extended Display Panel	5-20
Figure 5-11	CMCC Extended Display	5-21
Figure 5-12	Channel Panel	5-22



Figure 5-13	CMCC and Channel Show Commands Panel	5-23
Figure 5-14	Router Command Interface Panel.	5-24
Figure 5-15	Redisplayed Router Command Interface	5-25
Figure 5-16	Router Command Interface Panel—TN3270 Server	5-26
Figure 5-17	Router Command Interface Panel—Current PU Configuration.	5-27
Figure 5-18	Cisco Resource Manager Main Window	5-29
Figure 5-19	Add a Single Device Window	5-30
Figure 5-20	Add Passwords Window.	5-31
Figure 5-21	Enter Authentication Information Window	5-32
Figure 5-22	Add Dynamic Views Window	5-33
Figure 5-23	Filter Select Devices Window	5-33
Figure 5-24	Save Dynamic View Window	5-34
Figure 5-25	Browse Dynamic Views	5-34
Figure 5-26	Select Polled Views Window	5-35
Figure 5-27	Change Polling Options Window.	5-35
Figure 5-28	Select Devices Window	5-37
Figure 5-29	Availability Monitor Window.	5-38
Figure 5-30	Interface Details Window.	5-39
Figure 5-31	Define Custom Reports Window	5-40
Figure 5-32	Add Custom Report (Advanced) Window—TN3270 Server Messages	5-41
Figure 5-33	Add Custom Report (Advanced) Window—CIP and CPA Messages	5-42
Figure 5-34	Cisco Mainframe Channel Connections Panel.	5-44
Figure 5-35	Interfaces Type =C Panel	5-45
Figure 5-36	Router Status Panel.	5-46
Figure 5-37	TN3270 Session Possible Points of Failure	5-49
Figure 5-38	TN3270 Monitor Events Window	5-50
Figure 5-39	IPM:Target Window	5-52

Figure 5-40	Add Target Window	5-52
Figure 5-41	IPM-Add Operation Window	5-53
Figure 5-42	IPM: Add Collector Window	5-55
Figure 5-43	IPM: Add Collector Window (Start Time and Duration)	5-56
Figure 5-44	Global Statistics Window	5-57
Figure 5-45	Router Status Panel	5-59
Figure 5-46	Router Status Panel	5-60
Figure 5-47	Router Status Extended Panel	5-61
Figure 5-48	Router Performance History Panel	5-62
Figure 5-49	Router Command Interface Panel with show process mem Command	5-63
Figure 5-50	CMCC History Panel	5-64
Figure 5-51	ISM CMCC Administration Panel	5-65

Table 2-1	LU Naming Summary	2-11
Table 2-2	DLUR LSAP Configuration Mode	2-22
Table 2-3	Returning to DLUR LSAP Configuration Mode	2-22
Table 2-4	Removing a DLUR LSAP Entity	2-23
Table 2-5	TN3270 Server Configuration Tasks	2-24
Table 2-6	IP Precedence Configuration Tasks	2-26
Table 2-7	IP ToS Configuration Tasks	2-26
Table 2-8	PU Configuration Tasks	2-27
Table 2-9	DLUR Configuration Tasks	2-28
Table 2-10	DLUR SAP Configuration Tasks	2-28
Table 2-11	DLUR PU Configuration Tasks	2-29
Table 2-12	LU Nailing Configuration Tasks	2-29
Table 2-13	Monitoring the TN3270 Server	2-30
Table 5-1	TN3270 Management Feature Matrix	5-4
Table 5-2	SNMP and SYSLOG Router Configuration Commands	5-5
Table 5-3	RSRB Configuration Examples	5-6
Table 5-4	TN3270 Server Router Commands	5-6
Table 5-7	Statistics on the PU Detail Window	5-12
Table 5-8	Statistics on the LU Detail Window	5-13
Table 5-9	Information Needed in Problem Diagnosis	5-47

About this Guide

This document describes how you can use the Cisco Channel Interface Processor (CIP) and the Channel Port Adapter (CPA) in conjunction with the Telnet 3270 (TN3270) Server feature of the Cisco IOS software to:

- Address requirements for accessing mainframe applications while moving to IP networks
- Protect your investment in your mainframe and mainframe applications
- Allow you to run your business more efficiently by utilizing the skills of your network specialists most effectively

The document provides an overview of TN3270, describes how to configure and manage the TN3270 Server, and provides migration scenarios.

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** in the toolbar, select **Documentation**, and click **Enter the feedback form**. After you complete the form, click **Submit** to send it to Cisco. We appreciate your comments.

Intended Audience

This document is for anyone who wants to learn more about Cisco's data center solutions. It begins with an overview that is appropriate for all audiences. It also includes design guidelines and sample configurations appropriate for network designers, systems engineers, consulting engineers, and network support personnel. The document assumes familiarity with networking and Cisco routers, but does not assume mastery of either.

Examples of key configuration commands are shown to aid in understanding a particular configuration. However, this document does not contain the exact and complete configurations. This information is available and regularly updated in Cisco Connection Online (CCO) and in the Cisco product documentation. CCO is Cisco's primary, real-time support system and is accessible at the World Wide Web address <http://www.cisco.com>.

Document Structure

This document contains the following chapters and appendixes:

- Introduction to Telnet 3270—Provides an overview of 3270 data streams and the use of TN3270.
- TN3270 Server Implementation—Provides an overview of Cisco's TN3270 Server and describes how to implement the server.
- TN3270 Client Implementation—Provides an overview of Cisco's TN3270 client offerings.
- Migration Scenarios—Provides a series of migration scenarios.
- Network Management—Describes options for managing the TN3270 Server.
- Glossary—Provides a list of terms and acronyms that are relevant to this guide.
- References—Provides a list of related documents.

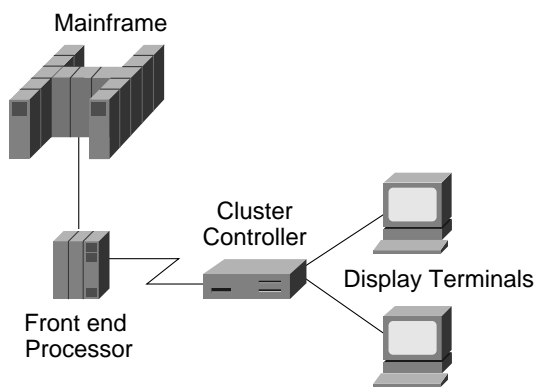
Cisco's Data Center Solutions

For the last 20 years, businesses have depended on mainframe applications. A trillion dollars have been spent on mainframe applications, and those applications will not disappear tomorrow. In addition, a great deal of development effort has been invested in mainframe security, backup, and redundancy, making the mainframe an excellent server for the networks of tomorrow. For these reasons and others, mainframes will continue to play a major role in networks for years to come. This reference guide describes how to use Cisco solutions to tightly integrate your mainframes with the rest of your network as it evolves to support higher bandwidth and Internet and intranet access.

Evolution of the Data Center

In the early 1970s, computing cycles and memory were very expensive. Most enterprises centralized their computing cycles in large mainframe computers. These mainframe computers resided in a data center—often called a “glass house.” End users accessed mainframe applications from teletype machines or display terminals (known as 3270 devices). IBM developed Systems Network Architecture (SNA) to define how display terminals could access applications and information in IBM mainframes. Figure i shows a simple SNA network and some of the key components.

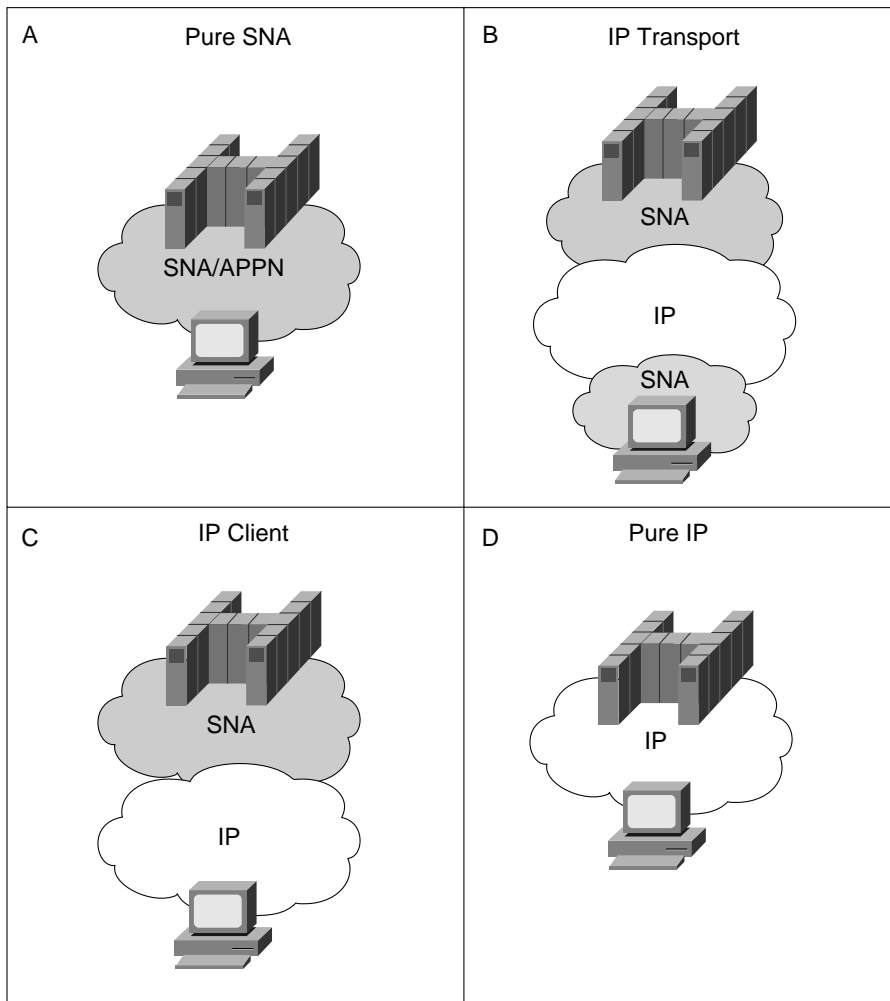
Figure i Sample SNA Network



Today, because computing cycles are so inexpensive, most desktop computers have more processing power than the mainframes of the 1970s. Processing power is spread throughout enterprises and is found not only on the desktop, but also in powerful workgroup computers. IBM mainframes are still used to support SNA applications, but access to those applications can be from 3270 display terminals, PCs running 3270 emulation programs, PCs

running more advanced SNA protocols, or TCP/IP end systems that use the TN3270 protocol. IBM mainframes are used for more than just SNA applications. More than 40 percent of the mainframes worldwide also run TCP/IP, and that number is expected to grow to 85 percent by the year 2000. Figure ii shows the four paradigms of IBM mainframe access.

Figure ii Evolution of IBM Networks



Today, many IBM networks still access SNA applications in the mainframe from SNA clients (Figure ii, quadrant A). However, more than 40 percent of organizations have migrated their backbone to TCP/IP (Figure ii, quadrant B). From a data center perspective, these two scenarios are the same. These scenarios are presented in the *SNA Internetworking Design and Implementation Guide*, which is volume 3 in Cisco's IBM Internetworking Design Guide Series. (This document was formerly called the *Data Center Design and Implementation Guide*.)

With the proliferation of Internet connections and because TCP/IP is included free with Windows, more organizations are looking at TN3270 as a low-cost way to access their SNA applications. TN3270 eliminates the requirement for dual stacks on the desktop and minimizes the cost of specialized desktop software.

Another alternative, provided by the OC://WebConnect Pro family, is to use a specialized Web server to download Java applets to clients. The Java applet provides access to a typical 3270-like interface or, optionally, a Web-browser interface. No specialized software is required at the desktop, and the Web server automatically downloads the most current Java applet, eliminating the cost of purchasing and maintaining specialized desktop software. Web browsers offer an intuitive interface that is well understood by customers, suppliers, and employees. The Web server maintains a permanent and secure TN3270 connection to either a TN3270 server in a Cisco router or a TN3270 server running in an IBM mainframe.

SNA is isolated to the data center, and the desktop has TCP/IP only. This scenario (Figure ii, quadrant C), is covered in this document.

Finally, some environments are either building new mainframe applications using TCP/IP or rewriting existing applications to use TCP/IP. This scenario (Figure ii, quadrant D) is covered in *IP for Mainframes Design and Implementation Guide*, which is volume 5 in Cisco's IBM Internetworking Design Guide Series.

Credits

Many people have contributed to this document. The technical owner, Craig Brown, wishes to thank the following people for their contributions:

Jon Beck
Michael Boe
Derek Bolton
Lori Bush
Kurt Iriart
David Katz
Donna Kidder
Volker Schuster
Herbert Szumovski

Cisco Connection Online


Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web. The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The Web version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- Web: <http://www.cisco.com>
- Web: <http://www-europe.cisco.com>
- Web: <http://www-china.cisco.com>

- 
- Telnet: cco.cisco.com
 - Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

Introduction to Telnet 3270

This section provides an introduction to Telnet 3270 (TN3270). It discusses why you use TN3270, provides some background information about TN3270, and discusses Cisco's product offerings for TN3270.

Why use Telnet 3270?

There are several key factors occurring that are determining the direction companies are taking in the networking arena. One of these factors is the advent of migrating from SNA networks to IP networks. As a part of this migration, companies are outfitting their end users with PCs that communicate via TCP/IP. As a result, they are replacing their SNA-based 3270 emulation packages with TN3270 clients and adding TN3270 servers to their networks. TN3270 is the method of transporting SNA 3270 data streams over an IP network. Some of the factors that are driving companies in this direction are:

- The role of the mainframe has shifted from a central server for all application and data processing to an enterprise server.

In the role of an enterprise server, the mainframe is now a peer with other servers, such as a UNIX or NT server. With the introduction of the mainframe operating system OpenEdition, the mainframe can now participate in a UNIX environment as a server. Because large companies continue to maintain more than 70 percent of their data on the mainframe, a method of transporting the SNA 3270 data stream over an IP network is necessary. In addition, network requirements such as providing a nondisruptive, redundant network must be met.

- User requirements have expanded.

Text-based applications are being replaced by applications with graphical user interfaces (GUIs). In addition, users require reduced screen input and enhanced application display methods, which can be provided by Web-based clients.

- The technical skills of the networking workforce are becoming stronger in TCP/IP and weaker in SNA.

The networks that are used and taught at the universities do not typically incorporate SNA. Students are taught TCP/IP and are expecting their future employers to have IP networks. Corporations are finding that while they can retrain their SNA network specialists to be IP specialists, it is much more difficult to teach SNA to an IP network specialist. SNA networking requires an understanding of historical hardware and software structures. Management of an SNA network requires mainframe knowledge, including dataset manipulation and operator console control. The combination of these factors makes it difficult for corporations to maintain existing mainframe applications and legacy SNA networks.

- Corporations that maintain legacy SNA networks, often establish a separate department to create and support the Internet/intranet to satisfy requirements such as Internet access and e-mail. Maintaining two separate networks (and two separate network support departments) is not a cost-effective, long-term solution. Maintaining the mainframe applications and transporting them over the intranet is an ideal situation.

The TN3270 solution addresses all of these factors. Implementing the TN3270 server is simple. The difficulty in this migration path arises when you have to incorporate existing application and network restrictions into a new topology. It is important to understand the application and network requirements of your corporation before you decide which of the TN3270 server's features best meets these requirements and how it should be implemented.

Background

Before we discuss the variety of options available, it is important to understand the basic concepts of SNA 3270 and TN3270. If you are already familiar with these concepts, proceed to “Cisco Product Offerings.”

What is a 3270 Data Stream?

3270 devices include a series of display devices, communications controllers, and printers that connect to an IBM mainframe. They support a special type of data stream, which is called the 3270 data stream. This data stream allows applications to include control characters that instruct the receiving device how to format or display the information. The control characters allow the application to use the entire screen, as opposed to a single command line, to display information and to receive input from various areas of the screen (called partitions).

What is SNA 3270?

SNA 3270 refers to 3270 data streams that are transported from the source to the destination using the SNA protocol. With SNA 3270, the data stream is transmitted over an LU-to-LU session between logical units. LU types 2 and 3 use only SNA 3270 data streams. LU types 6.1 and 6.2 use the SNA 3270 data stream in addition to other types of data streams.

With SNA 3270, the mainframe application creates a 3270 data stream using 3270 commands, the data stream is transported over an SNA network, and the data is displayed on a 3270-compliant device.

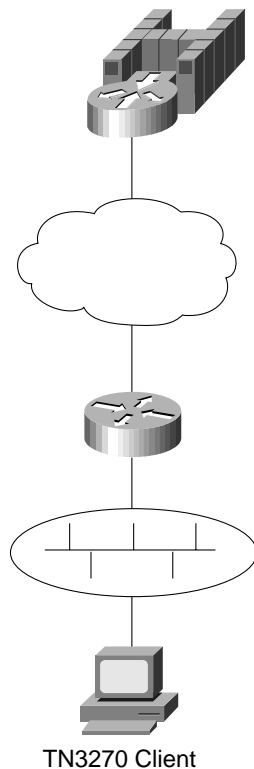
What is TN3270?

TN3270 is a protocol that defines how to transport 3270 data streams over a TCP/IP network. TN3270 was originally defined in RFC 1576 and is based on the Telnet protocol. The difference between a Telnet session and a TN3270 session is that a Telnet session uses the ASCII character set and sends a line of data at a time and a TN3270 session uses the EBCDIC character set and sends a block of data (a screen refresh) at a time.

The following elements work together to enable TN3270 communication:

- The end stations run a TN3270 client. The client emulates a 3270 display device.
- The client accesses a TN3270 server over an IP network.
- The TN3270 server converts the TN3270 data stream to SNA 3270 and passes the data to the mainframe. The TN3270 server resides on either the mainframe, in which case it is considered an *inboard* server, or a front-end processor (FEP) such as the Cisco CIP and CPA, in which case it is considered an *outboard* server.
- The mainframe provides Virtual Telecommunications Access Method (VTAM) and the mainframe application that the user is attempting to access.

Figure 1-1 Diagram of a TN3270 Session



In an SNA 3270 network, the user is known by the LU name. In a TCP/IP network, the user is known by an IP address. One of the tasks of the TN3270 server is to provide a correlation between these two addresses. This correlation allows the SNA applications to maintain the LU requirements and allows the network to use IP. Management of the LU-to-IP correlation is discussed in Chapter 5, Network Management.

What is TN3270E?

TN3270, as defined by RFC 1576, does not address several functions that are required to make the TN3270 server a viable migration solution. To address this problem, TN3270E was defined under RFC 2355 (which made obsolete RFC 1647). TN3270E added the following functions:

- **Emulation of 328x printers**—All IBM-type printers accept both LU 1 and LU 3 printer streams because a printer may be shared between multiple IBM host applications, such as JES and CICS. The JES can be configured for LU 1 data streams and the CICS can be configured for LU 3 data streams. A TN3270 server cannot function properly with mainframe applications and 3270 printers if it does not allow a mix of LU 1 and LU 3 data streams.
- **Client request of a particular name**—Many host applications behave differently depending on the network name of the terminal. In the case of printer emulation, many host applications use a method of predefining printer destinations. It is important that a Telnet client is allowed to request that a connection be associated with a specific 3270 device name.

- **3270 ATTN key**—The 3270 ATTN key is interpreted by many host applications in an SNA environment as an indication that the user wants to interrupt the execution of the current process. The Telnet Interrupt Process (IP) command was defined for this purpose and was used in implementing support for the 3270 ATTN key. TN3270E supports the 3270 ATTN key in both the client and server:
 - TN3270E clients allow a single key or a combination of keys to be mapped to the 3270 ATTN key. When the user presses the mapped keys, the client transmits a Telnet IP command to the server.
 - TN3270E servers translate the IP command received from a TN3270E client and pass it to the host application as an ATTN key. In other words, the server representing a secondary LU (SLU) in an SNA session sends a SIGNAL RU command to the host application.
- **SNA positive/negative responses**—A positive response indicates that the previously received data was successfully processed. A negative response is used to indicate that an error has occurred while processing the previously received data; this error may be caused by the host application building a 3270 data stream that contains an invalid command or by a mechanical error at the client side. Support for positive/negative responses is important in printer emulation, but it is also useful for some terminal applications.
- **Client access to bind information**—The Bind image contains a detailed description of the session between the Telnet server and the host application. TN3270 provided no way for the client to access session information. Certain clients require access to the Bind information so that they can determine the format of the data they are to receive. For example, printer clients require access to Bind information to distinguish whether the data stream is LU 1 or LU 3.

Cisco Product Offerings


Cisco offers a TN3270 Server as well as a couple of TN3270 clients.

TN3270 Server on a CIP or CPA

The implementation of TN3270 server on a channel-attached router, using the CIP or CPA, provides an efficient method of removing the processing of TN3270 sessions from the costly mainframe cycles to a faster, more efficient router. The CIP can be installed in a Cisco 7000 or 7500 series router. The CPA can be installed in a Cisco 7200 series router.

The Cisco TN3270 Server feature implements RFC 2355 and allows TN3270 or TN3270E clients to access TN3270 host data using a channel-attached router that is connected directly to a host or remotely through an FEP. It provides mapping between SNA 3270 hosts and TN3270 clients connected through a TCP/IP network. TN3270 clients with LU 2.0 and TN3270E clients with LU 1, 2, and 3 are supported. (The server also supports printing as defined by RFC 1646.) From the perspective of an SNA 3270 host connected to the channel-attached router, the TN3270 server is an SNA device that supports physical units (PUs), each supporting up to 255 LUs. The SNA host is unaware of the existence of the TCP/IP extension on the implementation of these LUs.

The LUs implemented by TN3270 server are all dependent LUs. To route these dependent LU sessions to multiple VTAM hosts connected to the server in the channel-attached router (rather than on the VTAM hosts), a MiniDLUR with end node (EN) Dependent LU Requester (DLUR) function is implemented as part of the TN3270 server. The use of DLUR is optional so that the TN3270 Server can also be used for non-APPN capable VTAMs (versions older than VTAM 4.2). Because the TN3270 Server feature implements the function of DLUR, it can be configured to communicate with the primary server and, in case of failure, the backup Dependent LU Server (DLUS) residing on the host.



From the perspective of a TN3270 client, Cisco's TN3270 Server on a channel-attached router is a Telnet server that can support up to 16,000 concurrent Telnet sessions at 850 transactions per second. The server has been tested with up to 30,000 sessions at lower transactions per second. The server supports Telnet connection negotiation and data format as specified in RFC 1576 (traditional TN3270), RFC 1646 (printer extensions to RFC 1576), and RFC 2355 (TN3270E).

Implementing the TN3270 Server on the channel-attached router requires a minimum of two commands; the first command initiates the TN3270 Server and the second defines the PU. No LU definitions are created on the TN3270 Server. The function of the server is to provide the interface between the IP network and the SNA network. The TN3270 Server performs an exchange ID (XID) negotiation at the time of startup. At this point the details regarding the PU and LU activation are passed from VTAM to the TN3270 Server.

TN3270 Server Implementation

This chapter discusses the following aspects of TN3270 Server implementation:

- TN3270 Server on the CIP/CPA
- Planning for Implementation
- TN3270 Configuration
- Monitoring the TN3270 Server

TN3270 Server on the CIP/CPA

The TN3270 Server feature of the Cisco IOS software can be used in the following situations:

- When an IP backbone needs to be maintained, but SNA 3270-type clients must be allowed.

With the TN3270 Server in a channel-attached router, SNA can be terminated in the data center and still support the legacy TN3270 applications. The backbone network outside the data center can be pure IP. Similarly, if clients in branch offices need TN3270 connectivity, this can be provided without having to support SNA stacks at the branch office.

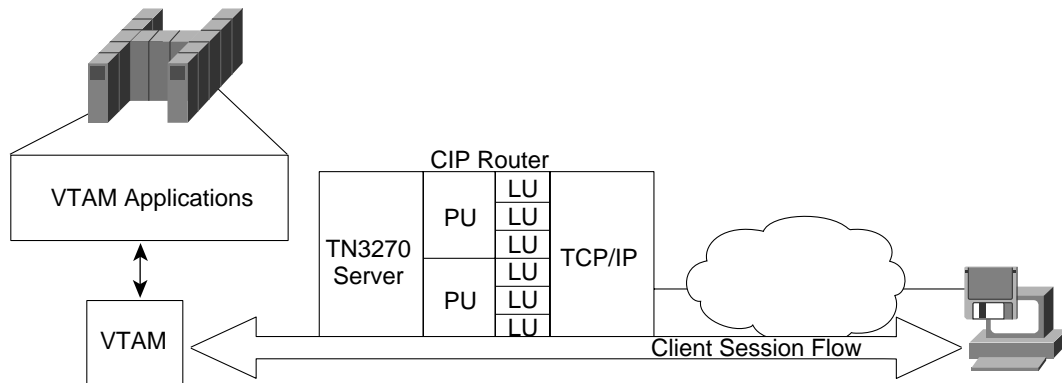
- When a TN3270 host TCP/IP stack is being used in conjunction with a TN3270 Server, but mainframe CPU cycles need to be off loaded.

Enabling the TN3270 Server functions in the router enables you to offload TN3270 and TCP/IP processing from the host and saves host CPU cycles.

- When support for high session density or high transactions per second is required. Up to 16,000 sessions are supported per CIP/CPA card.

This support makes the TN3270 Server an enterprise-wide 3270 access solution.

Figure 2-1 TN3270 Session Overview



Hardware and Software Requirements

This section provides information about the hardware and software required to use the TN3270 Server. For additional information about what is supported in the various releases of the Cisco IOS software and the CIP microcode, see the information on CCO.

Router Software Requirements

The TN3270 Server consists of a system image and a new microcode image. These are bundled as one combined image. The TN3270 Server feature was first included in the Cisco IOS Release 11.0BT special release. It is also included in release 11.2 and later. LU nailing, the process of mapping an IP address to an LU, was first included in the Cisco IOS Release 11.3.

Router Hardware Requirements

The CIP hardware microcode must be CIP22-23 or later. The CPA hardware level must be CIP26-2 or later with Cisco IOS Release 11.3T or later.

Mainframe Requirements

The hosts communicating via SNA with the TN3270 Server must be running VTAM V4R2. You can use VTAM V3R4, but DLUR operation is not supported in V3R4 and proper Dynamic Definition of Dependent LU (DDDLU) operation may require program temporary fixes (PTFs) to be applied to VTAM. We recommend using VTAM V4R2.

TN3270 Client Requirements

Based on the RFC standards, the Cisco TN3270 Server will work with any client that implements the TN3270 or TN3270E protocols.

Planning for Implementation

This section discusses the following considerations that must be addressed before implementing a TN3270 Server in your network:

- Where to Place the TN3270 Server and How Many Servers You Need
- Implementing TN3270 Server on a CIP/CPA
- Defining PUs

- Defining LUs
- Addressing LAN Printing Requirements
- Addressing SNA Routing in Multi-Domain Environments
- Addressing End User Service Level Requirements
- Addressing Availability Requirements (Redundancy/Load Balancing)
- Satisfying Expanding Network Address Requirements

Where to Place the TN3270 Server and How Many Servers You Need

The TN3270 Server can be placed on a local router (one that is directly attached to the mainframe) or a remote router. If the router is local, the TN3270 Server resides on a CIP or CPA that is connected to the mainframe via ESCON or bus-and-tag. However, many organizations use the TN3270 Server on remote routers as an intermediate step in their migration to using the CIP or CPA as the host connection option. In this case, the TN3270 Server is placed on a router that is connected to the mainframe via any channel connection device, such as the FEP. Although placing the TN3270 Server on a remote router is not an optimal, long-term solution, it allows sites that are migrating from the FEP to the CIP or CPA to have TN3270 server functionality immediately.

The Cisco TN3270 Server provides up to 16,000 concurrently active LUs per channel-attached router at a rate of 850 transactions per second. The TN3270 server will support considerably more LUs at a lower throughput rate. While most organizations would never reach 16,000 concurrent sessions in a production environment, the TN3270 Server was designed to accommodate this number of sessions to account for day-to-day usage and to provide a buffer for failover LUs in the event of a failure of another TN3270 Server. Most large companies use their TN3270 servers at 12,000 to 14,000 users on a daily basis. On average, they install eight to ten CIPs or CPAs to provide TN3270 access for approximately 100,000 users.

The number of sessions a single TN3270 Server can handle is directly related to the number of transactions per second and the amount of memory available to the CIP or CPA. The 16,000 LU session capacity is based on 850 transactions per second and a session size of 200 bytes inbound (from the terminal) and 800 bytes outbound (to the terminal). Normally, a single terminal (or LU) is rated at one transaction per minute. Therefore, if a server can handle 1 transaction per second, then it can accommodate 60 terminals. At a rate of 850 transactions per second, it can accommodate 16,000 terminals. Printer LUs and file transfers reduce the number of available sessions.

Although the TN3270 Server can manage tens of thousands of sessions, you should consider the impact of gateway disruption when designing your network. How many users can you afford to disrupt if a gateway goes down? A typical number is 12,000 to 14,000 sessions, which allows them to benefit from the increased throughput rate.

The TN3270 Server has been tested with up to 30,000 concurrently active LUs.

Implementing TN3270 Server on a CIP/CPA

The TN3270 Server feature of Cisco IOS software can be implemented on either a CIP or a CPA.

- Each CIP has up to two Enterprise Systems Connection (ESCON) or two bus-and-tag (parallel) interfaces and a single virtual interface. The TN3270 Server is installed on the virtual interface. Therefore, each CIP can have a single TN3270 Server. Because a router can accommodate more than one CIP, each router can support multiple TN3270 Servers.
- Each CPA has a single ESCON interface and a single virtual interface. As with the CIP, a single TN3270 Server can be installed on each CPA. Because a router can accommodate more than one CPA, each router can support multiple TN3270 Servers.

Note: The subnet of the virtual channel interface must be the same as the subnet of the listening IP addresses. Otherwise, the router will not know that the listening addresses are directly connected, and will not pass the routes to the listening addresses to the other routers in the network. Without the address, clients are not be able to reach the CIP/CPA.

Defining PUs

SNA communication is based on the concept of PUs and LUs. When deciding how to configure a TN3270 Server, one of the first things you must consider is the type of PUs you will use and how you want to define them. The TN3270 Server supports two types of PUs:

- Direct PUs—Used in subarea SNA.
- DLUR PUs—Used with Advanced Peer-to-Peer Networking (APPN).

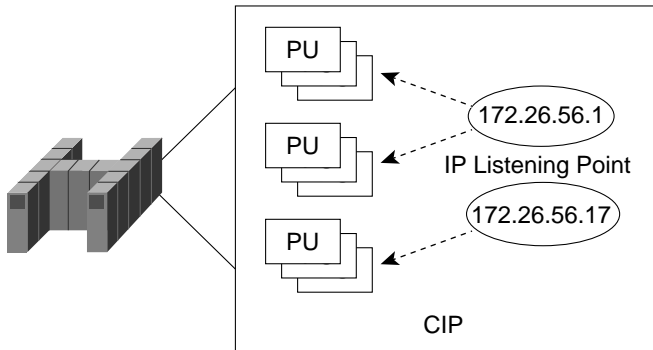
DLUR PUs and direct PUs can coexist on the same CIP/CPA.

The definition of each direct PU within the router requires a local service access point (SAP) to be defined. Traditionally, SNA uses SAP 04, 08, 0C, and so forth (multiples of four). But the source SAP used by the TN3270 adapter must be an even value. Each PU on a TN3270 adapter on the CIP must, however, have a unique local/remote media access control (MAC)/SAP quadruple. If the PUs are on the same adapter and are to connect to the same remote MAC (RMAC) and remote SAP (RSAP), then each must have a different link SAP (LSAP). Therefore, to create dozens of PUs tied to one TN3270 adapter, separate the SAPs by two or four. SAPs are in hexadecimal format and starting at AA are reserved for other uses (such as Subnetwork Access Protocol [SNAP] headers, IP, and address resolution protocol [ARP]). If you start with SAP 02 and increment each SAP by two, you can tie about 120 SAPs to an adapter. To define more SAPs, create another adapter and start over with SAP 4.

Each direct PU is defined on the CIP/CPA with a listening IP address and a target MAC address that goes to a particular logical partition (LPAR). The listening address is the IP address that the client addresses when requesting an LU from the associated PU. Multiple PUs can be defined with the same IP listening address and thereby create a pool of LUs. This pool of LUs is 255 LUs times the number of PUs with the same listening address. When a user requests an LU using the listening address that is associated with the group of PUs, the client will receive an LU from that pool. There is a predefined algorithm that is used to decide what LU the clients receives. (See the “Monitoring the TN3270 Server” section.) One TN3270 Server can simultaneously service multiple LPARs if you create a single PU or a pool of PUs per LPAR. To identify which PU or pool of PUs is associated with which LPAR, create a different listening port for each LPAR.

Figure 2-2 shows an example of three PUs within the same TN3270 Server. Two of the PUs are allocated to the same listening address. The third PU is assigned to a different listening address.

Figure 2-2 Allocation PUs



The TN3270 Server can support configurations where a group of PUs have the same IP listening address, each PU has its own separate listening address, or a combination of the two. Likewise, when defining a PU, you can define static LUs, dynamic LUs, or a combination of both.

Defining LUs

TN3270 clients need only an IP address and an optional LU name or type to connect to the TN3270 Server. The server then maps requested sessions with actual LUs available on the hosts.

Each PU can have up to 255 LUs defined. With historical SNA networks, an LU was a physical device attached to a remote communications controller, such as an IBM 3274. Each port on these devices was a local address known as a LOCADDR. When a LOCADDR was defined, each LU within a PU was statically defined to match the static hardware. Today, with the virtual allocation of LOCADDRs, either static or dynamic LUs can be established.

The TN3270 Server supports static and dynamic LUs.

- Static LUs are defined individually within VTAM and are known by the client. Static LUs require a specific LU/PU name to be supplied. Static LUs are typically printers or secure terminals.
- Dynamic LUs use the DDDL feature of VTAM. These LUs are given to the TN3270 client without the client knowing the PU or LU name of the session defined in VTAM. If the PU allows dynamic LUs, any LOCADDR not defined as a static LU, within a PU definition, can be used as a dynamic LU.

When a standard TN3270 client establishes a connection, there is no mechanism for requesting an LU by name. In this case, you must use dynamic LU pools or LU nailing. Because TN3270E supports requesting LUs by name, a TN3270E client can use either dynamic or static LUs.

In most environments, it is more advantageous for TN3270 clients to specify a dynamic LU rather than a static LU. For static LUs, the PU on the TN3270 Server allocates the required memory when the mainframe activates the LU. For dynamic LUs, the memory is not allocated until the LU is requested. Therefore, memory on the TN3270 Server is not allocated unnecessarily.

Activation of LUs

The LU activation process differs depending on whether the client is using a static or a dynamic LU.

For static LUs, the first phase is LU activation. The LU requested must be defined at the host under the PU. The activation process is as follows:

1. The LU is activated by the host.
2. The client issues a connect with server request. If the device is listed in the table of LU names and is not being used, then the router sends a positive response. If the device is being used, then the router sends an “in use” response.
3. If the client connection is successful, the router sends a NOTIFY(ENABLED) request to the host.

Network Management Vector Transports (NMVTs) are also sent to any running network management application, which allows the host to track the IP address of any device connecting to each LU.

For dynamic LUs, the first phase is session negotiation. This phase includes steps necessary to initiate the client-to-CIP/CPA connection and to select the LU:

1. The TN3270 client requests a pooled LU session. The client’s request includes the terminal type. The TN3270 client must be configured with a destination IP address, TCP port, and terminal type for a pooled LU session to occur.
2. The TN3270 Server forms an EBCDIC string based on the model type and number requested by the TN3270 client. The server uses this string as a field in the REPLY product-set identification (PSID) NMVT field it sends to the host.
3. The TN3270 Server allocates a LOCADDR from the next available LU in the LU pool for the chosen IP address. Subject to configuration control, all LUs that the host does not immediately activate are automatically placed in the pools. The LOCADDR is sent in the REPLY-PSID(power-on) NMVT. When VTAM receives the NMVT, it uses the EBCDIC model type and number string to look up an LU template under the LUGROUP. An activate logical unit (ACTLU) is sent and a terminal session is established.

The second phase is session bind and data transfer. This phase includes the steps of the TN3270 host-to-client SNA session bind and data transfer:

1. After the ACTLU is provided by the host, the information is transferred between the system services control point (SSCP) and the LU. The CIP manages the necessary protocol conversions. At this stage, the type of TN3270 client is important. If you are using a TN3270 client, SSCP must be configured to communicate with the LU using the TN3270 data stream (using host parameters USSTAB and SSCPFM). If TN3270E clients are used and they request the BIND-IMAGE function (normally LU 1 and LU 3 printers), they must communicate with SSCP using the SNA character string (SCS). In some cases, the client LU bypasses SSCP completely (using the host variable LOGAPPL) and connects directly to a host application.
2. When the LU data is received by the SSCP, it requests a bind with the LU, which is locally acknowledged by the CIP/CPA.
3. The LU-to-LU data is transferred.

The third phase is session termination. Sessions are terminated in the following conditions:

- The client logs off the LU-to-LU session, causing the server to send an UNBIND message followed by a NOTIFY (UNAVAIL) message to the host.
- The client disconnects at the TCP layer and the LU is configured to disconnect on UNBIND. The TCP session is disconnected and the host is sent a NOTIFY (UNAVAIL) message.
- The client is idle too long or will not respond to a DO TIMING MARK message. The server sends UNBIND message to the host and then sends a NOTIFY (UNAVAIL) message.

- The host issues a deactivate physical unit (DACTPU) or disconnects the link.
- The router console is instructed to deconfigure the PU.

Determining How LUs Will Be Named

There are several ways in which an LU can be named and assigned to a TN3270 client. It is important to understand how LU naming and allocation work before designing a TN3270 Server network. The same LU can be known to VTAM with one name and to the CIP/CPA with a different name. This can be by design, but also can be accidental, leading to client connection problems and network management problems.

The LU name assigned within the TN3270 Server is created using one of several methods. The method depends on the configuration of the TN3270 Server and the PU. PUs can be configured as either direct or DLUR-based.

- **Direct**—With direct PUs, the TN3270 Server LU names do not necessarily match the LU names defined in VTAM. To ensure that the LU name used in VTAM matches the LU name used by the TN3270 Server, ensure that the configuration matches. With the introduction of the function INCLUD0E within the VTAM PU definition, VTAM will pass information regarding the real LU names to the TN3270 Server. At this time, the Network Control Program (NCP) does not support the 0E control vector. Remote TN3270 Servers will not get the INCLUD0E information.
- **DLUR**—With DLUR PUs, LU names on the TN3270 Server match names in VTAM. If you use DLUR PUs, you always get the correct LUNAME information from VTAM. Therefore, you don't need to specify an LU-SEED on the router PUs.

In a multihost environment, hosts with DLUS/DLUR implemented require less configuration of the PUs and LUs on the TN3270 Server.

Other factors that impact the LU naming process are:

- Whether the LU uses DDDL
- How the LUGROUP is configured for dynamic LUs
- How the LUSEED is specified (if at all)
- Whether INCLUD0E is used
- Whether LU nailing is used

Dynamic Definition of Dependent LUs

Most of the current offerings of TN3270 server implementation use predefined pools of LUs to support different terminal types requested by the TN3270 clients. To simplify the management of such configurations, the Cisco IOS software TN3270 Server feature supports a VTAM V3R4 feature, called DDDL, which allows you to dynamically request LUs using the terminal type provided by TN3270 clients. This feature eliminates the need to define any LU configuration in the server to support TN3270 clients emulating a generic 3270 terminal. Only the PUs need to be configured. Configuration for LUs in the server is necessary only for clients that require specific LU names to be secured (such as printers) or use IP addresses for authorization or application selection.

Dynamic LU allocation is the most common form of request from TN3270 clients emulating a TN3270 terminal. The client is typically concerned with emulating a particular terminal type, but is not normally interested in what LOCADDR or LU name is allocated by the host as long as a USS10 menu is presented or an LU-to-LU session is started (via the LOGAPPL facility).

The server performs the following tasks on such a session request:

- Forms an EBCDIC string based on the model type and number requested by the client. This string is used as a field in a Reply PSID NMVT.
- Allocates a LOCADDR from the next available LU in the generic LU pool. This LOCADDR is used in the NMVT.
- Sends the formatted Reply PSID NMVT to VTAM.

When VTAM receives the NMVT, it uses the EBCDIC model type and number string to look up an LU template under the LUGROUP. An ACTLU is sent and a terminal session with the model and type requested by the client can be established.

Note: DDDLU requires that the ISTEXCSD exit is active in VTAM. You can check to see that the DDDLU exit is active by running this VTAM command:

```
D NET,EXIT$
```

The output should say that ISTEXCSD is active and has exit ISTEXCSD in place.

LUGROUP Parameter

To use dynamic LUs, you must create and activate a VTAM LUGROUP major node, which contains the model types and definitions for the variety of terminal types used. Each model type provides different screen functions. The LUGROUP definition is used by the requesting LU to define terminal type settings, such as the default logmode, mode table, and USS table.

When defining an LUGROUP, it is best to define all combinations of model types that are typically found in your network as well as a default model statement. The default model statement acts as a catch-all definition for combinations not defined. You do not specify a model name in the default model statement. Instead, you begin the statement with the @ sign. The @ sign can also be used as a wildcard in other entries.

To cover all combinations of machine, model, and extension type, when creating the LUGROUP, you would include definitions to cover the following:

- Two machine types: IBM 3278 and 3279
- Four model types: 2, 3, 4, 5
- Two extension types: 0 and S

A 0 extension specifies a classic TN3270 connection. The client expects all data to be in a TN3270 data stream. An S extension indicates that the client expects the SSCP-to-LU data to be in SCS control code format. All entries with an S extension to the machine type should have SSCPFM=USSSCS coded. All others should have SSCPFM=USS3270 coded.

- Two 3270 data-stream mode types: <> or E

An E mode type indicates that the client supports the host sending a read-partition query to the client to determine the client's capabilities.

The combinations of the machine, model, and extension types result in 32 model entries plus the default entry. However, you can specify an SSCPFM of USSSCS for all clients regardless of type. This reduces the entries to 16. Then if you use the wildcard to represent both the 3278 and 3279 machine types, the number of entries is reduced to eight (plus the default).

The switched major node definition must specify the LUGROUP name of the LUGROUP parameter defined in the major node. The LU names of these dynamic LUs are generated by the LUSEED parameter. Alternatively, you can code the VTAM-exit ISTEEXCSD and use an in-house algorithm for assigning LU names.

For an example of an LUGROUP and a explanation of the contents, see the "PU and LU Definitions" section in the Migration Scenarios chapter.

LUSEED Parameter

LUSEED is a parameter used to reduce the configuration required for the definitions of LUs. The LUSEED parameter is required for dynamic LUs and can be used for static LUs.

The LUSEED parameter can be specified on both the channel-attached router and in VTAM. When configuring PUs in the channel-attached router, the parameter is LU-SEED. In VTAM, the parameter is LUSEED. The LU-SEED parameter is not valid on the channel-attached router if DLUR is used.

The LUSEED is a prefix that is used in the creation of LU names. The resulting LU name depends on the method used to specify the LU-SEED:

- If the parameter LU-SEED is specified with two '#' characters, then the hexadecimal representation of the LOCADDR is added to the suffix of the LU name. For example, if the parameter "LU-SEED LU1##" is specified with the LOCADDR of 10 decimal, the LU will be named LU10A.
- If the parameter LU-SEED is specified with three '#' characters, then the decimal equivalent of the LOCADDR is added to the suffix of the LU name. For example, if the parameter "LU-SEED LU1###" is specified with the LOCADDR of 10 decimal, the LU will be named LU1010.

The TN3270 Server LU-SEED parameter defaults to the first six characters of the PU name concatenated with the two hexadecimal character LOCADDR number. For example, if the PU is named PUXCPA01 and no LU-SEED is coded on the CIP or CPA, then the LU with LOCADDR 10 decimal will be named PUXCPA0A.

Be sure to define each dynamic PU with a unique LU-SEED parameter in the VTAM switched definition. Otherwise, VTAM will attempt to define two LUs with the same name and the second request will fail. The TN3270 client will show connected, but the CIP/CPA will be waiting for the ACTLU to flow and the session will never flow.

We recommend that you make the LU-SEED on CIP/CPA and the LUSEED on VTAM identical for the same PU to ensure that dynamic LUs have the same name on both the channel-attached router and VTAM.

Note that even if the LU-SEED is coded the same on both VTAM and the CIP/CPA, static LU names may not match because they are hardcoded in VTAM. Unless VTAM passes the LU name to the CIP/CPA or the VTAM static LU names match the CIP LU-SEED naming convention the LU names in each will be different. The best

solution to this problem is to use DLUR PUs or direct PUs with INCLUD0E so that VTAM passes all LU names (static and dynamic LUs) to the CIP/CPA. As an alternative, you can code LU-SEED in the CIP to match VTAM's static LU names, if possible.

INCLUD0E

INCLUD0E is a VTAM parameter that can be used with direct PUs to instruct the XCA to allow the LU name to be included in the ACTLU. If the TN3270 Server receives the LU name as part of the ACTLU, it uses this LU name and does not relearn the name from the Bind.

The INCLUD0E is available and supported in VTAM Version 4.4. If you use INCLUD0E, you must also apply the PTFs for the following authorized program analysis reports (APARs):

- APAR OW25501
- APAR OW31436
- APAR OW31805

LU Nailing

DDDLU and LU pooling are increasing in popularity and can be used for most LU needs. The exception, however, is if a client must use a specific LU name because of application requirements. For example, Information Management System (IMS) applications use a security mechanism to control access that is based on the LU name. These clients are often groups such as personnel departments or office branches. For these clients the requirement is to lock their LU to an IP address. There are two methods of locking an LU to an IP address. The first method is for the client to use the TN3270E function, which allows the client to specify the LU name. The second method is to use the client LU nailing feature of the Cisco IOS software TN3270 Server feature.

LU address mapping allows a client IP address to be mapped, or “nailed,” to one or more LU local addresses on one or more PUs. You can then control the relationship between the TN3270 client and the LU. Clients from traditional TN3270 (non-TN3270E) devices can connect to specific LUs, which overcomes a limitation of TN3270 devices that cannot specify a CONNECT LU. LU nailing is also useful for TN3270E clients because it allows you to perform the configuration of the client at the router, providing central control, rather than at the client.

The “model matching” feature of the TN3270 Server is designed for efficient use of dynamic LUs. Each client specifies a terminal model type at connection. When a non-nailed client connects and does not request a specific LU, the LU allocation algorithm attempts to allocate an LU that operated with that terminal model the last time it was used. If no such model is available, the next choice is an LU that has not been used since the PU was last activated. Failing that, any available LU is used. For dynamic LUs, however, there is a short delay in connecting the session.

Where a client or set of clients is nailed to more than one LU, the same logic applies. If the configured LU nailing maps a screen client to a set of LUs, the LU nailing algorithm attempts to match the client to a previously used LU that was most recently used with the same terminal model type as requested by the client for this connection. If a match is found, that LU is used. If a match is not found, any LU in the set that is not currently in use is chosen. If there is no available LU in the set, the connection is rejected.

The client LU nailing feature associates particular LU names to particular client IP addresses or IP subnets. The LU nailing is used to:

- Control (from a central location) the clients that can connect to certain LUs.
- Allow non-TN3270E clients to access a specific LU or pool of LUs.
- Provide guaranteed ownership for printers that need a predefined name.
- Provide guaranteed ownership for applications that use terminal based security.
- Control which group of users, based on IP address, is associated with a certain pool of LUs.

The CLIENT command nails client IP addresses to specific LUs. The parameter is configured using the “client ip” or “client printer” statement under a TN3270 Server PU. Each client statement is configured on a per PU basic. A client statement can specify one IP address or a group of IP addresses within a subnet. A specific IP address can be included in more than one client statement.

DHCP with Client Nailing

Some clients may require the use of client LU nailing but belong to a Dynamic Host Configuration Protocol (DHCP) group. Therefore, their specific IP address is not going to vary. The client LU nailing feature works with DHCP by using the subnet parameter. This means that a DHCP group that is part of a particular subnet can be specified to access a single LU or a group of LUs based upon the subnet address.

TN3270E and Statically Defined LUs with Client Nailing

Consider the situation where a TN3270E client requests an LU that is statically defined in the PU. If neither the LU nor the client are subjects of nailing statements, the client will get the LU that it requested. If the client is nailed and the requested LU is available and in the set to which the client is nailed, the client will get the LU that is requested. Otherwise the request is refused.

LU Assignment and Naming Summary

Table 2-1 discusses the factors that impact how an LU name is assigned and explains the result.

Table 2-1 LU Naming Summary

Factors	How the Name Is Assigned
Static LU with DLUR PU	The LU-SEED parameter on the channel-attached router cannot be configured under DLUR. Therefore, the LU names must be hardcoded in VTAM. The TN3270 Server learns the LU names from VTAM.
Static LU on direct PU with INCLUD0E	The LU names are hardcoded in VTAM. The TN3270 Server learns the LU names from VTAM.
Static LU on direct PU without INCLUD0E	<p>If you use the LU-SEED parameter on the channel-attached router, the LU names on the router are created according to the LU-SEED parameter. If you want the LU names to be identical on the router and in VTAM, you must create the VTAM LU names according to the naming convention established by the router’s LU-SEED parameter.</p> <p>If you do not use the LU-SEED parameter on the channel-attached router, the LU names on the router default to the first 6 characters of the configured PU followed by the 2-byte hexadecimal number of the respective LOCADDR of this LU. If you want the LU names to be identical on the router and in VTAM, you must create the VTAM LU names according to the naming convention described above.</p>

Factors	How the Name Is Assigned
DDDLU, LUSEED on SWMN, DLUR PU	The LU-SEED parameter on the channel-attached router cannot be configured under DLUR. Therefore, the LU names must be created in VTAM based on the VTAM LUSEED parameter. The TN3270 Server learns the LU names from VTAM.
DDDLU, LUSEED on SWMN, INCLUD0E on direct PU	The LU names are created in VTAM based on the VTAM LUSEED parameter. The TN3270 Server learns the LU names from VTAM.
DDDLU, LUSEED on SWMN, direct PU without INCLUD0E	<p>If you use the LU-SEED parameter on the channel-attached router, the LU names on the router are created according to the LU-SEED parameter. The LU names in VTAM are created according to VTAM LUSEED parameter. This means that the LU names might not match. It is a good idea to make LU-SEED parameters on the router and in VTAM identical. However, the TN3270 Server will learn the name of the LU from the first Bind received (if it carries the SLU name).</p> <p>If you do not use the LU-SEED parameter on the channel-attached router, the LU names on the router default to the first six characters of the configured PU followed by the two-byte hexadecimal number of the respective LOCADDR of this LU. If you want the LU names to be identical on the router and in VTAM, you must create the VTAM LU names according to the naming convention described above.</p>

Note: If the LUSEED is not configured in VTAM, then you cannot use the DDDLU function.

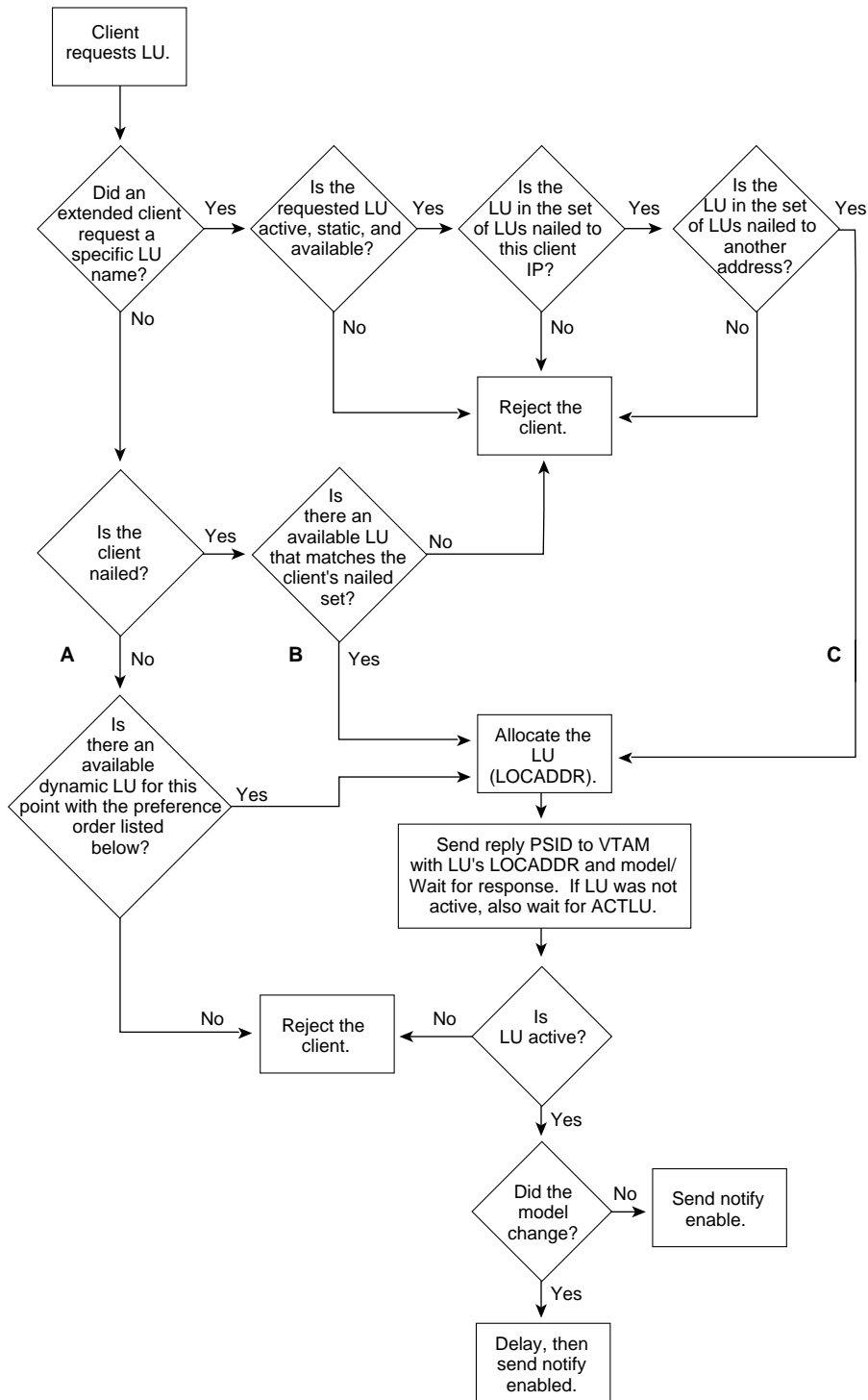
LU Selection Algorithm

When a user requests an LU from the LU pool, an allocation algorithm that reuses resources is used. The algorithm gives preference to LUs that are already active, provided the last use was with the same model as the new client. In the following two situations the algorithm will choose an LU that has not been used before:

- If the used LU was last used with a different model.
- If the last time the LU was used there was a failure on the mainframe side (a time-out occurred while getting the ACTLU or Bind/USS10). If such a failure occurs, the LU is moved to the “bad” list.

Figure 2-3 illustrates the decision process used by the LU selection algorithm.

Figure 2-3 LU Selection Algorithm



Preference order:

- 1) Active, correct model, 2) Inactive, no model, 3) Active, wrong model, 4) Active, correct model, but had a prior problem?

Addressing LAN Printing Requirements

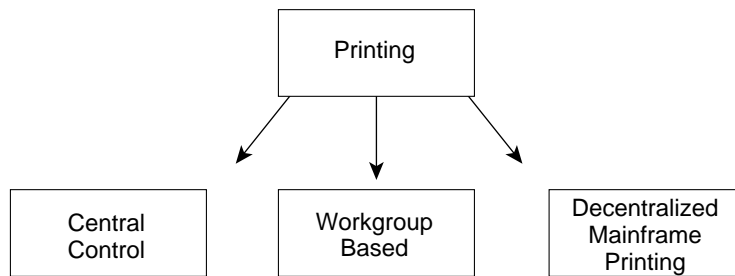
In the past, large amounts of mainframe print output would be printed in the data center and then distributed to the various branch offices overnight. Today, users expect the ability to print the host output on a LAN printer and also to specify which LAN printer is used. For various groups, such as a sales group, this may mean that the same type of output will be printed to different offices, depending on where they are traveling that week. This situation raises two immediate concerns, first is security of document and second is control of printing.

Printing security of document printing can be resolved by specifying the client LU naming parameter. This restricts access to an LU to only a particular IP address or group of IP addresses. This control is important for groups such as a personnel department.

Printing control is more difficult to address.

Figure 2-4 illustrates the control of a printing environment. The printing output is the starting point and the control of this output can be controlled with one or many of the three choices.

Figure 2-4 Control of a Printing Environment




Central control indicates that the print definition setup and print allocation is controlled from the mainframe. This choice is the least flexible of all the options and requires the most maintenance to control. Central control printer administration means that the printer LU and printer output definitions are statically defined in the mainframe printer application.

Workgroup-based printing is the recommended option for departments that share a common printer. The workgroup option works with the central control option. A group of printers is defined for a particular output group or groups and all printer output is sent there. Workgroup-based printing does not require central control. This option requires less control at the mainframe application and makes host modifications easier. This option works well when old PCs (386/486 PCs) are decommissioned and are reused as a permanent print servers.

Decentralized mainframe printing is ideal for the traveling client. This option allows clients to specify the LU name (using the TN3270E function) for their output and to receive their print output regardless of where they are logged in. This provides greater flexibility, but it comes with a price. For every client that uses this option, there must be a separate printer LU.

Which method you choose to manage your LAN printing depends upon your client requirements. The most commonly implemented solution is to use workgroup-based printing for permanently located groups and decentralized mainframe printing for the roaming client.



The client nailing feature of Cisco's TN3270 Server simplifies mainframe printing. If you have statically defined printer sessions, it is necessary to have printer LUs predefined in the switched major node. The client must request the name of one of these printer LUs. If the client requests the name of a printer that is already in use, then the session request is rejected. With LU nailing, you can use the **client printer ip** command to define printers for a client. LU nailing provides a better method of defining printers for a client because the assignment is centrally managed and the client cannot request an incorrect LU.

Addressing SNA Routing in Multi-Domain Environments

Another requirement is the ability to route traffic through the TN3270 server to data application without routing the traffic through the VTAM, which could be on a different host. To allow this, APPN is installed on the hosts and on the TN3270 Server router.

Note: Separate APPN code is not required on the router as the necessary code is part of the TN3270 Server. A separate license fee is incurred for this feature.

To enable the TN3270 session to pass between the router and VTAM an LU 6.2 session pipe is established between the DLUR, which is the Cisco router, and the DLUS, which is VTAM. Once a pair of LU 6.2 sessions has been brought up between the DLUR and DLUS, dependent PU/LU flows (SSCP-to-PU and SSCP-to-LU sessions) are encapsulated over the LU 6.2 sessions between the DLUR and DLUS SSCP. These LU 6.2 sessions are known as the control point (CP)-to-server pipe. In this way, SSCP services are provided from VTAM without requiring the distribution of SSCP code or definition.

When the SNA network uses APPN and the TN3270 Server can reach multiple hosts, we recommend that you use DLUR and configure your PUs under DLUR. You can also use DLUR to reach a mix of APPN and non-APPN hosts. The host that owns the PUs must be an APPN network node. When a secondary LU starts a session with any of the APPN hosts, it can use session switching to reach that host directly. When it starts a session with a non-APPN host, the traffic is routed through the owning host.

The implementation of DLUR/DLUS requires no changes to existing applications or dependent terminals. DLUR requires VTAM Version 4.2 or later with APPN activated and VTAM configured as a network node(NN). VTAM can be configured either a pure NN or an interchange node (ICN). To implement session switching requires additional knowledge of the VTAM configuration and the implementation of the APPN network.

How DLUR and DLUS Works

All dependent LUs, and the PUs that support them, require sessions to their owning SSCP. These sessions carry various control messages and management requests. These messages always take the form of SSCP-to-PU and SSCP-to-LU sessions that cannot cross domain boundaries or network boundaries. A PU serving dependent LUs must be connected directly to its owning VTAM or to a CIP or CPA connected to that VTAM.

In addition, routing in a subarea network is always done at the subarea level. In other words, any session involving a dependent LU must pass through the same adjacent subarea node as the SSCP-to-LU session, even if the dependent LU happens to reside in an APPN node.

To address these restrictions, the DLUS and DLUR were created.

The DLUS is a product feature (APPN option set 1066) of a T5 (VTAM) network node supporting session services extensions. The DLUS function enables VTAM to provide SSCP services for dependent LUs in remote APPN ENs or NNs. The DLUS provides SSCP services through standard SSCP-to-PU and SSCP-to-LU session flows that are encapsulated and sent over LU 6.2 sessions.

The DLUR is a function (APPN option set 1067) of an APPN EN or NN that owns dependent LUs but obtains services from a DLUS. The DLUR function is configured on the CIP or CPA under the TN3270 Server. The PUs are defined under the DLUR statement. The hierarchical structure is: TN3270 Server, DLUR, and PU. The DLUR function provides a remote boundary function for dependent LUs; that is, it removes the requirement that a node supporting dependent LUs must be adjacent to a subarea boundary node.

DLUR/DLUS removes these restrictions by providing the following functions:

- The session between the dependent LU (or PU) and its SSCP is encapsulated in an LU 6.2 pipe.

This CP-to-server pipe consists of a pair of sessions between the CPs in the DLUR and DLUS nodes. These sessions are called CPSVRMGR sessions. The pipe can carry a number of SSCP-to-PU and SSCP-to-LU sessions and does not need to be between adjacent CPs. The pipe can cross network boundaries.

- LU-to-LU session routing is performed by the APPN function, not the subarea function.

When a primary LU requests a search for a dependent LU, it normally receives a positive response from the DLUS, not the DLUR. The response identifies the DLUS as the server for the dependent LU and includes the correct CP name (the DLUR). The route can then be calculated directly to the DLUR, typically by the NN server of the primary LU (which is never the dependent LU). In cases where the DLUR supports cross-network CPSVRMGR sessions, the DLUR may respond to a search, but it still indicates that it is the owning CP.

Because the DLUS presents itself as the NN server for the dependent LUs, it must always be an NN.

Using the DLUR/DLUS, or CP-to-server pipe, SSCP-to-PU and SSCP-to-LU control messages can be exchanged between VTAM, the PU, and the local dependent LUs. SSCP-to-PU and SSCP-to-LU control messages are required for PU and LU activation and to initiate LU-to-LU session establishment. LU-LU sessions can, for example, be initiated by a LOGON request from a terminal operator. The LOGON request is forwarded to VTAM, which locates the destination LU using existing subarea (SSCP-to-SSCP) or APPN (CP-to-CP) data flows. Following the activation flows, the primary LU sends a BIND to establish the session. The BIND, and successive LU-to-LU session data, will be using the best route between the two session partners for the desired Class of Service (COS).

When you plan to use DLUR/DLUS, remember the following guidelines:

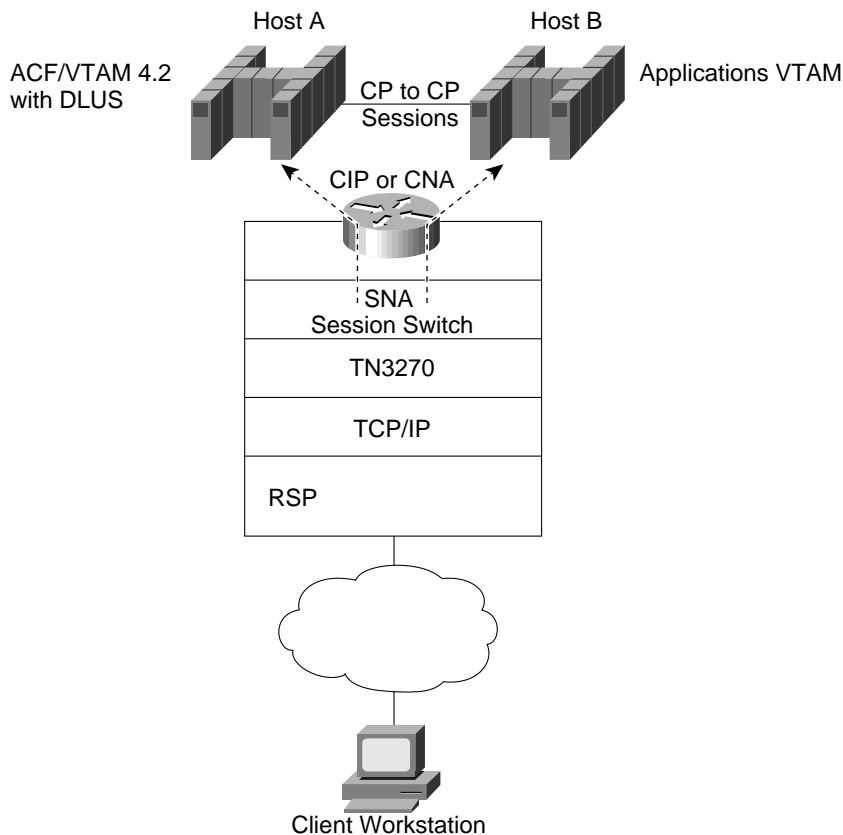
- To participate in an APPN network, a VTAM APPN EN must have an extended session services-capable NN server if it is to do any type of session initiation other than LU 6.2. Currently this function is only provided in VTAM, so all VTAM ENs must have VTAM NNs as their NN servers.
- The DLUS feature in VTAM is offered only on NNs. A VTAM EN cannot be a DLUS.
- The APPN EN TN3270 DLUR function allows you to route TN3270 LUs to multiple VTAM hosts from the CIP or CPA rather than on the VTAM hosts. This feature is particularly useful with the introduction of the new multi-CPU Complementary Metal Oxide Semiconductor (CMOS) mainframe, which is composed of up to 16 CPUs that appear as separate VTAMs.

How Session Switching Works

The LUs implemented by the TN3270 Server are dependent LUs. To route these dependent LU sessions to multiple VTAM hosts connected to the server in the channel-attached router (rather than routing in the VTAM hosts), the TN3270 Server implements an SNA session switch with the EN DLUR function.

Figure 2-5 illustrates how session switching works.

Figure 2-5 How Session Switching Works



To illustrate how session switching works, consider the situation in which a client's owning VTAM is on Host A and the client wants to reach an application on Host B:

- Without a subarea network, the client would be continuously routed from VTAM A to VTAM B. This process causes the mainframe to expend cycles performing the routing function.
- If you migrate the host to an ICN, the subarea network still exists and the APPN functionality is now available. Using the TN3270 Server installed on the channel-attached router and the DLUR function of VTAM, the Cisco router can session switch the user to Host B without passing through Host A.

To implement session switching, a CP-to-CP session between the two VTAMs is required. This can be achieved three ways:

- CP-to-CP connection using the DIAL parameter and not implementing APPN on the router

- CP-to-CP connection using virtual routing node parameters and implementing APPN on the router using the connection network configuration
- CP-to-CP connection configuring APPN with VTAM and implementing APPN on the router using the NN configuration

Addressing End User Service Level Requirements

As traffic on the Internet increases, there is increased congestion. One way to address this problem is to discriminate between different types of traffic and provide the appropriate quality of service (QoS). For example, interactive traffic should have a higher priority than bulk data transfer. IP precedence and type of service (ToS) is part of the IP specification that provides this prioritization.

The TN3270 Server allows you to specify IP precedence and ToS. At the protocol level, IP precedence allows a router network to discriminate between different types of traffic by assigning different priorities to them. IP ToS allows router networks to discriminate between different types of traffic by assigning different routing characteristics to them. Precedence and ToS values complement one another and provide flexibility in managing your network traffic.

In TN3270 Server, two types of TN3270 clients can be connected: screens or printers. Screens are interactive and printers need bulk data transfer. IP ToS and IP precedence allow you to discriminate between these types of sessions and assign different precedence values to the interactive connection and the bulk data connection.


IP ToS and IP precedence values can be specified for either the TN3270 Server as a whole or individual PUs. Values can be specified on both levels, in which case *siftdown* determines the value on an individual PU. Siftdown allows you to configure values that apply to all entities of the server in TN3270 Server configuration and to configure values for individual PUs at the PU configuration mode.

The Cisco implementation of IP precedence allows values of 0 to 7. The Cisco implementation of ToS allows values from 0 to 15. It is up to the administrator to choose values consistent with organizational policies when configuring IP precedence and ToS. Also, whether these values work depends on what the organization or Internet Service Provider's (ISP's) router does with packets with different IP ToS/precedence values. If you are using a Cisco router network, configuring weighted fair queuing (WFQ) or priority queuing allow you to prioritize traffic using IP precedence. The Open Shortest Path First (OSPF) protocol can discriminate between different routes based on IP ToS value; functions such as WFQ and NetFlow switching are also affected by ToS values.

Addressing Availability Requirements (Redundancy/Load Balancing)

Moving the 3270 access from the host to an outboard server provides many benefits, but also raises the issues of server redundancy. Having a "single point of failure" is an issue for sites that cannot allow for disruptive session failure. With legacy SNA, when a path is broken, the session is lost and the user must reconnect. With the outboard gateways, the data travels from the client to the server via TCP and then from the server to VTAM via SNA. As a result, any loss between the server and VTAM will result in a disrupted session.

Cisco offers several options for providing redundancy, including LocalDirector, DistributedDirector, and Hot Standby Router Protocol (HSRP).



Note: If you need to use client LU nailing and provide redundancy, the solution is difficult. With LU nailing, requesting a specific LU for an IP address requires a connection to a specific PU and TN3270 Server. A secondary TN3270 Server cannot be used to service these clients. In this case, we could use HSRP. HSRP provides redundancy, but does not provide load balancing.

LocalDirector

LocalDirector dynamically load-balances traffic between multiple servers to ensure timely access and response to requests. It is independent of domain name servers and applications; rather, it functions as a front end to a group of servers by load balancing traffic demands between servers and speeding user access to server-based applications. Servers can be added and removed transparently, but to end users LocalDirector provides the appearance of a single, virtual server.

LocalDirector is a high-performance networking device with over 45 Mbps throughput. It supports up to 8,000 virtual IP addresses and domain names. It can also direct traffic to 8,000 servers that can be a collection of heterogeneous hardware platforms and operating systems, and it efficiently handles over 700,000 simultaneous TCP connections.

In addition to its directing capabilities, LocalDirector also serves as a simple bridge to forward data packets between its interfaces. This bridging ensures that LocalDirector does not interfere with network operation while it is in service and it can be brought online immediately after powering up without affecting network connectivity.

The LocalDirector does not use Domain Name System (DNS) for domain name lookup. Networks without a DNS or that do not require their TN3270 sessions to reference the DNS for mainframe connectivity are suited to use the LocalDirector.

Most data centers implement a redundant CIP or CPA and TN3270 Server solution to create multiple IP addresses for the end user to reference for host connectivity. LocalDirector is installed with the TN3270 Server to provide consolidation of the IP addresses and load balancing.

The IP addressing consolidation is achieved by creating a virtual IP address on the LocalDirector. The real IP addresses, as defined in the TN3270 Server, are included in the LocalDirector. The real IP addresses are bound to the virtual address creating a pool of host connection addresses. A typical configuration binds all the real IP addresses to a single virtual IP address, which creates a simple environment to administer. There is a range of configuration possibilities available, such as creating multiple virtual addresses and allocating a particular address to a particular group or region. The best type of virtual address allocation will depend on the needs of the company.

DistributedDirector

DistributedDirector can be run on either a Cisco 2500 or 4700-M router. With DistributedDirector, users need only a single DNS host name or URL-embedded host name for accessing a globally distributed set of servers, thus providing the appearance of a single virtual server. This eliminates the need for users to choose a server from a list of possible sites.

DistributedDirector enables transparent distribution of all common TCP/IP network services, such as Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Telnet, TN3270, and gopher.

Using the Director Response Protocol (DRP), a simple User Datagram Protocol (UDP)-based application developed by Cisco, the Director can query properly configured Cisco routers in the field for Exterior Gateway Protocol (EGP) and Internal Gateway Protocol (IGP) topological “distance” metrics. With this information and other configuration metrics, the Director can assign an optimal distributed server to each client. As a result, users can be transparently and automatically assigned a distributed server anywhere on the Internet.

DistributedDirector monitors the status of the TN3270 Server by opening a Telnet port. If DistributedDirector cannot open the port it marks the server as unavailable.

DistributedDirector works in conjunction with a DNS server. More than one DistributedDirector can exist in the network. For redundancy, we suggest that you install one DistributedDirector on every major DNS server.

DNS

The use of either LocalDirector or DistributedDirector is not the only option to provide redundancy. DNS is also a valid option. To provide redundancy using DNS, you must install more than one TN3270 Server. For each TN3270 Server, assign all the PUs to the same IP listening address. Configure the DNS server to include a DNS entry for all the defined IP listening addresses. The result is that the client requests a server and the request is processed using a round-robin method. The disadvantage of this method is that a client still may be sent to an inactive TN3270 Server because the DNS server does not have the capability to monitor the status of the TN3270 Servers. Also, because some clients ignore IP addresses returned by a DNS server after the initial response, this solution may not work for all clients.

Satisfying Expanding Network Address Requirements

For VTAM to control routing in a network, it must know the location of its resources (LUs, PUs, and other SSCPs). VTAM uses element addresses in conjunction with the subarea address to identify the location of resources (also known as network addressable units[NAUs]). The subarea address indicates where the resource is located; the element address indicates the unique address within the subarea.

Minor nodes, such as an application program or LU, require a single element address. Some minor nodes, such as local non-SNA devices and application programs that use parallel sessions, require more than one element address. This requirement increases the number of element addresses that are used in a subarea.

These element addresses are available up to various ranges dependent on the level of VTAM. The TN3270 Server supports the following methods of addressing:

- Pre-extended network addressing—Used by releases prior to VTAM V3R1. Prior to extended network addressing, you could define 255 subareas and 254 elements.
- Extended network addressing—Used by VTAM V3R1 and releases prior to VTAM V3R2. Extended network addressing supports 255 subarea address and extends element addressing to 32,768 elements.
- Extended subarea addressing—Used by VTAM V3R2 (with compatibility PTF) and later. Extended subarea addressing increased the size of the subarea addresses to 65535 and the number of explicit routes for each destination subarea to 16.

Use the MAXSUBA start option or the MAXSUBA operand in NCP to enable communication between subareas with different addressing structures. The MAXSUBA start option specifies the highest subarea value used in the network. A MAXSUBA of 63, for example, defines a network with up to 63 subareas and 1024 elements in each

subarea. You must code the MAXSUBA start option in VTAM's start option list if you want VTAM to communicate with nonextended addressing nodes or if the MAXSUBA operand is coded in an NCP with which VTAM communicates.

Note: According the IBM announcement letter 298-049 dated February 24, 1998, the APAR OW31455 increases the number of subarea elements from 64,000 to 1.6 million LUs. The APAR applies only to OS/390 R5 and later.

TN3270 Configuration

For TN3270 configuration, the mainframe remains the same as with a PU 2.1 definition. A switched major node member in SYS1.VTAMLST is defined and, within that member, the PU is defined. The LU definitions within each PU can be defined statically or dynamically. A static LU definition means that each LU with a LOCADDR parameter is hard-coded within the switched major node member. A dynamic LU is defined using DDDLUs.

TN3270 Server Configuration Modes

There are several TN3270 configuration modes and router command prompts that you use when configuring the TN3270 Server. These configuration modes and command prompts are described in this section. The TN3270 Server can be configured only on port 2, the internal LAN port, of a CIP card or port 0 of the CPA.

TN3270 configuration modes described in this section include the following:

- TN3270 Server Configuration Mode
- DLUR Configuration Mode
- DLUR SAP Configuration Mode
- PU Configuration Mode

The following sections describe how to move within configuration modes and identify the configuration commands:

- Moving Between Configuration Modes
- Commands Allowed in Multiple Modes

TN3270 Server Configuration Mode

From interface configuration mode, the **tn3270-server** command puts you in TN3270 Server configuration mode.

The following prompt appears:

```
tn3270-server>
```

DLUR Configuration Mode

From TN3270 Server configuration mode, the **dlur** command puts you in DLUR configuration mode.

The following prompt appears:

```
tn3270-dlur>
```

DLUR SAP Configuration Mode

From DLUR server configuration mode, the **lsap** command puts you in DLUR SAP configuration mode.

The following prompt appears:

```
tn3270-dlur-lsap>
```

PU Configuration Mode

You access the PU configuration mode from the TN3270 Server configuration mode or from the DLUR configuration mode. In either mode, the **pu** command puts you in PU configuration mode.

For direct PUs, from TN3270 configuration mode issue the **pu** command to create a new PU:

```
pu pu-name idblk-idnum ip-address type adapno lsap [rmac rmac] [rsap rsap] [lu-seed lu-name-stem]
```

The following prompt appears:

```
tn3270-pu>
```

For DLUR PUs, from DLUR configuration mode issue the **pu** command to create a new PU:

```
pu pu-name idblk-idnum ip-address
```

The following prompt appears:

```
tn3270-dlur-pu>
```

From either mode, to return to PU configuration mode on PU *pu-name* the command is:

```
pu pu-name
```

Moving Between Configuration Modes

Some configuration commands create entities on the CIP or CPA. For most of these, the command changes to the mode associated with that entity (for example, a PU). In general, the parameters provided to create the entity come in two sets: those that identify the specific instance of the entity (for example, a PU name) and those that merely set operating parameters. To return to the mode, the same command is used but with only the first set of parameters. Tables 2-2, 2-3, and 2-4 show example tasks to return to a command mode without creating a new entity.

To create a DLUR LSAP and enter DLUR LSAP configuration mode, perform the following task beginning in TN3270 DLUR configuration mode:

Table 2-2 DLUR LSAP Configuration Mode

Task	Command
Create a DLUR LSAP and enter DLUR LSAP configuration mode.	lsap token-adapter 1 84

To return later to the DLUR LSAP configuration mode on the same entity, perform the following task beginning in TN3270 DLUR configuration mode:

Table 2-3 Returning to DLUR LSAP Configuration Mode

Task	Command
Enter DLUR LSAP configuration mode on the same LSAP.	lsap token-adapter 1

To remove an entity, the same identification parameters are needed. Perform the following task beginning in TN3270 DLUR configuration mode:

Table 2-4 Removing a DLUR LSAP Entity

Task	Command
Remove a previously defined DLUR LSAP entity.	no lsap token-adapter 1

Commands Allowed in Multiple Modes

The following commands are valid in TN3270 configuration mode or in either variation of PU configuration mode:

- **generic-pool** {**permit** | **deny**}
- **idle-time** *seconds*
- **ip precedence** {**screen** | **printer**} *value*
- **ip tos** {**screen** | **printer**} *value*
- **keepalive** *seconds*
- **shutdown**
- **tcp-port** *port-number*
- **unbind-action** {**keep** | **disconnect**}

Values entered in PU configuration mode override settings made in TN3270 configuration mode. In addition, the **no** form of these commands entered in PU configuration mode will restore the command value entered in TN3270 command mode.

Configuring the TN3270 Server

This section describes how to configure TN3270 Server support on the CIP and CPA for the following:

- Configuring Multiple APPN Hosts
- Configuring Non-APPN Hosts

Not all tasks are required.

Note: The TN3270 Server is configured on the virtual interface, which is port 2 of a CIP or CPA.

Configuring Multiple APPN Hosts

When the host site uses APPN and the TN3270 Server can reach multiple mainframe hosts, we recommend that you use DLUR and configure your PUs under DLUR by performing the following tasks:

- Configuring SNA Support
- Initiating the TN3270 Server
- Configuring IP Precedence and ToS Support (Optional)
- Configuring DLUR Parameters

- Configuring SAPs under DLUR
- Configuring PUs under DLUR
- Configuring LU Nailing (Optional)

Note: You can also use DLUR to reach a mix of APPN and non-APPN hosts. The host owning the PUs must be an APPN NN that also supports the subarea (that is, an ICN). When an SLU starts a session with any of the APPN hosts, it can use session switching to reach that host directly. When it starts a session with a non-APPN host, the traffic is routed through the owning host.

Configuring Non-APPN Hosts

When the host site does not use APPN, you configure your PU parameters for a directly connected mainframe host by performing the following tasks:

- Configuring SNA Support
- Initiating the TN3270 Server
- Configuring IP Precedence and ToS Support (Optional)
- Configuring PU Parameters on the TN3270 Server
- Configuring LU Nailing (Optional)

Configuring SNA Support

CSNA must be configured prior to configuring TN3270 support. Refer to the “Configure IBM Channel Attach for CSNA Support” section of the “Configuring IBM Channel Attach” chapter of the *IOS Bridging and IBM Networking Configuration Guide*.

Initiating the TN3270 Server

To establish a TN3270 Server on the internal LAN interface on the CIP, perform the following tasks (Table 2-5) beginning in global configuration mode:

Table 2-5 TN3270 Server Configuration Tasks

Task	Command
Select the channel attach internal LAN interface and enter interface configuration mode.	interface channel slot/2
Specify a TN3270 Server on the internal LAN interface and enter TN3270 configuration mode.	tn3270-server
(Optional) Configure maximum number of LUs allowed. This number is based on the number of sessions licensed.	maximum-lus max-number-of-lu-allocated
(Optional) Configure LU session limits for each client IP address or IP subnetwork address.	client [ip [ip-mask]] lu maximum number
(Optional) Configure transmission of a WILL TIMING-MARK.	timing-mark
(Optional) Assign a TCP port other than the default of 23. This command is also available in PU configuration mode.	tcp-port port-nbr

Table 2-5 TN3270 Server Configuration Tasks

Task	Command
(Optional) Specify the idle time for server disconnect. This command is also available in PU configuration mode.	idle-time <i>num-of-seconds</i>
(Optional) Specify the maximum time allowed between keepalive marks before the server disconnects. This command is also available in PU configuration mode.	keepalive <i>num-of-seconds</i>
(Optional) Specify whether the TN3270 session will disconnect when an UNBIND command is received. This command is also available in PU configuration mode.	unbind-action { keep disconnect }
(Optional) Select whether “left-over” LUs can be used from a generic LU pool. This command is also available in PU configuration mode.	generic-pool { permit deny }

When you use the **tn3270-server** command, you enter TN3270 configuration mode and are able to use all other commands in the task list. You can override many configuration values you enter in TN3270 configuration mode from PU configuration mode. On IBM host systems, these types of commands are often referred to as “sift-down” commands because their values sift down through several levels of configuration and can be optionally altered at each configuration level.

Maximum-LUs Command

The **maximum-lus** command sets a limit on the number of LU control blocks that are allocated for the TN3270 Server. It can be used to prevent the TN3270 Server from inhibiting other applications on the CIP or CPA.

The TN3270 Server attempts to allocate one LU control block for each LU activated by the hosts. For DDDL, the control block is allocated when the client requests the LU (in anticipation of an ACTLU from the mainframe host).

Valid values are from 0 to 32000. The default is 2100. However, memory and other limitations may prevent the maximum value from being achieved. Although this value may be changed at any time, reducing it below the number currently allocated will not force control blocks to be released. In fact, no LU control blocks will be released to the system until the PU is inactivated.

Idle Time Disconnect Command

The **idle time disconnect** command specifies the number of seconds of LU inactivity, from both host and client, before the TN3270 session is disconnected. Specifying zero seconds means that LU sessions are not disconnected when inactive.

Keepalive Command

Use the **keepalive** command (when issued under the TN3270 command context) to monitor active LUs. For example, **keepalive 600** sends a Telnet TIMING-MARK every 10 minutes if there is no other traffic flowing between the server and the client. If, after a timeout period of between one and three minutes, the end client does not respond, then the CIP or CPA disconnects the session. This action is useful for cleaning up partially disconnected TCP sessions.

If you are using static LUs, then use one of the following code releases: CIP22-27, CIP24-5 or CIP25-6 and higher. These releases handle partially disconnected sessions without use of the **keepalive** command.

UNBIND-Action Command

A session unbind (specified using the **unbind-action** command) indicates whether or not a TN3270 session is disconnected upon UNBIND. A value of *disconnect* indicates that the TN3270 Server disconnects the TN3270 client upon receipt of an UNBIND. A value of *keep* indicates that no automatic disconnect is made by the TN3270 Server upon receipt of an UNBIND.

Generic-pool Command

Use the **generic-pool** TN3270 configuration command to specify whether or not leftover LUs are made available to TN3270 sessions that do not request a specific LU or LU pool through TN3270E. A leftover LU is an LU from the pool of dynamic LUs that you have specify in the switched major node using the LU-SEED parameter and the LUGROUP parameter.

The **generic-pool** command can be used as a global TN3270-server command, but is also used in PU-configuration mode to change the value (permit or deny) for specific PUs:

- **generic-pool permit**—This is the default. Left over LUs can be used by clients that request a generic session (non-TN3270E-clients; or TN3270E-clients).
- **generic-pool deny**—The TN3270 Server will not attempt dynamic definition of any LUs on a PU. That is, only static LUs are supported. You might deny the use of the generic pool for security reasons.

Older TN3270 clients cannot request an LU session using a specific LU name. In earlier versions of the Cisco IOS software, the **generic-pool deny** command prevented non-TN3270E clients from obtaining a session. But with the current release of the Cisco IOS software you can nail LUs to IP addresses in the router configuration. This feature allows non-TN3270E clients to establish a session even if the **generic-pool deny** command has been specified.

Configuring IP Precedence and ToS Support (Optional)

There are two commands that support IP precedence and IP ToS.

To configure IP precedence, perform the following task (Table 2-6) in TN3270 Server or TN3270 PU configuration mode:

Table 2-6 IP Precedence Configuration Tasks

Task	Command
Configure the IP level.	ip precedence {screen printer} value

Use the **no ip precedence screen** or the **no ip precedence printer** command to return the precedence value to a default of 0.

To configure IP ToS, perform the following task (Table 2-7) in TN3270 Server or TN3270 PU configuration mode:

Table 2-7 IP ToS Configuration Tasks

Task	Command
Configure the IP ToS delay level.	ip tos {screen printer} value

Use the **no ip tos screen** or the **no ip tos printer** command to return the precedence value to a default of 0.

These commands can be specified in the TN3270 Server configuration mode the DLUR/Direct PU configuration mode. The commands affect all the LUs under the PU based on the siftdown value.

The default value for the IP precedence screen and printer parameters is 0. If IP precedence is not configured, the IP precedence field is set to 0 for both screen and printer. The default value for the IP ToS screen is 0.

When Telnet negotiation is taking place, IP precedence and IP ToS values of 0 are used. These values are used until the Bind takes place. If it is a type 2 Bind, the TN3270 client is assumed to be screen. Otherwise, it is assumed to be printer. These definitions of screen and printer might not be consistent with implementations in other configurations or products. The IP precedence and IP ToS values are used until the TN3270 session is terminated.

The **show** command displays four distinct values for IP precedence and the IP ToS. The values correspond to the screen and printer. The following example shows the IP precedence and IP ToS as displayed in the **show extended** command.

```
redback#show extended channel 3/2 tn3270-server

<current stats> <connection stats> <response time(ms)>
server-ip:tcp      lu in-use connect disconn fail host tcp
172.28.1.99:23    0  0  1  1  0  0  20
total             0  0
configured max_lu 2100
idle-time 3600    keepalive 1800    unbind-action disconnect
ip-preced-screen 0  ip-preced-printer 0  ip-tos-screen 0  ip-tos-printer 0
tcp-port 23      generic-pool permit no timing-mark
dlur MPX.REDBCP          status RESET
dlus MPX.NGMVMPC

name(index) ip:tcp xid state link destination r-lsap
PUS1(1) 172.28.1.99:23 05D19001 XID tok 0 4000.7470.00e7 08 A8
```

Configuring PU Parameters on the TN3270 Server

Configuring PU parameters is required when you configure PUs that do not use DLUR. To configure PU parameters for the TN3270 Server, perform the following tasks (Table 2-8) beginning in TN3270 configuration mode:

Table 2-8 PU Configuration Tasks

Task	Command
Enter PU configuration mode and create or delete PUs with direct host links.	pu <i>pu-name idblk-idnum ip-address type adapno lsap [rmac rmac] [rsap rsap] [lu-seed lu-name-stem]</i>
(Optional) Assign a TCP port other than the default of 23. This command is also available in TN3270 configuration mode.	tcp-port <i>port-nbr</i>
(Optional) Specify the idle time for server disconnect. This command is also available in TN3270 configuration mode.	idle-time <i>num-of-seconds</i>
(Optional) Specify the maximum time allowed between keepalive marks before the server disconnects. This command is also available in TN3270 configuration mode.	keepalive <i>num-of-seconds</i>

Table 2-8 PU Configuration Tasks

Task	Command
(Optional) Specify whether the TN3270 session will disconnect when an UNBIND command is received. This command is also available in TN3270 configuration mode.	unbind-action { keep disconnect }
(Optional) Select whether “leftover” LUs can be used from a generic LU pool. This command is also available in TN3270 configuration mode.	generic-pool { permit deny }

When you use the **pu** command, you enter PU configuration mode and can use all other commands in this task list. Configuration values you enter in PU configuration mode override other values entered while in TN3270 configuration mode. In addition, you can enter PU configuration mode from the DLUR configuration mode when configuring PUs that are connected by means of DLUR.

If you are configuring PUs for directly connected hosts, you need not perform any additional configuration tasks.

Configuring DLUR Parameters

Configuring DLUR parameters is required when if you configure DLUR connected hosts. To configure DLUR parameters for the TN3270 Server, perform the following tasks (Table 2-9) beginning in TN3270 configuration mode:

Table 2-9 DLUR Configuration Tasks

Task	Command
Create a DLUR function in the TN3270 Server and enter DLUR configuration mode.	dlur <i>fq-cpname fq-dlusname</i>
(Optional) Specify the fallback choice for the DLUR DLUS.	dlus-backup <i>dlusname2</i>
(Optional) Specify the preferred network node (NN) server.	preferred-nnserver <i>NNserver</i>

Configuring SAPs under DLUR

To configure SAPs under the DLUR function, perform the following tasks (Table 2-10) beginning in DLUR configuration mode:

Table 2-10 DLUR SAP Configuration Tasks

Task	Command
Create a SAP function under DLUR and enter DLUR SAP configuration mode.	lsap <i>type adapno [lsap]</i>
(Optional) Identify an APPN virtual routing node.	vrn <i>vrn-name</i>
(Optional) Create named links to hosts. A link should be configured to each potential NN server. (The alternative is to configure the NN servers to connect to DLUR.) If virtual routing node is used it is not necessary to configure links to other hosts. Do not configure multiple links to the same host.	link <i>name [rmac rmac] [rsap rsap]</i>

Configuring PUs under DLUR

This task is required when configuring DLUR connected hosts. To configure PUs under the DLUR function, perform the following tasks (Table 2-11) beginning in DLUR configuration mode:

Table 2-11 DLUR PU Configuration Tasks

Task	Command
Create a PU function under DLUR and enter PU configuration mode.	pu <i>pu-name idblk-idnum ip-address</i>
Assign a TCP port other than the default of 23.	tcp-port <i>port-nbr</i>
Specify the idle time for server disconnect.	idle-time <i>num-of-seconds</i>
Specify the maximum time allowed between keepalive marks before the server disconnects.	keepalive <i>num-of-seconds</i>
Specify whether the TN3270 session will disconnect when an UNBIND command is received.	unbind-action { keep disconnect }
Select whether “left over” LUs can be used from a generic LU pool.	generic-pool { permit deny }

Note: The **pu** command entered in DLUR configuration mode has different parameters than when it is entered from TN3270 configuration mode.

Configuring LU Nailing (Optional)

To configure LU nailing, perform the following task (Task 2-12) in TN3270 PU configuration mode:

Table 2-12 LU Nailing Configuration Tasks

Task	Command
Configure the IP address and nail type and specify the LOCADDR range.	client [printer] ip <i>ip-address [mask]</i> lu <i>first-locaddr [last-locaddr]</i>

The **client** command allows a client with multiple TN3270 connections from the same IP address to nail their screen connections to LUs that are configured as screen LUs at the host and to nail printer connections to LUs that are configured as printers at the host. When the connection is made, a device type of “328*” is matched to a printer definition, and any other device type is matched to a screen definition.

Creating a Pool of Static LUs Using LU Nailing

Unlike dynamic pools, the definition of static LUs does not allow LU pooling. Static LUs require the client to address the LU by name. To work around this problem, static LUs can be defined with a client IP statement that allows any user to access any LU. This parameter turns the static LUs into a pool of LUs.

In the following example, all clients in subnet 10.1.1.0 are assigned an LU in the range between LOCADDR 1 and 255:

```
PU PU1 0CB00001 10.8.8.8 token-adapter 0 48
CLIENT IP 10.1.1.0 255.255.255.0 LU 1 255
```

LU nailing also limits access to the TN3270 Server to a specific network. For example, if all the PUs specified use the “CLIENT IP 148.149.0.0 255.255.0.0 LU 1 255” command, then only clients on this specific network (148.149.0.0) have access to those PUs defined on the TN3270 Server.

Monitoring the TN3270 Server

Table 2-13 lists some of the monitoring tasks specific to the TN3270 Server. To display the full list of **show** commands, enter **show ?** at the EXEC prompt.

Use the following **show** command in privileged EXEC mode:

Table 2-13 Monitoring the TN3270 Server

Task	Command
Display the current server configuration parameters and the status of the PUs defined in each server.	show extended channel interface tn3270-server
Display the PU configuration parameters, statistics and all the LUs currently attached to the PU.	show extended channel interface tn3270-server pu pu-name
Display mappings between a nailed client IP address and nailed LUs	show extended channel interface tn3270-server nailed-ip ip-address
Display the status of the LU.	show extended channel interface tn3270-server pu pu-name lu lu-number [history]
Display the information about LUs that are defined under an IP address.	show extended channel interface tn3270-server client-ip-address ip-address
Display information about the DLUR components.	show extended channel interface tn3270-server dlur

Other methods of monitoring the TN3270 Server are discussed in Chapter 5, Network Management.

TN3270 Client Implementation

This chapter discusses the following aspects of TN3270 client implementation:

- How TN3270 Clients Work
- Types of TN3270 Clients
- TN3270 Client of OC://WebConnect Pro
- Cisco WebClient

How TN3270 Clients Work

As discussed in the previous chapters, the 3270 data stream used by SNA mainframe application is unique and requires special handling at the end user station. Initially, any of the 3270 terminals, such as the IBM 3278 and the IBM 3279, could accommodate the 3270 data stream. When organizations started replacing these 'dumb terminals' with PCs, companies created 3270 emulators (software that made the PC appear to the mainframe as a 3270 terminal). Prior to the integration of IP in SNA networks, 3270 emulators had three primary tasks:

- Negotiate a connection with the mainframe application using an LU name
- Interpret the control characters and data received from the mainframe application and display the information properly in the emulator window
- Format the user responses in a data stream, using control characters to indicate the format of the data, and forward the data to the mainframe application

Once companies started integrating an IP network between the mainframe application and the end user, TN3270 clients were introduced. The job of the TN3270 client is more complex than that of the 3270 emulator.

Because LU names are not relevant outside an SNA network, the session negotiation process involves more steps. Primarily, the allocation of an LU name to a client is handled by the TN3270 server. The client must, however, provide information about its terminal type and whether it is a standard TN3270 client or a TN3270E client.

With TN3270, the 3270 data stream is encapsulated in a Telnet message. Therefore, in addition to interpreting data and formatting responses, the TN3270 client must open the Telnet messages that it receives and extract the 3270 data. The client encapsulates the formatted responses in a Telnet message that is suitable for transport over an IP network.

Types of TN3270 Clients

When TN3270 was introduced, the new Telnet clients were created. Initially, the TN3270 clients offered for PCs were 16-bit clients based on existing Telnet clients. Later, as Windows 95 and Windows NT were introduced, 32-bit clients were developed. Similarly, UNIX-based Telnet clients were modified to accommodate the 3270 data stream. The result was X3270.

Later, Java-based Web clients were introduced for use with TN3270 connections. Because Java is a portable language, these clients overcome the problem of using a different TN3270 client for each operating system.

First-generation browser-to-host solutions did not provide support for all the options of TN3270. They lacked functionality because Java lacked functionality. Therefore, they were deployed only for point applications and not as general desktop replacements. They were used to provide mainframe access to new users, customers, suppliers, and partners, and were also used to provide remote access for mobile and home users.

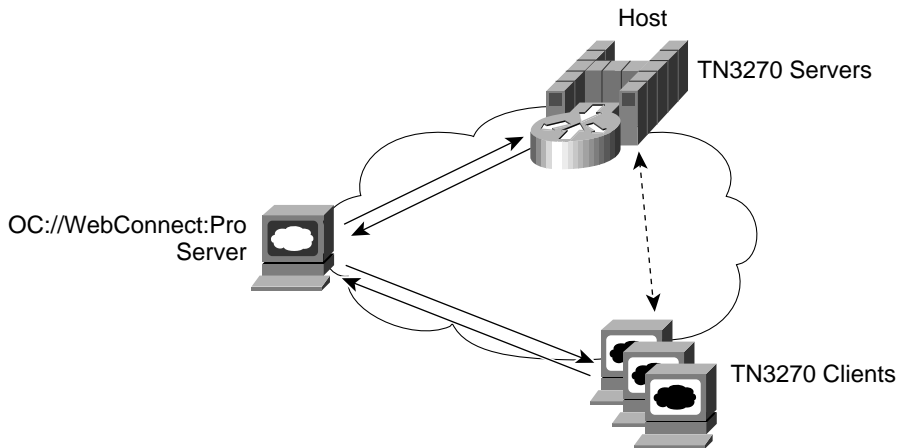
With the new version of Java, Java Developer's Kit (JDK) 1.1, these issues have been resolved. Second-generation browser-to-host solutions now include support for local and SNA printing, copy and paste functions, and INDSFILE transfers, making them viable desktop replacements.

Within the realm of Web-based TN3270 clients, there are two types of solutions: three-tier and two-tier.

With a three-tier solution (Figure 3-1), three network devices are required to access the mainframe. Using a Web browser, the user accesses a specified Web server and selects various options. The Web server replies by sending a Java applet that is stored in cache on the user's end station. The Java applet opens a socket connection to OC://WebConnect Pro. The OC://WebConnect Pro daemon establishes a connection to the TN3270 server, which establishes a connection to the mainframe application. All communication between the user and the mainframe application passes through three devices: the Web browser on the end station, the Web server, and the TN3270 server. Because the Java applet is stored temporarily in cache, if the connection is lost or times out, the entire process must be repeated. The advantage of this design is that only required screen output is sent to the client. The OC://WebConnect Pro server knows the current screen output and will not retransmit existing screen information. This can significantly reduce the amount of data transmitted between the OC://WebConnect Pro server and the client.

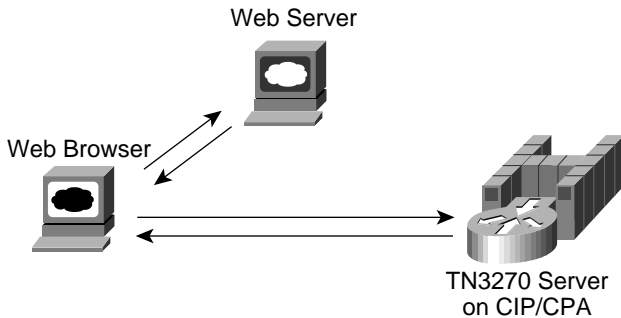
The OC://WebConnect Pro server also provides access to other platforms, such as AS/400 via 5250 and UNIX via VT. This provides a central point of administration of all Telnet sessions and allows a single configuration change to be shared automatically between all clients.

Figure 3-1 Three-tier TN3270 Web Client Solution



With a two-tier solution (Figure 3-2), communication between the user and the mainframe requires only two devices (although three network devices are required initially). With a two-tier solution, the user starts at the Web browser and accesses a specified Web server. The Web server replies by sending a Java applet that is installed on the end station. This Java applet allows the user to establish a connection directly with the TN3270 server (the Web server is no longer required). From then on, the only time that the user would need to access the Web server is to load an upgraded version of the Java applet.

Figure 3-2 Two-tier TN3270 Web Client Solution



TN3270 Client of OC://WebConnect Pro

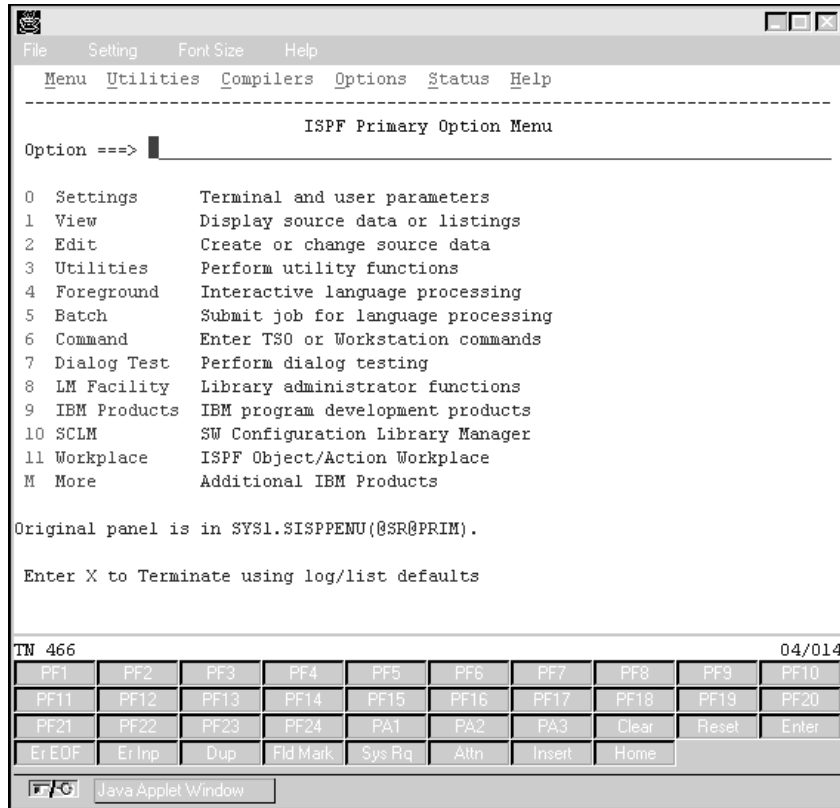
OC://WebConnect Pro is a three-tier TN3270 Web client solution offered by Cisco. It enables mainframe access to Web clients without requiring special software. The client requires only a Java-capable Web browser. In addition, no changes are required at the mainframe.

The OC://WebConnect server runs on HP/UX, Sun Solaris, IBM AIX, or Windows NT servers. Once the server is installed, the end user simply accesses the appropriate URL and, after the client is authorized, a Java applet is downloaded to the client PC. This Java applet provides a 3270-like screen capability and allows the user to log on to mainframe applications using a secure, persistent session. OC://WebConnect Pro uses encryption code, which is downloaded with the Java applet, to protect data flowing between the client and the OC://WebConnect Pro server.

The OC://WebConnect Pro server interoperates with any standard TCP/IP server or gateway including the Cisco Mainframe Channel Connection (CMCC) TN3270 Server. To the mainframe, the OC://WebConnect Pro server appears to be a standard TN3270 or TN3270E client.

To the end user, the Web interface looks like a typical TN3270 client, as shown in Figure 3-3.

Figure 3-3 OC://WebConnect Pro TN3270 Window



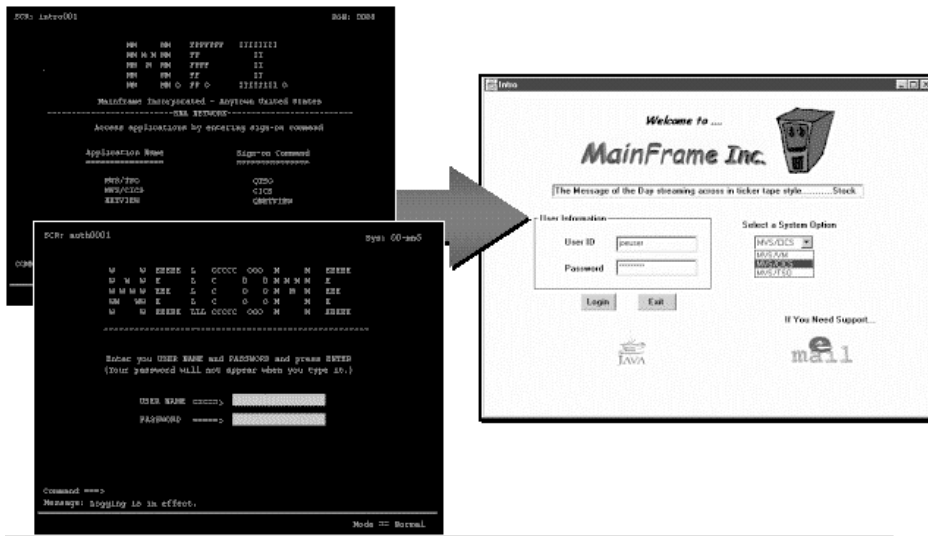
Hot Spots are a configurable option with the Automatic GUI. Host session action keys (such as PF3, PF7, and PF8) become “clickable.” For example, a user can double click on the PF3 function key to execute an exit sequence.

Optionally, you can use the OpenVista component of OC://WebConnect Pro to “update” the appearance of the 3270 screen. The Automatic GUI option enables instant transformation of “green screens” into the familiar “Web like” GUI.

OpenVista (a component of OC://WebConnect Pro) allows an easy rejuvenation of the green-screen interface to the new, standard Web-style interface. It runs on all major UNIX platforms and Windows NT. OpenVista creates the Java code that is downloaded to individual desktops when a rejuvenated application is initiated.

With OpenVista, you can consolidate multiple screens onto a single screen, thus enhancing end-user productivity. Figure 3-4 shows a traditional sign-on screen and a traditional authentication screen combined into a single screen.

Figure 3-4 OpenVista Screen Consolidation



OC://WebConnect Pro offers the following features:

- Printing—Print the 3270 or Java screen to a local or networked printer. OC://WebConnect Pro supports 3287 printing to a local or networked printer.
- File transfers—INDSFILE transfers are enabled. (LU 0 or LU 6.2 file transfers are not enabled.)
- Copy and paste—Data can be copied from the Java screen and pasted into a desktop application such as Word, Excel, or PowerPoint.
- Font support—With Automatic Font Sizing, when a session window is resized by the user, all text displayed is resized to fit within the new session window.
- Multiple language support—Double-byte character support enables applications to support Japanese, Korean, and Chinese characters.
- Security—Support is provided for Secure Sockets Layer (SSL) for server and message authentication. SSL provides a means for the server and the client to authenticate each other. Once authentication is complete, they negotiate the type of encryption algorithm and cryptographic key they will use. OC://WebConnect Pro supports either DES or RSA RC2/4 encryption (40 bit or 128 bit) between the NT or UNIX server and the browser so that all data flows are encrypted. In addition, it maintains a secure connection between the server and the mainframe. Unlike HTML conversion approaches, there is a persistent connection between client and server. If the user closes the OC://WebConnect Pro window on the desktop, the upstream TN3270 session is automatically disconnected. The connection between the browser and the server is a proprietary data stream over IP, and is designed so that the amount of data downloaded to the browser and the ensuing flow of session data make optimum use of the bandwidth to the browser.

To enhance scalability, OC://WebConnect Pro can determine whether a TN3270 Server has available LUs. (It is possible for a product such as LocalDirector to indicate that a TN3270 server is available from an IP perspective, when in fact the server may be out of LUs.) OC://WebConnect Pro cycles through available TN3270 Servers until it finds one with available LUs.

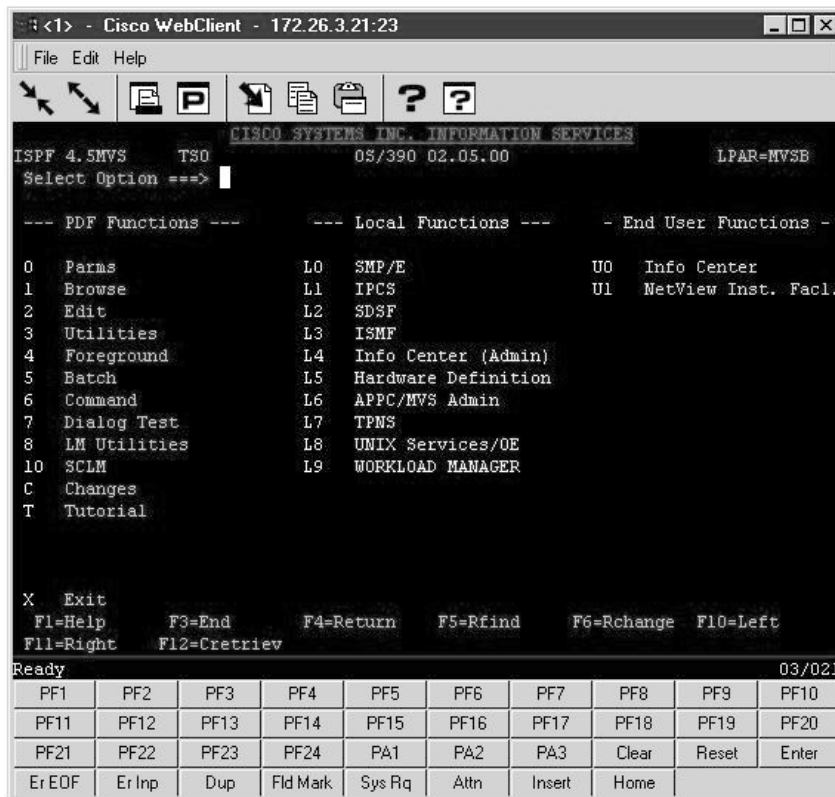
Administrators can choose the functions to which users have access by selecting from three applets; Ultra Lite, Enhanced, and Power user.

- Ultra Lite—Provides standard screen and keyboard support for 3270, 5250, and VT220 applications, but no support for cut and paste or file transfers.
- Enhanced—Adds printing and selectable client session types (3270, 5250, or VT220), which shortens download time.
- Power User—Includes printing, INDSFILE transfer, automatic GUI, and Hot Spots. This option is recommended for full client capabilities.

Cisco WebClient

Cisco WebClient is a two-tier TN3270 Web client solution offered by Cisco. Like the OC://WebConnect Pro product, it enables mainframe access to Web clients without requiring any special software or changes to the mainframe. Also like the OC://WebConnect Pro product, the client requires a Java-capable Web browser. However, Cisco WebClient requires a higher level of Java (JDK 1.1 with the latest patch). TN3270 WebClient can be used with Netscape Navigator or Internet Explorer.

Figure 3-5 Cisco WebClient Window



The Cisco WebClient offers the following features:

- TN3270 and TN3270E emulation—The Cisco WebClient is compliant with RFC 1647 (TN3270E). It allows users to specify whether or not they want to use TN3270E. If “Allow 3270E” is not selected, the client will attempt to negotiate the following device types (in order):
 - IBM-3279-2-E
 - IBM-3278-2-E
 - IBM-3279-2
 - IBM-3278-2

If “Allow 3270E” is selected, the client can use Models 2 through 5 with the following screen sizes: 24x80, 32x80, 43x80, or 27x132. The Cisco WebClient can dynamically switch between these screen sizes as required by the host emulation session.

Alternately, the user can also specify the Primary and Alternate model types they want to use.

- Printing—The first release of the Cisco WebClient supports local screen printing only. The local screen printing capabilities are provided using JDK 1.1 printing. The user is prompted with the normal operating system print dialog box to choose alternate printers and other print parameters.
- Copy and Paste—Data can be copied from the Java screen and pasted into a desktop application such as Word, Excel, or PowerPoint.
- Persistent Connections—The Cisco WebClient provides a persistent connection between the client browser and a mainframe via a TN3270 server. The user can specify an inactivity timeout value, if desired.
- Configurable Host/Port Address—The Cisco WebClient supports a user-configurable pairing of host to port address. The user can edit the Default Configuration session parameters to connect to a different host and port.
- Firewall Support (Telnet Proxy Support)—The Cisco WebClient provides Telnet Proxy firewall support. Although, the Cisco WebClient does not negotiate through the firewall, it does allow the user to communicate with the firewall.
- Trace Capability—If the Trace facility is selected before a connection to the mainframe is established, the TN3270 WebClient creates a session trace file on the user’s local machine.
- Help Desk Facility—A Help Desk facility is provided that displays information about the current session. This information is useful in solving connection problems. The following information is displayed:

Field	Description	Example
Host Name Requested	Host that was requested	MVS
Connected to Host	Actual host to which connection was made	198.3.241.22
Port Request	Port that was requested	23
Connected to Port	Actual port to which connection was made	23
TN3270E Status	Disabled or allowed	Allowed
Physical Unit	PU connection	MVSPU1
Logical Unit	LU to which you are connected	MVS00029
Device Type	Emulation device type	IBM-3279-2-E
Default Size	Default screen size	2 (80x24)
Alternate Size	Second choice for screen size	2 (80x24)

Field	Description	Example
Current Size	Current screen size	2 (80x24)

Migration Scenarios

This chapter describes migration scenarios for TN3270 Server. Each scenario describes the purpose of the new configuration, considerations for implementing the new configuration, and the configuration steps involved. This chapter contains the following scenarios:

- Scenario 1: TN3270 Server with Static LUs
- Scenario 2: TN3270 Server with Dynamic LUs
- Scenario 3: TN3270 Server Using LU Nailing
- Scenario 4: TN3270 Server Using LU Nailing with Static LUs
- Scenario 5: TN3270 Server Using Nailing for Printer LUs
- Scenario 6: Using a Remote TN3270 Server
- Scenario 7: TN3270 Server with LocalDirector
- Scenario 8: TN3270 Server Using DistributedDirector
- Scenario 9: TN3270 Server Using a Direct PU and INCLUD0E
- Scenario 10: TN3270 Server with Session Switching

PU and LU Definitions

The definitions of PUs and LUs have not changed from the SNA 3270 definition mechanism. A VTAM XCA node definition is used for channel connectivity and then single or multiple switched major nodes are used to define the PU and LU. If you are migrating from an existing network that already uses switched major nodes, no change is required in the PU and LU definitions.

XCA Major Node

The common configuration parameters for defining the XCA major node are shown in the following example. This configuration is standard and does not change throughout the scenarios.

```
CBXCA38  VBUILD TYPE=XCA
CBPRT38  PORT  ADAPNO=0,CUADDR=3800,SAPADDR=04,MEDIUM=RING,TIMER=60
CBGRP38  GROUP ANSWER=ON,
          AUTOGEN=(10,L,P),
          CALL=INOUT,
          DIAL=YES,
          ISTATUS=ACTIVE
```

LUGROUP Major Node

As explained in Chapter 2, TN3270 Server Implementation, some devices (such as TN3270E clients) can request a specific LU by name. For those devices that do not request an LU by name, VTAM allocates LUs from a pool. You must define an LUGROUP that instructs VTAM how to allocate the LUs.

Look at the definitions for the LUGROUP and see how they are defined. Figure 4-1 shows the common configuration parameters for defining the LUGROUP. This configuration is standard and does not change throughout the scenarios.

Figure 4-1 LUGROUP Major Node Definition

```
CBDDDLU  VBUILD TYPE=LUGROUP
*****
*        LUGROUP MAJOR NODE FOR TN3270S TESTING        *
*****
*        MM/DD/YY - WHO - WHAT                        *
*****
DDDMVSLU LUGROUP
327@@2   LU    DLOGMOD=D4A32782,
             MODETAB=ISTINCLM,
             USSTAB=USSSNA,
             SSCPFM=USSSCS
327@@3   LU    DLOGMOD=D4A32783,
             MODETAB=ISTINCLM,
             USSTAB=USSSNA,
             SSCPFM=USSSCS
327@@4   LU    DLOGMOD=D4A32784,
             MODETAB=ISTINCLM,
             USSTAB=USSSNA,
             SSCPFM=USSSCS
327@@5   LU    DLOGMOD=D4A32785,
             MMODETAB=ISTINCLM,
             USSTAB=USSSNA,
             SSCPFM=USSSCS
327@@2E  LU    DLOGMOD=SNX32702,
             MODETAB=ISTINCLM,
             USSTAB=USSSNA,
             SSCPFM=USSSCS
327@@3E  LU    DLOGMOD=SNX32703,
             MODETAB=ISTINCLM,
             USSTAB=USSSNA,
             SSCPFM=USSSCS
```

```

327@@4E LU DLOGMOD=SNX32704,
           MODETAB=ISTINCLM,
           USSTAB=USSSNA,
           SSCPFM=USSSCS
327@@5E LU DLOGMOD=SNX32705,
           MODETAB=ISTINCLM,
           USSTAB=USSSNA,
           SSCPFM=USSSCS
@        LU DLOGMOD=BADMOD,
           MODETAB=ISTINCLM,
           USSTAB=USSSNA,
           SSCPFM=USSSCS

```

At the top of the file is the name of this major node, CBDDDLU. The name of a LUGROUP is DDDMVSLU. This is the name that the LUGROUP parameter in the PU definition maps to.

Below the LU group name is a list of mapping instructions for VTAM. In the left column are terms like 3@7@@2, which correspond with terminal types. The @ sign is used as a wildcard.

The fifth character in the model string that TN3270 Server sends indicates whether a client is TN3270 or TN3270E. You can use a 0 for standard TN3270 clients and an S for TN3270E (SCS) clients.

To accommodate both types of clients, you would need LU model entries like the following:

```

327802 LU  MODETAB=.,,
           DLOGMOD=.,,
           SSCPFM=USS3270,
           USSTAB=(label of USSTAB with a USS10 in 3270DS)
3278S2 LU  MODETAB=.,,
           DLOGMOD=.,,
           SSCPFM=USSSCS,
           USSTAB=(label of USSTAB with a USS10 in SCS)

```

Alternatively, you can do as we have in our example and make all clients work with SCS (using the translation feature in the TN3270 Server) by using a wildcard in the fifth position of the character model string as shown below:

```

3278@2 LU  MODETAB=.,,
           DLOGMOD=.,,
           SSCPFM=USSSCS,
           USSTAB=(label of USSTAB with a USS10 in SCS)

```

If the client is using a 3270 data stream and the mainframe is expecting an SCS data stream, the TN3270 Server translates the 3270 data stream from the client into an SCS data stream for the mainframe and then translates the response into a 3270 data stream. The TN3270 Server cannot translate an SCS data stream from the client into a 3270 data stream for the mainframe. You can specify an SSCPFM of USSSCS for all clients regardless of the type of client.

In the following situations, you might prefer to specify an SSCPFM of USS3270:

- If you currently have all LUs configured for the 3270 data stream and do not want to create a new USSTAB. This situation is relevant only if none of the TN3270 clients uses SCS.
- If you want to use the 3270 data stream to make use of the highlighting and multiple-field screens in the USS10. This situation results in a different look for the two kinds of clients.
- If you are using login scripts. In a 3270 data stream, there must be a blank on the screen to the left of the input field (or in column 80 of the preceding line). The translation algorithm of the TN3270 Server inserts this blank as necessary and shifts the input field one column to the right. The results can confuse login scripts.

Note: This works only for TN3270 clients or TN3270E clients that do not negotiate the Bind image and, therefore, do not require the SCS-formatted SSCPFM-LU dialog.

If you use SCS for TN3270E clients and 3270DS for non-E clients, create separate LU group entries as follows:

- 327@S2 (old model 2)—specify an SSCPFM of USSSCS
- 327@02 (old model 2)—specify an SSCPFM of 3270DS
- 327@S2E (model 2, extended data stream)—specify an SSCPFM of USSSCS
- 327@02E (model 2, extended data stream)—specify an SSCPFM of 3270DS

Parameters in the LUGROUP Major Node

The lines following the terminal types define the characteristics of the client to VTAM, including screen size. These lines instruct VTAM how to format the character stream that is sent to the client and identify what to expect from the client. If this mapping is incorrect, the data displayed at the client could be corrupted or the connection might fail to work. In addition, these lines tell VTAM what functions are supported. The parameters in this file are as follows:

- DLOGMOD (default logon mode table entry name)—Defines which logon mode is used in the table specified by the MOETAB entry. If this parameter is not specified, the first entry in the table is used.
- MODETAB (logon mode table)—Defines the list of rules that are in effect at logon. This table defines parameters, such as response unit (RU) size, encryption, character set, and type of bind. The MODETAB contains different rules for different logon modes. The default is MODETAB=ISTINCLM.
- USSTAB (unformatted system services tables)—Defines operator messages and certain commands. There are two types of USS tables. The session-level USS table defines the messages and commands for a dependent logical unit (DLU). The default session level is USSTAB=ISTINCDT. The operation-level USS table contains commands and messages that are sent to and received from the VTAM operator. The default operation level is USSTAB=ISTINCNO.
- SSCPFM (system services control point format)—Defines which RU types are used by the LU. Specifying USS3270 causes the USSMSG10 (USS message number 10) to flow to the LU at logon time. This is the logon panel that is displayed when a connection is established (such as the VM/ESA logo).

There are only two valid combinations of these parameters.

– For a SCS data stream, use the following:

SSCPFM=USSSCS

In this case, the USSTAB is the name of a USS table that contains a USS10 message coded in SCS data stream.

– For a 3270 data stream(3270DS), use the following:

SSCPFM=USS3270

In this case, the USSTAB is the name of a USS table that contains a USS10 message coded in 3270 data stream.

When a client establishes a connection, it tells the server its device type. VTAM matches the device type to one of the entries in the LUGROUP and assigns the parameters.

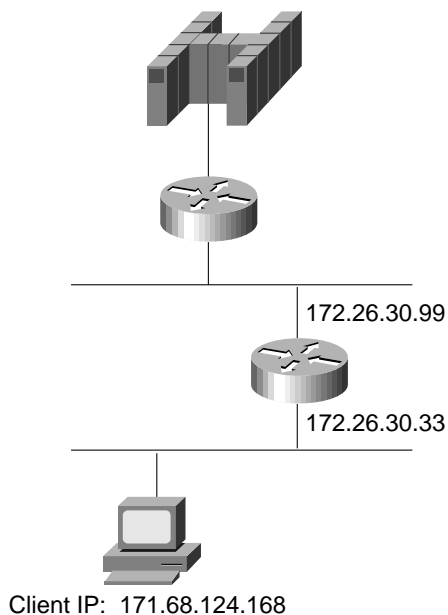
VTAM also allows default mapping for clients when they specify a device type that is not mapped. This situation is covered by the @ LU entry. Anything that does not map to a specific device type in the list is treated as if it has the characteristics mapped to the @ entry. This wildcard entry is used to accept all other clients. It can also be used to reject all other clients and isolate all non-standard terminals.

Scenario 1: TN3270 Server with Static LUs

In this scenario, we are starting with a legacy SNA network that contains 3174 controllers connected to 3278 type terminals. It is a pure SNA network. We are implementing IP in the network and so we have replaced all our 3278 type terminals with PCs. The network restrictions require the clients to use the same LU names that were defined in the SNA network, so we are going to use static LUs. Static LUs are predefined LUs in the switched PU VTAM definition. Static LUs must be used if extended clients are going to request specific LU names. This configuration is useful for printers, for applications that have terminal-based security, or other situations where the network administrator must control which LU a user is assigned.

We can use the existing switched major node and PU and LU definitions. Because we are using static LUs, either the client software must support TN3270E capabilities or the client nailing parameter must be configured on the TN3270 Server. We have chosen the first option because it reduces the maintenance of the TN3270 Server definitions.

Figure 4-2 TN3270 Server with Static LUs



Design Considerations

When implementing static LUs with the TN3270 Server, keep in mind the following guidelines:

- If you use only static LUs without LU nailing, as in this scenario, then only TN3270E clients that present an LU name to the channel-attached router are able to connect. TN3270 clients are rejected because they do not request a specific LU name unless you configure LU nailing.

- If the client requests an LU name that VTAM knows, but the channel-attached router does not know this LU name, the request will fail. On the other hand, if the client requests an LU name and the channel-attached router knows this LU name, the activation occurs, even if VTAM knows this LOCADDR is a different LU name.
- If a client requests an LU that is inactive in VTAM, the client is rejected because the channel-attached router does not know the names of inactive LUs. That LOCADDR shows up as a blank name with a status of inactive.
- In most cases it is preferable for the LU name in VTAM to match the LU name in the channel-attached router for static LUs. This way, if a TN3270 client requests an LU name then the channel-attached router knows the correct LU name. Some organizations do not name their LUs based on the LU-seed naming standard. This makes network management difficult because the client and the channel-attached router know one LU name while VTAM knows another LU name. This design is achieved by the PU naming standards. For more information, see “Determining How LUs Will Be Named” in the TN3270 Server Implementation chapter.
- Specific logmodes must be defined for each LU in the switched major node depending on what type of model is going to connect. This increases the management burden because the client cannot change the device type it requests without a corresponding change in the VTAM definitions (unless it also requests a different LU to go with that model).

Router Configuration

To implement IP in our network, we installed a CIP/CPA in our Cisco 7000 series router with Cisco IOS Release 11.3. We configured CSNA and are ready to implement our TN3270 Server. In this scenario, we need to:

- Initiate the TN3270 Server
- Define the LUs
- Verify the Configuration

It is a good idea to use separate adapters for the TN3270 Server and the CSNA. If the same adapter is used and the External Communications Adapter (XCA) goes down, the adapter will still answer logical link control (LLC) test polls, which will mislead SNA clients that the host connection is still up.

Note: The TN3270 Server can also access the host through a Multi-Path Channel (MPC) device.

Initiate the TN3270 Server

To initiate the TN3270 Server on the router, issue the following commands:

```
! enter interface configuration mode for the virtual interface in slot 1
router(config)#int channel 1/2
! create TN3270 Server entity
router(config-if)#tn3270-server
router(config-if)#lan token 0
router(cfg-lan-Token 0)#adapter 0 4000.4000.0001
router(config-if)#lan token 31
router(cfg-lan-Token 0)#adapter 31 4000.4000.4444
! set server-wide defaults for PU parameters
router(cfg-tn3270)#unbind-action keep
router(cfg-tn3270)#generic-pool permit
```

Define the LUs

To define the static LUs, issue the following commands:

```
router(cfg-tn3270)#pu puxcpa 0CBCB001 172.26.20.33 tok 31 10 rmac 4000.4000.0001
router(tn3270-pu)#pu puxcpb 0CBCB002 172.26.20.33 tok 31 12 rmac 4000.4000.0001
```

Note: Defining the PUs to an adapter other than adapter 0 (we have used adapter 31) means that error messages will not be sent to the adapter that connects to the XCA major node. This is optional. Many sites use a single adapter for both the XCA and PU connections.

Verify the Configuration

To verify the configuration, use the Cisco IOS **show** commands. You can view the general TN3270 Server configuration as well as configuration information about the specific PUs and LUs.

Viewing the Current Router Configuration

To display the current router configuration, enter the following command:

```
router#show run
Building configuration...

< information deleted >

interface Channell/2
 ip address 172.26.20.34 255.255.255.240
 no keepalive
 lan TokenRing 0
 adapter 31 4000.4000.4444
 TN3270-server
 unbind-action keep
 PU PUXCPA01 0CBCB001 172.26.20.33 token-adapter 31 10 rmac 4000.4000.0001
 PU PUXCPB01 0CBCB002 172.26.20.33 token-adapter 31 12 rmac 4000.4000.0001
```

Viewing the Status of PUs

To display the current server configuration parameters and the status of the PUs defined in the server, enter the following command:

```
router#show extended channel 1/2 TN3270-server
<current stats < connection stats <response time(ms)
server-ip:tcp      LU in-use  connect disconn fail  host  tcp
172.26.20.33:23    20      0      0      0      0      0
total              20      0
configured max_LU 2100
idle-time 0      keepalive 0      unbind-action keep
ip-preced-screen 0 ip-preced-printer 0 ip-tos-screen 0 ip-tos-printer 0
tcp-port 23      generic-pool permit no timing-mark

name(index)  ip:tcp      xid  state  link  destination  r-lsap
PUXCPA01(9)  172.26.20.33:23  0CBCB001 ACTIVE tok 31 4000.4000.0001 04 10
PUXCPB01(10) 172.26.20.33:23  0CBCB002 ACTIVE tok 31 4000.4000.0001 04 12
```

Viewing a List of LUs

To display the PU configuration parameters, statistics, and all the LUs currently attached to the PU, enter the following command:

```
router#show extended channel 1/2 TN3270-server PU puxcpa01
name(index)  ip:tcp          xid  state   link  destination  r-lsap
PUXCPA01(9)  172.26.20.33:23    0CBCB001 ACTIVE tok 31 4000.4000.0001 04 10

idle-time    0      keepalive 0      unbind-act keep      generic-pool perm
ip-preced-screen 0 ip-preced-printer 0 ip-tos-screen 0 ip-tos-printer 0
bytes 250 in, 141 out; frames 10 in, 11 out; NegRsp 0 in, 0 out
actLUs 10, dactLUs 0, binds 0
Note: if state is ACT/NA then the client is disconnected
```

LU	name	client-ip:tcp	nail	state	model	frames	in	out	idle	for
2	PUXCPA02	171.68.124.168:1196	N	P-BIND	3278S4E	4		3	0:1:12	
3	PUXCPA03	never connected	N	ACT/NA		1		1	0:4:16	
4	PUXCPA04	never connected	N	ACT/NA		1		1	0:4:16	
5	PUXCPA05	never connected	N	ACT/NA		1		1	0:4:16	
6	PUXCPA06	never connected	N	ACT/NA		1		1	0:4:16	
7	PUXCPA07	never connected	N	ACT/NA		1		1	0:4:16	
8	PUXCPA08	never connected	N	ACT/NA		1		1	0:4:16	
9	PUXCPA09	never connected	N	ACT/NA		1		1	0:4:16	
10	PUXCPA0A	never connected	N	ACT/NA		1		1	0:4:16	
11	PUXCPA0B	never connected	N	ACT/NA		1		1	0:4:16	

Viewing the Status of an LU

To display the status of an LU, enter the following command:

```
router#show extended channel 1/2 TN3270-server PU puxcpa01 LU 02
LU  name  client-ip:tcp  nail state  model  frames in out  idle for
2   PUXCPA02 171.68.124.168:1196 N  P-BIND  3278S4E 4 3 0:1:12

PU is PUXCPA01, LU is STATIC unbound, negotiated TN3270E
bytes 155 in, 1531 out; RuSize 256 in, 256 out; NegRsp 0 in, 0 out
pacing window 0 in, 0 out; credits 0 in, queue-size 0 in, 0 out
```

Viewing Historical Data for an LU

To display the trace history of an LU, enter the following command:

```
router#show extended channel 1/2 TN3270-server PU puxcpa01 LU 02 history
LU  name  client-ip:tcp  nail state  model  frames in out  idle for
2   PUXCPA02 171.68.124.168:1196 N  P-BIND  3278S4E 4 3 0:1:20

PU is PUXCPA01, LU is STATIC unbound, negotiated TN3270E
bytes 155 in, 1531 out; RuSize 256 in, 256 out; NegRsp 0 in, 0 out
pacing window 0 in, 0 out; credits 0 in, queue-size 0 in, 0 out
traces:
    actLU req
    Client connect req
    Reply PSID neg rsp
    notify resp
OUT len=12  2Dxxxxxxxx426B80000D0201
IN  len=25  xxxxxxxxxxx42EB80000D0201000000
IN  len=101 xxxxxxxxxxx110B820041038D000000
OUT len=16  2Cxxxxxxxx118F92001003000041
IN  len=20  xxxxxxxxxxx010B80008106200C0603
OUT len=12  2Cxxxxxxxx018B8000810620
OUT len=1507 2Cxxxxxxxx01038000C3C9E2C3D6
IN  len=9   2C0000020001838000
```

Host Configuration

The router configuration does not specify whether a TN3270 Server PU uses static LUs, dynamic LUs, or both. This type of LU is specified only in the VTAM switched major node. All LUs that are predefined in the switched major node are static.

Note: Although a LOCADDR of 1 is valid (unlike traditional SNA controllers), we did not use it in this sample. The LOACADDR starts with 2, the first LU name starts with 01. Also, because the LU-seed is not used on the channel-attached router, the LU names on the channel-attached router are different from the ones in VTAM. For example, the VTAM name LUXCPA01 corresponds to the TN3270 Server name PUXCPA02. For more information, see “Determining How LUs Will Be Named” in the TN3270 Server Implementation chapter.

Figure 4-3 shows the configuration of the switched major node for this scenario.

Figure 4-3 Scenario 1: Switched Major Node

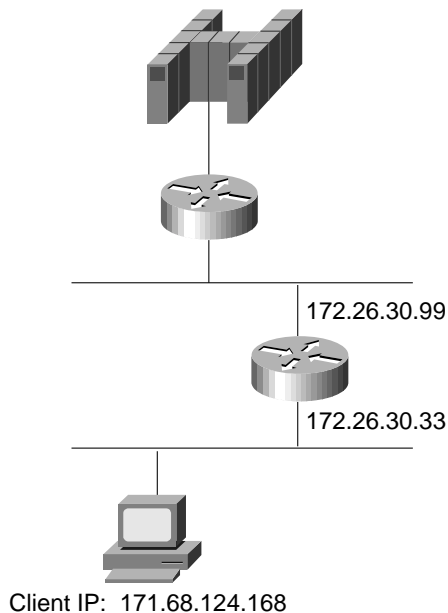
```
*****
*      SWITCHED MAJOR NODE      *
*****
CBSWN1 VBUILD TYPE=SWNET,MAXGRP=10,MAXNO=10
PUXCPA01 PU      ADDR=01,
                PUTYPE=2,ANS=CONT,
                IDBLK=0CB, IDNUM=CB001,
                USSTAB=USSSNA, DLOGMOD= SX32702S, MODETAB=ALAMODE
LUXCPA02 LU      LOCADDR=2
LUXCPA03 LU      LOCADDR=3
LUXCPA04 LU      LOCADDR=4
LUXCPA05 LU      LOCADDR=5
LUXCPA06 LU      LOCADDR=6
LUXCPA07 LU      LOCADDR=7
LUXCPA08 LU      LOCADDR=8
LUXCPA09 LU      LOCADDR=9
LUXCPA10 LU      LOCADDR=10
LUXCPA11 LU      LOCADDR=11
*
PUXCPB01 PU      ADDR=01,
                PUTYPE=2,ANS=CONT,
                IDBLK=0CB, IDNUM=CB002,
                USSTAB=USSSNA, DLOGMOD= SX32702S, MODETAB=ALAMODE
LUXCPB02 LU      LOCADDR=2
LUXCPB03 LU      LOCADDR=3
LUXCPB04 LU      LOCADDR=4
LUXCPB05 LU      LOCADDR=5
LUXCPB06 LU      LOCADDR=6
LUXCPB07 LU      LOCADDR=7
LUXCPB08 LU      LOCADDR=8
LUXCPB09 LU      LOCADDR=9
LUXCPB10 LU      LOCADDR=10
LUXCPB11 LU      LOCADDR=11
```

Scenario 2: TN3270 Server with Dynamic LUs

In this scenario, we started with our legacy SNA network and have introduced IP and replaced our 3278 type terminals with PCs. This time the design requirement is to minimize the number of LU definitions in VTAM. Using the DDDL U feature of VTAM, we can define several switched PUs, which use dynamic LUs. As clients request a 3270 connection, the channel-attached router requests an LU and VTAM dynamically provides one. Each client receives an LU based on the model and type that it specifies. This process reduces the setup and maintenance cycle for VTAM LUs.

This process also provides greater flexibility to service client requirements without providing an individual LU for every client. For example, this is useful if you have 10,000 clients but only 5,000 log on at the same time. Using static LUs, you must define 10,000 LUs and assign each client a unique LU name. Using DDDL U, however, you can define a pool of 5,000 LUs without creating the static definitions. Each client is assigned an LU name from the pool when they request a connection. With DDDL U, the TN3270 Server can support standard TN3270 clients as well as TN3270E clients.

Figure 4-4 TN3270 Server with Dynamic LUs



Design Considerations

When implementing dynamic LUs with the TN3270 Server, keep in mind the following guidelines:

- If DDDL U is used and static LUs are not defined, then TN3270E clients that request a specific LU name are rejected.
- Define each dynamic PU with a unique LU-seed parameter in the VTAM switched definition. Otherwise, VTAM attempts to define two LUs with the same name and the second request fails. The TN3270 client shows connected, but the channel-attached router is waiting for the ACTLU to flow.

- The LUGROUP in the switched major node must match the name of LUGROUP in the LU group major node.
- LUs marked as ACT/NA are reused by clients requesting the same model type. Clients requesting a different model type are assigned a new LU from VTAM.

Router Configuration

The router configuration in this scenario is similar to the configuration in Scenario 1. To implement IP in our network, we installed a CIP/CPA in our Cisco 7000 series router with Cisco IOS Release 11.3. We configured CSNA and are ready to implement our TN3270 Server. In this scenario, we need to:

- Initiate the TN3270 Server
- Define the LUs
- Verify the Configuration

Initiate the TN3270 Server

To initiate the TN3270 Server on the router, enter the following commands:

```
! enter interface configuration mode for the virtual interface in slot 1
router(config)#int channel 1/2
! create TN3270 Server entity
router(config-if)#tn3270-server
router(config-if)#lan token 0
router(cfg-lan-Token 0)#adapter 0 4000.4000.0001
router(config-if)#lan token 31
router(cfg-lan-Token 0)#adapter 31 4000.4000.4444
! set server-wide defaults for PU parameters
router(cfg-tn3270)#unbind-action keep
router(cfg-tn3270)#generic-pool permit
```

Define the LUs

To define the static LUs, enter the following commands:

```
router(cfg-tn3270)#pu puxcpa 05d00001 172.26.20.33 tok 31 10 rmac 4000.4000.0001
router(tn3270-pu)#pu puxcpb 05d00002 172.26.20.34 tok 31 12 rmac 4000.4000.0001
lu-seed pub##
router(tn3270-pu)#pu puxcpc 05d00003 172.26.20.35 tok 31 14 rmac 4000.4000.0001
lu-seed pu3###
```

Verify the Configuration

To verify the configuration, use the Cisco IOS **show** commands. You can view the general TN3270 Server configuration as well as configuration information about the specific PUs and LUs.

Viewing the Current Router Configuration

To display the current router configuration, enter the following command:

```
router#show run
Building configuration...

<deleted information>

interface Channell/2
 ip address 172.26.20.33 255.255.255.240
 no keepalive
 lan TokenRing 0
  adapter 0 4000.4000.0001
  adapter 31 4000.4000.4444
 TN3270-server
  unbind-action keep
  PU PUXCPA01 0CBCB001 172.26.20.34 token-adapter 31 10 rmac 4000.4000.0001
  PU PUXCPB01 0CBCB002 172.26.20.34 token-adapter 31 12 rmac 4000.4000.0001 LU-seed
  PUB##
  PU PUXCPC01 0CBCB003 172.26.20.35 token-adapter 31 14 rmac 4000.4000.0001 LU-seed
  PU3###
```

Viewing the Status of PUs

To display the current server configuration parameters and the status of the PUs defined in the server, enter the following command:

```
router#show extended channel 1/2 TN3270-server
          <current stats < connection stats <response time(ms)
server-ip:tcp      LU in-use  connect disconn fail  host  tcp
172.26.20.34:23    510     1       2       1     0     0     0
172.26.20.35:23    255     1       1       0     0     0     0
total              765     2
configured max_LU 2100
idle-time         0         keepalive 1800         unbind-action keep
ip-preced-screen 0 ip-preced-printer 0 ip-tos-screen 0 ip-tos-printer 0
tcp-port         23         generic-pool permit no timing-mark

name(index)  ip:tcp          xid  state  link  destination  r-lsap
PUXCPA01(15) 172.26.20.34:23 0CBCB001 ACTIVE tok 31 4000.4000.0001 04 10
PUXCPB01(16) 172.26.20.34:23 0CBCB002 ACTIVE tok 31 4000.4000.0001 04 12
PUXCPC01(14) 172.26.20.35:23 0CBCB003 ACTIVE tok 31 4000.4000.0001 04 14
```

Viewing a List of LUs

To display the PU configuration parameters, statistics, and all the LUs currently attached to each PU, enter the following commands:

```
router#show extended channel 1/2 TN3270-server PU puxcpa01
name(index)  ip:tcp          xid  state  link  destination  r-lsap
PUXCPA01(15) 172.26.20.34:23 0CBCB001 ACTIVE tok 31 4000.4000.0001 04 10

idle-time         0         keepalive 1800         unbind-act keep  generic-pool perm
ip-preced-screen 0 ip-preced-printer 0 ip-tos-screen 0 ip-tos-printer 0
bytes 0 in, 21 out; frames 0 in, 1 out; NegRsp 0 in, 0 out
actLUs 0, dactLUs 0, binds 0
LU  name  client-ip:tcp          nail state  model  frames in out  idle for
```

To view the PU with static LUs, enter the following command:

```
router#show extended channel 1/2 TN3270-server PU puxcpb01
name(index)  ip:tcp          xid  state  link  destination  r-lsap
PUXCPB01(16) 172.26.20.34:23         0CBCB002 ACTIVE tok 31 4000.4000.0001 04 12
```

```
LU-seed PUB##
idle-time 0      keepalive 1800      unbind-act keep      generic-pool perm
ip-preced-screen 0 ip-preced-printer 0 ip-tos-screen 0 ip-tos-printer 0
bytes 582 in, 2281 out; frames 26 in, 27 out; NegRsp 0 in, 0 out
actLUs 2, dactLUs 0, binds 1
LU  name  client-ip:tcp      nail state  model  frames in out  idle for
1  PUB01  171.68.124.165:1065  N  ACT/NA  VT400  5  3  0:8:2
2  PUB02  171.68.124.168:1215  N  ACT/SESS 327904E 21  20  0:3:33
```

```
router#show extended channel 1/2 TN3270-server PU puxcpc01
name(index)  ip:tcp          xid  state  link  destination  r-lsap
PUXCPC01(14) 172.26.20.35:23         0CBCB003 ACTIVE tok 31 4000.4000.0001 04 14
```

```
LU-seed PU3###
idle-time 0      keepalive 1800      unbind-act keep      generic-pool perm
ip-preced-screen 0 ip-preced-printer 0 ip-tos-screen 0 ip-tos-printer 0
bytes 1420 in, 4141 out; frames 21 in, 22 out; NegRsp 0 in, 0 out
actLUs 2, dactLUs 0, binds 1
Note: If state is ACT/NA then the client is disconnected
LU  name  client-ip:tcp      nail state  model  frames in out  idle for
2  PU3002  never connected    N  ACT/NA          1  1  0:10:54
3  PU3003  171.68.124.168:1213  N  ACT/SESS 3278S4E 20  19  0:3:31
```

Viewing the Status of an LU

To display the status of the LUs, enter the following commands for each LU:

```
router#show extended channel 1/2 TN3270-server PU puxcpb01 LU 02
Note: If state is ACT/NA then the client is disconnected
LU  name  client-ip:tcp      nail state  model  frames in out  idle for
2  PUB02  171.68.124.168:1215  N  ACT/SESS 327904E 21  20  0:4:4
```

PU is PUXCPB01, LU is **DYNAMIC** type 2, negotiated TN3270
bytes 326 in, 689 out; RuSize 1024 in, 3840 out; NegRsp 0 in, 6 out
pacing window 0 in, 1 out; credits 0 in, queue-size 0 in, 0 out

```
router#show extended channel 1/2 TN3270-server PU puxcpc01 LU 03
Note: If state is ACT/NA then the client is disconnected
LU  name  client-ip:tcp      nail state  model  frames in out  idle for
3  PU3003  171.68.124.168:1213  N  ACT/SESS 3278S4E 20  19  0:4:16
```

PU is PUXCPC01, LU is **STATIC** type 2, negotiated TN3270E
bytes 1395 in, 4096 out; RuSize 1024 in, 3840 out; NegRsp 0 in, 5 out
pacing window 0 in, 1 out; credits 0 in, queue-size 0 in, 0 out

In the examples above, we see that LU 02 is a dynamic LU and LU 03 is static.

Viewing LUs Associated with an IP Address

To display information about LUs defined under an IP address, enter the following command:

```
router#sh ext ch 1/2 tn client-ip-address 171.68.124.168
Note: If state is ACT/NA then the client is disconnected
LU   name      client-ip:tcp      nail state  model  frames in out  idle for
3   PU3003     171.68.124.168:1213  N   ACT/SESS 3278S4E  20    19    0:4:47

PU is PUXCPC01, LU is STATIC type 2, negotiated TN3270E
bytes 1395 in, 4096 out; RuSize 1024 in, 3840 out; NegRsp 0 in, 5 out
pacing window 0 in, 1 out; credits 0 in, queue-size 0 in, 0 out
Note: if state is ACT/NA then the client is disconnected

LU   name      client-ip:tcp      nail state  model  frames in out  idle for
2   PUB02     171.68.124.168:1215  N   ACT/SESS 327904E  21    20    0:4:55

PU is PUXCPB01, LU is DYNAMIC type 2, negotiated TN3270
bytes 326 in, 689 out; RuSize 1024 in, 3840 out; NegRsp 0 in, 6 out
pacing window 0 in, 1 out; credits 0 in, queue-size 0 in, 0 out
Total 2 clients found using 171.68.124.168
```

Host Configuration

The router configuration does not specify whether a TN3270 server PU uses static LUs, dynamic LUs, or both. The type of LU is specified only in the VTAM switched major node. Any LOCADDRs not defined in the switched major node (potential LOCADDRs are between 1 and 255) are used as dynamic LUs.

Figure 4-5 shows the configuration of the switched major node for this scenario.

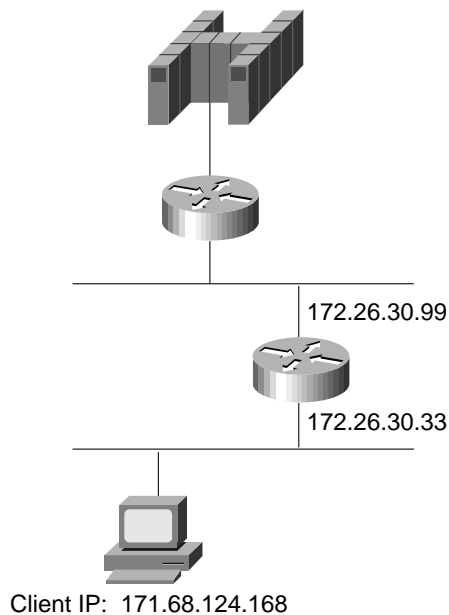
Figure 4-5 Scenario 2: Switched Major Node

```
*****
*   SWITCHED MAJOR NODE   *
*****
CBSWN1 VBUILD TYPE=SWNET,MAXGRP=10,MAXNO=10
*
PUXCFA01 PU   ADDR=01,
              PUTYPE=2,ANS=CONT,
              LUGROUP=DDDMVSLU,
              IDBLK=0CB,IDNUM=CB001,
              USSTAB=USSSNA,DLOGMOD= SX32702S,MODETAB=ALAMODE
*
PUXCPB01 PU   ADDR=01,
              PUTYPE=2,INCLUDE=YES,ANS=CONT,
              LUGROUP=DDDMVSLU,LUSEED=PUB###,
              IDBLK=0CB,IDNUM=CB002,
              USSTAB=USSSNA,DLOGMOD= SX32702S,MODETAB=ALAMODE
*
PUXCPC01 PU   ADDR=01,
              PUTYPE=2,INCLUDE=YES,ANS=CONT,
              LUGROUP=DDDMVSLU,LUSEED=PU3###,
              IDBLK=0CB,IDNUM=CB003,
              USSTAB=USSSNA,DLOGMOD= SX32702S,MODETAB=ALAMODE
LUXCPC01 LU   LOCADDR=1
LUXCPC02 LU   LOCADDR=2
```


Scenario 3: TN3270 Server Using LU Nailing

In this scenario, we are going to use LU nailing to control the LU that is assigned to a particular IP address. In an SNA environment, there are often requirements to control the LUs that are assigned to particular clients, such as printers. This control is important for printers that need a predefined name and applications that use terminal-based security, such as IMS applications. There are two methods to address this requirement; the first option is to have the client use TN3270E and specify the LU name; the second option is to control the LU names allocated using LU nailing. Using LU nailing allows you to centrally control which clients can connect to certain LUs. It also allows standard TN3270 clients to access a specific LU or pool of LUs.

Figure 4-6 TN3270 Server Using LU Nailing



Design Considerations

When implementing LU nailing with the TN3270 Server, keep in mind that new client statements are added to the end of the list for that particular PU (similar to configuring access lists).

Note: For more information on LU nailing, see “LU Nailing” in the TN3270 Server Implementation chapter.

Router Configuration

The router configuration in this scenario is similar to Scenario 2. In this scenario, we need to:

- Initiate the TN3270 Server
- Define the LUs
- Configure LU Nailing
- Limit the Number of TN3270 Sessions (Optional)
- Verify the Configuration

Initiate the TN3270 Server

To initiate the TN3270 Server on the router, enter the following commands:

```
! enter interface configuration mode for the virtual interface in slot 1
router(config)#int channel 1/2
! create TN3270 Server entity
router(config-if)#tn3270-server
router(config-if)#lan token 0
router(cfg-lan-Token 0)#adapter 0 4000.4000.0001
router(config-if)#lan token 31
router(cfg-lan-Token 0)#adapter 31 4000.4000.4444
! set server-wide defaults for PU parameters
router(cfg-tn3270)#unbind-action keep
router(cfg-tn3270)#generic-pool permit
```

Define the LUs

To define the static LUs, enter the following commands:

```
router(cfg-tn3270)#pu puxcpa 0CBCB001 172.26.20.34 tok 31 10 rmac 4000.4000.0001
LU-seed LU1###
```

Configure LU Nailing

To specify the LUs that are to be assigned to specific clients, enter the following commands:

```
router(cfg-tn3270)#pu puxcpa
router(tn3270-pu)#client ip 171.68.124.168 LU 1
router(tn3270-pu)#client ip 171.68.124.0 255.255.255.0 LU 3 50
router(tn3270-pu)#client ip 171.68.110.40 LU 51
router(tn3270-pu)#client ip 171.68.110.0 255.255.255.0 LU 52 100
```

Limit the Number of TN3270 Sessions (Optional)

To limit the number of TN3270 sessions that can be established by a particular client, enter the following command:

```
router(cfg-tn3270)#client 172.1.1.1 LU maximum 2
```

In this case 172.1.1.1 is never allocated more than two LOCADDRs and can establish only up to two TN3270 sessions. This action is called LU capping.

Verify the Configuration

To verify the configuration, use the Cisco IOS **show** commands. The **show** commands allow you to view the general TN3270 Server configuration and configuration information about the specific PUs and LUs.

Viewing the Current Router Configuration

To display the current router configuration, enter the following command:

```
router#show run
Building configuration...

<deleted information>

interface Channel1/2
 ip address 172.26.20.33 255.255.255.240
 no keepalive
 lan TokenRing 0
  adapter 0 4000.4000.0001
  adapter 31 4000.4000.4444
```

```

TN3270-server
  unbind-action keep
  PU PUXCPA01 0CBCB001 172.26.20.34 token-adapter 31 10 rmac 4000.4000.0001 LU-seed
  LU1###
    client ip 171.68.124.168 LU 1
    client ip 171.68.124.0 255.255.255.0 LU 3 50
    client ip 171.68.110.40 LU 51
    client ip 171.68.110.0 255.255.255.0 LU 52 100

```

Viewing the Status of PUs

To display the current server configuration parameters and the status of the PUs defined in the server, enter the following command:

```

router#show extended channel 1/2 TN3270-server
      <current stats < connection stats <response time(ms)
server-ip:tcp      LU in-use  connect disconn fail  host  tcp
172.26.20.34:23   255    3      10      7    0    0    0
total             255    3
configured max_LU 2100
idle-time 0      keepalive 1800      unbind-action keep
ip-preced-screen 0 ip-preced-printer 0 ip-tos-screen 0 ip-tos-printer 0
tcp-port 23      generic-pool permit no timing-mark

name(index)  ip:tcp      xid  state  link  destination  r-lsap
PUXCPA01(18) 172.26.20.34:23 0CBCB001 ACTIVE tok 31 4000.4000.0001 04 10

```

Viewing a List of LUs

To display the PU configuration parameters, statistics, and all the LUs currently attached to each PU, enter the following command:

```

router#show extended channel 1/2 TN3270-server PU puxcpa01

name(index)  ip:tcp      xid  state  link  destination  r-lsap
PUXCPA01(18) 172.26.20.34:23 0CBCB001 ACTIVE tok 31 4000.4000.0001 04 10

LU-seed LU1###
idle-time 0      keepalive 1800      unbind-act keep  generic-pool perm
ip-preced-screen 0 ip-preced-printer 0 ip-tos-screen 0 ip-tos-printer 0
bytes 2032 in, 6176 out; frames 40 in, 43 out; NegRsp 0 in, 0 out
actLUs 7, dactLUs 0, binds 0
Note: if state is ACT/NA then the client is disconnected

```

LU	name	client-ip:tcp	nail	state	model	frames	in	out	idle for
1	LU1001	171.68.124.168:1448	Y	P-BIND	327904	3		2	0:19:59
3	LU1003	171.68.124.168:1444	Y	ACT/NA	327904	10		6	0:20:7
4	LU1004	171.68.124.165:2035	Y	ACT/NA	VT400	5		3	0:11:1
5	LU1005	171.68.124.165:2075	Y	ACT/NA	VT400	5		3	0:11:13
6	LU1006	171.68.124.165:2080	Y	ACT/NA	VT400	5		3	0:10:48
51	LU1051	171.68.110.40:36186	Y	P-BIND	327904E	8		5	0:8:12
52	LU1052	171.68.110.40:36187	Y	P-BIND	327904E	3		2	0:7:55

client ip	mask	nail-type	LU first	LU last
171.68.124.168		screen	1	
171.68.124.0	255.255.255.0	screen	3	50
171.68.110.40		screen	51	
171.68.110.0	255.255.255.0	screen	52	100

Note: This command also displays the specific nailed LUs.

Viewing the Status of an LU

To display the status of the LUs, enter the following command for each LU:

```
router#show extended channel 1/2 tn3270-server PU puxcpa01 LU 01
Note: If state is ACT/NA then the client is disconnected
LU  name  client-ip:tcp      nail state  model  frames in out  idle for
1  LU1001  171.68.124.168:1448  Y  P-BIND  327904  3      2      0:20:20
```

```
PU is PUXCPA01, LU is DYNAMIC unbound, negotiated TN3270
bytes 135 in, 213 out; RuSize 256 in, 256 out; NegRsp 0 in, 0 out
pacing window 0 in, 0 out; credits 0 in, queue-size 0 in, 0 out
```

Viewing Nailed LUs

To display mappings between a nailed client IP address and nailed LUs, enter the following command:

```
router#show extended channel 1/2 tn3270-server nailed-ip 171.68.124.168
171.68.124.168          LU PUXCPA01 LU 1
171.68.124.0           255.255.255.0    LU PUXCPA01 LU 3  50
171.68.110.40          LU PUXCPA01 LU 51
171.68.110.0           255.255.255.0    LU PUXCPA01 LU 52 100
```

Note: The output of this command is a subset of the **show extended channel TN3270-Server PU** command.

Viewing LUs Associated with an IP Address

To display information about LUs defined under an IP address, enter the following command:

```
router#show extended channel 1/2 tn3270-server client-ip-address 171.68.124.168
Note: If state is ACT/NA then the client is disconnected
LU  name  client-ip:tcp      nail state  model  frames in out  idle for
3  LU1003  171.68.124.168:1444  Y  ACT/NA  327904  10     6     0:24:0
```

```
PU is PUXCPA01, LU is DYNAMIC unbound, negotiated TN3270
bytes 507 in, 450 out; RuSize 0 in, 0 out; NegRsp 0 in, 0 out
pacing window 0 in, 0 out; credits 0 in, queue-size 0 in, 0 out
Note: if state is ACT/NA then the client is disconnected
```

```
LU  name  client-ip:tcp      nail state  model  frames in out  idle for
1  LU1001  171.68.124.168:1448  Y  P-BIND  327904  3      2      0:23:52
```

```
PU is PUXCPA01, LU is DYNAMIC unbound, negotiated TN3270
bytes 135 in, 213 out; RuSize 256 in, 256 out; NegRsp 0 in, 0 out
pacing window 0 in, 0 out; credits 0 in, queue-size 0 in, 0 out
Total 2 clients found using 171.68.124.168
```

Note: The IP address shown has two LUs assigned.

Host Configuration

Figure 4-7 shows the configuration of the switched major node for this scenario.

Figure 4-7 Scenario 3: Switched Major Node

```
*****
*      SWITCHED MAJOR NODE      *
*****
CBSWN5  VBUILD  TYPE=SWNET,MAXGRP=10,MAXNO=10
*
PUXCPA01  PU      ADDR=01,                      X
                PUTYPE=2,ANS=CONT,              X
                LUGROUP=DDDMVSLU,LUSEED=LU1###,  X
                IDBLK=0CB,IDNUM=CB001,          X

```

Verify the VTAM Configuration

To display the status of the switched major node, enter the following command:

```
D NET, ID=CBSWN5, E
IST097I DISPLAY ACCEPTED
IST075I NAME = CBSWN5, TYPE = SW SNA MAJ NODE 537
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST1656I VTAMTOPO = REPORT, NODE REPORTED - YES
IST084I NETWORK RESOURCES:
IST089I PUXCPA01 TYPE = PU_T2.1                , ACTIV
IST089I LU1052  TYPE = LOGICAL UNIT            , ACTIV---X-
IST089I LU1051  TYPE = LOGICAL UNIT            , ACTIV---X-
IST089I LU1006  TYPE = LOGICAL UNIT            , ACTIV---X-
IST089I LU1005  TYPE = LOGICAL UNIT            , ACTIV---X-
IST089I LU1004  TYPE = LOGICAL UNIT            , ACTIV---X-
IST089I LU1001  TYPE = LOGICAL UNIT            , ACTIV---X-
IST089I LU1003  TYPE = LOGICAL UNIT            , ACTIV---X-
IST314I END
```

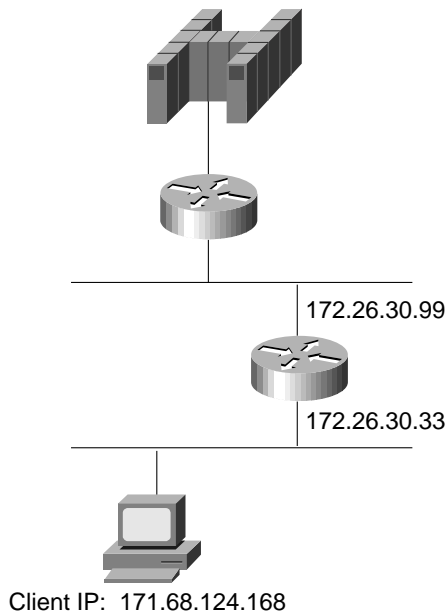
The **ACTIV---X-** indicates that these LUs were dynamically created.

Note: The LU names defined in the switched major node are different from the ones assigned at the TN3270 Server. For more information about LU names, see “Determining How LUs Will Be Named” in the TN3270 Server Implementation chapter.

Scenario 4: TN3270 Server Using LU Nailing with Static LUs

In this scenario, we address the situation in which you have a group of statically defined LUs that are not available for use by a pool of LUs. The only clients that can request and use these static LUs must be TN3270E-capable clients. The Cisco solution for this is to configure the PU with client nailing to allow all IP addresses to request the group of static LUs. Configuring this parameter creates a pool of LUs, even though the LUs are static, and allow clients that are not TN3270E clients to access the static LUs.

Figure 4-8 TN3270 Server Using LU Nailing with Static LUs



Router Configuration

We have configured CSNA and are now ready to implement our TN3270 Server. In this scenario, we need to:

- Initiate the TN3270 Server
- Define the LUs
- Configure LU Nailing
- Limit the Number of TN3270 Sessions (Optional)
- Verify the Configuration

Initiate the TN3270 Server

To initiate the TN3270 Server on the router, enter the following commands:

```
! enter interface configuration mode for the virtual interface in slot 1
router(config)#int channel 1/2
! create TN3270 Server entity
router(config-if)#tn3270-server
router(config-if)#lan token 0
router(cfg-lan-Token 0)#adapter 0 4000.4000.0001
router(config-if)#lan token 31
router(cfg-lan-Token 0)#adapter 31 4000.4000.4444
! set server-wide defaults for PU parameters
router(cfg-tn3270)#unbind-action keep
router(cfg-tn3270)#generic-pool permit
```

Define the LUs

To define the LU-seed used by the router, enter the following command:

```
router(cfg-tn3270)#pu puxcpa06 0CBCBA06 172.26.20.34 tok 31 10 rmac 4000.4000.0001
LU-seed LUXCPA##
```

Configure LU Nailing

To specify the LUs that are assigned to specific clients, enter the following commands:

```
router(cfg-tn3270)#pu puxcpa06
router(tn3270-pu)#client ip 171.68.124.165 LU 1 2
router(tn3270-pu)#client ip 171.68.124.0 255.255.255.0 LU 3 5
router(tn3270-pu)#client ip 171.68.110.0 255.255.255.0 LU 6 10
router(tn3270-pu)#client ip 171.68.120.0 255.255.255.0 LU 11 15
router(tn3270-pu)#client ip 171.68.130.0 255.255.255.0 LU 16 20
```

Limit the Number of TN3270 Sessions (Optional)

To limit the number of TN3270 sessions that can be established by a particular client, enter the following command:

```
router(cfg-tn3270)#client 172.1.1.1 LU maximum 2
```

In this case 172.1.1.1 will never be allocated more than two LOCADDRs and can, therefore, only establish up to two TN3270 sessions. This is called LU capping.

Verify the Configuration

To verify the configuration, use the Cisco IOS **show** commands. The **show** commands allow you to view the general TN3270 Server configuration and configuration information about the specific PUs and LUs.

Viewing the Current Router Configuration

To display the current router configuration, enter the following command:

```
router#show run
Building configuration...

<deleted information>

interface Channell/2
 ip address 172.26.20.33 255.255.255.240
 no keepalive
 lan TokenRing 0
  adapter 0 4000.4000.0001
  adapter 31 4000.4000.4444
```

```

TN3270-server
  unbind-action keep
  PU PUXCPA06 0CBCBA06 172.26.20.34 token-adapter 31 10 rmac 4000.4000.0001 LU-seed
LUXCPA##
  client ip 171.68.124.165 LU 1 2
  client ip 171.68.124.0 255.255.255.0 LU 3 5
  client ip 171.68.110.0 255.255.255.0 LU 6 10
  client ip 171.68.120.0 255.255.255.0 LU 11 15
  client ip 171.68.130.0 255.255.255.0 LU 16 20

```

Viewing the Status of PUs

To display the current server configuration parameters and the status of the PUs defined in the server, enter the following command:

```

router#show extended channel 1/2 tn3270-server
          <current stats < connection stats <response time(ms)
server-ip:tcp      LU in-use  connect disconn fail  host  tcp
172.26.20.34:23    20      6      6      0      0      0      0
total              20      6
configured max_LU 2100
idle-time 0        keepalive 1800    unbind-action keep
ip-prec-d-screen 0 ip-prec-d-printer 0 ip-tos-screen 0 ip-tos-printer 0
tcp-port 23       generic-pool permit no timing-mark

name(index)  ip:tcp      xid  state  link  destination  r-lsap
PUXCPA06(22) 172.26.20.34:23 0CBCBA06 ACTIVE tok 31 4000.4000.0001 04 10

```

Viewing a List of LUs

To display the PU configuration parameters, statistics, and all the LUs currently attached to each PU, enter the following command:

```

router#show extended channel 1/2 tn3270-server PU puxcpa06
name(index)  ip:tcp      xid  state  link  destination  r-lsap
PUXCPA06(22) 172.26.20.34:23 0CBCBA06 ACTIVE tok 31 4000.4000.0001 04 10

```

```

LU-seed LUXCPA##
idle-time 0        keepalive 1800    unbind-act keep    generic-pool perm
ip-prec-d-screen 0 ip-prec-d-printer 0 ip-tos-screen 0 ip-tos-printer 0
bytes 1280 in, 9471 out; frames 38 in, 39 out; NegRsp 0 in, 0 out
actLUs 20, dactLUs 0, binds 0

```

Note: If state is ACT/NA then the client is disconnected

LU	name	client-ip:tcp	nail	state	model	frames in	frames out	idle for
1	LUXCPA01	171.68.124.165:1364	Y	P-BIND	327802	4	3	0:1:27
2	LUXCPA02	171.68.124.165:1365	Y	P-BIND	327802	4	3	0:1:22
3	LUXCPA03	171.68.124.168:1617	Y	P-BIND	327904	4	3	0:1:29
4	LUXCPA04	171.68.124.165:1366	Y	P-BIND	327902E	4	3	0:1:16
5	LUXCPA05	never connected	Y	ACT/NA		1	1	0:1:57
6	LUXCPA06	171.68.110.40:36202	Y	P-BIND	327904E	4	3	0:0:57
7	LUXCPA07	171.68.110.40:36203	Y	P-BIND	327904E	4	3	0:0:48
8	LUXCPA08	never connected	Y	ACT/NA		1	1	0:1:57
9	LUXCPA09	never connected	Y	ACT/NA		1	1	0:1:57
10	LUXCPA0A	never connected	Y	ACT/NA		1	1	0:1:57
11	LUXCPA0B	never connected	Y	ACT/NA		1	1	0:1:57
12	LUXCPA0C	never connected	Y	ACT/NA		1	1	0:1:57
13	LUXCPA0D	never connected	Y	ACT/NA		1	1	0:1:57
14	LUXCPA0E	never connected	Y	ACT/NA		1	1	0:1:58
15	LUXCPA0F	never connected	Y	ACT/NA		1	1	0:1:58
16	LUXCPA10	never connected	Y	ACT/NA		1	1	0:1:58
17	LUXCPA11	never connected	Y	ACT/NA		1	1	0:1:58
18	LUXCPA12	never connected	Y	ACT/NA		1	1	0:1:58

```

19 LUXCPA13 never connected      Y  ACT/NA          1      1      0:1:58
20 LUXCPA14 never connected      Y  ACT/NA          1      1      0:1:58

```

```

client ip      mask      nail-type  LU first  LU last
171.68.124.165      screen    1          2
171.68.124.0       255.255.255.0  screen    3          5
171.68.110.0       255.255.255.0  screen    6          10
171.68.120.0       255.255.255.0  screen    11         15
171.68.130.0       255.255.255.0  screen    16         20

```

Viewing Nailed LUs

To display mappings between a nailed client IP address and nailed LUs, enter the following command:

```

router#show extended channel 1/2 tn nailed-ip 171.68.124.168
 171.68.124.165      PU PUXCPA06 LU 1  2
 171.68.124.0       255.255.255.0  PU PUXCPA06 LU 3  5
 171.68.110.0       255.255.255.0  PU PUXCPA06 LU 6  10
 171.68.120.0       255.255.255.0  PU PUXCPA06 LU 11 15
 171.68.130.0       255.255.255.0  PU PUXCPA06 LU 16 20

```

Viewing the Status of an LU

To display the status of the LUs, enter the following command for each LU:

```

router#show extended channel 1/2 tn3270-server PU puxcpa06 LU 06
Note: If state is ACT/NA then the client is disconnected
LU   name   client-ip:tcp      nail state   model   frames in out   idle for
6    LUXCPA06 171.68.110.40:36202 Y   P-BIND   327904E 4      3      0:3:10

```

PU is PUXCPA06, LU is STATIC unbound, negotiated TN3270
bytes 155 in, 1531 out; RuSize 256 in, 256 out; NegRsp 0 in, 0 out
pacing window 0 in, 0 out; credits 0 in, queue-size 0 in, 0 out

Although the client is a TN3270 non-E client, the LU assigned is a static LU.

Host Configuration

Figure 4-9 shows the configuration of the switched major node for this scenario. The LUs are configured as static LUs.

Figure 4-9 Scenario 4: Switched Major Node

```

*****
*      SWITCHED MAJOR NODE      *
*****
CBSWN6 VBUILD TYPE=SWNET,MAXGRP=10,MAXNO=10
*
PUXCPA06 PU      ADDR=01,
                PUTYPE=2,ANS=CONT,
                IDBLK=0CB,IDNUM=CBA06,
                USSTAB=USSSNA,DLOGMOD= SX32702S,MODETAB=ALAMODE

LUXCPA01 LU      LOCADDR=1
LUXCPA02 LU      LOCADDR=2
LUXCPA03 LU      LOCADDR=3
LUXCPA04 LU      LOCADDR=4
LUXCPA05 LU      LOCADDR=5
LUXCPA06 LU      LOCADDR=6
LUXCPA07 LU      LOCADDR=7
LUXCPA08 LU      LOCADDR=8
LUXCPA09 LU      LOCADDR=9
LUXCPA0A LU      LOCADDR=10

```

```

LUXCPA0B LU      LOCADDR=11
LUXCPA0C LU      LOCADDR=12
LUXCPA0D LU      LOCADDR=13
LUXCPA0E LU      LOCADDR=14
LUXCPA0F LU      LOCADDR=15
LUXCPA10 LU      LOCADDR=16
LUXCPA11 LU      LOCADDR=17
LUXCPA12 LU      LOCADDR=18
LUXCPA13 LU      LOCADDR=19
LUXCPA14 LU      LOCADDR=20
LUXCPA15 LU      LOCADDR=21

```

Verify the VTAM Configuration

To display the status of the switched major node, enter the following command:

```

D NET, ID=CBSWN6, E
IST097I DISPLAY ACCEPTED
IST075I NAME = CBSWN6, TYPE = SW SNA MAJ NODE 223
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST1656I VTAMTOPO = REPORT, NODE REPORTED - YES
IST084I NETWORK RESOURCES:
IST089I PUXCPA06 TYPE = PU_T2.1           , ACTIV
IST089I LUXCPA01 TYPE = LOGICAL UNIT      , ACTIV
IST089I LUXCPA02 TYPE = LOGICAL UNIT      , ACTIV
IST089I LUXCPA03 TYPE = LOGICAL UNIT      , ACTIV
IST089I LUXCPA04 TYPE = LOGICAL UNIT      , ACTIV
IST089I LUXCPA05 TYPE = LOGICAL UNIT      , ACTIV
IST089I LUXCPA06 TYPE = LOGICAL UNIT      , ACTIV
IST089I LUXCPA07 TYPE = LOGICAL UNIT      , ACTIV
IST089I LUXCPA08 TYPE = LOGICAL UNIT      , ACTIV
IST089I LUXCPA09 TYPE = LOGICAL UNIT      , ACTIV
IST089I LUXCPA0A TYPE = LOGICAL UNIT      , ACTIV
IST089I LUXCPA0B TYPE = LOGICAL UNIT      , ACTIV
IST089I LUXCPA0C TYPE = LOGICAL UNIT      , ACTIV
IST089I LUXCPA0D TYPE = LOGICAL UNIT      , ACTIV
IST089I LUXCPA0E TYPE = LOGICAL UNIT      , ACTIV
IST089I LUXCPA0F TYPE = LOGICAL UNIT      , ACTIV
IST089I LUXCPA10 TYPE = LOGICAL UNIT      , ACTIV
IST089I LUXCPA11 TYPE = LOGICAL UNIT      , ACTIV
IST089I LUXCPA12 TYPE = LOGICAL UNIT      , ACTIV
IST089I LUXCPA13 TYPE = LOGICAL UNIT      , ACTIV
IST089I LUXCPA14 TYPE = LOGICAL UNIT      , ACTIV
IST089I LUXCPA15 TYPE = LOGICAL UNIT      , ACTIV

```

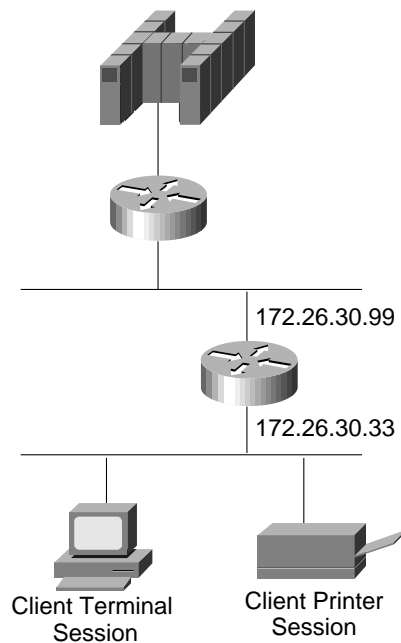
Scenario 5: TN3270 Server Using Nailing for Printer LUs

In this scenario, we are using LU nailing to control the LU names associated with printers sessions. In many environments, it is important for printer sessions to be controlled so that only a particular print server can access the output being sent to a given LU.

With TN3270E clients, it is possible to request printer sessions from a workstation to the mainframe. For example, if you want to establish a TN3270E printer session to an NT server that is associated with one of the LAN printers designated for 3270 printing, you can create a logical connection between a VTAM 3287 printer definition and the LAN or local printer (RFC 2355, LU 1 or LU 3).

However, if you used your TN3270 client to established a session with Customer Information Control System (CICS) and then you want to print from CICS to your local PC printer, you must open another TN3270 client session with the channel-attached router and establish a connection as a printer LU. To do this, the print client must request a static printer LU name, which must be defined in the switched major node as an LU 1 or LU 3. Alternatively, you can use LU nailing to associate a specific printer LU with a print client in the channel-attached router configuration. This method is called passthrough printing and keeps the client from requesting an incorrect LU name.

Figure 4-10 TN3270 Server Using Nailing for Printer LUs



Design Considerations

When implementing LU nailing for printer sessions, keep in mind the following guidelines:

- The easiest way to define printers is to use static LUs. If you define printers using dynamic LUs, you must note the LU name for printing. In this case, the LU name might change each time the client connects to its printer unless the print client is nailed to the DDDL.

- At this time, printer LUs can be assigned only using a connect request. You cannot use an associate request (see RFC 2355). IOS 11.2(17)BC and above support associate requests. Associate request makes it possible to define a partner printer in the TN3270 Server for a given terminal LU pool or single terminal. The client does not need to know the LU name of the partner printer in advance. If the client requests a printer using associate request, it sends its terminal LU name with the request and receives the printer LU that is associated with its terminal LU from the TN3270 Server. If the client uses a connect request, it must specify a printer LU name for the request or a printer LU must be nailed to the client on the channel-attached router. In most cases, nailing printer LUs is more straightforward and easier to manage than an associate request.
- If the TN3270 Server contains a nail statement that assigns a specific printer LU to a client and this client specifies another LU name for its request, the client's session request is rejected.
- If the client requests a printer session with an LU name that is defined as a terminal in the switched major node, the request is rejected at the Bind.

Router Configuration

We have configured CSNA and are ready to implement our TN3270 Server. In this scenario, we need to:

- Initiate the TN3270 Server
- Define the LUs
- Configure LU Nailing
- Verify the Configuration

Initiate the TN3270 Server

To initiate the TN3270 Server on the router, enter the following commands:

```
! enter interface configuration mode for the virtual interface in slot 1
router(config)#int channel 1/2
! create TN3270 Server entity
router(config-if)#tn3270-server
router(config-if)#lan token 0
router(cfg-lan-Token 0)#adapter 0 4000.4000.0001
router(config-if)#lan token 31
router(cfg-lan-Token 0)#adapter 31 4000.4000.4444
! set server-wide defaults for PU parameters
router(cfg-tn3270)#unbind-action keep
router(cfg-tn3270)#generic-pool permit
```

Define the LUs

To define the static LUs, enter the following command:

```
router(cfg-tn3270)#pu puxcpa07 0CBCB007 172.26.30.34 token-adapter 31 08 rmac
4000.2222.0000 LU-seed LUXCP7##
```

Configure LU Nailing

To specify the LUs that are assigned to specific clients, enter the following commands:

```
router(cfg-tn3270)#pu puxcpa07
router(tn3270-pu)#client ip 171.68.124.166 LU 1 2
router(tn3270-pu)#client printer ip 171.68.124.166 LU 7
```

Based on the configuration commands above, the client's terminal sessions will be nailed to LUXCP701 and LUXCP702. If the client requests a printer session, the TN3270 Server will assign the LU at LOCADDR 7.

Verify the Configuration

To verify the configuration, use the Cisco IOS **show** commands. The **show** commands allow you to view the general TN3270 Server configuration and configuration information about the specific PUs and LUs.

Viewing the Current Router Configuration

To display the current router configuration, enter the following command:

```
router#show run
Current configuration:
```

```
<deleted information>
```

```
interface Channell/2
 ip address 172.26.30.33 255.255.255.240
 no keepalive
 lan TokenRing 0
 adapter 0 4000.2222.0000
 adapter 31 4000.2222.1111
 TN3270-server
 PU PUXCPA07 0CBCB007 172.26.30.34 token-adapter 31 08 rmac 4000.2222.0000 LU-seed
 LUXCP7##
 client ip 171.68.124.166 LU 1 2
 client printer ip 171.68.124.166 LU 7
```

Viewing a List of LUs

To display the PU configuration parameters, statistics, and all the LUs currently attached to each PU, enter the following command:

```
router#show extended channel 1/2 tn3270-server PU puxcpa07
```

```
name(index)  ip:tcp          xid  state    link  destination  r-lsap
PUXCPA07(2)  172.26.30.34:23      0CBCB007 ACTIVE   tok 31 4000.2222.0000 04 08
```

```
LU-seed LUXCP7##
```

```
idle-time 0      keepalive 1800      unbind-act discon  generic-pool perm
ip-preced-screen 0 ip-preced-printer 0 ip-tos-screen 0 ip-tos-printer 0
```

```
bytes 3947 in, 19272 out; frames 97 in, 101 out; NegRsp 0 in, 0 out
```

```
actLUs 39, dactLUs 0, binds 0
```

Note: If state is ACT/NA then the client is disconnected

LU	name	client-ip:tcp	nail	state	model	frames	in	out	idle for
1	LUXCP701	never connected	Y	ACT/NA		1	1		0:17:32
2	LUXCP702	never connected	Y	ACT/NA		1	1		0:17:32
3	LUXCP703	never connected	N	ACT/NA		1	1		0:17:32
4	LUXCP704	never connected	N	ACT/NA		1	1		0:17:32
5	LUXCP705	never connected	N	ACT/NA		1	1		0:17:32
6	LUXCP706	never connected	N	ACT/NA		1	1		0:17:32
7	LUXCP707	171.68.124.166:1133	Y	P-BIND	3287S1	6	4		0:16:33
8	LUXCP708	never connected	N	ACT/NA		1	1		0:17:32
9	LUXCP709	never connected	N	ACT/NA		1	1		0:17:32
10	LUXCP70A	never connected	N	ACT/NA		1	1		0:17:32

client ip	mask	nail-type	LU first	LU last
171.68.124.166		screen	1	2
171.68.124.166		printer	7	

Host Configuration

Figure 4-11 shows the configuration of the switched major node for this scenario.

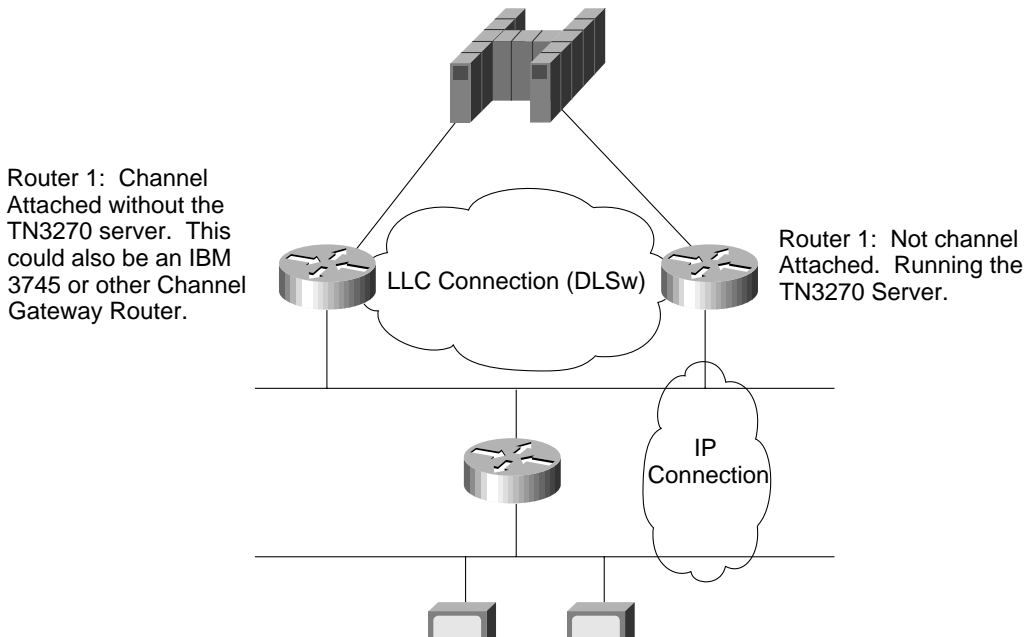
Figure 4-11 Scenario 5: Switched Major Node

```
*      SWITCHED MAJOR NODE
CBSWN7  VBUILD  TYPE=SWNET,MAXGRP=10,MAXNO=10
PUXCPA07  PU      ADDR=01,
           PUTYPE=2,ANS=CONT,
           IDBLK=0CB,IDNUM=CB007,
           USSTAB=USSSNA,DLOGMOD= SX32702S,MODETAB=ALAMODE
LUXCP701  LU      LOCADDR=1
LUXCP702  LU      LOCADDR=2
LUXCP703  LU      LOCADDR=3
LUXCP704  LU      LOCADDR=4
LUXCP705  LU      LOCADDR=5
LUXCP706  LU      LOCADDR=6,DLOGMOD=SCS,MODETAB=ISTINCLM
LUXCP707  LU      LOCADDR=7,DLOGMOD=SCS,MODETAB=ISTINCLM
LUXCP708  LU      LOCADDR=8,DLOGMOD=DSC4K,MODETAB=ISTINCLM
LUXCP709  LU      LOCADDR=9,DLOGMOD=DSC4K,MODETAB=ISTINCLM
LUXCP70A  LU      LOCADDR=10,DLOGMOD=DSC4K,MODETAB=ISTINCLM
```

Scenario 6: Using a Remote TN3270 Server

Sometimes it is necessary to run a TN3270 Server in a remote location with no channel attachment to the mainframe. In this case it is possible to bridge the resulting SNA traffic from the TN3270 Server to a channel gateway via RSRB, DLSw+, SRB, or SR/TLB. In this scenario, we describe how to configure a remote TN3270 Server using a channel-attached Cisco 7500 series router as a channel gateway. You can also use an IBM 3745 or any other device that offers the necessary functionality.

Figure 4-12 Using a Remote TN3270 Server



Design Considerations

When implementing a remote TN3270 Server, keep in mind the following guidelines:

- The TN3270 Server runs independently from the physical channel connection to the mainframe. The TN3270 Server no longer forwards the traffic from its internal virtual Token Ring adapter to another internal CSNA adapter. Instead, the traffic is now bridged from the TN3270 adapter in one of the CIP/CPA's internal virtual Token Rings to a remote adapter elsewhere. This remote adapter can be an external MAC address on a Token Ring (for example, an IBM 3745) or another virtual adapter on another virtual Token Ring (for example, a remote CIP/CPA). Performance can be affected by the network between the TN3270 Server and the channel gateway.
- This design requires you to configure an SRB connection between the channel-attached router internal LAN and the SRB ring group on the router. The traffic is then handled by DLSw or RSRB.

Router Configuration

There are two routers in this scenario. Router 1 provides the channel connection to the mainframe. It does not contain a TN3270 Server. It is using DLSw to transport the traffic from the remote router with the TN3270 Server (Router 2) to the mainframe. Router 2 contains the TN3270 Server and is connected to Router 1. In this scenario, we need to:

- Configure DLSw on Router 1
- Configure DLSw on Router 2
- Initiate the TN3270 Server
- Define the LUs
- Configure the Virtual Interface to Participate in the Source-Bridge Group
- Verify the Configuration

Configure DLSw on Router 1

This section discusses the steps required to configure Router 1.

Configuring the Source-Route Bridge and DLSw

To configure the source-route bridge and DLSw on Router 1, enter the following commands:

```
router1 (config)#source-bridge ring-group 1000
router1 (config)#dlsw local-peer peer-id 172.26.30.65
router1 (config)#dlsw remote-peer 0 tcp 172.26.30.81
```

Configure DLSw on Router 2

This section discusses the steps required to configure Router 2.

Configuring the Source-Route Bridge and DLSw

To configure the source-route bridge and DLSw on Router 2, enter the following commands:

```
router2 (config)#source-bridge ring-group 1000
router2 (config)#dlsw local-peer peer-id 172.26.30.81
router2 (config)#dlsw remote-peer 0 tcp 172.26.30.65
```

Initiate the TN3270 Server

To initiate the TN3270 Server on Router 2, enter the following commands:

```
! enter interface configuration mode for the virtual interface in slot 1
router(config)#int channel 1/2
! create TN3270 Server entity
router(config-if)#tn3270-server
router(config-if)#lan token 0
router(cfg-lan-Token 0)#adapter 0 4000.4000.0001
router(config-if)#lan token 31
router(cfg-lan-Token 0)#adapter 31 4000.4000.4444
! set server-wide defaults for PU parameters
router(cfg-tn3270)#unbind-action keep
router(cfg-tn3270)#generic-pool permit
```

Define the LUs

To define the static LUs, enter the following command:

```
router2(cfg-tn3270)#pu puxcpa07 0CBCB007 172.26.30.50 token-adapter 31 12 rmac
4000.2222.0000 lu-seed LUXCP7##
```

Configure the Virtual Interface to Participate in the Source-Bridge Group

To configure the Token Ring virtual interface of the channel-attached router to participate in the source-bridge group, enter the following commands:

```
router2 (config)#int channel 1/2
router2(config-if)#lan tokenring 0
router2(config-if)#source-bridge 999 1 1000
```

Verify the Configuration

To verify the configuration, use the Cisco IOS **show** commands. You need to verify the configuration on both routers. In the following command examples, the TN3270 Server on the virtual channel port of Router 1 is up and running. The real channel, however, is in shutdown state. The TN3270 Server PUs from Router 1 reach their destination XCA adapter via DLSW.

Viewing the Configuration of Router 1

To display the current configuration of Router 1, enter the following command:

```
router1#show run
Current configuration:

<deleted information>

source-bridge ring-group 1000
dlsw local-peer peer-id 172.26.30.65
dlsw remote-peer 0 tcp 172.26.30.81
!
interface Loopback0
 ip address 172.26.30.65 255.255.255.255
!
interface Ethernet0/0
 ip address 172.26.14.116 255.255.254.0
!
interface Channell/0
 no ip address
 no keepalive
 shutdown
!
interface Channell/1
 no ip address
 no keepalive
 csna 0120 00
!
interface Channell/2
 no ip address
 no keepalive
 lan TokenRing 0
 source-bridge 999 1 1000
 adapter 0 4000.2222.0000
```

Viewing the Configuration of Router 2

To display the current configuration of Router 2, enter the following command:

```
router1#show run
Current configuration:

<deleted information>

source-bridge ring-group 1000
dlsw local-peer peer-id 172.26.30.81
dlsw remote-peer 0 tcp 172.26.30.65
!
interface Loopback0
 ip address 172.26.30.81 255.255.255.255
!
interface Ethernet0/0
 ip address 172.26.14.114 255.255.254.0
!
interface Channell1/0
 no ip address
 no keepalive
 shutdown
!
interface Channell1/2
 ip address 172.26.30.49 255.255.255.240
 no keepalive
 lan TokenRing 0
 source-bridge 998 1 1000
 adapter 31 4000.4444.4444
 TN3270-server
 PU PUXCPA07 0CBCB007 172.26.30.50 token-adapter 31 12 rmac 4000.2222.0000 lu-seed
 LUXCP7##
```

Verifying DLSw Reachability on Router 2

To display DLSw+ reachability information, enter the following command:

```
router2#show dlsw reachability
DLSw Local MAC address reachability cache list
Mac Addr      status      Loc.   port          rif
4000.4444.4444 FOUND      LOCAL  Channell1/2  06B0.3E61.3E80

DLSw Remote MAC address reachability cache list
Mac Addr      status      Loc.   peer
4000.2222.0000 FOUND      REMOTE 172.26.30.65(2065) max-lf(4472)
```

Displaying Interface Status

To display the current status of the channel interface, enter the following command:

```
router2#show interface channell1/0
Channell1/0 is administratively down, line protocol is down
 Hardware is cyBus Channel Interface
 MTU 4096 bytes, BW 98304 Kbit, DLY 100 usec, rely 255/255, load 1/255
 Encapsulation CHANNEL, loopback not set
 ECA adapter card
```

Viewing the Status of the TN3270 Server and Its PUs

To display the current server configuration parameters and the status of the PUs defined in the server, enter the following command:

```
router2#show extended channel1/2 tn3270-server
              <current stats < connection stats   <response time(ms)
server-ip:tcp      LU in-use  connect disconn fail   host   tcp
172.26.30.50:23    255    0      1      1    0     0     0
total              255    0
configured max_LU 2100
idle-time         0          keepalive 1800      unbind-action disconnect
ip-precad-screen 0 ip-precad-printer 0 ip-tos-screen 0 ip-tos-printer 0
tcp-port         23          generic-pool permit no timing-mark

name(index)   ip:tcp      xid  state   link  destination  r-lsap
PUCXCPA07(1) 172.26.30.50:23 0CBCB007 ACTIVE tok 31 4000.2222.0000 04 12
```

Host Configuration

Figure 4-13 shows the configuration of the switched major node for this scenario.

Figure 4-13 Scenario 6: Switched Major Node

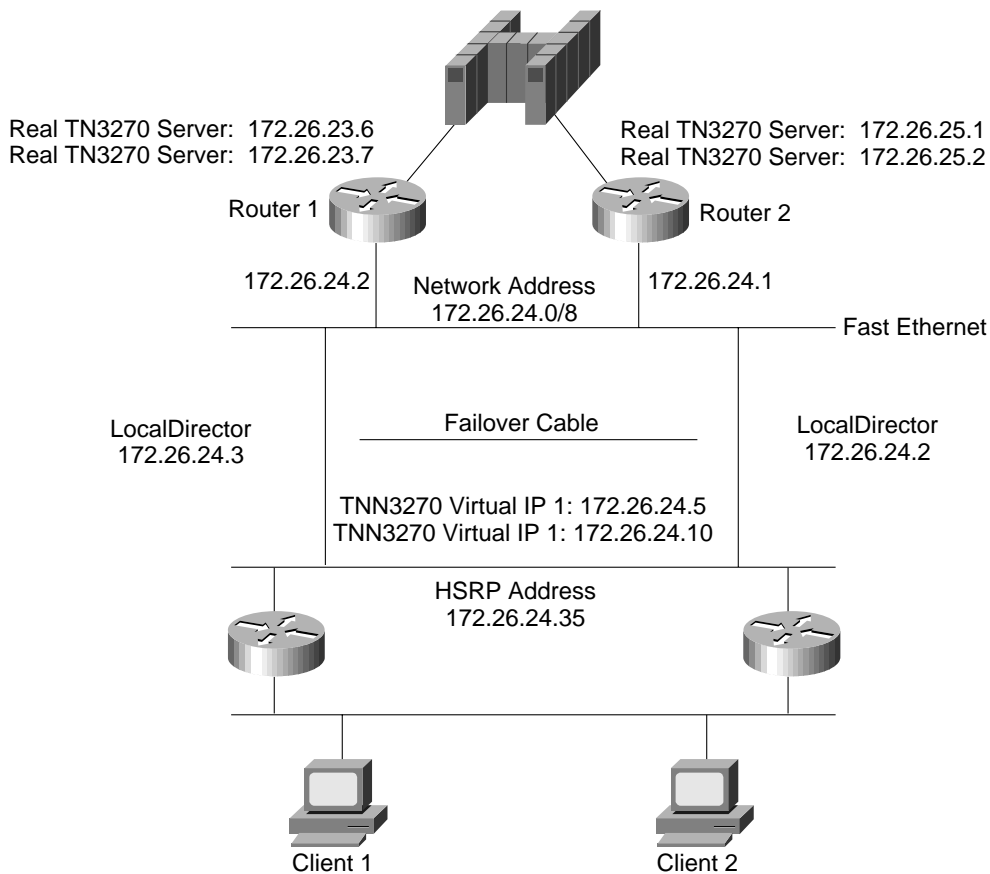
```
*          SWITCHED MAJOR NODE
CBSWN7 VBUILD TYPE=SWNET,MAXGRP=10,MAXNO=10
PUCXCPA07 PU   ADDR=01,
              PUTYPE=2,ANS=CONT,
              IDBLK=0CB,IDNUM=CB007,
              USSTAB=USSSNA,DLOGMOD= SX32702S,MODETAB=ALAMODE
LUXCP701 LU   LOCADDR=1
LUXCP702 LU   LOCADDR=2
LUXCP703 LU   LOCADDR=3
LUXCP704 LU   LOCADDR=4
LUXCP705 LU   LOCADDR=5
LUXCP706 LU   LOCADDR=6,DLOGMOD=SCS,MODETAB=ISTINCLM
LUXCP707 LU   LOCADDR=7,DLOGMOD=SCS,MODETAB=ISTINCLM
LUXCP708 LU   LOCADDR=8,DLOGMOD=DSC4K,MODETAB=ISTINCLM
LUXCP709 LU   LOCADDR=9,DLOGMOD=DSC4K,MODETAB=ISTINCLM
LUXCP70A LU   LOCADDR=10,DLOGMOD=DSC4K,MODETAB=ISTINCLM
```

Scenario 7: TN3270 Server with LocalDirector

One of the basic elements to any SNA network is network reliability through redundancy. Redundancy is also important when you implement a TN3270 Server. One way to get redundancy is to install a second TN3270 Server, but this does not solve the issue because the client still has to point to a single IP address. The solution is to provide a method of using multiple servers (for backup and load balancing) while providing the client a single IP address.

LocalDirector is used to achieve redundancy. LocalDirector is a device that dynamically load balances traffic between multiple servers to ensure timely access and response to requests. With LocalDirector, all traffic to the TN3270 Server passes through the LocalDirectors, which look like two PIX firewall machines connected with a failover cable. LocalDirector acts like a bridge, passing all packets from the client to the server after the connection is established. In this scenario, we describe how to implement a TN3270 Server with LocalDirector.

Figure 4-14 TN3270 Server with LocalDirector



Design Considerations

When implementing LocalDirector with a TN3270 Server, keep in mind the following guidelines:

- The LocalDirector behaves like a transparent bridge to forward data packets between its interfaces. Because of its bridge capability, LocalDirector must not be installed on the network parallel to another bridge.
- When you use two LocalDirectors, one is active and the other operates in standby mode.

- The virtual IP addresses defined on the LocalDirector must be part of an existing IP subnetwork, which is routed. Otherwise, you will not be able to reach the virtual IP addresses even though you can ping the real IP addresses. Preferably, the addresses should be part of the subnet that contains the local LAN segment where the TN3270 Servers and the LocalDirectors are located. Because LocalDirector uses a method comparable to network address translation (NAT) for the virtual server addresses, the virtual server addresses are not required to be in the same IP subnet as the LocalDirector. However, to avoid confusion in this scenario, we are configuring our network this way.
- The route command in the LocalDirector specifies a default gateway. This gateway is necessary to allow the LocalDirector and the virtual servers that are configured on it to reach the outside world. Because the default gateway is a single point of failure, you should run HSRP on your gateway routers and the LocalDirector should use the HSRP address for its default gateway on the route command.
- Because this solution supports load balancing, static LU definitions are not supported. If you must support a combination of static and dynamic LUs, you should configure all the clients that require dynamic LUs to point to the IP address of the LocalDirector and all the clients that require static LUs to point directly to the required PU. To further avoid issues of load balancing to a PU that is also being directly referenced we recommend that static LUs are defined on a PU that is not put in the same pool as the dynamic LUs.
- DNS is not necessary to support this solution.
- Future versions of LocalDirector will provide non-disruptive session recovery in case of a LocalDirector failure.
- LocalDirector supports only Ethernet and Fast Ethernet. For Token Ring networks, you must use DistributedDirector or HSRP. DistributedDirector, which is discussed in Scenario 8: TN3270 Server Using DistributedDirector, sends the client the target IP address of a TN3270 Server at session initiation and then establishes an end-to-end-session between the client and the server.
- If the LocalDirector is used in a switched environment, you must define two VLANs for the LocalDirector segments. Otherwise, a bridging loop occurs because the LocalDirector does not participate in the spanning-tree algorithm.

LocalDirector Configuration

After you have installed the LocalDirector, you must configure it for use with the TN3270 Servers.

Assigning an IP Address

To assign the LocalDirector IP address and subnet mask, enter the following command:

```
LocalDirector1 (config)#ip address 172.26.24.3 255.255.255.0
```

Defining the Virtual Servers

To define virtual servers and specify whether they are in or out of service, enter the following command:

```
LocalDirector1(config)#virtual 172.26.24.10:0:0 is
LocalDirector1(config)#virtual 172.26.24.5:0:0 is
```

This command specifies the virtual IP addresses of your TN3270 Servers. Normally, you will have only one, but to show a more complicated sample, we have defined two virtual server addresses in our scenario. Behind each of these virtual addresses is a cluster of several TN3270 Servers. The LocalDirector load balances the sessions between these servers and, if one TN3270 Server fails, the sessions can be reestablished at another server.

Setting the Load Balancing

To set the type of load balancing for each virtual server, use the following command:

```
predictor virtual_id {fastest|roundrobin|leastconns|weighted} [roundrobin|none]
```

Defining a Route to the Default Gateway

To define the route to the default gateway for the LocalDirector, enter the following command:

```
LocalDirector1(config)#route 0.0.0.0 0.0.0.0 172.26.24.35 1
```

The route command should point to the HSRP address of the gateway routers.

Defining the Backup Server

To identify the second, or backup, LocalDirector, enter the following commands:

```
LocalDirector1(config)#failover active
LocalDirector1(config)#failover ip address 172.26.24.4
```

Defining the Real Servers

To define the addresses of the real TN3270 Servers and specify whether they are in or out of service, enter the following commands:

```
LocalDirector1(config)#real 172.26.25.1:0 is
LocalDirector1(config)#real 172.26.25.2:0 is
LocalDirector1(config)#real 172.26.23.7:0 is
LocalDirector1(config)#real 172.26.23.6:0 is
```

Binding the Servers

To associate each virtual server to real servers, enter the following commands:

```
LocalDirector1(config)#bind 172.26.24.10:0:0 172.26.23.7:0
LocalDirector1(config)#bind 172.26.24.10:0:0 172.26.25.1:0
LocalDirector1(config)#bind 172.26.24.5:0:0 172.26.25.2:0
LocalDirector1(config)#bind 172.26.24.5:0:0 172.26.23.6:0
```

The clients use the virtual server IP address to establish a TN3270 session.

Verifying the LocalDirector Configuration

To verify the configuration of the LocalDirector, enter the following command:

```
LocalDirector #show run
Building configuration...
: Saved
: LocalDirector 415 Version 2.1.0.127
syslog output 20.7
no syslog console
enable password dfeaf10390e560aea745ccba53e044 encrypted
hostname adelaide
interface ethernet 0 100full
interface ethernet 0
interface ethernet 1 100full
interface ethernet 1
mtu 0 1500
mtu 1 1500
no secure 0
no secure 1
ping-allow 0
ping-allow 1
ip address 172.26.24.3 255.255.255.0
route 0.0.0.0 0.0.0.0 172.26.24.35 1
no rip passive
failover
failover ip address 172.26.24.4
```

```

password cisco
telnet 172.26.0.0 255.255.0.0
no snmp-server contact
no snmp-server location
virtual          172.26.24.10:0:0 is
virtual          172.26.24.5:0:0 is
real             172.26.25.1:0 is
real             172.26.25.2:0 is
real             172.26.23.7:0 is
real             172.26.23.6:0 is
name 172.26.25.1 router232701
name 172.26.25.2 router232702
name 172.26.25.3 router232703
name 172.26.25.4 router232704
name 172.26.23.9 router132704
name 172.26.23.8 router132703
name 172.26.23.7 router132702
name 172.26.23.6 router132701
bind             172.26.24.10:0:0      172.26.23.7:0
bind             172.26.24.10:0:0      172.26.25.1:0
bind             172.26.24.5:0:0       172.26.25.2:0
bind             172.26.24.5:0:0       172.26.23.6:0
threshold       172.26.25.1:0 0
threshold       172.26.25.2:0 0
threshold       172.26.23.7:0 0
threshold       172.26.23.6:0 0
: end

```

To display information about all the real servers defined, enter the following command:

```

LocalDirector1#show real
Real Machines:

```

Machine	Connect	State	Thresh	No Answer	TCP Reset	DataIn
				Reassigns	Reassigns	Conns
router232701:0	0	IS	0	0	0	0
router232702:0	3	IS	0	0	0	0
router132702:0	0	IS	0	0	0	0
router132701:0	2	IS	0	0	0	0

To display information about all the virtual servers defined, enter the following command:

```

LocalDirector1#show virtual

```

Virtual Machines:

Machine	State	Connect	Sticky	Predictor	Slowstart
172.26.24.10:0:0	IS	0	0	leastconns	roundrobin*
172.26.24.5:0:0	IS	5	0	leastconns*	roundrobin

To display information about all the bindings defined, enter the following command:

```

adelaide 3#show bind

```

Virtual	Real
172.26.24.10:0:0(IS)	maroubra32702:0(IS) sydney32701-:0(IS)
172.26.24.5:0:0(IS)	sydney32702:0(IS) maroubra32701:0(IS)

Router Configuration

There are two routers in this scenario. Each provides a TN3270 Server. Both are channel attached to the mainframe and both have an Ethernet connection to the 172.26.24.0 network that contains the LocalDirectors. In this scenario, we need to:

- Configure Router 1
- Configure Router 2
- Verify the Configuration

Configure Router 1

This section discusses the steps required to configure Router 1.

Initiating the TN3270 Server

To initiate the TN3270 Server, enter the following commands:

```
! enter interface configuration mode for the virtual interface in slot 1
router(config)#int channel 1/2
! create TN3270 Server entity
router(config-if)#tn3270-server
router(config-if)#lan token 0
router(cfg-lan-Token 0)#adapter 0 4000.4000.0001
router(config-if)#lan token 31
router(cfg-lan-Token 0)#adapter 31 4000.4000.4444
! set server-wide defaults for PU parameters
router(cfg-tn3270)#unbind-action keep
router(cfg-tn3270)#generic-pool permit
```

Defining the LUs

To define the LUs on Router 1, enter the following commands:

```
router1(cfg-tn3270)#pu pucc 12345674 172.26.23.6 token-adapter 2 04 rmac
4000.7505.0006 lu-seed LUCC##
router1(cfg-tn3270)#pu pudd 12345675 172.26.23.7 token-adapter 2 08 rmac
4000.7505.0006 lu-seed LUDD##
```

Configure Router 2

This section discusses the steps required to configure Router 2.

Initiating the TN3270 Server

To initiate the TN3270 Server, enter the following commands:

```
! enter interface configuration mode for the virtual interface in slot 2
router(config)#int channel 2/2
! create TN3270 Server entity
router(config-if)#tn3270-server
router(config-if)#lan token 0
router(cfg-lan-Token 0)#adapter 0 4000.4000.0001
router(config-if)#lan token 31
router(cfg-lan-Token 0)#adapter 31 4000.4000.4444
! set server-wide defaults for PU parameters
router(cfg-tn3270)#unbind-action keep
router(cfg-tn3270)#generic-pool permit
```

Defining the LUs

To define the LUs on Router 2, enter the following commands:

```
router1(cfg-tn3270)#pu puaaa 12345678 172.26.25.1 token-adapter 2 04 rmac
4000.7505.0001 lu-seed LUAAA##
router1(cfg-tn3270)#pu pubbb 12345677 172.26.25.2 token-adapter 2 08 rmac
4000.7505.0001 lu-seed LUBBB##
```

Verify the Configuration

To verify the configuration, use the Cisco IOS **show** commands. Verify the configuration on both routers. In the following command examples, each router is running a TN3270 Server, both have channel connections to the mainframe, and both have Ethernet connections to the 176.26.24.0 network.

Viewing the Configuration of Router 1

To display the current configuration of Router 1, enter the following command:

```
router1#show run
Current configuration:

<deleted information>

microcode CIP flash slot0:CIP25-7.exe
microcode reload
!
interface FastEthernet0/1/0
 ip address 172.26.24.2 255.255.255.0
 no ip redirects
 no keepalive
!
interface Channel1/0
 no ip address
 no keepalive
 csna 0110 00
!
interface Channel1/1
 no ip address
 no keepalive
 shutdown
!
interface Channel1/2
 ip address 172.26.23.11 255.255.255.0
 no keepalive
 lan TokenRing 0
 adapter 1 4000.7505.0006
 adapter 2 4000.7505.9999
TN3270-server
 PU PUCCC 12345674 172.26.23.6 token-adapter 2 04 rmac 4000.7505.0006 lu-seed
 LUCCC##
 PU PUDDD 12345675 172.26.23.7 token-adapter 2 08 rmac 4000.7505.0006 lu-seed
 LUDDD##
```

Viewing the Status of PUs on Router 1

To display the current server configuration parameters and the status of the PUs defined in the server, enter the following command:

```
router1#show extended channel1/2 tn3370-server
          <current stats < connection stats <response time(ms)
server-ip:tcp      LU in-use  connect disconn fail  host  tcp
172.26.23.6:23    255    3      943    940    0     0     0
172.26.23.7:23    255    2       2       0     0     0     0
total              510    5
configured max_LU 2100
idle-time 0        keepalive 1800      unbind-action disconnect
ip-prec-d-screen 0 ip-prec-d-printer 0 ip-tos-screen 0 ip-tos-printer 0
tcp-port 23        generic-pool permit no timing-mark

name(index)  ip:tcp      xid  state  link  destination  r-lsap
PUCCC(9)    172.26.23.6:23  12345674 ACTIVE tok 2 4000.7505.0006 04 04
PUDDD(11)   172.26.23.7:23  12345675 ACTIVE tok 2 4000.7505.0006 04 08
```

Viewing a List of LUs on Router 1

To display the PU configuration parameters, PU statistics, and all the LUs currently attached to each PU, enter the following command:

```
router1#show extended channel1/2 tn3270-server PU puccc

name(index)  ip:tcp      xid  state  link  destination  r-lsap
PUCCC(9)    172.26.23.6:23  12345674 ACTIVE tok 2 4000.7505.0006 04 04

LU-seed LUCCC##
idle-time 0        keepalive 1800      unbind-act discon generic-pool perm
ip-prec-d-screen 0 ip-prec-d-printer 0 ip-tos-screen 0 ip-tos-printer 0
bytes 656 in, 937 out; frames 14 in, 15 out; NegRsp 0 in, 0 out
actLUs 3, dactLUs 0, binds 0
Note: If state is ACT/NA then the client is disconnected
LU  name  client-ip:tcp  nail state  model  frames in out  idle for
1  LUCCC01  172.26.2.202:1163  N  P-BIND  327802E  3  2  1:16:18
2  LUCCC02  172.26.2.204:1301  N  P-BIND  327802  8  5  0:4:56
3  LUCCC03  172.26.2.203:1674  N  P-BIND  327902E  3  2  0:6:32
```

Viewing the Configuration of Router 2

To display the current configuration of Router 2, enter the following command:

```
router2#show run
Current configuration:
```

```
<deleted information>
```

```
microcode CIP flash slot1:CIP25-7
microcode reload
!
interface Channel2/0
  no ip address
  no keepalive
  csna 0110 00
!
interface Channel2/1
  no ip address
  no keepalive
!
interface Channel2/2
  ip address 172.26.25.10 255.255.255.0
  no keepalive
  lan TokenRing 0
  adapter 0 4000.7505.0001
  adapter 2 4000.7505.8888
TN3270-server
  PU PUA   12345678 172.26.25.1 token-adapter 2 04 rmac 4000.7505.0001 lu-seed
  LUAAA##
  PU PUB   12345677 172.26.25.2 token-adapter 2 08 rmac 4000.7505.0001 lu-seed
  LUBBB##
!
interface FastEthernet3/1/0
  ip address 172.26.24.1 255.255.255.0
  no ip redirects
```

Viewing the Status of PUs on Router 2

To display the current server configuration parameters and the status of the PUs defined in the server, enter the following command:

```
router2#show extended channel2/2 tn3270-server
          <current stats < connection stats <response time(ms)
server-ip:tcp      LU in-use  connect disconn fail  host  tcp
172.26.25.1:23    255    8    1371    1363    0    0    0
172.26.25.2:23    255    3    168     165    0    0    0
total              510    11
configured max_LU 2100
idle-time 0        keepalive 1800    unbind-action disconnect
ip-precend-screen 0 ip-precend-printer 0 ip-tos-screen 0 ip-tos-printer 0
tcp-port 23        generic-pool permit no timing-mark

name(index)  ip:tcp      xid  state  link  destination  r-lsap
PUAAA(9)     172.26.25.1:23 12345678 ACTIVE tok 2 4000.7505.0001 04 04
PUBBB(11)    172.26.25.2:23 12345677 ACTIVE tok 2 4000.7505.0001 04 08
```

Viewing a List of LUs on Router 2

To display the PU configuration parameters, PU statistics, and all the LUs currently attached to each PU, enter the following command:

```
router2#show extended channel2/2 tn3270-server PU puaaa
```

```
name(index)   ip:tcp           xid  state    link  destination  r-lsap
PUAAA(9)      172.26.25.1:23  12345678 ACTIVE  tok 2  4000.7505.0001 04 04
```

```
LU-seed LUAAA##
```

```
idle-time 0      keepalive 1800      unbind-act discon  generic-pool perm
```

```
ip-precad-screen 0 ip-precad-printer 0 ip-tos-screen 0 ip-tos-printer 0
```

```
bytes 9173 in, 40475 out; frames 222 in, 209 out; NegRsp 0 in, 0 out
```

```
actLUs 11, dactLUs 0, binds 4
```

```
Note: if state is ACT/NA then the client is disconnected
```

LU	name	client-ip:tcp	nail	state	model	frames in	frames out	idle for
1	LUAAA01	172.26.2.202:1160	N	P-BIND	327802E	14	11	1:15:2
2	LUAAA02	172.26.2.202:1232	N	P-BIND	327802E	14	11	0:39:8
3	LUAAA03	172.26.2.202:1133	N	ACT/NA	327802E	11	9	1:19:21
4	LUAAA04	172.26.2.202:1169	N	ACT/NA	327802E	44	30	0:39:17
5	LUAAA05	172.26.24.50:1036	N	ACT/NA	327802E	5	3	1:26:31
6	LUAAA06	172.26.2.202:1166	N	P-BIND	327802E	8	5	1:14:52
7	LUAAA07	172.26.24.50:1081	N	P-BIND	327802E	28	17	0:3:29
8	LUAAA08	172.26.24.50:1086	N	P-BIND	327802E	23	14	0:3:26
9	LUAAA09	172.26.24.50:1087	N	P-BIND	3278S2E	44	29	0:3:23
10	LUAAA0A	172.26.24.50:1084	N	P-BIND	3278S2E	23	14	0:3:28
11	LUAAA0B	172.26.2.204:1303	N	P-BIND	327802	8	5	0:2:53

Host Configuration

Figure 4-15 shows the configuration of the switched major node for this scenario.

Figure 4-15 Scenario 7: Switched Major Node

```
LLBSMNA VBUILD TYPE=SWNET,MAXGRP=10,MAXNO=10
```

```
*
```

```
PUAAA  PU      ADDR=01,                                     X
        PUTYPE=2, IDBLK=123, IDNUM=45678, ANS=CONT,   X
        LUSEED=LUAAA##, LUGROUP=LLBDDD1
PUBBB  PU      ADDR=02,                                     X
        PUTYPE=2, IDBLK=123, IDNUM=45677, ANS=CONT,   X
        LUSEED=LUBBB##, LUGROUP=LLBDDD1
PUCCC  PU      ADDR=03,                                     X
        PUTYPE=2, IDBLK=123, IDNUM=45674, ANS=CONT,   X
        LUSEED=LUCCC##, LUGROUP=LLBDDD1
PUDDD  PU      ADDR=04,                                     X
        PUTYPE=2, IDBLK=123, IDNUM=45675, ANS=CONT,   X
        LUSEED=LUDDD##, LUGROUP=LLBDDD1
```

Scenario 8: TN3270 Server Using DistributedDirector

As discussed in the previous scenario, the issue of redundancy is a high priority in the data center. There are several methods of load balancing the TN3270 Servers. The DistributedDirector is one of these methods.

The Cisco DistributedDirector is a device that efficiently distributes Internet services among topologically dispersed servers on the Internet or an intranet. It provides scalable, transparent, and network-intelligent traffic load distribution. Using the DRP, a simple User Datagram Protocol (UDP)-based application developed by Cisco, the DistributedDirector queries properly configured Cisco routers in the field for Exterior Gateway Protocol (EGP) and Internal Gateway Protocol (IGP) topological “distance” metrics. With this information and other configuration metrics, the DistributedDirector assigns an optimal distributed server to each client. As a result, users are transparently and automatically assigned a distributed server anywhere on the Internet.

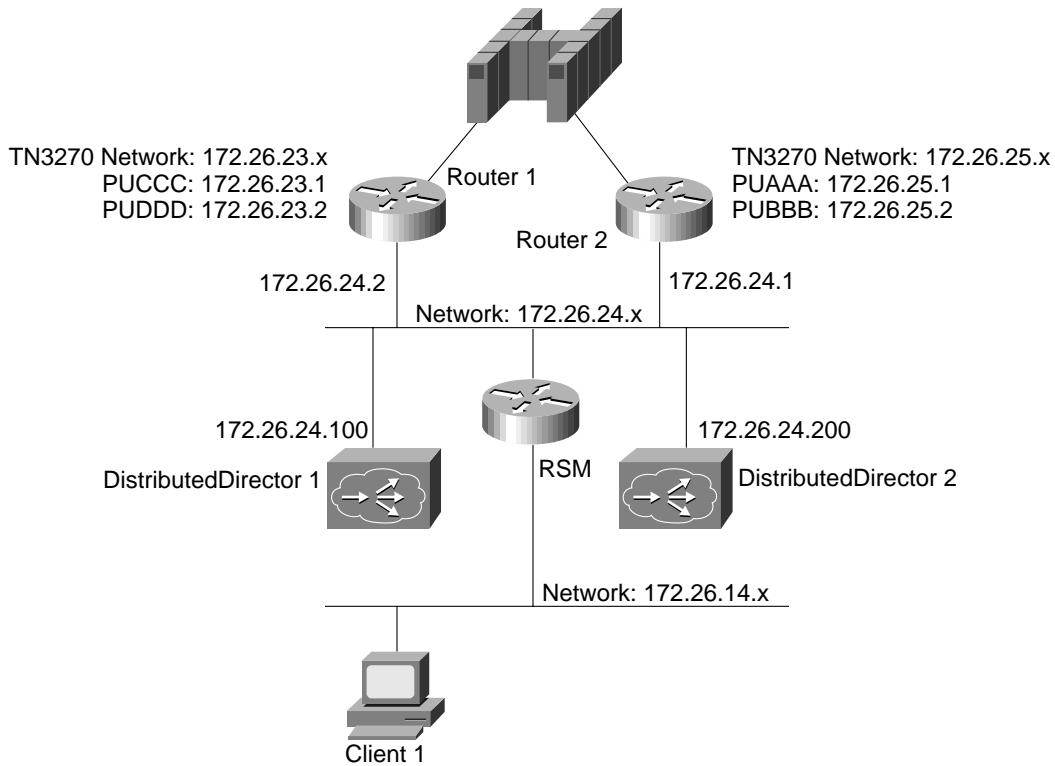
DistributedDirector requires a DNS server in the network. The DistributedDirector can be configured to act as a DNS. When you use DistributedDirector, you should configure your clients with a primary DNS IP address and a backup DNS IP address. The DistributedDirectors are known to the DNS. The primary DNS receives the request from the client and passes the request on to a DistributedDirector, which resolves the name to one of the servers. The method used to select the server depends on the configuration of the DistributedDirector. You can configure the DistributedDirector to use one of the following methods:

- Preference—The DistributedDirector always chooses a specific active server.
- Random—The DistributedDirector randomly chooses between the servers.
- Portion—You assign a relative portion metric to each server and each server gets that portion of the connections. For example, if server A is assigned a portion of 1 and server B is assigned a portion of 2, then server A receives one third of the connections and server B receives two-thirds of the connections.

The DistributedDirector determines whether a TN3270 Server is active by periodically checking it with Telnet. You configure the Telnet port and the timers that specify how often the DistributedDirector should Telnet to the server (or retry upon failure). If the TN3270 Server goes down, the DistributedDirector will discover this in one timer interval. In our scenario, we set this timer to 10 seconds. If the DistributedDirector is unable to reach the server, the DistributedDirector stops passing this server’s IP address to clients and continues to attempt to Telnet to the server to determine if the server recovers. Upon recovery, the DistributedDirector starts passing the server’s address to clients again.

In this scenario, we describe how to implement a TN3270 Server with DistributedDirector

Figure 4-16 TN3270 Server Using DistributedDirector



Design Considerations

When configuring the DistributedDirector and TN3270 Server, keep in mind the following guidelines:

- Unlike LocalDirector, the DistributedDirector does not participate in the packet flow after a connection is established. DistributedDirector resolves DNS names for the client and then the client connects directly to the server.
- The DistributedDirector must fit into the existing DNS scheme. The DistributedDirector for the channel-attached router becomes a start of authority for certain domain names and the primary DNSs must know about the DistributedDirector and start of authority.
- If a primary DNS is used, you must give the authority of the TN3270 subdomain to the DistributedDirectors.
- The DistributedDirector DNS system is a modification of the normal DNS system and allows the DNS server to determine the best IP address for clients connecting to a server. The DNS caching name server mode is the appropriate DistributedDirector mode for use with TN3270 Servers.
- The DistributedDirector periodically Telnets to each TN3270 Server to determine whether the server is active. Therefore, you can expect to see more connects and disconnects when you display the TN3270 Server statistics.
- If the TN3270 client resides on a machine that contains other applications that need to consult the parent domain for addresses, the primary DNS needs to be configured to direct queries for the TN3270 Server subdomain to the DistributedDirector DNS.

- When using DistributedDirector as the DNS, all higher level DNS servers and all secondary DNS servers must be upgraded to Bind level 4.8.3 or higher. Versions of Bind prior to 4.8.3 contain a problem that causes the DNS server to hold information for up to 5 minutes even if the Time-To-Live (TTL) value is set to zero. If a previous version of Bind is running on any of the higher level DNS servers that clients might contact when translating the servers hostname and if these DNS servers decide to recursively ask the query themselves and cache the result (the normal case for Bind), then they cache only one of the many potential IP addresses for the hostname. This process defeats the purpose of the DistributedDirector system.

Note: In our scenario the DistributedDirectors are used as DNSs and each client is configured with the IP addresses of both DistributedDirectors. Therefore, when we bring down one DistributedDirector, the client tries the other and there is no perceptible downtime.

DistributedDirector Configuration

Once you install and set up the DistributedDirector devices, you must configure the devices to receive DNS queries and to correlate them with the IP address of the desired server.

Note: The DistributedDirector documentation focuses on the use of the DistributedDirector with Web servers, which are likely to be located in different geographical locations. There are additional metrics and configuration parameters required in support of Web servers that are not necessary for the TN3270 Server scenario described in this configuration.

Configure the Primary DNS

To configure the IP address of the primary DNS, enter the following command:

```
DistributedDirector1#ip name-server 172.26.24.100
```

Configure the Virtual Host Name for the Servers

To define the virtual host name to be used for the set of TN3270 Servers, enter the following command:

```
DistributedDirector1#ip director host TN3270.xyz.com
```

Associate Real Servers with the Virtual Host Name

To identify the IP addresses of the TN3270 Servers associated with the virtual host name, enter the following command:

```
DistributedDirector1#ip host TN3270.xyz.com 172.26.25.1 172.26.23.6 172.26.30.51
```

Up to 8 IP addresses per name can be specified.

Configure Verification Parameters

DistributedDirector is designed to avoid returning the address of an inactive server by periodically checking whether a Telnet connection can be opened to each of them. To define the parameters for the connectivity check on the TN3270 Servers, enter the following command:

```
DistributedDirector1#ip director host TN3270.xyz connect 23 interval 10
```

This command indicates that the DistributedDirector should attempt to establish a connection using port 23 (Telnet) every 2 minutes. For the connection interval, a value of 1 or 2 is recommended. If you specify a larger value, there may be a delay between the time that a server goes down and the time that the DistributedDirector becomes aware of its status. As a result, users could be directed to a server that is not available.

Configure the Selection Method

There are three methods of determining which IP address will be sent in response to the DNS request for the TN3270 server. In our scenario, we are configuring the DistributedDirector to select the IP address randomly. To set the default weights to use the random metric for sorting, so that a server IP address is randomly selected from among the servers that are considered active, enter the following command:

```
DistributedDirector1#ip director default-weights ran 1
```

Designate the DistributedDirector as a Primary DNS

To configure the DistributedDirector as the primary DNS server for the new subdomain, enter the following command:

```
DistributedDirector1#ip dns primary TN3270.xyz.com soa distributeddirector1.xyz.com  
sysadmin.xyz.com 60 10 10 10
```

This command tells the DistributedDirector1 that it is the primary DNS server authoritative for the domain. It indicates that the DNS host name of the DistributedDirector is distributeddirector1.xyz.com, and defines the administrative contact.

Turn off Caching

If several client queries come from a single IP address, such as when the client software is used from terminals run on one machine, then you should disable DistributedDirector caching. To turn off caching, issue the following command:

```
DistributedDirector #no ip dir cache
```

If you do not enter this command, there is a timeout of 60 seconds in which the same server IP address is returned to requests from the same client IP address.

Restrict the Names Sorted by the DistributedDirector

If the DistributedDirector is to be used to service queries for other names, then you should restrict sorting to the name or names designating TN3270 Servers. This example permits the sorting of names that start with “TN3270” and denies all other requests:

```
DistributedDirector1#ip director access-group 1  
DistributedDirector1#ip director access-list 1 permit ^TN3270.*  
DistributedDirector1#ip director access-list 1 deny .*
```

Designate Authority for the Subdomain

To give authority for the TN3270 Server subdomain to the DistributedDirector DNS, you must modify the configuration of the DNS server. This modification is done by inserting the following lines in the DNS database:

```
TN3270.xyz.com. IN NS distributeddirector1.xyz.com  
distributeddirector1.xyz.com. IN A 172.26.24.100
```

Note: This step can be left out if the TN3270 clients will consult the DistributedDirector DNS directly.

If a backup DistributedDirector is used (to provide redundancy), you would add additional lines to the DNS configuration to allow for the backup DD.

Configure the TN3270 Clients

Configure the TN3270 client to use the domain name “TN3270” to look up the IP address before connecting to TN3270 server.

The DNS used by the resolver on the client machine may be either the DistributedDirector DNS or the DNS for “xyz.com.” It would typically be xyz.com if there were other applications running on the machine that needed to use other domain names. If the client resolver uses a default domain other than xyz.com, then specify the full domain name (in other words, TN3270.xyz.com) when configuring the TN3270 client.

Verify the Configuration

To verify the configuration, use the Cisco IOS **show** commands. Verify the configuration on both DistributedDirectors.

Viewing the Configuration of DistributedDirector 1

To display the current configuration of DistributedDirector 1, enter the following command:

```
DistributedDirector1#show run
Building configuration...
```

```
Current configuration:
!
version 11.1
service udp-small-servers
service tcp-small-servers
!
hostname distributeddirector1
!
boot system flash c4500-w3-mz_11-19_IA.bin
enable password cisco
!
!
interface Ethernet0
 ip address 172.26.24.100 255.255.255.0
 media-type 10BaseT
!
router eigrp 777
 network 172.26.0.0
!
ip default-gateway 172.26.24.100
ip host TN3270.xyz.com 172.26.25.1 172.26.23.6 172.26.30.51
ip name-server 172.26.24.100
no ip classless
ip dns primary TN3270.xyz.com soa distributeddirector1.xyz.com sysadmin.xyz.com 60 10
 10 10
no ip director cache
ip director server 172.26.25.1 23 portion 2
ip director server 172.26.23.6 23 portion 1
ip director server 172.26.30.51 23 portion 2
ip director hosts TN3270.xyz.com priority drp-s 1
ip director hosts TN3270.xyz.com connect 23 interval 10
ip director hosts TN3270.xyz.com port-service 23
logging buffered
snmp-server community public RO
snmp-server community private RW
snmp-server packetsize 4096
end
```

Viewing the Configuration of DistributedDirector 2

To display the current configuration of DistributedDirector 2, enter the following command:

```
DistributedDirector2#show run
Building configuration...

Current configuration:
!
version 11.1
service udp-small-servers
service tcp-small-servers
!
hostname distributeddirector2
!
boot system flash c4500-w3-mz_11-19_IA.bin
enable password cisco
!
interface Ethernet0
 ip address 172.26.24.200 255.255.255.0
 no ip mroute-cache
 no ip route-cache
 media-type 10BaseT
!
router eigrp 777
 network 172.26.0.0
!
ip default-gateway 172.26.24.200
ip host TN3270.xyz.com 172.26.25.1 172.26.23.6
ip domain-name xyz.com
ip name-server 172.26.24.200
no ip classless
ip dns primary TN3270.xyz.com soa distributeddirector1.xyz.com sysadmin.xyz.com 60 10
 10 10
no ip director cache
ip director server 172.26.25.1 23 portion 2
ip director server 172.26.23.6 23 portion 1
ip director hosts TN3270.xyz.com priority por 1
ip director hosts TN3270.xyz.com connect 23 interval 10
ip director hosts TN3270.xyz.com port-service 23
logging buffered
!
end
```

Configure Extra LUs

For the DistributedDirector system to work well with TN3270 Servers at times when most or all of the clients are active, and for redundancy when servers go down, there must be extra LUs available on each of the servers.

The DistributedDirector random metric is used to distribute the load among the servers. Although this randomness tends to distribute the sessions evenly over time, it also means that there are times when one server is advertised to clients more than others.

When the number of active clients approaches 100 percent of the total number of clients, some servers must cope with more than total-no-of-client/no-of-servers LUs. When the limit is reached on one server, clients retry the DNS name until they are sent to a server that is not full. The number of extra LUs you define here must be balanced against the likelihood of close to 100 percent client activation occurring in the particular network and the client dissatisfaction with the retry option.

For redundancy, extra LUs must be configured on each server to allow the system to cope if one or more of the TN3270 Servers go down. The best case is to have each server capable of handling the full total-no-of-clients load.

To provide redundancy each channel-attached router needs maximum-LUs (the maximum number of simultaneously connected clients) configured for the worst case situation.

Host Configuration

Figure 4-17 shows the switched major node for this scenario.

Figure 4-17 Scenario 8: Switched Major Node

```

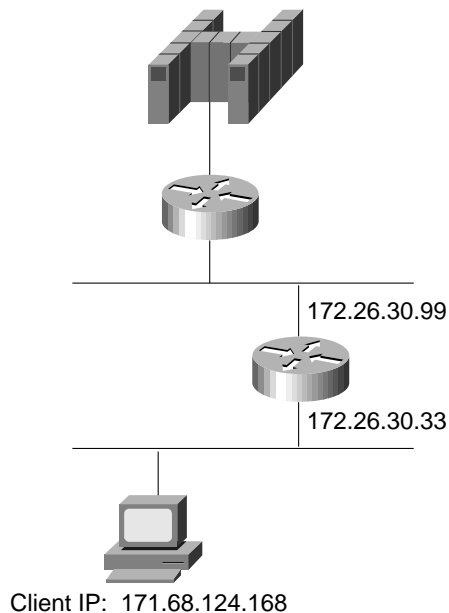
LLBSMNA VBUILD TYPE=SWNET,MAXGRP=10,MAXNO=10
*
PUAAA PU ADDR=01, X
PUTYPE=2, IDBLK=123, IDNUM=45678, ANS=CONT, X
LUSEED=LUAAA##, LUGROUP=LLBDDD1
PUBBB PU ADDR=02, X
PUTYPE=2, IDBLK=123, IDNUM=45677, ANS=CONT, X
LUSEED=LUBBB##, LUGROUP=LLBDDD1
PUCCC PU ADDR=03, X
PUTYPE=2, IDBLK=123, IDNUM=45674, ANS=CONT, X
LUSEED=LUCCC##, LUGROUP=LLBDDD1
PUDDD PU ADDR=04, X
PUTYPE=2, IDBLK=123, IDNUM=45675, ANS=CONT, X
LUSEED=LUDDD##, LUGROUP=LLBDDD1

```

Scenario 9: TN3270 Server Using a Direct PU and INCLUD0E

With direct PUs, there is a potential problem because the LU names in VTAM and LU names on the channel-attached router can be different. This happens for both static and dynamic LUs. When migrating to a network that uses both SNA and IP, some administrators may find that they are using an LU naming convention that results in names that the LU-seed parameter cannot generate. To solve this problem, use direct PUs and the INCLUD0E parameter. By coding INCLUD0E on the VTAM switched PU, VTAM sends each LU name in a 0E control vector of the ACTLU to the channel-attached router. The channel-attached router uses this name as the LU name rather than using the name produced by the LU-seed.

Figure 4-18 TN3270 Server Using a Direct PU and INCLUD0E



Design Considerations

When using direct PUs and the INCLUD0E parameter with the TN3270 Server, keep in mind the following guidelines:

- You cannot use this solution if you are using the TN3270 Server as a remote server (that is, not connecting to the host via XCA, but connecting through an FEP). The current releases of NCP do not support the INCLUD0E parameter, and the 0E vector will stop at the FEP and will not pass through to the router.
- If you want the LU names on the channel-attached router to be different from the LU names on VTAM, do not use the INCLUD0E parameter on the switched PU.
- To use INCLUD0E, you must be using VTAM 4.4 and you must apply the PTFs for the following APARS:
 - APAR OW25501
 - APAR OW31436
 - APAR OW31805

- INCLUD0E is relevant only for direct PUs. For DLUR PUs, the LU name is always passed from VTAM to the channel-attached router at ACTLU time.
- If you want to use the INCLUD0E parameter and you are using an FEP, the FEP will require updates.

Router Configuration

We have configured CSNA and are now ready to implement our TN3270 Server. In this scenario, we need to:

- Initiate the TN3270 Server
- Define the LUs
- Verify the Configuration

Initiate the TN3270 Server

To initiate the TN3270 Server on the router, enter the following commands:

```
! enter interface configuration mode for the virtual interface in slot 1
router(config)#int channel 1/2
! create TN3270 Server entity
router(config-if)#tn3270-server
router(config-if)#lan token 0
router(cfg-lan-Token 0)#adapter 0 4000.4000.0001
router(config-if)#lan token 31
router(cfg-lan-Token 0)#adapter 31 4000.4000.4444
! set server-wide defaults for PU parameters
router(cfg-tn3270)#unbind-action keep
router(cfg-tn3270)#generic-pool permit
```

Define the LUs

To define the static LUs, enter the following command:

```
router(cfg-tn3270)#pu pui0e 12345678 172.26.20.34 token-adapter 31 10 rmac
4000.4000.1111 lu-seed LUI0E##
```

Verify the Configuration

To verify the configuration, use the Cisco IOS **show** commands. The IOS show commands allow you to view the general TN3270 Server configuration as well as configuration information about the specific PUs and LUs.

Viewing the Current Router Configuration

To display the current router configuration, enter the following command:

```
router1 #show run
Building configuration...

<deleted information>

microcode CIP flash slot0:CIP25-7
microcode reload
source-bridge ring-group 400
!
interface Ethernet0/0
 ip address 172.26.14.112 255.255.254.0
 shutdown
!
interface Ethernet0/1
 ip address 172.26.20.97 255.255.255.240
!
```

```

interface Channel1/0
 ip address 172.26.20.18 255.255.255.240
 no keepalive
 csna 0110 01
 csna 0120 02
!
interface Channel1/2
 ip address 172.26.20.33 255.255.255.240
 no keepalive
 lan TokenRing 0
 source-bridge 401 1 400
 adapter 1 4000.4000.1111
 adapter 2 4000.4000.2222
 adapter 31 4000.4000.4444
TN3270-server
 unbind-action keep
 PU PUI0E 12345678 172.26.20.34 token-adapter 31 10 rmac 4000.4000.1111 lu-seed
LUI0E##
 timing-mark
!
interface TokenRing10/3
 ip address 10.100.100.1 255.255.255.0
 shutdown
 ring-speed 16
 source-bridge 500 1 400
 source-bridge spanning

```

Notice the LU-seed of LUI0E.

Viewing a List of LUs

To display the PU configuration parameters, PU statistics, and all the LUs currently attached to each PU, enter the following command:

```
router#show extended channel1/2 tn3270-server PU pui0e
```

```

name(index)   ip:tcp           xid  state    link  destination  r-lsap
PUI0E(2)      172.26.20.34:23 12345678 ACTIVE  tok 31 4000.4000.1111 04 10

```

```
LU-seed LUI0E##
```

```

idle-time 0 keepalive 1800 unbind-act keep generic-pool perm
ip-preced-screen 0 ip-preced-printer 0 ip-tos-screen 0 ip-tos-printer 0
bytes 2264 in, 2764 out; frames 47 in, 54 out; NegRsp 0 in, 0 out
actLUs 14, dactLUs 9, binds 0

```

Note: if state is ACT/NA then the client is disconnected

LU	name	client-ip:tcp	nail	state	model	frames in	frames out	idle for
1	LUNAME1	never connected	N	ACT/NA		1	1	0:9:2
2	LU2NAM1	never connected	N	ACT/NA		1	1	0:9:2
3	SOMENAM	never connected	N	ACT/NA		1	1	0:9:2
4	LUEEE04	172.26.2.199:1902	N	ACT/NA	327802E	5	3	0:6:39
5	LUEEE05	172.26.2.197:1741	N	P-BIND	327802	3	2	0:2:15

Note: The LU names on the channel-attached router and in VTAM are the same. The dynamic LUs that were created (LUEEE04 and LUEEE05) match VTAM's LUSEED naming convention instead of the naming convention used by the LU-seed on the channel-attached router.

Host Configuration

Figure 4-19 shows the switched major node for this scenario.

Figure 4-19 Scenario 9: Switched Major Node

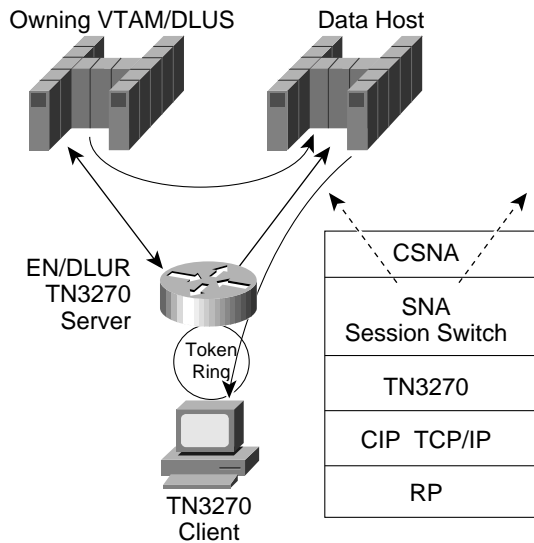
```
LLBSMNB VBUILD TYPE=SWNET,MAXGRP=10,MAXNO=10
PUIOE   PU      ADDR=01,
          PUTYPE=2, IDBLK=123, IDNUM=45678, ANS=CONT,
          LUSEED=LUEEE##, LUGROUP=DDDMVSLU,
          INCLUDE=YES,
          USSTAB=USSSNA, DLOGMOD= SX32702S, MODETAB=ALAMODE
LUNAME1 LU      LOCADDR=1
LU2NAM1 LU      LOCADDR=2
SOMENAM LU      LOCADDR=3
```

Note: The static LUs have names that are not generated by the LU-seed parameter on the channel-attached router. LUSEED on the PU and LU-seed on the channel-attached router are different. Without INCLUDE coded, static and dynamic LUs would have different names on the channel-attached router and in VTAM.

Scenario 10: TN3270 Server with Session Switching

In a typical SNA environment, all sessions flow from the client to the owning VTAM/DLUS and then across to the application. This flow means that every packet traverses the VTAM host even though the application is on another host. The way to avoid this problem is to implement session switching. Session switching routes the user directly to the application host and bypasses the VTAM host. In this scenario, we discuss how to implement session switching for a TN3270 Server.

Figure 4-20 TN3270 Server with Session Switching



Design Considerations

When using session switching with the TN3270 Server, keep in mind the following guidelines:

- An LSAP statement is required for each adapter on which DLUR is to open an SAP. There must be at least one statement (one is usually sufficient). You may want more than one statement to provide a way to shut down a subset of the links using a configuration command.
- We recommend that you configure one LINK statement for each LPAR that can be reached directly (that is, without traversing an Intermediate Session Routing node). If this change requires a great deal of configuration or is difficult for you to maintain as the mainframe network changes, use a virtual routing node. A virtual routing node makes a LAN look like an APPN NN with a link to each node on the LAN. Each of those nodes is configured with the virtual routing node name of the LAN. At the mainframe, this name is configured in the XCA major node. When an APPN node selects a route through the network to carry a session, it may select a route via the VRN. For example, the route could go from the PLU node to node X then to the virtual routing node then to node Y and then to the SLU node. When the Bind arrives at node X, it notices that the next hop is to a VRN. Details in the route information provide the MAC and SAP address of node Y. Node X checks whether it now has a link to node Y and, if not, starts setting up a link. When the link comes up, it forwards the Bind over the new link.

When using virtual routing node, keep in mind the following guidelines:

- Virtual routing node is not a substitute for all link configurations. There must be enough statically defined links to allow the DLUR/EN to find a suitable NN server.
- All nodes must have the same name for the virtual routing node.
- There may be problems using virtual routing node in mixed APPN/subarea networks.
- It is not essential to configure any links under DLUR. The links can be configured at the mainframe using path statements. However, configuring the links from the DLUR end is recommended because retrying from the mainframe uses up mainframe cycles.
- There must be a base set of statically configured links between the DLUR and potential NN servers to provide a reasonable guarantee of connectivity. The static configuration of a link can be done from the DLUR end, from the mainframe, or both. Static configuration of the link from the DLUR end is recommended. Additional links will be generated as needed if virtual routing node is configured.
- Each LPAR to which DLUR may become adjacent (that is, with which it may have an LLC link) must be configured to accept such a connection. It should have either a switched major node entry for the DLUR CP or be configured with DYNADJCP=YES.

Router Configuration

In this scenario, we have installed Cisco IOS Release 11.3 on the router and need to:

- Configure CSNA
- Initiate the TN3270 Server and Configure DLUR
- Verify the Current Configuration

Configure CSNA

To configure CSNA to provide the XCA connection, enter the following commands:

```
router1 (config)#interface Channel13/0
router1 (config-if)#csna 0110 00
router1 (config-if)#csna 0120 08
```

Initiate the TN3270 Server and Configure DLUR

To initiate the TN3270 Server and configure DLUR on the router, enter the following commands:

```
! enter interface configuration mode for the virtual interface in slot 1
router(config)#int channel 1/2
! create TN3270 Server entity
router(config-if)#tn3270-server
router(config-if)#lan token 1
router(cfg-lan-Token 0)#adapter 1 4000.cbcb.0001
router(config-if)#lan token 2
router(cfg-lan-Token 0)#adapter 2 4000.cbcb.0002
router(cfg-tn3270)#dlur NETA.COLORADO NETA.HDSMVS3
router(cfg-tn3270)#dlus-backup NETA.HDSMVS4
router(tn3270-dlur)#lsap token-adapter 1
router(tn3270-dlur-lsap)#link HDS1
router(tn3270-dlur)#lsap token-adapter 2
router(tn3270-dlur-lsap)#link HDS2
router(tn3270-dlur)#pu cbpu1 0cbcb001 172.26.56.2
```

Verify the Current Configuration

To display the current router configuration, enter the following command:

```
router1 #show run
Building configuration...

<deleted information>

interface Channel3/2
 ip address 172.26.56.1 255.255.255.240
 load-interval 30
 no keepalive
 lan TokenRing 1
  adapter 1 4000.cbc.0001
 lan TokenRing 2
  adapter 2 4000.cbc.0002
TN3270-server
 dlur NETA.COLORADO NETA.HDSMVS3
 dlus-backup NETA.HDSMVS4
 lsap token-adapter 1
  link HDS1
 lsap token-adapter 2
  link HDS2
 PU CBPU1 0CBCB001 172.26.56.2
```

Host Configuration

On the host, we must configure LPAR1 and LPAR2.

Configure LPAR1

For LPAR1, we must configure an XCA major node for each channel connection, a switched major node for the TN3270 Server, and an LUGROUP.

XCA Major Node for Each Channel Connection

The XCA major node definition is used to connect the channel device to the channel-attached router. Dynamic PU (DYNPU) and dynamic PU prefix (DYNPUPFX) are required for the path link. The path link is used for the adjacent CP between HDS1 and HDS2. Figure 4-21 shows the XCA major node for LPAR1.

Figure 4-21 Scenario 10: XCA Major Node

```
CBXCA41  VBUILD  TYPE=XCA
CBPRT41  PORT    ADAPNO=1 , CUADDR=4100 , SAPADDR=04 , MEDIUM=RING , TIMER=31
CBGRP41  GROUP   ANSWER=ON,                                     X
          AUTOGEN=( 100 , L , P ) ,                           X
          CALL=INOUT ,                                         X
          DIAL=YES ,                                           X
          DYNPU=YES , DYNPUPFX=CB ,                             X
          ISTATUS=ACTIVE
```

Switched Major Node for TN3270 Server

The switched major node defines the PUs for the TN3270 Server. Although not mandatory, it is recommended that the PU name in the switched major node match the PU name as defined in the TN3270 Server. This provides easier problem tracking and maintenance. Figure 4-22 shows the switched major node.

Figure 4-22 Scenario 10: Switched Major Node for TN3270 Server

```

CBSWN1  VBUILD TYPE=SWNET,MAXGRP=10,MAXNO=10
*
CBPU1   PU      ADDR=01,                                     X
          PUTYPE=2,ANS=CONT,                                 X
          LUGROUP=DDDCB,LUSEED=CBPU1###,                   X
          IDBLK=0CB,IDNUM=CB001,ANS=CONT
  
```

LU Group Member

The LU group member is a VTAM member that is required when LUSEED is used. Figure 4-23 shows part of the LUGROUP.

Figure 4-23 Scenario 10: LU Group Member

```

CBDDDLU  VBUILD TYPE=LUGROUP
*****
*          LUGROUP MAJOR NODE FOR TN3270S TESTING          *
*****
*   MM/DD/YY - WHO - WHAT                                  *
*****
DDDMVSLU LUGROUP
327@@2   LU      DLOGMOD=D4A32782,
          MODETAB=ISTINCLM,
          USSTAB=USSSNA,
          SSCPFM=USSSCS
327@@3   LU      DLOGMOD=D4A32783,
          MODETAB=ISTINCLM,
          USSTAB=USSSNA,
          SSCPFM=USSSCS
327@@4   LU      DLOGMOD=D4A32784,
          MODETAB=ISTINCLM,
          USSTAB=USSSNA,
          SSCPFM=USSSCS
327@@5   LU      DLOGMOD=D4A32785,
          MMODETAB=ISTINCLM,
          USSTAB=USSSNA,
          SSCPFM=USSSCS
327@@2E  LU      DLOGMOD=SNX32702,
          MODETAB=ISTINCLM,
          USSTAB=USSSNA,
          SSCPFM=USSSCS
327@@3E  LU      DLOGMOD=SNX32703,
          MODETAB=ISTINCLM,
          USSTAB=USSSNA,
          SSCPFM=USSSCS
327@@4E  LU      DLOGMOD=SNX32704,
          MODETAB=ISTINCLM,
          USSTAB=USSSNA,
          SSCPFM=USSSCS
327@@5E  LU      DLOGMOD=SNX32705,
          MODETAB=ISTINCLM,
          USSTAB=USSSNA,
          SSCPFM=USSSCS
@         LU      DLOGMOD=BADMOD,
          MODETAB=ISTINCLM,
          USSTAB=USSSNA,
          SSCPFM=USSSCS
  
```

Switched Major Node for DLUR Links with the TN3270 Server

The PU definition is required to allow the link statement on the router to connect to VTAM. The CP name defined in the PU must match the CP name defined in the DLUR statement. Figure 4-24 shows the switched major node for the DLUR links.

Figure 4-24 Switched Major Node for DLUR Links

```
CBLINK1  PU      ADDR=01 ,PUTYPE=2 ,ANS=CONT ,                X
          CPCP=YES ,NETID=NETA ,                            X
          CONNTYPE=APPN ,CPNAME=COLORADO ,                 X
          ISTATUS=ACTIVE
CBLINK2  PU      ADDR=01 ,PUTYPE=2 ,ANS=CONT ,                X
          CPCP=YES ,NETID=NETA ,                            X
          CONNTYPE=APPN ,CPNAME=COLORADO ,                 X
          ISTATUS=ACTIVE
```

Displaying VTAMLST Parameters

To display the VTAMLST parameters, enter the following command:

```
D NET ,VTAMOPTS ,FUNCTION=APPNCHAR
IST097I DISPLAY ACCEPTED
IST1188I ACF/VTAM V4R4 STARTED AT 21:12:45 ON 03/08/98 810
IST1349I COMPONENT ID IS 5695-11701-401
IST1348I VTAM STARTED AS INTERCHANGE NODE
IST1189I APPNCOS   = NONE                BN           = YES
IST1189I BNDYN     = FULL                BNORD        = PRIORITY
IST1189I CDSERVR   = YES                 CDSREFER     = ***NA***
IST1189I CONNTYPE  = APPN                CPCP         = YES
IST1189I DIRSIZE   = 0                   DIRTIME      = 691200S
IST1189I DYNADJCP  = YES                 HPR          = (RTP,RTP)
IST1189I HPRNCPBF  = NO                  HPRPST       = LOW           480S
IST1189I HPRPST    = MEDIUM              240S        HPRPST       = HIGH           120S
IST1189I HPRPST    = NETWRK              60S         INITDB       = NONE
IST1189I IOPURGE   = 300S                MAXLOCAT     = 5000
IST1189I NODETYPE  = NN                  NUMTREES     = 200
IST1189I PSRETRY   = LOW                  0S          PSRETRY      = MEDIUM        0S
IST1189I PSRETRY   = HIGH                 0S          PSRETRY      = NETWRK        0S
IST1189I RESUSAGE  = 100                 ROUTERES     = 128
IST1189I SECLVLCP  = ***NA***            SNVC         = 15
IST1189I SORDER    = APPN                SRCHRED      = OFF
IST1189I SRCOUNT   = 10                  SRTIMER      = 30S
IST1189I SSEARCH   = CACHE               VERIFYCP     = NONE
IST1189I VFYRED    = YES                  VFYREDTI     = OFF
IST1189I VRTG      = NO                   VRTGCPCP    = YES
IST1189I XCFINIT   = ***NA***
IST314I END
```

Configure LPAR2

For LPAR2, we must configure an XCA major node for each channel connection and a switched major node for the VTAM-to-VTAM CP-to-CP session.

XCA Major Node for Each Channel Connection

Figure 4-25 shows the XCA major node for LPAR2.

Figure 4-25 Scenario 10: XCA Major Node

```
CBXCA418 VBUILD TYPE=XCA
CBPRT418 PORT ADAPNO=2,CUADDR=4108,SAPADDR=04,MEDIUM=RING,TIMER=31
CBGRP418 GROUP ANSWER=ON, X
          AUTOGEN=(100,L,P), X
          CALL=INOUT, X
          DIAL=YES, X
          ISTATUS=ACTIVE
```

Switched Major Node for VTAM-VTAM CP-CP Session

Figure 4-26 shows the switched major node for the VTAM-to-VTAM CP-to-CP Session.

Figure 4-26 Scenario 10: Switched Major Node for the VTAM-VTAM CP-CP Session

```
CBLINK3 PU ADDR=01,PUTYPE=2,MAXPATH=1,ANS=CONT, X
        CPCP=YES,NETID=NETA,DWACT=YES, X
        CONNTYPE=APPN,CPNAME=HDSMVS3, X
        ISTATUS=ACTIVE
*
CBPATH1 PATH DIALNO=1A044000CBCB0001, X
          GRPNM=CBGRP418
```

Displaying VTAMLST Parameters

To display the VTAMLST parameters, enter the following command:

D NET,VTAMOPTS,FUNCTION=APPNCHAR

```
IST097I DISPLAY ACCEPTED
IST1188I ACF/VTAM V4R4 STARTED AT 21:08:06 ON 03/08/98 719
IST1349I COMPONENT ID IS 5695-11701-401
IST1348I VTAM STARTED AS INTERCHANGE NODE
IST1189I APPNCOS = NONE BN = YES
IST1189I BNDYN = FULL BNORD = PRIORITY
IST1189I CDSERVR = YES CDSREFER = ***NA***
IST1189I CONNTYPE = APPN CPCP = YES
IST1189I DIRSIZE = 0 DIRTIME = 691200S
IST1189I DYNADJCP = YES HPR = (RTP,RTP)
IST1189I HPRNCPBF = NO HPRPST = LOW 480S
IST1189I HPRPST = MEDIUM 240S HPRPST = HIGH 120S
IST1189I HPRPST = NETWRK 60S INITDB = NONE
IST1189I IOPURGE = 300S MAXLOCAT = 5000
IST1189I NODETYPE = NN NUMTREES = 200
IST1189I PSRETRY = LOW 0S PSRETRY = MEDIUM 0S
IST1189I PSRETRY = HIGH 0S PSRETRY = NETWRK 0S
IST1189I RESUSAGE = 100 ROUTERES = 128
IST1189I SECLVLCP = ***NA*** SNVC = 15
IST1189I SORDER = APPN SRCHRED = OFF
IST1189I SRCOUNT = 10 SRTIMER = 30S
IST1189I SSEARCH = CACHE VERIFYCP = NONE
IST1189I VFYRED = YES VFYREDTI = OFF
IST1189I VRTG = NO VRTGCPCP = YES
IST1189I XCFINIT = ***NA***
IST314I END
```

Network Management

This chapter discusses how to configure and use Cisco software products in your network management system to manage a TN3270 environment. It contains the following sections:

- Enabling Management of Cisco Routers
- Viewing TN3270 Server Configuration and Statistics
- Monitoring TN3270 Server Availability
- Diagnosing Problems
- Monitoring TN3270 Response Time
- Monitoring TN3270 Server Performance

Managing a TN3270 environment is composed of several tasks, including:

- Enabling management on Cisco networking devices
- Monitoring TN3270 Server availability
- Viewing TN3270 Server configuration and statistics
- Troubleshooting TN3270 Server configuration
- Troubleshooting connectivity between a TN3270 client and the mainframe
- Monitoring TN3270 network response time
- Monitoring TN3270 network performance statistics

Accomplishing these tasks involves using a network management system based on either a workstation or mainframe, depending on the expertise of your network administrators and operators. The network management system is composed of one or more software products configured to manage routers running TN3270 Server as well as other important network devices.

Each section in this chapter is divided into two areas: managing from the workstation, and managing from the mainframe. In some cases, a section about managing from the router is included.

Overview of Network Management Products

This section provides an overview of Cisco's network management products that can be used to manage a TN3270 environment.

Workstation-based Network Management Products

Cisco provides three workstation products to help manage a TN3270 environment:

- CiscoWorks Blue TN3270 Monitor
- Internetwork Performance Monitor (IPM)
- Cisco Resource Manager (CRM)

These products can coexist on the same UNIX workstation or be installed on different workstations. These products are often integrated into the network management system with a network management platform such as Tivoli TME/10 NetView for AIX (NetView for AIX) or Hewlett-Packard OpenView Network Node Manager (HP OpenView).

Note: CRM has been recently superseded by CiscoWorks 2000 Resource Manager Essentials (RME). The user interface for CiscoWorks 2000 RME is similar to that of CRM. All CRM functionality described in this document is also in CiscoWorks 2000 RME.

CiscoWorks Blue TN3270 Monitor

Cisco's primary solution for managing TN3270 Server from a workstation is a UNIX-based product called TN3270 Monitor. This application allows you to monitor the PU and LU sessions and provides access to the logging information created by TN3270 Server for the CIP and CPA. The log function provides extensive search capabilities for session monitoring and diagnosis.

This product is free and is available as a standalone product on CCO. It is also available as a CiscoView applet that integrates with the CiscoView packages for the Cisco 7200 and 7500 series routers.

Internetwork Performance Monitor


IPM provides extensive response time information about both the IP-only and combined SNA/IP routed environment. IPM measures response times between a source router and a target device. The target can be an IP-addressable device (a router or workstation) or an IBM Multiple Virtual Storage (MVS) mainframe (SNA response time only, running an IPM VTAM application called NSPECHO). There are two types of measurements that you can take: Echo and PathEcho.

- Echo measures the total response time from the source router to the target device.
- PathEcho measures the total response time and the incremental response time for each hop in the path between the source router and the target device. PathEcho is for the IP protocol only.

The IPM application is used to configure the response time reporter (RTR) agent in each source router and then extract and display the response-time information. The RTR agent in the router takes the actual response-time samples between itself and the target device. The IPM application normally extracts the response-time data every hour from each source router. There is also a real-time feature that allows you to immediately display the response-time data.

Cisco Resource Manager

CRM is a Web-based management solution for enterprise networks, offered on both Solaris and NT. It can run alongside CiscoWorks and CiscoWorks for Switched Internetworks, providing enhanced inventory and software distribution utilities for both routers and switches.



CRM consists of four key management applications: Inventory Manager, Availability Manager, Syslog Analyzer, and Software Image Manager. Together, these applications automate the task of finding software updates, speed device software deployment, provide multidevice views of network change, report on year 2000 compliance, track device availability, and report, categorize, and analyze SYSLOG messages, providing you probable cause and suggested actions.

The Syslog Analyzer provides analysis of important SYSLOG messages generated by routers, including those relevant to the TN3270 Server. It filters SYSLOG messages logged by Cisco IOS-based routers and then it provides probable cause explanations and recommended actions. The network-level reports generated by Syslog Analyzer are based on user-defined filters that highlight specific errors, severity conditions, or specific devices and help identify when specific events occur (such as a link down or a device reboot).

Syslog Analyzer allows SYSLOG messages to be linked to customized information such as an organizations Web-based “run book” procedures or launches Common Gateway Interface (CGI) scripts to take corrective actions.

Mainframe-based Network Management Products

Many companies continue to support the LUs that are driven through the TN3270 Server from the data center. To address this need, Cisco provides a mainframe product, called CiscoWorks Blue Internetwork Status Monitor (ISM), to help manage a TN3270 environment.

In addition, Cisco endorses Sterling’s SOLVE:Netmaster for TCP/IP as another way to manage the TN3270 Server function on a CIP or CPA.

CiscoWorks Blue Internetwork Status Monitor

ISM manages Cisco routers, including CIP and CPA cards, from a mainframe user interface. This product integrates with Tivoli TME/10 NetView for OS/390 and SOLVE:Netmaster.

ISM monitors the availability and performance of Cisco routers through the SNA Service Point feature of the Cisco IOS software. The performance of the CIP and CPA cards in channel-attached routers may also be monitored by ISM. These performance statistics are a good indicator for the impact TN3270 Server processing has on the router.

Sterling SOLVE:Netmaster for TCP/IP

SOLVE:Netmaster for TCP/IP is a mainframe-based network management product offered by Sterling Software. It runs on both Netmaster and NetView.

SOLVE:Netmaster for TCP/IP provides monitoring, diagnosing, and management capabilities that allow help desk personnel and operators to monitor TN3270 connections throughout SNA, MVS TCP/IP, and IP network components and to diagnose and automatically correct problems that arise in a mixed SNA and TCP/IP environment. The latest release provides management support for the CIP and CPA, including TN3270 Server management capabilities.

The Cisco channel processor support provided by SOLVE:Netmaster for TCP/IP allows for centralized management of multiple Cisco CIP/CPAs and TN3270 Servers. This centralized monitoring of multiple CIP/CPAs and centralized view of status, configuration, and statistics related to multiple TN3270 Servers increases network reliability by providing early warnings about problem areas.

TN3270 Management Feature Matrix

Table 5-1 lists the network management applications that can be used to perform tasks and obtain information

Table 5-1 TN3270 Management Feature Matrix.

	Configuration	Availability	Fault	Response Time	Performance
Mainframe	<ul style="list-style-type: none"> • ISM • VTAM • SOLVE: Netmaster for TCP/IP 	<ul style="list-style-type: none"> • ISM • VTAM • SOLVE: Netmaster for TCP/IP 	<ul style="list-style-type: none"> • ISM • VTAM • SOLVE: Netmaster for TCP/IP 	<ul style="list-style-type: none"> • ISM 	<ul style="list-style-type: none"> • ISM
Workstation	<ul style="list-style-type: none"> • Router command line 	<ul style="list-style-type: none"> • Cisco Resource Manager • HP OpenView • NetView for AIX 	<ul style="list-style-type: none"> • Cisco Resource Manager • TN3270 Monitor 	<ul style="list-style-type: none"> • IPM • TN3270 Monitor 	<ul style="list-style-type: none"> • TN3270 Monitor • HP OpenView • NetView for AIX

Enabling Management of Cisco Routers

The first step in managing a TN3270 Server environment is to enable the management of your network devices. This task is separated into the following areas of router configuration:

- Enabling Simple Network Management Protocol (SNMP) and SYSLOG
- Enabling management from the mainframe by configuring SNA Service Point

SNMP and SYSLOG are typically used by workstation-based network management software including:

- CiscoWorks Blue TN3270 Monitor
- Internetwork Performance Monitor
- Cisco Resource Manager
- NetView for AIX
- HP OpenView

SNA Service Point is used by mainframe-based network management software, including:

- CiscoWorks Blue Internetwork Status Monitor
- NetView for OS/390
- SOLVE:Netmaster

Managing from the Workstation

Routers running TN3270 Server must have SNMP configured to enable the SNMP-based management products, such as TN3270 Monitor, IPM, and Cisco Resource Manager, to view TN3270 Server configuration parameters, performance statistics, and events.

Configuring SNMP and SYSLOG

Each router to be managed must have SNMP and SYSLOG configured or the management software cannot communicate with the router.

Table 5-2 shows SNMP and SYSLOG router configuration commands. In this example, the network management system has an IP address of 10.1.1.1.

Table 5-2 SNMP and SYSLOG Router Configuration Commands

Router Configuration Command Line	Description
logging 10.1.1.1	Enable SYSLOG messages to be sent to the network management system with IP address 10.1.1.1 .
snmp-server community public RO	Enable SNMP; allow read-only SNMP access with community string public . You can set this string to any value.
snmp-server community private RW	Allow read-write SNMP access with community string private . You can set this string to any value.
snmp-server trap-source Channel0/2	Configure SNMP traps to be sent from the router with the IP address configured on interface Channel0/2 . You should set this configuration parameter to the interface that is used by clients to connect to the TN3270 Server. The IP address associated with this interface will be used by the network management system for management.
snmp-server location RTP, NC	Set a textual description of the location of the router. This value is for informational purposes only.
snmp-server contact Network Administrator	Set a textual description of the contact for the router. This value is for informational purposes only.
snmp-server enable traps	Enable all SNMP traps. You can restrict which traps are enabled. See the Cisco IOS command reference for the snmp-server command for a complete list of traps that can be selectively enabled.
snmp-server host 10.1.1.1 public	Specify that all SNMP traps are to be sent to the network management system with IP address 10.1.1.1 .

The SNMP and SYSLOG configuration process is extensively discussed in the command reference documentation for each release of the Cisco IOS software.

Managing from the Mainframe

Configuring SNA Service Point on your routers allows the routers to be managed from the mainframe by ISM, which is integrated with NetView for OS/390 or SOLVE:Netmaster.

Configuring SNA Service Point

Cisco's implementation of SNA Service Point support includes support for the following:

- Alerts
- RUNCMDs
- Vital product data

Alert support is provided as the router sends unsolicited alerts to the network management application at the host. This function occurs at the various router interfaces and protocol layers within the router.

RUNCMD support enables you to send router commands to the router from the mainframe network management console using the NetView RUNCMD facility. The router then sends the relevant replies back to the RUNCMD screen.

Vital product data support allows you to request vital product data from the mainframe network management console. The router replies with the relevant information.

Table 5-3 shows examples of RSRB configuration commands that implement SNA Service Point.

Table 5-3 RSRB Configuration Examples

Router Configuration Command Line	Description
source-bridge ring-group 99	Create the ring group for the RSRB network. When you connect Token Rings using non-Token Ring media, you must treat that non-Token Ring media as a virtual ring by assigning it to a ring group. Every router with which you wish to exchange Token Ring traffic must be a member of this ring group. These routers are referred to as remote peer bridges. The ring group is made up of interfaces that reside on separate routers.
source-bridge remote-peer 99 tcp 150.10.13.2 local-ack	Identify the interface over which to send SRB traffic to another router in ring group 99.
sna rsrb 88 1 99 4000.fff.0001	Define the service point/RSRB interface, where 88 is the local virtual ring, 2 is the bridge number, 99 is the target virtual ring, and 4000.fff.0001 is the virtual MAC address.
sna host CNM02 xid-snd 05dbc000 rmac 4001.3745.1088 rsap 4 lsap 4 focalpoint	Define a link to the SNA host (with a hostname of CNM02 and an XID of 05dbc000) over the RSRB connection, where the MAC address of the remote router is 4001.3745.1088. The remote SAP and the local SAP are both 4.
sna rsrb enable-host lsap 4	Enable local SAP 4 for the hosts.
sna rsrb start CNM02	Initiate connection with CNM02 via RSRB.

The SNA Service Point configuration process is extensively discussed in the Cisco IOS software documentation.

Viewing TN3270 Server Configuration and Statistics

Before TN3270 problems can be diagnosed, you must have an understanding of how to view all TN3270 Server configuration and operating parameters. This information can be viewed by using:

- Command-line interface of the router
- TN3270 Monitor
- ISM

Managing from the Router

Although we recommend using TN3270 Monitor for viewing TN3270 Server configurations, you can also view TN3270 Server configurations by opening a Telnet or console session to the router running TN3270 Server and issuing **show** commands.

Table 5-4 shows useful TN3270 Server router commands. In these examples, TN3270 Server is running on the CIP or CPA card associated with channel interface **1/2**.

Table 5-4 TN3270 Server Router Commands

Router Configuration Command Line	Description
show extended channel 1/2 tn3270-server	Display the TN3270 Server configuration parameters for the specified channel and the status of the PUs defined in the server.

Router Configuration Command Line	Description
show extended channel 1/2 tn3270-server pu PU-NAME	Display the specified channels TN3270 Server PU configuration parameters, statistics, and all the LUs currently attached to the specified PU-NAME .
show extended channel 1/2 tn3270-server nailed-ip IP-ADDRESS	For the specified channel and IP-ADDRESS , display mappings between a nailed client IP address and nailed LUs.
show extended channel 1/2 tn3270-server pu PU-NAME lu LU-NUMBER [history]	Display the status of the specified LU-NUMBER for the PU-NAME . For DLUR, this shows the link and LFSID. If the optional history command parameter is included, the last few transaction types and sizes are listed.
show extended channel 1/2 tn3270-server client-ip-address CLIENT-IP-ADDRESS	For the specified client IP address, display recent LUs used by that IP address.
show extended channel 1/2 tn3270-server dlur	Display information about the DLUR components. List all DLUR links.

More extensive documentation on these commands is in the Cisco IOS software command references.

Managing from the Workstation

You can use Cisco's TN3270 Monitor program to access configuration information and operational parameters from the workstation.

TN3270 Monitor

TN3270 Monitor uses SNMP to query configuration and operational information from a router running TN3270 Server. The program allows you to view information from one TN3270 Server at a time.

TN3270 Monitor queries the ciscoTn3270ServerMIB, which is described in the Cisco IOS software *MIB Quick Reference*.

Starting TN3270 Monitor

TN3270 Monitor is started from the command line or from CiscoView. This section describes how to invoke TN3270 Monitor from a UNIX command line. It is assumed that your UNIX platform is running X-Windows, all display environment variables are configured properly, and the **tn3270** command is in your PATH environment variable.

To start the TN3270 Monitor, issue the following command:

```
tn3270 [router_ip_address] [ro_community_string]
```

Where:

- **tn3270** is the name of the command that starts the TN3270 Monitor product.
- **router_ip_address** is the IP address or hostname of the router running TN3270 Server. If this parameter is omitted, TN3270 Monitor prompts you for the router's IP address or hostname.
- **ro_community_string** is the SNMP read-only community string for the router. If this parameter is omitted, TN3270 Monitor prompts you for the router's SNMP read-only community string.

For example, the following command initiates the TN3270 Monitor product and instructs it to monitor the TN3270 Server running on a router with the hostname of trillian and an SNMP read-only community string of public.

```
tn3270 trillian public
```

Because TN3270 Monitor displays information from one TN3270 Server at a time, you must invoke multiple instances of TN3270 Monitor to view all the PUs and LUs defined to all your TN3270 Servers. You can write a UNIX shell script that invokes multiple instances of the TN3270 Monitor applications, one for each TN3270 Server.

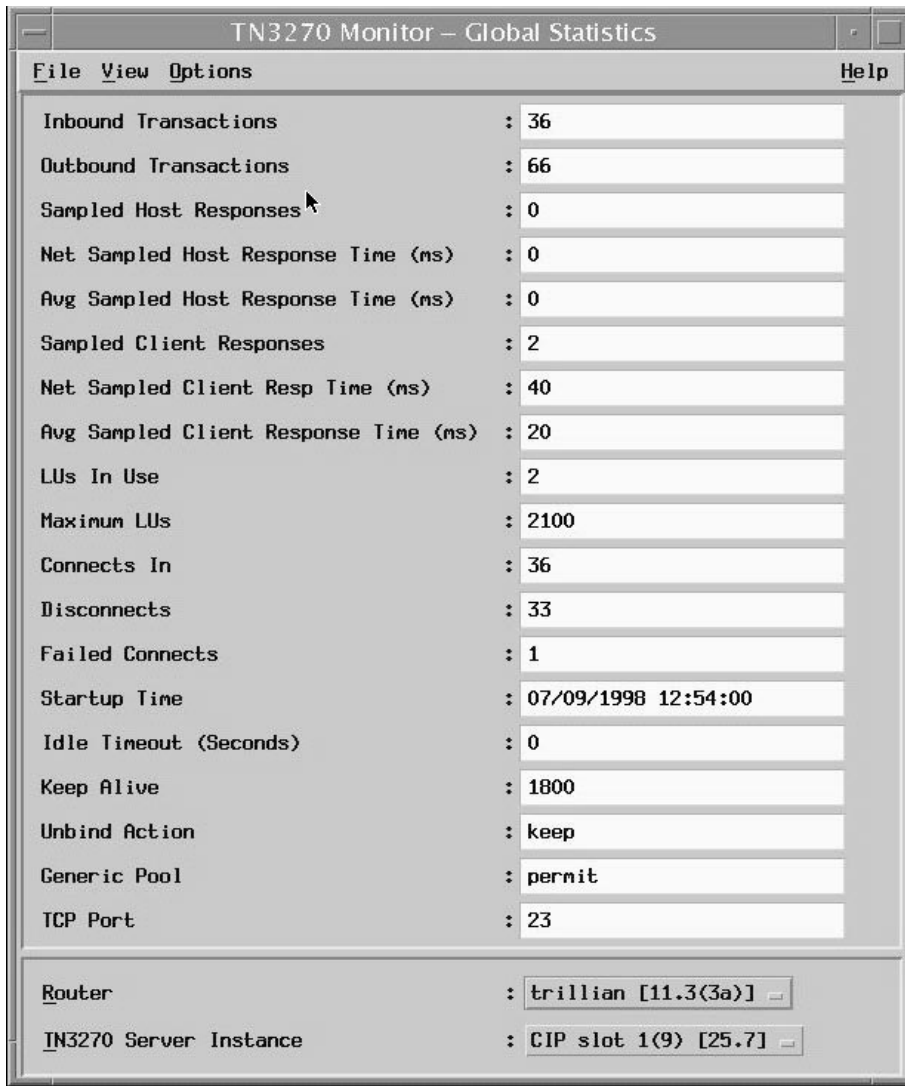
For example, the following is a KORN shell script that invokes TN3270 Monitor for four different TN3270 Server IP addresses. It starts TN3270 Monitor four times and assumes that the SNMP read-only community string is public.

```
#!/bin/ksh
TN_SERVERS="10.1.1.1 10.1.1.2 10.1.1.3 10.1.1.4"
for router in $(echo $TN_SERVERS) ; do
tn3270 "$router" public
done
```

Viewing Global Configuration and Statistics

When the TN3270 Monitor program is started, the Global Statistics window (Figure 5-1) is displayed. This window shows several configuration and operational statistics for the TN3270 Server.

Figure 5-1 TN3270 Monitor—Global Statistics



This window includes configuration parameters and performance statistics. Table 5-5 lists the configuration parameters of interest that are displayed in the Global Statistics window.

Table 5-5 Global Statistics Window: Configuration Parameters

Statistic	Description	Relevance	ciscoTn3270Server MIB Object
Maximum LUs	Maximum number of LUs supported by this TN3270 Server.	If the value of LUs in Use approaches Maximum LUs, then another TN3270 Server instance may be required to maintain good TN3270 performance.	tn3270sMaxLus

Statistic	Description	Relevance	ciscoTn3270Server MIB Object
Idle Timeout	Number of seconds the LU can be inactive (from either host or client) before the TN3270 session is disconnected. Zero means that LU sessions, by default, are not disconnected when inactive, regardless of the amount of idle time.	Setting an idle timeout too low can result in valid TN3270 client sessions being disconnected.	tn3270sGlobalIdleTimeout
Keepalive	Number of seconds the client can be inactive before the TN3270 Server sends a DO-TIMING-MARK. If the client does not reply within 30 minutes of such a TIMING-MARK sending, the server disconnects the TN3270 session. Zero indicates that no keepalives will be sent.	If you set the keepalive and adjusting the idle timeout, you can cause bad LU sessions to timeout in less than 30 minutes	tn3270sGlobalKeepAlive
TCP Port	Default TCP port of this TN3270 Server, which is inherited by the PU if it does not have the TCP port defined in the router configuration for this PU.	Default is port 23.	tn3270sGlobalTcpPort

Table 5-6 lists the performance statistics of interest that are displayed in the Global Statistics window.

Table 5-6 Performance Statistics

Statistic	Description	Relevance	ciscoTn3270Server MIB object
Inbound Txns	Number of inbound (from the client to the host) RU chains (identified by end of record [EOR]) processed.	This value is a count of the number of client transactions.	tn3270sStatsInboundChains
Avg Sampled Host Response Time	Average Sampled Host Response Time in deciseconds (10 ms).	States the average time the mainframe spends processing each TN3270 transaction.	tn3270sStatsNetSampledHostResponseTime / tn3270sStatsSampledHostResponses
Avg Sampled Client Response Time	Average Sampled Client Response Time in deciseconds (10 ms). Note: This number is meaningful only if the timing mark is configured for the TN3270 Server.	States the average time each TN3270 transaction spends traversing the network.	tn3270sStatsNetSampledClientResponseTime / tn3270sStatsSampledClientResponses
Failed Connects	Total number of attempted sessions that failed to negotiate TN3270E or were rejected by control point.		tn3270sStatsTN3270ConnectsFailed
LUs in Use	Number of LUs currently in use on the server.	If the value of LUs in Use approaches Maximum LUs, then another TN3270 Server instance may be required to maintain good TN3270 performance.	tn3270sLusInUse

If a single router has multiple instances of TN3270 Server, you will be able to switch between viewing these instances on the Global Statistics window by changing the selection of TN3270 Server Instance. This parameter is located at the bottom of the Global Statistics window.

Viewing PU Information

All the PUs defined for the TN3270 Server instance that is being monitored by TN3270 Monitor can be viewed by selecting **View->PU List**. The PU List window (Figure 5-2) is displayed.

Figure 5-2 PU List Window

PU	IP Address	Port	Status
PUXCP07	172.26.20.34	23	active
PUXCP08	172.26.20.35	23	active
PUXCP09	172.26.20.35	23	active

The PU List window shows all PUs, their associated IP address and TCP port, and the PU state.

Additional PU details can be viewed by selecting a PU and then selecting **View->PU Detail**. The PU Detail window (Figure 5-3) is displayed.

Figure 5-3 PU Detail Window

PU Name	: PUXCP07
PU State	: active
PU Type	: dlur
IP Address	: 172.26.20.35
TCP Port	: 23
Idle Timeout (Seconds)	: 0
Keep Alive (Seconds)	: 1800
Unbind Action	: keep
Generic Pool	: permit
LI Seed	:
Local Sap Address (hex)	: 0
Remote Sap Address(hex)	: 0
Remote Mac Address	: 00 00 00 00 00 00
IP Precedence Screen	: 0
IP Precedence Printer	: 0
IP TOS Screen	: 0
IP TOS Printer	: 0

Table 5-7 lists the fields that are displayed in the PU Detail window.

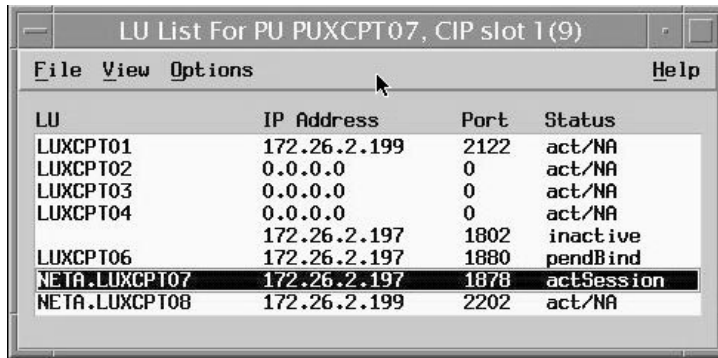
Table 5-7 Statistics on the PU Detail Window

Statistic	Description	ciscoTn3270Server MIB Object
PU State	The current state of the PU. Possible values are: <ul style="list-style-type: none"> • shut—PU is configured, but is in a shut state. • reset—Link station of this PU is not active. • inactive—PU is not activated and the link-station or DLUR state is unknown. • test—PU is sending a TEST to establish link. • xid—TEST responds received, XID is sent. • pActpu—Link station is up, but no ACTPU is received. • active—ACTPU is received and acknowledged positively. • act/busy—Awaiting host to acknowledge the SSCP-PU data. 	tn3270sPuState
PU Type	Indicates whether the connection to the host is via DLUR or direct link.	tn3270sPuType
IP Address	IP address associated with this TN3270 Server.	tn3270sPuIpAddr
Local SAP Address	SAP for this local Direct PU.	tn3270sLocalSapAddress
Remote SAP Address	SAP of the remote PU. This is valid only if the local PU type is Direct.	tn3270sRemoteMacAddress

Viewing LU Information

A list of all the LUs defined for a specific TN3270 Server PU can be viewed using the TN3270 Monitor. To view all non-nailed LUs, access the PU List window and select **View->LU List**. The LU List window (Figure 5-4) is displayed.

Figure 5-4 LU List Window



The LU List window displays a list of all the LUs for an individual PU, the associated client IP address and TCP port, and the LU status. If the LU state indicates that the session is not currently active, the last known client IP address and TCP port are displayed.

The LU List window maps the PU to LU to IP address for a TN3270 session. Nailed LU information can also be displayed from the PU List window, by selecting **View->LU Nailed List**.

Additional LU details can be displayed by selecting an LU and then selecting **View→LU Details**. The LU Detail window (Figure 5-5) is displayed.

Figure 5-5 LU Detail Window

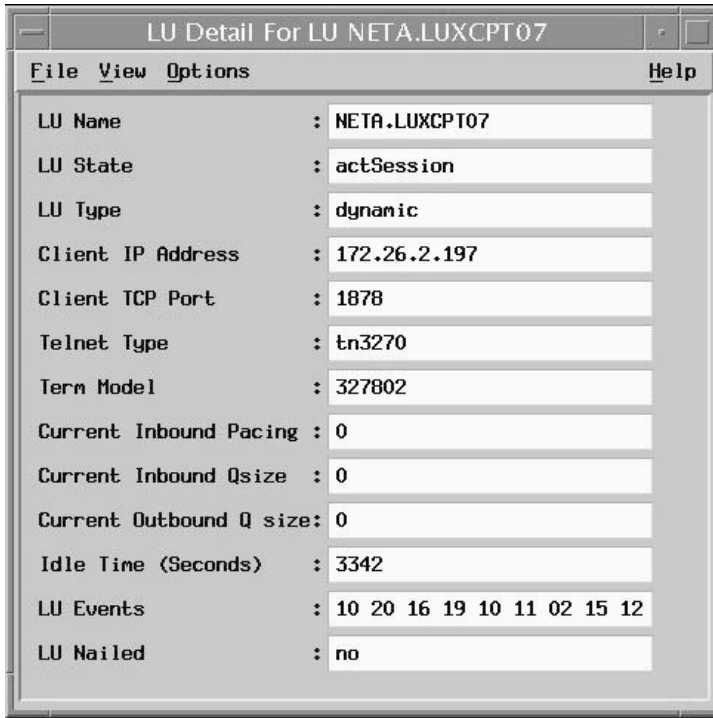


Table 5-8 lists the fields displayed in the LU Detail window.

Table 5-8 Statistics on the LU Detail Window

Statistic	Description	ciscoTn3270Server MIB Object
LU Name	Index used to uniquely identify the LU instance within a PU. It is the LOCADDR.	tn3270sLuIndex

Statistic	Description	ciscoTn3270Server MIB Object
LU State	<p>Current LU state. Possible values are:</p> <ul style="list-style-type: none"> • inactive—LU did not receive ACTLU. • active—LU received ACTLU and acknowledged positively. • pSdt— LU is bound but there is no SDT yet. • act/session—LU is bound and in session. • pActlu—Telnet connects in and is waiting for ACTLU. • pNotifyAv—Awaiting host notify-available response. • pNotifyUa—Awaiting host notify-unavailable response. • pReset—Awaiting for a buffer to send DACTLU response. • pPsid—Awaiting NMVT Reply PSID response. • pBind—Awaiting host to send bind. • pUnbind—Awaiting host unbind response. • unbindWt—Awaiting client to acknowledge disconnection. • sdtWt—Awaiting client to acknowledge SDT 	tn3270sLuState
LU Type	Indicates whether the LU is static or dynamic.	tn3270sLuType
Client IP Address	IP address of the TN3270 client connected to this LU.	tn3270sLuClientAddr
Client TCP Port	TCP port of the TN3270 client connected to this LU.	tn3270sLuClientTcpPort
Telnet Type	Indicates whether the negotiated TN3270 session is TN3270, TN3270E, or never connected.	tn3270sLuTelnetType
Term Model	Terminal type or model number of the incoming TN3270 client.	tn3270sLuTermModel
Current Inbound Pacing	Number of inbound frames allowed to be sent to the host without receiving a pacing response from the host.	tn3270sLuCurInbPacing
Current Inbound Qsize	After inbound pacing credit is exhausted, the inbound data is queued. This is the number of inbound frames queued waiting for host pacing response.	tn3270sLuCurInbQsize
Current Outbound Qsize	Number of TCP packets in the server queued for transmission to the client.	tn3270sLuCurOutQsize
Idle Time (seconds)	Time, in seconds, since activity was last recorded on this LU.	tn3270sLuIdleTime

Statistic	Description	ciscoTn3270Server MIB Object
LU Events	<p>List of numbers that indicate the latest events that occurred in this LU. The first number identifies the most recent event. Although the maximum number of events kept is 16, the actual number of events kept may be lower than that. When more events are generated than are kept, the oldest ones are discarded.</p> <p>Events are encoded as follows:</p> <ul style="list-style-type: none"> • 1—Inactivity timer expired • 2—Dynamic timer expired • 3—ACTLU from host • 4—Bind from host • 5—Clear from host • 6—DACTLU from host • 7—Hierarchical reset from PU (warn ACTPU) • 8—SDT from host • 9—Unbind from host • 10—Notify response from host • 11—Reply PSID negative response from host • 12—Reply PSID positive response from host • 13—Unbind response from host • 14—Hierarchical reset from PU • 15—Connect from client • 16—Disconnect from client • 17—Timing-mark response from client • 18—Flow control timer expired • 19—Negative response to host • 20—Negative response from host • 21—Data contention occurred • 22—No buffer to send response • 23—Receive an SNA response while inbound 	tn3270sLuEvents
LU Nailed	Indicates whether this LU has been configured (nailed) for a specific TN3270 client.	tn3270sLuNail

Viewing Events

The TN3270 Monitor receives and logs events from the monitored TN3270 Server. These events contain information about session initiation and termination. The event log contains information about the correlation between PU, LU, and IP address for each TN3270 session. Error conditions are also flagged in the event log.

To view the event log, access the Global Statistics window and select **View**→**Events**. A window is displayed that allows you to selectively filter events. To view all events, select all from the list of filters and click **New View**. The Events window (Figure 5-6) is displayed.

Figure 5-6 Events Window

Time	Src	Conn	CIP	PU	LU	New IP Address	RPort	Loc IP Address	LPort
07/05/1990 21:40:17	H	LI Disc frn host ses	1	PUBDP107	HE3A.LDRCP100	172.26.2.199	2202		
07/05/1990 21:40:18	H	Inst sess connected	1	PUBDP107		172.26.2.197	3800	172.26.20.25	23
07/05/1990 21:40:58	H	LI Disc frn host ses	1	PUBDP107	LJRD004	172.26.2.197	3879		
07/05/1990 21:40:44	H	Inst sess connected	1	PUBDP107		172.26.2.197	3879	172.26.20.24	23
07/05/1990 21:47:42	H	Inst listen status ch	1					172.26.20.25	23
07/05/1990 21:47:12	F	Static LU activated	1	PUBDP107	LJRD104				
07/05/1990 21:47:12	F	Static LU activated	1	PUBDP107	LJRD102				
07/05/1990 21:47:12	F	Static LU activated	1	PUBDP107	LJRD103				
07/05/1990 21:47:12	F	Static LU activated	1	PUBDP107	LJRD105				
07/05/1990 21:47:12	H	PU status changed	1	PUBDP107				172.26.20.25	23
07/05/1990 21:47:12	H	PU status changed	1	PUBDP107				172.26.20.25	23
07/05/1990 21:46:56	M	Link to BUIS lost	1						
07/05/1990 21:46:56	M	Link lost	1						
07/05/1990 21:46:56	M	Link close by remote	1						
07/05/1990 21:46:56	M	Connr linked by BUIS	1						
07/05/1990 21:46:56	H	Inst listen status ch	1					172.26.20.25	23
07/05/1990 21:46:56	H	PU status changed	1	PUBDP107				172.26.20.25	23
07/05/1990 21:46:56	H	PU status changed	1	PUBDP107				172.26.20.25	23
07/05/1990 21:46:56	M	Connr linked by BUIS	1						
07/05/1990 21:43:16	M	CP Controller Released	1						
07/05/1990 21:43:16	M	CP Controller Released	1						
07/05/1990 21:39:00	H	LI-LI sess started	1	PUBDP107	HE3A.LDRCP107	172.26.2.197	3870	172.26.20.25	23
07/05/1990 21:39:00	F	LI Disc	1	PUBDP107	HE3A.LDRCP107	172.26.2.197	3870		
07/05/1990 21:38:51	H	Inst sess connected	1	PUBDP107	LJRD107	172.26.2.197	3870	172.26.20.25	23
07/05/1990 21:38:40	H	LI Disc frn host ses	1	PUBDP107	LJRD107	172.26.2.197	3847		
07/05/1990 21:38:29	H	LI-LI sess started	1	PUBDP107	HE3A.LDRCP100	172.26.2.199	2202	172.26.20.25	23

You can search for any text in this window. For example, you can use the Events window to search for an IP address and find the corresponding LU and PU names.

Managing from the Mainframe

There are several options for viewing configuration and operation parameters from the mainframe. In this section, we discuss how to view these parameters from ISM and VTAM.

ISM

ISM is a mainframe-based network management application that can be integrated with NetView for S/390 or SOLVE:Netmaster. In this section we are using ISM from NetView to display configuration and operation parameters for our TN3270 sessions.

This example assumes that you have installed ISM and configured it to monitor the routers on which you are running the TN3270 Server.

Viewing Router Status

To access ISM, enter ISM at the NetView console. The ISM main menu (Figure 5-7) is displayed.

Figure 5-7 ISM Main Menu

```
NSPVMAIF          Internetwork Status Monitor (ISM)          CNM01  09/10/98
                  TARGET: CNM01  15:29

Options   Description
* FPM     Focal Point Manager Status - BOTH
* SUM     ISM Status Summary
* MGR     Router Status Display
* CMD     New Router Contact. Service Point Name:
* IDIS    Interface status display. Type:
          A=Async M=ATM C=Channel E=Ethernet
          D=FastEthernet F=FDDI H=HSSI B=ISDN
          L=Loopback S=Serial T=Tokenring U=Tunnel
* DSPU    DSPU Monitor.
* CMCC    Cisco Mainframe Channel Connection (CMCC) Monitor.
* SNA     Session Monitoring   PU:          MAC:

* USER   User Profile Management.          Userid:
* SETUP  Setup Menu for ISM Router management.
* LOG    Browse ACTIV   Log From:          to
* HELP   Command Descriptions.

ISM Last Initialized: 09/06/98 20:11 ISMMGR

Action==>
1=HELP 2=MAIN 3=RTN          6=ROLL
```

Next, to view the status of all known routers, place your cursor in front of the ISM Status Summary option and press **Enter**. The Status Summary panel (Figure 5-8) is displayed.

Figure 5-8 ISM Status Summary Panel

```

NSPVSUM          ISM Status Summary                      CNM01  09/10/98
  Last Refresh: 15:44                                TARGET: CNM01  15:45
|<-----Active----->|<-----UNKNOWN----->|
Total             ACTIV  PERF ALERT | INOP  INVALID  CONCT  INACT  NOMON
  38 Routers       5     2   4   |   0    7     13   1    6
  10 CMCCs        5     0   |   0    0
                Desired Status=UP | Desired Status=Down
Total  Interfaces  UP    DOWN  INVALID  UNKNOWN | DOWN  UNKNOWN
  72  Tokenring    9     1      25      25 | 25    12
  55  Ethernet     8      27      14      6
   1  FDDI         6      18      3      1
  24  Loopback    6      18      1      1
   1  ASYNC        15     2      1      1
  18  Channel     6      3      1      1
   0  HSSI         21     3      15     46
   3  ISDN         6      3      2      4
   3  Tunnel       6      3      15     46
   2  ATM          6      3      2      4
  14  FastEthernet 6      3      2      4
 158  Serial      21     3      15     46
Frame-Relay:   19  HDLC: 6  X.25: 0  BSTUN: 0  SDLC: 0

==>
1=HELP 2=MAIN 3=RTN 6=ROLL 12=REFRESH

```

This panel displays a status summary for all the routers known to this instance of ISM and for all the interfaces on those routers. The TN3270 Server is implemented on a channel connection.

Viewing Channel Connection Status

To view information about all the channel connections, on the ISM main menu place your cursor in front of CMCC and press **Enter**. The CMCC Monitoring Options panel is displayed. Place your cursor beside LIST and press **Enter**. The Cisco Mainframe Channel Connections panel (Figure 5-9) is displayed.

Figure 5-9 Cisco Mainframe Channel Connections Panel

```
NSPVCLIS          Cisco Mainframe Channel Connections          CNM01  09/10/98
Total Number of CMCCs: 10          Filter:          TARGET: CNM01  15:47
Router   Slot  Version          Status  Overrides          Last Change-Previous
CWBC01   3     CIP 4.132 210.40    ACTIV   C=75               08:59 09/10/98 UNKNOWN
CWBC07   3     ECPA 0.1 214.4     ACTIV                   17:28 09/09/98 UNKNOWN
TRAILMIX 1     ECPA 1.0 26.2      ACTIV                   20:16 09/06/98 UNKNOWN
CWBC01   4     CIP 4.4 210.40     ACTIV                   08:59 09/10/98 UNKNOWN
MHONVPU1 3     CIP2 5.0 214.40    ACTIV                   18:42 09/09/98 UNKNOWN

==>
1=HELP 2=MAIN 3=RTN 5=STAT 6=ROLL          9=ADMIN 10=CMDS 11=HIST 12=CHAN
```

This panel displays the status of all channel connections in the known routers.

For this example, we are interested in the channel connection with the SP name of MHONVPU1. To view the status of this channel connection, place your cursor on MHONVPU1 and press **PF5**. The CMCC Extended Display panel (Figure 5-10) is displayed.

Figure 5-11 CMCC Extended Display

```

NSPVCDI0                CMCC Extended Display                CNM01  09/10/98
                        Target: CNM01  16:04

-----
|  Spname  |  ----  |  CMCC  |  -----  |  Channel  |  ----  |  SUB CHANNEL  |
|  MHONVPU1  |  |  Slot 3  |  |  3/2  |  |  No Subchannels  |
|-----|  |-----|  |-----|  |-----|
|-----|  |-----|  |-----|  |-----|
Status= ALERT           Status= ACTIV
EXT= CM                 Hardware= CIP2
                        Level= 5.0
                        Software= 214.40

Tab to a resource name and press enter
to obtain details about the resource.

Action==>
1=HELP 2=MAIN 3=RTN          6=ROLL 7=BACK

```

This panel shows that interface 3/2 is up and that no subchannels are configured on this interface. To view additional information about the interface, tab to the Channel box and press **Enter**. The Channel panel (Figure 5-12) is displayed.

Figure 5-12 Channel Panel

```
NSPVIDI3          Interfaces Type= C    Channel          CNM01  09/10/98
Number of Interfaces: 18      Filter:          Target: CNM01  15:47
Router  Interface          Status  Encaps          Last Change  Previous
MHONVPU1 CHANNEL3/0          DOWN
MHONVPU1 CHANNEL3/1          UP
MHONVPU1 CHANNEL3/2          UP
18:27 09/09/98 UNKNOWN
18:27 09/09/98 UNKNOWN
18:27 09/09/98 UNKNOWN

==>
1=HELP 2=MAIN 3=RTN 5=STAT 6=ROLL          9=ADMIN 10=CMDS 11=HIST 12=CIP
```

This panel displays general status information about all the channels configured on the card.

Viewing TN3270 Server Status

To access information about interface 3/2, tab to line that contains Channel 3/2 and press **PF10**. The CMCC and Channel Show Commands panel (Figure 5-13) is displayed.

Figure 5-13 CMCC and Channel Show Commands Panel

```
NSPVCCMF          CMCC and Channel Show Commands          CNM01  09/10/98
                                                           TARGET: CNM01  15:48

The following show commands are useful when monitoring CMCC interfaces.
Service Point Name: MHONVPU1 CHANNEL: 3/2
  Show Command
1: show extended channel 3/2      icmp-stack
2: show extended channel 3/2      ip-stack
3: show extended channel 3/2      llc2
4: show extended channel 3/2      statistics
5: show extended channel 3/2      subchannel
6: show extended channel 3/2      tcp-stack
7: show extended channel 3/2      udp-listeners
8: show extended channel 3/2      udp-stack
9: show interfaces channel 3/2
10: Show controller CBUS
11: Show controller channel 3/2
Press PF1 for more command details or enter option number and press PF1.

To issue a command, ensure the required arguments have been specified,
type the command number, and press Enter.
Enter the command number followed with a ? to get help from the router.

Action==>
1=HELP 2=MAIN 3=RTN          6=ROLL
```

Because there is no **show** command preconfigured in ISM to display the status of the TN3270 Server, we must create one. Type **1** and press **Enter**. The Router Command Interface panel (Figure 5-14) is displayed.

Figure 5-14 Router Command Interface Panel

```
NSPVCMDA          Router Command Interface          CNM01  09/10/98
SPname: MHONVPUI   Log:( NO | YES ) NO             Target: CNM01  15:49
Hostname= Kona>    Password:
  show extended channel 3/2 icmp-stack

ICMP Statistics for IP Address 11.11.14.4
  InMsgs           : 0           InErrors           : 0           InDestUnreachs:
  InTimeExcds     : 0           InParmProbs        : 0           InSrcQuenchs  :
  InRedirects     : 0           InEchos            : 0           OutEchoReps   :
  OutTimestamps   : 0           OutTimestampReps  : 0           OutAddrMasks  :
  OutAddrMaskReps: 0

Kona>

==>
1=HELP 2=MAIN 3=RTN 5=COPY 6=ROLL           11=RIGHT 12=RECALL
```

On this panel, replace icmp-stack with **tn3270-server ?** and press **Enter**. The Router Command Interface panel (Figure 5-15) is displayed again and icmp-stack is replaced by tn3270 server ?.

Figure 5-15 Redisplayed Router Command Interface

```
NSPVCMDA          Router Command Interface          CNM01  09/10/98
SPname: MHONVPU1   Log:( NO | YES ) NO             Target: CNM01  15:49
Hostname= Kona>    Password:
show extended channel 3/2 tn3270-server ?

client-ip-address  status of clients with given IP address
dlur               status of DLUR
dlurlink           status of a DLUR link
nailed-ip          status of nailed clients with given IP address
pu                status of a PU
<cr>
Kona>

==>
1=HELP 2=MAIN 3=RTN 5=COPY 6=ROLL                11=RIGHT 12=RECALL
```

This panel displays all the possible options for the **show extended channel tn3270-server** command. To view the general status of the server, delete the question mark at the end of the command and press **Enter**. The Router Command Interface panel (Figure 5-16) is redisplayed.

Figure 5-16 Router Command Interface Panel—TN3270 Server

```

NSPVCMDA          Router Command Interface          CNM01  09/10/98
SPname: MHONVPU1   Log:( NO | YES ) NO           Target: CNM01  15:50
Hostname= Kona>   Password:
  show extended channel 3/2 tn3270-server

          <current stats> < connection stats > <response time(ms)>
server-ip:tcp      lu in-use  connect disconn fail  host  tcp
11.11.14.4:23     510    0      0      0    0    0
total             510    0
configured max_lu 80
idle-time      0          keepalive 1800          unbind-action disconnect
ip-preced-screen 0 ip-preced-printer 0 ip-tos-screen 0 ip-tos-printer 0
tcp-port      23          generic-pool permit no timing-mark
name(index)   ip:tcp          xid  state  link  destination  r-lsap
MHOPU(1)     11.11.14.4:23  01732051 ACTIVE tok 5 4000.1234.5656 04 18
MHOPU04(2)   11.11.14.4:23  01732047 ACTIVE tok 5 4000.1234.5656 04 10
Kona>

==>
1=HELP 2=MAIN 3=RTN 5=COPY 6=ROLL          11=RIGHT 12=RECALL

```

This panel displays the status of the server and lists the PUs configured on the server.

Viewing the Status of a PU and Its LUs

To display additional information about a specific PU, including the LUs currently in use on that PU, add **pu** **mhopu** to the command and press **Enter**. The Router Command Interface panel (Figure 5-17) is redisplayed.

Figure 5-17 Router Command Interface Panel—Current PU Configuration

```

NSPVCMDA          Router Command Interface          CNM01  09/10/98
SPname: MHONVPU1      Log:( NO | YES ) NO          Target: CNM01  15:51
Hostname= Kona>          Password:
  show extended channel 3/2 tn3270-server pu mhopu

name(index)      ip:tcp          xid  state      link  destination  r-lsap
MHOPU(1)         11.11.14.4:23      01732051 ACTIVE   tok 5  4000.1234.5656 04 18
luseed MHO08L##
idle-time      0          keepalive 1800      unbind-act discon  generic-pool perm
ip-preced-screen 0 ip-preced-printer 0 ip-tos-screen 0 ip-tos-printer 0
bytes 0 in, 21 out; frames 0 in, 1 out; NegRsp 0 in, 0 out
actlus 0, dactlus 0, binds 0
Note: if state is ACT/NA then the client is disconnected
lu   name  client-ip:tcp      nail state  model  frames in out  idle for
1   MHO08L01 11.68.124.165:1065  N  ACT/NA  VT400  5      3      0:8:2
2   MHO08L02 11.68.124.168:1215  N  ACT/SESS 327904E 21     20     0:3:33
3   MHO08L03 11.68.124.168:1213  N  ACT/SESS 3278S4E 20     19     0:3:31
4   MHO08L04 never connected     N  ACT/NA      1      1      0:10:54

==>
1=HELP 2=MAIN 3=RTN 5=COPY 6=ROLL          11=RIGHT 12=RECALL

```

This panel displays the current configuration of the PU and lists the LUs in use and their status.

VTAM

To view the PU definitions for the PUs used by TN3270 server, enter the **D NET** command and specify the PU for which you want to view information. In the following example, the status of PUXCPC01 is displayed.

```

D NET, ID=PUXCPC01, E
IST097I DISPLAY ACCEPTED
IST075I NAME = PUXCPC01, TYPE = PU_T2.1 597
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST1058I MODEL LU GROUP = DDDMVSLU, LU-SEED = PU3###
IST1043I CP NAME = PUXCPC01, CP NETID = NETA, DYNAMIC LU = YES
IST1589I XNETALS = YES
IST1105I RESOURCE STATUS TGN CP-CP TG CHARACTERISTICS
IST1106I PUXCPC01 AC/R      0 YES  9075000000000000000014C00808080
IST1482I HPR = RTP - OVERRIDE = N/A - CONNECTION = NO
IST136I SWITCHED SNA MAJOR NODE = CBSWN2
IST081I LINE NAME = L3800000, LINE GROUP = CBGRP38, MAJNOD = CBXCA38
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST1656I VTAMTOPO = REPORT, NODE REPORTED - YES
IST1657I MAJOR NODE VTAMTOPO = REPORT
IST355I LOGICAL UNITS:
IST080I PU3001  ACTIV---X- LUXCPC01 ACTIV          LUXCPC02 ACTIV
IST314I END

```

To view the status of the switched major node, enter the **D NET** command and specify the ID of the network node. In the following example, the status of the resources associated with CBSWN2 is displayed.

```
D NET, ID=CBSWN2, E
IST097I DISPLAY ACCEPTED
IST075I NAME = CBSWN2, TYPE = SW SNA MAJ NODE 572
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST1656I VTAMTOPO = REPORT, NODE REPORTED - YES
IST084I NETWORK RESOURCES:
IST089I PUXCPA01 TYPE = PU_T2.1           , ACTIV
IST089I PUXCPB01 TYPE = PU_T2.1           , ACTIV
IST089I PUB02   TYPE = LOGICAL UNIT       , ACTIV---X-
IST089I PUB01   TYPE = LOGICAL UNIT       , ACTIV---X-
IST089I PUXCPC01 TYPE = PU_T2.1           , ACTIV
IST089I PU3001  TYPE = LOGICAL UNIT       , ACTIV---X-
IST089I LUXCPC01 TYPE = LOGICAL UNIT       , ACTIV
IST089I LUXCPC02 TYPE = LOGICAL UNIT       , ACTIV
IST314I END
```

Monitoring TN3270 Server Availability

The TN3270 Server software runs on a CIP or CPA card in routers. If the router is not functional, then the CIP or CPA card is not functional and TN3270 Server will not operate. Cisco provides tools for monitoring the availability of these routers.

Managing from the Workstation

You can use the Cisco Resource Manager to monitor the availability of the TN3270 Server from the workstation. You can also use Hewlett-Packard's OpenView or IBM's NetView for AIX.

Cisco Resource Manager

CRM can be used to monitor the current status of all routers that you have configured to run TN3270 Server. Each TN3270 Server has an IP address to which TN3270 clients connect. The connectivity of this IP address can be monitored by Cisco Resource Manager. This section explains how to configure Cisco Resource Manager to monitor the IP address of the TN3270 Server, and how to view availability reports for the TN3270 Servers.

In addition, SYSLOG messages may be analyzed by Cisco Resource Manager. A discussion of how to configure Cisco Resource Manager to monitor TN3270 Server SYSLOG messages is in the Configuring TN3270 Server SYSLOG Reports section.

These instructions assume that you have successfully installed Cisco Resource Manager on a UNIX or NT workstation.

Configuring TN3270 Server Availability Reports

The following steps detail how to configure availability polling for a group of routers running the TN3270 Server. At the conclusion of this section, you will have created a Device View, or a grouping of routers, named TN3270 Servers.

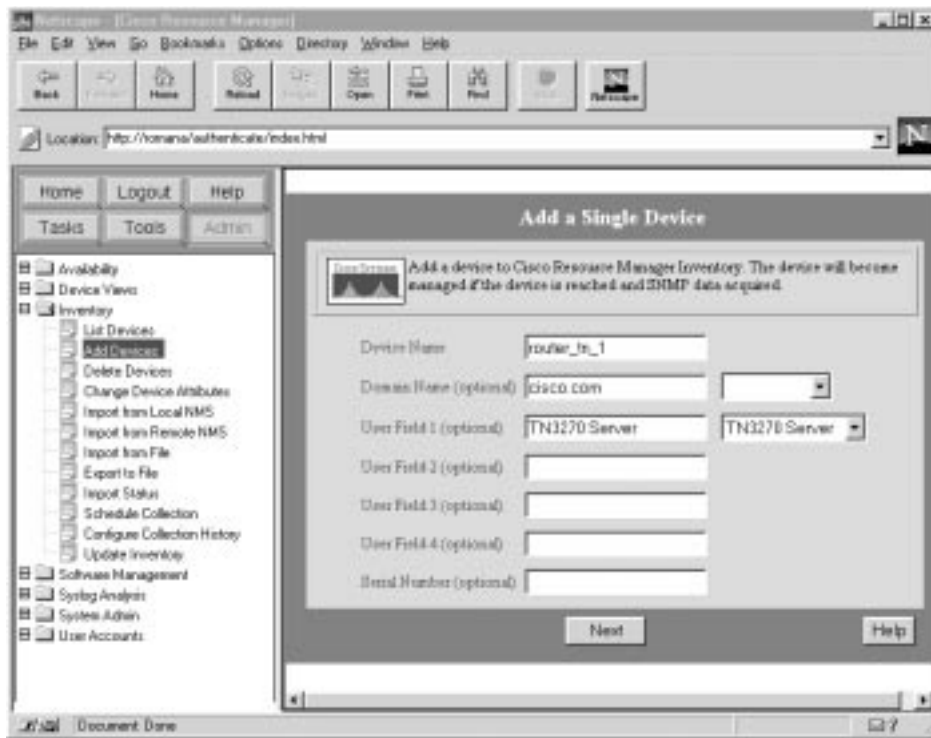
- Step 1. From a Java-compliant Web browser, browse the network management system workstation that is currently running Cisco Resource Manager. In this example, Cisco Resource Manager is running on a workstation named romana. The Cisco Resource Manager main window (Figure 5-18) is displayed.

Figure 5-18 Cisco Resource Manager Main Window



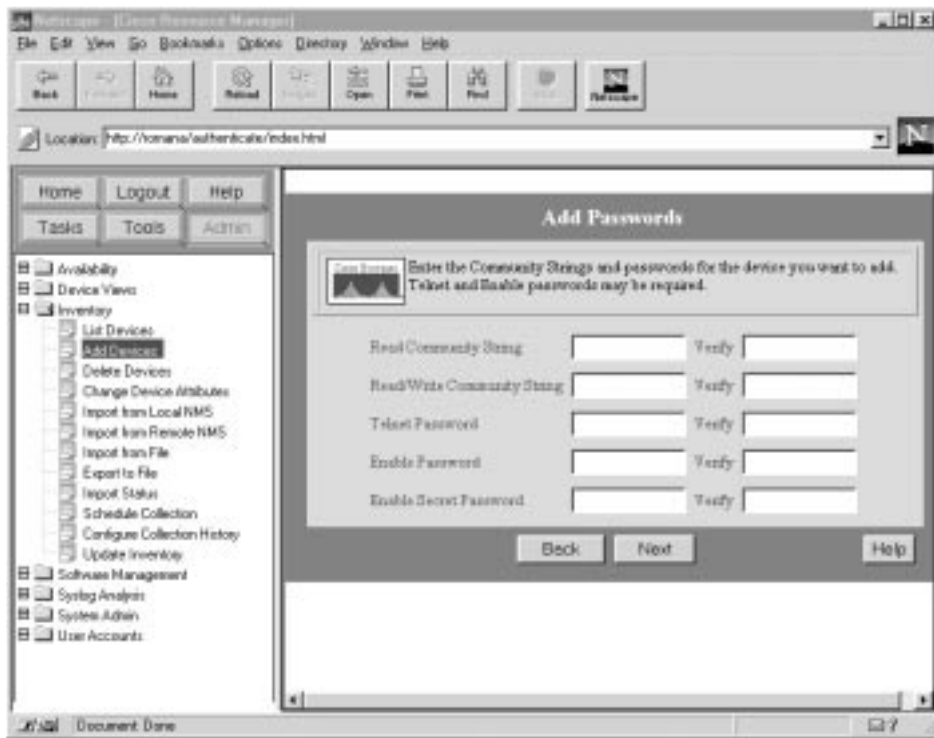
- Step 2. Click **Login** and log in with administrator privileges. The Cisco Resource Manager default user name and password are **admin**.
- Step 3. Add all of the routers running the TN3270 Server by doing the following:
 - Click **Admin**.
 - Click the **Inventory** folder.
 - Click **Add Devices**. The Add a Single Device window (Figure 5-19) is displayed.

Figure 5-19 Add a Single Device Window



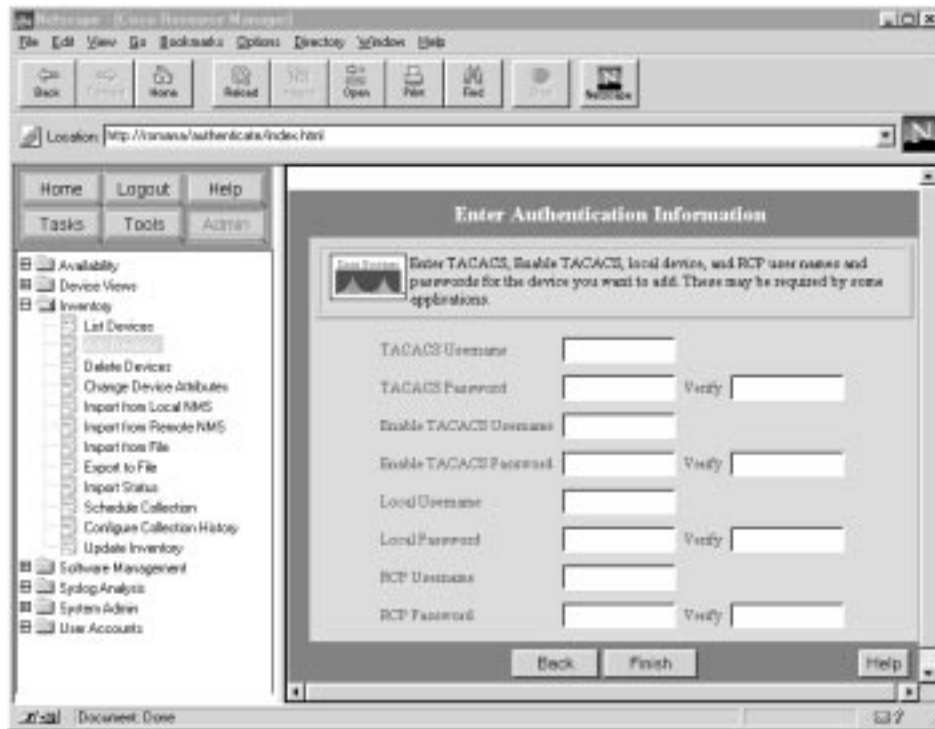
- Enter the IP address or host name of a router running TN3270 Server. The IP address should be the address used by TN3270 clients to connect to the TN3270 Server on that router.
- In the User Field 1 field, enter **TN3270 Server** to identify this router as running the TN3270 Server.
- Click **Next**. The Add Passwords window (Figure 5-20) is displayed.

Figure 5-20 Add Passwords Window



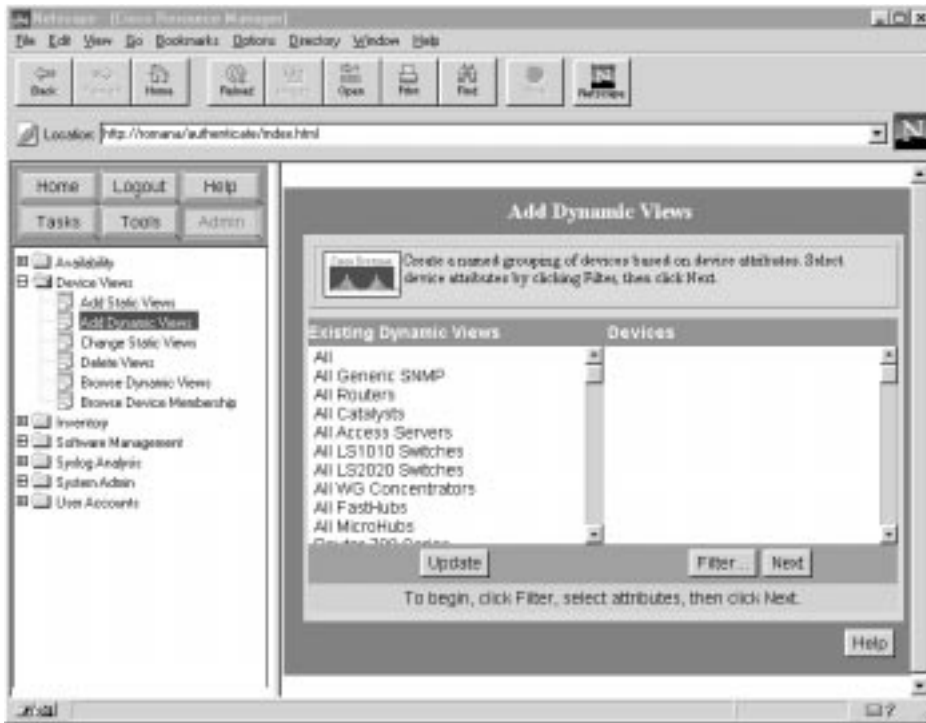
- Enter the Read and Read/Write community strings that are configured for the router.
- Enter the Telnet and Enable passwords for the router.
- Click **Next**. The Enter Authentication Information window (Figure 5-21) is displayed. If you are using TACACS, enter that information in this window.

Figure 5-21 Enter Authentication Information Window



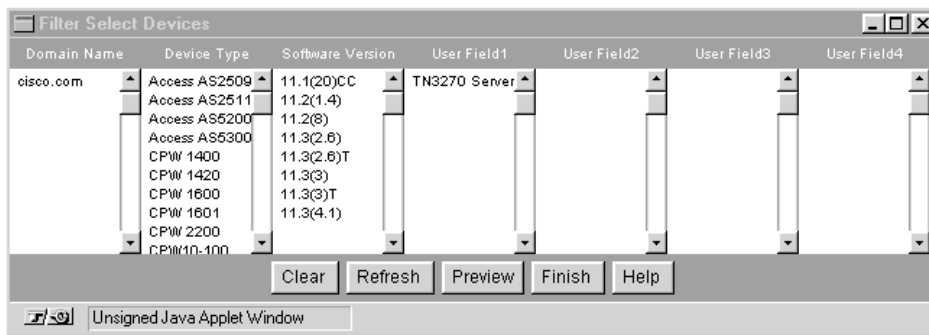
- Click **Finish** to add the router to the Cisco Resource Manager database.
 - Repeat this process for each router that is running the TN3270 Server.
- Step 4. Configure a Dynamic Device View for all routers running TN3270 Server by doing the following:
- Click **Admin**.
 - Click the **Device Views** folder.
 - Click **Add Dynamic Views**. The Add Dynamic Views window (Figure 5-22) is displayed.

Figure 5-22 Add Dynamic Views Window



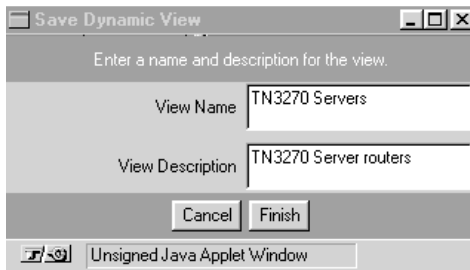
- Click **Filter**. The Filter Select Devices window (Figure 5-23) is displayed.

Figure 5-23 Filter Select Devices Window



- On this window, in the column User Field 1, click **TN3270 Server**.
- Click **Finish**. The window is closed.
- On the Add Dynamic Views screen, click **Next**. The Save Dynamic View window (Figure 5-24) is displayed.

Figure 5-24 Save Dynamic View Window

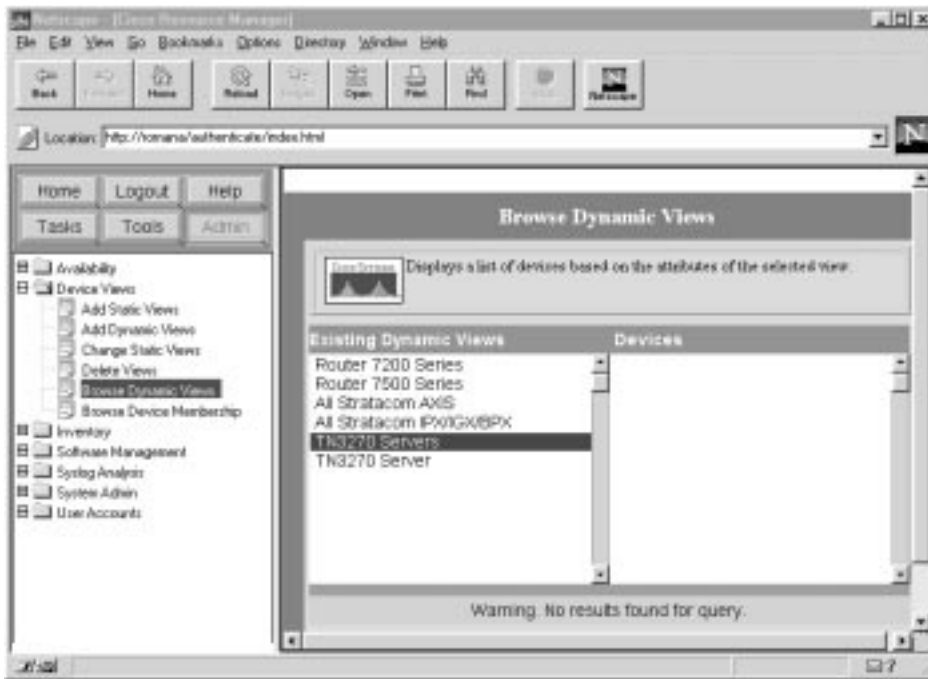


- In the View Name field, enter **TN3270 Servers** and in the View Description field, enter a brief description of the view.
- Click **Finish**. This process defines a group of routers entitled TN3270 Servers to the Cisco Resource Manager database.

Step 5. To verify that all routers you defined as having TN3270 Server are in this device view, do the following:

- Click **Admin**.
- Click the **Device Views** folder.
- Click **Browse Dynamic Views**. The Browse Dynamic Views window (Figure 5-25) is displayed.
- In the column entitled **Existing Dynamic Views**, click **TN3270 Servers**.
- The Devices column displays the list of routers that you defined as having TN3270 Server.

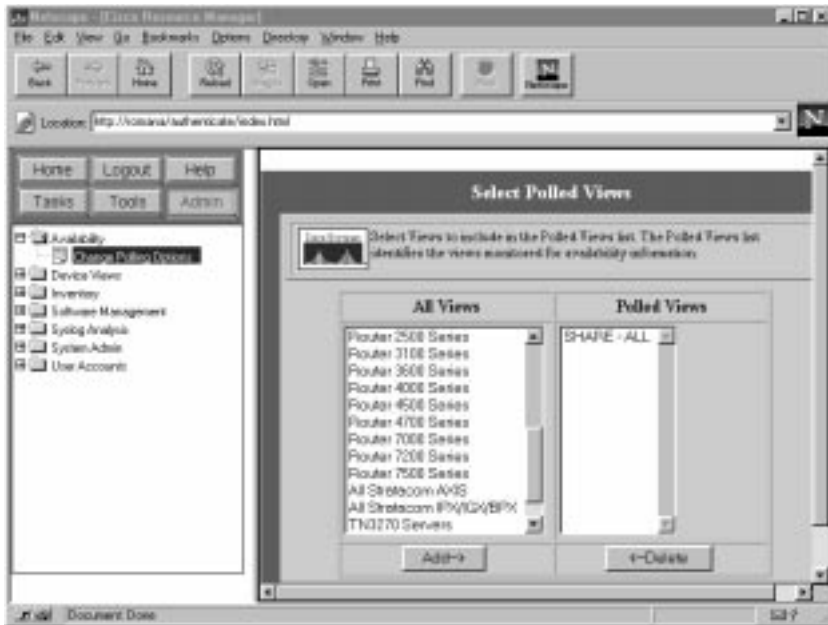
Figure 5-25 Browse Dynamic Views



Step 6. Configure Availability Polling of your routers by doing the following:

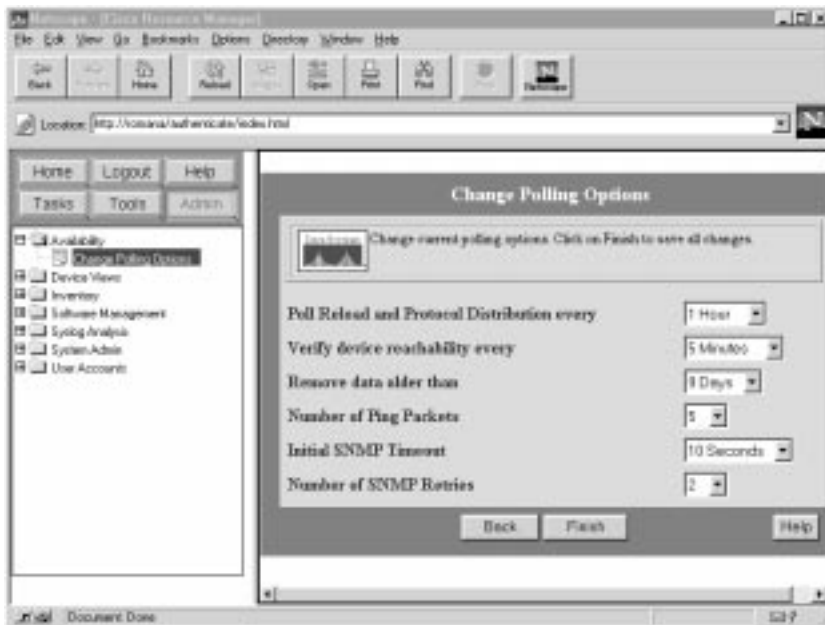
- Click **Admin**.
- Click the **Availability** folder.
- Click **Change Polling Options**. The Select Polled Views window (Figure 5-26) is displayed.

Figure 5-26 Select Polled Views Window



- In the All Views column, click **TN3270 Servers**.
- Click **Add**. This adds the TN3270 Servers view to the list of devices polled by Cisco Resource Manager.
- Click **Next**. The Change Polling Options window (Figure 5-27) is displayed.

Figure 5-27 Change Polling Options Window



- You can change these polling options, but the default values are recommended.
- Click **Finish**.

The Cisco Resource Manager device view is now configured and availability polling has been initiated for the routers you defined to be running TN3270 Server.

Viewing TN3270 Server Availability Reports

Cisco Resource Manager provides several types of useful availability information for groups of devices, including the following reports applicable to TN3270 networks:

- **Availability Monitor**—Displays IP status of the polled devices, including the IP addresses of your TN3270 servers.
- **Reloads Report**—Displays which devices have been reloaded (rebooted), when they were reloaded and, if applicable, why they were reloaded.
- **Offline Device Report**—Displays the managed devices that have not responded to polling for more than a specified period of time.

Using the Availability Monitor

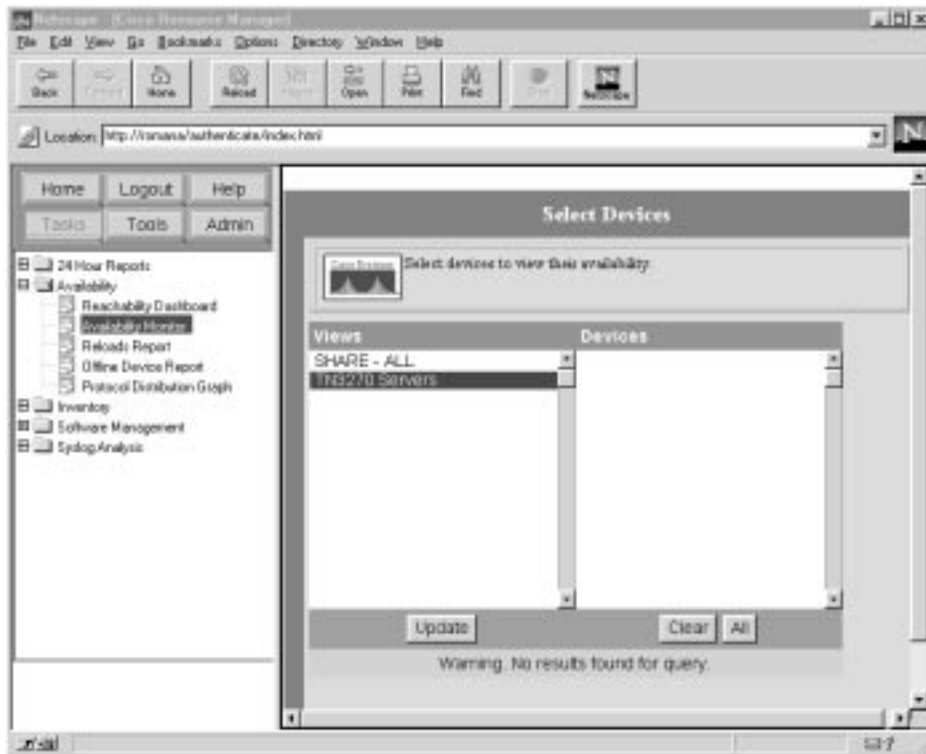
Use the Availability Monitor to continuously check selected devices. You can view device reachability status and response time. Availability Monitor information is updated at half the SNMP polling rate. For example, if your SNMP polling interval is set to 10 minutes, the Availability Monitor is updated every 5 minutes. If you followed the Cisco Resource Manager configuration process outlined in the previous section, this report will contain the current IP status of all your TN3270 Servers.

Note: It is a good idea to leave the Availability Monitor window open at all times. Cisco Resource Manager continuously updates this window with the most recent IP status of your TN3270 Servers.

To access the Availability Monitor do the following:

- Step 1. From the Cisco Resource Manager main window, click **Tasks**.
- Step 2. Click the **Availability** folder.
- Step 3. Click **Availability Monitor**. The Select Devices window (Figure 5-28) is displayed.

Figure 5-28 Select Devices Window



- Step 4. In the Views column, click **TN3270 Servers**. All of the routers running TN3270 Server are displayed.
- Step 5. Click **All** to select all of the routers.
- Step 6. Click **Finish**. The Availability Monitor window (Figure 5-29) is displayed.

Figure 5-29 Availability Monitor Window

The screenshot shows a web browser window titled "Availability Monitor". The window contains a table with the following data:

Device Name	Last Response	Device Reachability (%)	Response Time (ms)	Interface Status
*h0m1ebr0sh	Jul 31 1998 09:43:11	0	N/A	Unknown
*h0m1ebr0sh	Sep 28 1998 15:08:12	100	17	
*h0m1ebr0sh	Sep 28 1998 15:08:12	100	16	
*h0m1ebr0sh	Sep 28 1998 15:08:12	100	15	
*h0m1ebr0sh	Sep 28 1998 15:08:12	100	4	
*h0m1ebr0sh	Sep 28 1998 15:08:12	100	2	
*h0m1ebr0sh	Sep 28 1998 15:08:12	100	11	
*h0m1ebr0sh	Sep 28 1998 15:08:12	100	10	

The Availability Monitor window displays the following information:

- Devices selected and the time they last responded. Unreachable devices appear at the top with a red down arrow. Reachable devices appear with a green up arrow and are sorted alphabetically by device name. The TN3270 Server will be unavailable if the router is unreachable.
- Device reachability in percentages. This percentage is the number of ICMP packets received from a device divided by the number of packets sent. You can specify the number of ping packets to send to a device in the availability polling options. If this value is not 100 percent, then TN3270 clients may be experiencing intermittent connectivity problems.
- Response time in milliseconds. This is the round trip time for an ICMP ping response between Cisco Resource Manager and the IP address of the managed device.
- Interface status. You can click the icons in this column to view the status of this interface.

Viewing Interface Status

The status of channel interfaces of a router are very important to TN3270 Server. If the channel interfaces are not up, then TN3270 Server will experience problems.

To access interface status, begin at the Availability Monitor report. Click **Interface Status** beside the desired device. The Interface Details window (Figure 5-30) is displayed.

Figure 5-30 Interface Details Window

Interface	Update Time	Operational Status	Admin Status	Speed (bps)	Physical Address	Network Address
Ethernet0/0	Sep 28 1998 15:16:16	down	down	3000000	00:60:3e:27:4e:80	Unknown
Ethernet0/1	Sep 28 1998 15:16:16	up	up	3000000	00:60:3e:27:4e:81	172.26.2.52
Ethernet0/2	Sep 28 1998 15:16:16	down	up	3000000	00:60:3e:27:4e:82	172.26.50.202
Ethernet0/3	Sep 28 1998 15:16:16	down	down	3000000	00:60:3e:27:4e:83	Unknown
TokenRing0/0	Sep 28 1998 15:16:16	up	up	1600000	00:06:7c:e4:72:18	172.26.50.1
TokenRing0/1	Sep 28 1998 15:16:16	up	up	1600000	00:06:7c:e4:72:99	172.26.50.9
TokenRing0/2	Sep 28 1998 15:16:16	down	down	1600000	00:06:7c:e4:72:58	Unknown
TokenRing0/3	Sep 28 1998 15:16:16	down	down	1600000	00:06:7c:e4:72:88	Unknown
Channel0/0	Sep 28 1998 15:16:28	down	up	83304000	Unknown	Unknown
Channel0/2	Sep 28 1998 15:16:28	up	up	83304000	Unknown	Unknown
Loopback0	Sep 28 1998 15:16:28	up	up	4294967295	Unknown	172.26.50.240

Examine the status of all channel interfaces. If any channel interfaces have an Admin Status of up and an Operational Status of down, TN3270 Server may not be operating properly.

Accessing Device Center Reports

The Device Center provides several reports about reachability history and current router configuration. The reports available for individual devices include:

- Reachability Trend
- Response Time Trend
- Reloads History
- Interface Status
- Detail Inventory

To access the Device Center, begin with the Availability Monitor report. Click the name of the desired device. The Data Center window is displayed. Select the type of report desired. If you select **Detail Inventory** and then select **Interfaces** from the list of tables, the Interfaces Status report is displayed. This report provides a summary of the current configuration of all channel interfaces.

Configuring TN3270 Server SYSLOG Reports

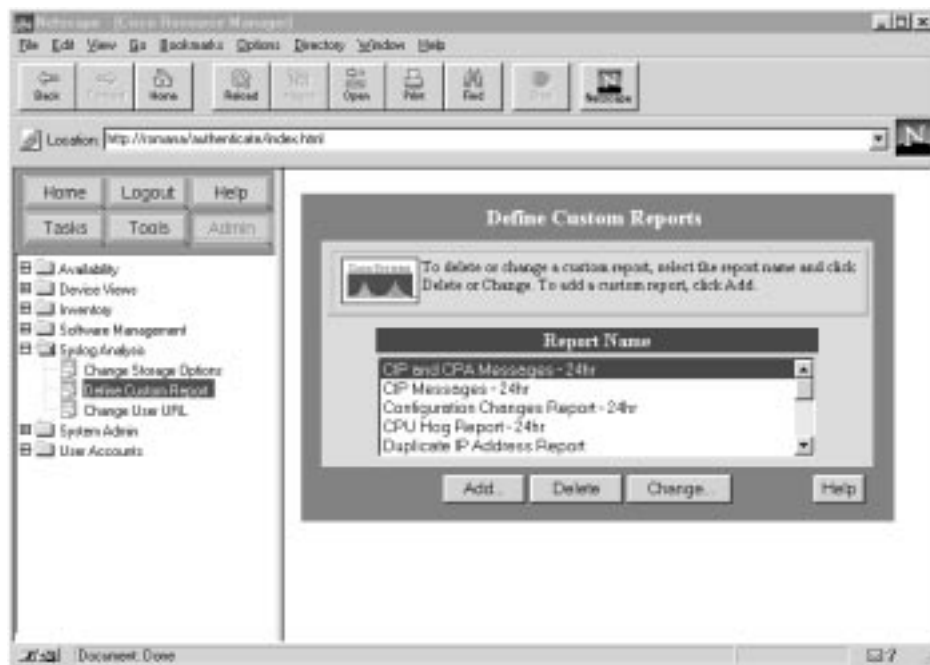
The TN3270 Server identifies error and informational messages using the SYSLOG facility. These messages are the best way for TN3270 Server software to notify the network operator that there is an operational or configuration error. Explanations and recommended corrective actions for all TN3270 Server SYSLOG messages are included in the Cisco IOS software *System Error Messages* document.

The TN3270 Server, as well as other components within the router, send SYSLOG messages to the network management system where they are stored for a period of time (a week by default). However, this parameter can be changed through Cisco Resource Manager. Although Cisco Resource Manager stores these messages, it is up to the network operator to periodically view the messages to identify problems or potential problems with the TN3270 Server.

To configure Cisco Resource Manager SYSLOG reports that analyze TN3270 Server messages and CIP/CPA messages, do the following:

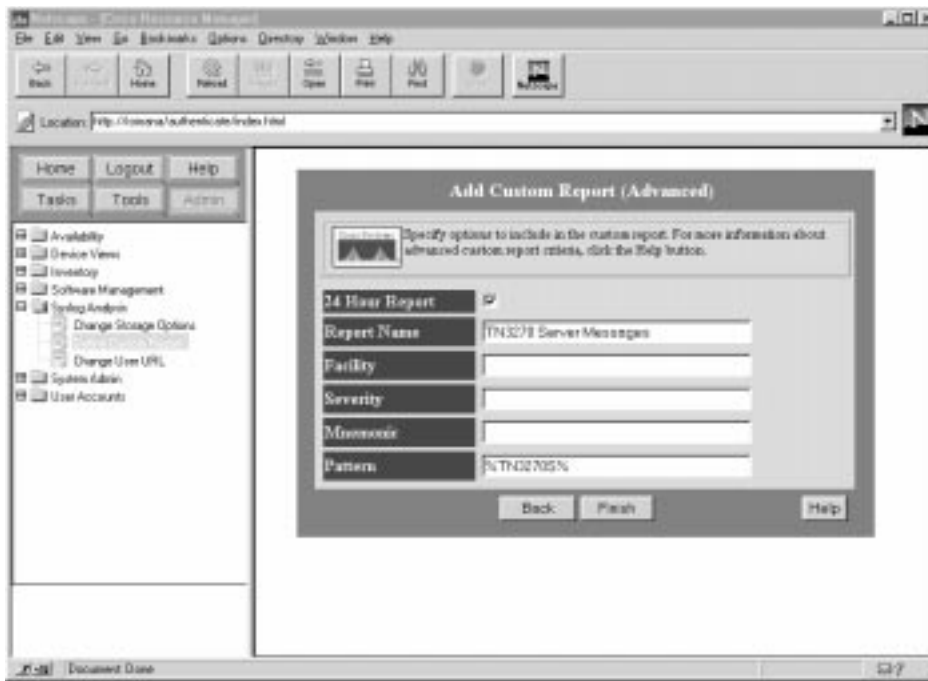
- Step 1. On the Cisco Resource Manager main window, click **Admin**.
- Step 2. Click the **Syslog Analysis** folder.
- Step 3. Click **Define Custom Report**. The Define Custom Reports window (Figure 5-31) is displayed.

Figure 5-31 Define Custom Reports Window



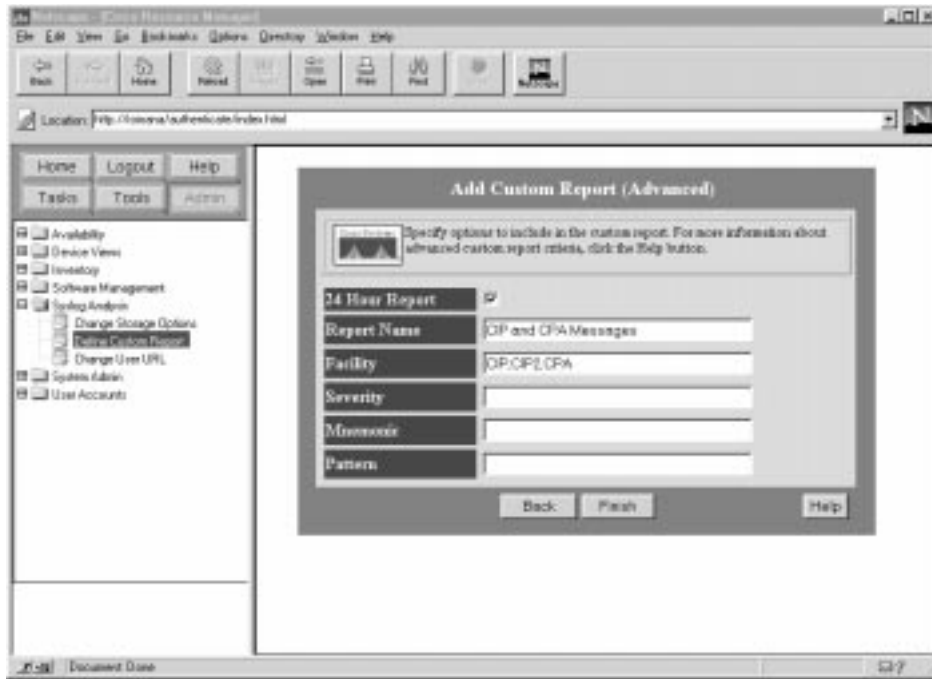
- Step 4. Click **Add**. The Add Custom Report window is displayed.
- Step 5. Click **Advanced**. The Add Custom Report (Advanced) window (Figure 5-32) is displayed.

Figure 5-32 Add Custom Report (Advanced) Window—TN3270 Server Messages



- Step 6. Select the **24-Hour Report** checkbox so that this report will appear in the 24 Hour Reports menu.
- Step 7. Type in the report name, such as **TN3270 Server Messages**.
- Step 8. In the Pattern field, type **%TN3270S%**. This pattern configures Cisco Resource Manager to search the SYSLOG message description for the text TN3270S.
- Step 9. Click **Finish**. A confirmation message appears.
- Step 10. You need to add another report to view all CIP and CPA messages, so click **Define Another**.
- Step 11. Click **Add**. The Add Custom Report window is displayed.
- Step 12. Click **Advanced**. The Add Custom Report (Advanced) window (Figure 5-33) is displayed.

Figure 5-33 Add Custom Report (Advanced) Window—CIP and CPA Messages



Step 13. Select the **24-Hour Report** checkbox.

Step 14. Type in the report name, such as **CIP and CPA Messages**.

Step 15. In the Facility field, type **CIP,CIP2,CPA**.

Step 16. Click **Finish**.

Viewing TN3270 Server SYSLOG Reports

The network operator should view SYSLOG reports daily to proactively search for potential operational or configuration problems with TN3270 Servers and CIP/CPA cards. In addition, the network operator can view reports for all messages stored by Cisco Resource Manager.

Viewing 24 Hour SYSLOG Reports

The 24 hour SYSLOG reports display messages received by Cisco Resource Manager over the past 24 hours. Follow this procedure once a day:

- Step 1. On the Cisco Resource Manager main window, click **Tasks**.
- Step 2. Click the **24 Hour Reports** folder.
- Step 3. Click **Syslog Messages**. The Syslog 24-Hour Report window is displayed. This window summarizes the number of messages applicable to each 24 hour report configured in Cisco Resource Manager.

Pay special attention to the TN3270 Server Messages and the CIP and CPA Messages reports. If either of these reports have messages, scroll to these messages and determine whether the condition is serious or informational.

In a message, click **Facility** to display a detailed description of the message as well as a recommended action. If the message is not documented in your version of Cisco Resource Manager, then you can look up the SYSLOG description and recommended action in the Cisco IOS software *System Error Messages* document.

You can also click on a device name to invoke the Cisco Resource Manager Device Center. Additional problem diagnosis for a specific router can be performed from the Device Center screen.

SYSLOG Analysis

SYSLOG reports can also be invoked to view messages received by Cisco Resource Manager for the past seven days. Follow this procedure when diagnosing problems with TN3270 Server:

- Step 1. On the Cisco Resource Manager main window, click **Tasks**.
- Step 2. Click the **Syslog Analysis** folder. Several reports are available here.
 - **Standard Reports**—Enables the operator to view all SYSLOG messages for all TN3270 Server routers in one window.
 - **Custom Reports**—Allows the operator to select a specific report to run, such as one of the two custom reports previously created by the operator.
 - **Custom Report Summary**—Consolidates information from all custom reports on one screen.

HP OpenView or NetView for AIX

A network management platform like HP OpenView or NetView for AIX can be used to view traps related to TN3270 Server routers. The discussion of how to use HP OpenView and NetView for AIX is beyond the scope of this document. However, it is worthwhile to briefly mention the SNMP trap management offered by these tools.

Viewing All SNMP Traps from the Event Display

Both HP OpenView and NetView for AIX support a window that displays SNMP traps. In this window, you can search for the IP address of a specific TN3270 Server router or a TN3270 client.

You can also display all SNMP traps that are in the Cisco or CiscoWorks category. These categories of events identify SNMP traps sent by Cisco devices and applications to the network management system.

Viewing All SNMP Traps for a Specific Router

Both HP OpenView and NetView for AIX support displaying events for a specific device. To display events for a specific device, first open the network map window that contains the device in question. To display a submap with a TN3270 Server router, search for the IP address of the TN3270 Server. Once you locate the router, select the router icon and invoke the network management system's SNMP trap display. The window lists SNMP traps received by the network management system for that router only.

Managing from the Mainframe

You can use the Cisco ISM to monitor the availability of the TN3270 Server from the mainframe. You can also use VTAM.

ISM

ISM allows you to monitor the status of all CMCC routers or interfaces. You can also define a group of routers that you want to monitor.

Monitoring All CMCC Routers and Interfaces

To display the status of all CMCC routers and interfaces, do the following:

- Step 1. On the ISM main menu, place the cursor beside CMCC and press **Enter**. The CMCC Monitoring Options window is displayed.
- Step 2. To display the status of all CMCC routers that IMS has discovered, move your cursor to LIST and press **Enter**. The Cisco Mainframe Channel Connections panel (Figure 5-34) is displayed. While on this panel, you can place your cursor beside any router and press **PF12** to view the status of the channel interfaces on the selected CIP or CPA.

Figure 5-34 Cisco Mainframe Channel Connections Panel

```
NSPVCLIS          Cisco Mainframe Channel Connections          CNM01  09/15/98
Total Number of CMCCs: 6          Filter:          TARGET: CNM01  17:10
Router  Slot Version          Status  Overrides          Last Change-Previous
CWBC01  3    CIP 4.132 210.40          ACTIV  C=75          14:31 09/15/98 UNKNOWN
CWBC01  4    CIP 4.4 210.40          ACTIV          14:31 09/15/98 UNKNOWN
CWBC07  3    ECPA 0.1 214.4          ACTIV          14:32 09/15/98 UNKNOWN
MHONVPU1 3    CIP2 5.0 214.50          ACTIV          14:34 09/15/98 UNKNOWN
MHONVPU2 5    ECPA 0.1 214.50          ACTIV          14:34 09/15/98 UNKNOWN
TRAILMIX 1    ECPA 1.0 26.2          ACTIV          14:34 09/15/98 UNKNOWN

==>
1=HELP 2=MAIN 3=RTN 5=STAT 6=ROLL          9=ADMIN 10=CMDS 11=HIST 12=CHAN
```

- Step 3. To display the status of all CMCC interfaces that IMS has discovered, move your cursor to CHAN and press **Enter**. The Interfaces Type=C panel (Figure 5-35) is displayed. While on this panel, you can place your cursor beside any interface and press **PF12** to view the status of the CIP or CPA to which the interface belongs.

Figure 5-35 Interfaces Type =C Panel

```

NSPVIDI3          Interfaces Type= C      Channel          CNM01  09/15/98
Number of Interfaces: 19      Filter:          Target: CNM01  17:12
Router  Interface          Status  Encaps          Last Change  Previous
CWBC01  CHANNEL3/0              UP      UP              14:31 09/15/98 UNKNOWN
CWBC01  CHANNEL3/1              UP      UP              14:31 09/15/98 UNKNOWN
CWBC01  CHANNEL3/2              UP      UP              14:31 09/15/98 UNKNOWN
CWBC01  CHANNEL4/0              UP      UP              14:31 09/15/98 UNKNOWN
CWBC01  CHANNEL4/1              UP      UP              14:31 09/15/98 UNKNOWN
CWBC01  CHANNEL4/2              UP      UP              14:31 09/15/98 UNKNOWN
CWBC07  CHANNEL3/0              UP      UP              14:32 09/15/98 UNKNOWN
CWBC07  CHANNEL5/0              UP      UP              14:32 09/15/98 UNKNOWN
MHONVPU1 CHANNEL3/0              DOWN   UP              14:34 09/15/98 UNKNOWN
MHONVPU1 CHANNEL3/1              UP      UP              14:34 09/15/98 UNKNOWN
MHONVPU1 CHANNEL3/2              UP      UP              14:34 09/15/98 UNKNOWN
MHONVPU1 CHANNEL3/2.1          UP      UP              16:45 09/15/98 INVALID
MHONVPU1 CHANNEL3/2.10        UP      UP              16:45 09/15/98 INVALID
MHONVPU1 CHANNEL3/2.2          UP      UP              16:45 09/15/98 INVALID
MHONVPU1 CHANNEL3/2.20        UP      UP              16:45 09/15/98 INVALID
MHONVPU1 CHANNEL3/2.5          UP      UP              16:45 09/15/98 INVALID
MHONVPU1 CHANNEL3/2.9          UP      UP              16:45 09/15/98 INVALID
MHONVPU2 CHANNEL5/0              UP      UP              14:34 09/15/98 UNKNOWN

==>
1=HELP 2=MAIN 3=RTN 5=STAT 6=ROLL          8=FWD 9=ADMIN 10=CMDS 11=HIST 12=CIP

```

Monitoring Routers in Groups

To manage large numbers of routers or to sort routers into meaningful groups, such as those that contain a TN3270 Server, you can assign up to two group names to be associated with each router. These groups can be used to filter views when monitoring router status and to manage ISM's monitoring load by scheduling different monitoring intervals for router groups in the ISM Scheduler application.

If you assign a router to more than one group and also set up the ISM Scheduler application, then ISM monitors the router according to the monitoring interval associated with the first group to which the router is assigned. The order in which you specify a group ID for a router affects the implementation of group scheduling.

You can assign routers to management groups using one of the following methods:

- To assign one or more routers to a group, use the first Router Management Settings panel. Type the name of the groups (up to two groups), with a space in between each value, in the GROUP IDs option for each of the routers that you want to update. For example, you could establish a group called TN3270.
- To assign a single router to a group, you can use the ISM Router Administration panel. Type the name of the groups (up to two groups), with a space in between each value, in the Group(s) option. Again, you could establish a group called TN3270.

Then, when you want to monitor all the routers in the TN3270 group, access the Router Status Display and enter TN3270 as the router group alias. The panel displays all the routers you have identified as running a TN3270 Server.

Monitoring the Status of the Group

To monitor the status of a defined group, do the following:

- Step 1. On the IMS main menu, place your cursor beside MGR and press **Enter**. The Router Status panel (Figure 5-36) is displayed.
- Step 2. In the Group/Router/Alias field, type TN3270 and press **Enter**. The Router Status panel is displayed again, but this time contains only the routers defined as part of the TN3270 group.

Figure 5-36 Router Status Panel

```
NSPVMGRF      Router Status      Routers: 40      CNM01  09/15/98
Group/Router/Alias: TN3270      1 to 6      Target: CNM01  17:17
SPname      SPname      SPname      SPname      SPname      SPname      SPname      Spname
CWBC01
CWBC07
MHONVPU1
MHONVPU2

NSP1186I Position cursor on resource and press PF5 to diagnose status.
==>
1=HELP 2=MAIN 3=RTN 5=DIAG 6=ROLL 9=DETAIL 10=MENU 12=RESET
```

The panel displays the list of routers and uses color to indicate the status of the router. The colors and their associated status are as follows:

- Green—All router functions are available.
- Red—Router is not connected to VTAM.
- Yellow—ISM detected a degraded function for the router. This can be the result of CPU or memory utilization, CMCC CPU or memory utilization, or an interface failure.
- Pink—Alert was detected for a router resource.
- Turquoise—Service point is unknown to VTAM or an operator has inactivated the router in VTAM.
- Blue—Router monitoring is disabled.

Diagnosing Problems

As with many networking environments, TN3270 sessions involve several elements. This makes problem diagnosis challenging. However, by following some simple procedures, you can narrow down the nature of the problem and the offending element.

Gathering Information

The first step in diagnosing a problem is to gather as much configuration information as possible from the end user, including these vital pieces of data:

- TN3270 client IP address
- TN3270 client LU
- TN3270 Server IP address the client needs for connectivity
- TN3270 Server PU the client needs for connectivity

The user is not likely to know any of this information. Table 5-9 provides instructions for locating data.

Table 5-9 Information Needed in Problem Diagnosis.

TN3270 Data	How to Find this Information
Client IP Address	For Windows 95 and 98 clients, run the winipcfg program. This program provides information about the IP stack on the PC, including the client IP address. For Windows NT clients, IP address information is in the networking section of the Control Panel . For UNIX clients, run ifconfig -a from a command line.
Server IP Address	Determine which program is being used for TN3270 emulation. Investigate the configuration file(s) for this program. The IP address of the server is usually stored in a configuration file so that the user does not have to enter it each time a connection is made to the mainframe.
Client LU	Use TN3270 Monitor Events window to search for the client IP address. When you locate the IP address, examine the event to determine the client LU and server PU. If you do not know which server contains the LU, then follow the procedure outlined in "Determining Which IP Addresses, PUs, and LUs Correspond to the TN3270 Servers".
Server PU	First, determine the server IP address. Invoke TN3270 Monitor to manage that IP address. List the PUs. One of the PUs for that router should be mapped to the server IP address. If it is not, you may have multiple CIP/CPA cards in the router, so use TN3270 Monitor to view all CIP/CPA cards in the router.

Determining the Nature of the Problem

Problems in a TN3270 environment are typically either connectivity problems or configuration problems. To determine whether the problem is related to connectivity or configuration, do the following:

- Step 1. Determine the client IP address.
- Step 2. Attempt to ping the client IP address. If the ping succeeds, it is likely that there is a configuration problem.
- Step 3. If the ping fails, the problem is likely a connectivity problem.

Determining Which IP Addresses, PUs, and LUs Correspond to the TN3270 Servers

If you have multiple TN3270 Servers, it might not be clear which server is associated with which PUs, LUs, and client IP addresses. To determine this association, you should first start an instance of the TN3270 Monitor for each TN3270 Server.

After all instances of TN3270 Monitor are started, open the Events window in each instance. Search for any client IP address, PU, or LU in those windows. Although you might have to search all instances of the Events windows to locate the desired PU, LU, or client IP address, this process is easier than issuing multiple router **show** commands.

After you have located the offending PU or LU, use TN3270 Monitor to view PU or LU Details, or to view additional information from the Events window.

Diagnosing Configuration Problems

This section describes the various tools that you can use to diagnose configuration problems in a TN3270 environment.

Managing from the Router

TN3270 Server configuration problems can be diagnosed from the router command line through the commands described in Viewing TN3270 Server Configuration and Statistics. These commands display overall TN3270 Server configuration parameters and list all defined PUs and LUs.

Managing from the Workstation

Because router configuration changes stimulate SYSLOG messages, you can use Cisco Resource Manager to view the SYSLOG messages and determine when recent configuration changes were made to the router. This aids in pinpointing a configuration change might have caused the problem.

Once you determine which TN3270 Server router is experiencing problems, you can view the SYSLOG messages for that device as described in Monitoring TN3270 Server Availability. This report includes when the router's configuration was last changed as one of the messages in the list.

Managing from the Mainframe

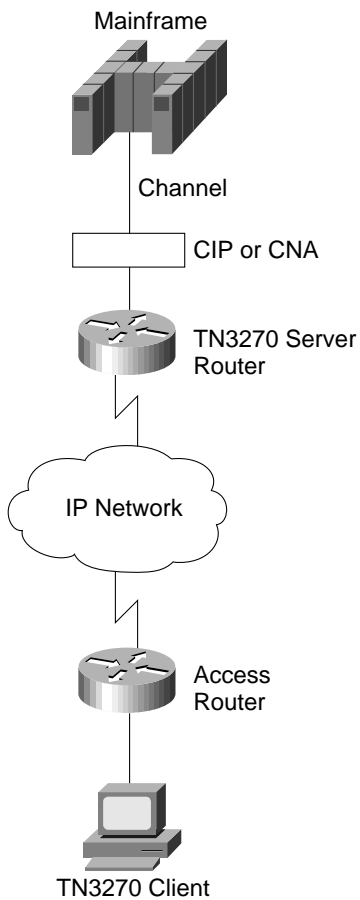
There are several options for diagnosing configuration problems from the mainframe. You can use ISM to isolate configuration problems.

TN3270 Server configuration problems can be diagnosed from ISM using the Router Command Interface panel as described in Viewing TN3270 Server Configuration and Statistics. These commands display overall TN3270 Server configuration parameters, as well as list all defined PUs and LUs.

Diagnosing Connectivity Problems

When diagnosing connectivity problems, it is important that you look at the network from the mainframe to the end user. Figure 5-37 shows possible points of failure in a TN3270 network.

Figure 5-37 TN3270 Session Possible Points of Failure



A connection between a TN3270 client and the mainframe can be disrupted for several reasons. The points of potential failure include:

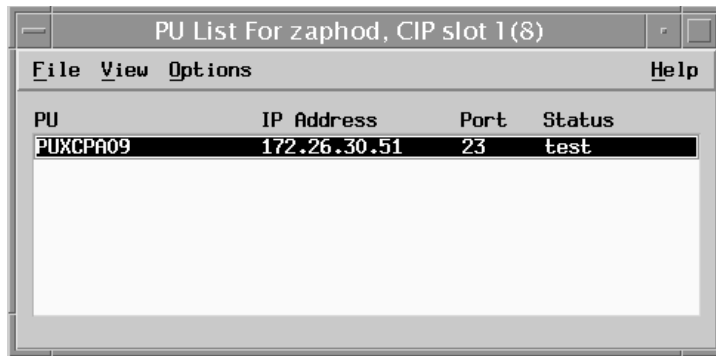
- Mainframe
- Connectivity between the mainframe and the TN3270 Server router
- CMCC (CIP or CPA)
- TN3270 Server software running on the CIP or CPA
- TN3270 Server router
- Connectivity between the TN3270 Server router and the access router, which is the IP network cloud in Figure 5-37
- Connectivity between the TN3270 client computer and the access router

Problem: CIP/CPA Loses Connectivity to the Mainframe

If no TN3270 sessions can traverse through the CIP/CPA card to the mainframe, in the TN3270 Monitor Events window, the Link disc by remote message appears. The last event in this window details the loss of connectivity and indicates which PU is effected.

You can also view the PU Details window and examine the PU state, which will be test rather than active, as shown in Figure 5-38.

Figure 5-38 TN3270 Monitor Events Window



The recommended action for this problem is to reestablish connectivity between the mainframe and the channel-attached router.

Problem: CIP/CPA Is Unavailable

The CIP or CPA running TN3270 Server might become unavailable. If you are using Cisco Resource Manager or ISM, you can determine this by viewing either the Cisco Resource Manager Availability Monitor or the ISM Cisco Mainframe Channel Connection panel. View the log files to determine why the router is experiencing problems.

You can check the log files in the following way:

- TN3270 Monitor—View the Events window
- Cisco Resource Manager—View the SYSLOG reports
- HP OpenView—View SNMP traps in the event window
- NetView for OS/390—View alerts in NPDA

Problem: TN3270 Server Unavailable

Both Cisco Resource Manager and ISM provide ways to continuously monitor TN3270 Server availability. The first line of defense in diagnosing TN3270 problems is knowing, at a basic network connectivity level, if the TN3270 Server IP address is available. This can be accomplished from a workstation-based or mainframe-based network management system.

- Cisco Resource Manager—Continuously display the Availability Monitor for the TN3270 Servers device view
- ISM—Continuously display the Router Status Display for the TN3270 Server group

In rare cases the TN3270 Server software might crash because of a lack of system resources or other problems. The server might log error messages before it ceases to function. View the log files to determine why the server is experiencing problems.

Problem: TN3270 Server Router Unavailable

The router running TN3270 Server might become unavailable. If you are using Cisco Resource Manager or ISM, you can determine this status by viewing either the Cisco Resource Manager Availability Monitor or ISM Router Status panel. View the log files to determine why the router is experiencing problems.

Problem: IP Network Cloud Unavailable

This problem may be indicated if all TN3270 Server routers are available from the perspective of the network operator, but not from the end user. The network operator should turn to an IP network management platform such as HP OpenView or NetView for AIX to troubleshoot problems in the IP cloud.

Problem: Access Router Unavailable

The network operator may not know which router is the access router. If that information is known, and the router is sending SNMP traps and SYSLOG messages to the network management system, then the same log file analysis may be performed as for other types of routers.

Problem: TN3270 Client Loses Connectivity

If a TN3270 client loses connectivity to a TN3270 Server, because of a client reboot or system crash, the TN3270 Server does not automatically release the LU associated with the client. TN3270 Server releases LUs after 30 minutes of idle time have passed since a Timing Mark was sent from the server to the client. However, by default, Timing Mark is not enabled in TN3270 Server.

The symptom of this problem is that a client cannot connect to the TN3270 Server, but the TN3270 Server keeps the LU state as actSession. This means that the TN3270 Server believes there is an active session when, in fact, there is not. Inactive LUs should be in the act/NA state.

The recommended solution to avoid this problem is to configure Timing Marks in TN3270 Server. However, some older versions of TN3270 emulators do not support Timing Marks properly, so this solution is not feasible for all customers.

Monitoring TN3270 Response Time

The TN3270 Server software runs on a CIP or CPA card in routers. If the network response time is degraded, then the users of the TN3270 Server will be impacted. Cisco provides tools for monitoring the response time of the routers.

Managing from the Workstation

Cisco's workstation product, IPM, is designed to measure response times. In addition, you can use data from TN3270 Monitor and HP OpenView to monitor response times.

IPM

With IPM, you can measure the end-to-end response time using an IP echo or SNA echo. IPM uses the response-time reporter feature of the Cisco IOS software to measure the response time on a hop-by-hop basis between the router and a configured target. To get a complete picture of the response time between the client and the mainframe, you take three measurements: one between the TN3270 Server router and the client and two between the TN3270 Server router and the mainframe (one using an IP echo and one using an SNA echo).

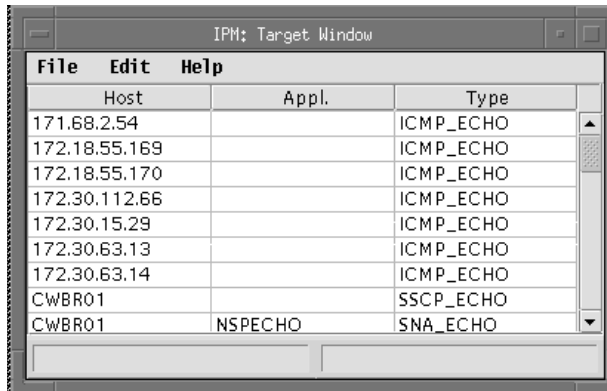
In this section, we assume that you have already defined the router on which the TN3270 Router is running as an IPM Source. For more information about defining IPM sources, see the *CiscoWorks Blue Internetwork Performance Monitor User's Guide*.

Defining the Targets

Because you are taking three measurements, you must define three targets. First, define a target for the client. To define a target in IPM, do the following:

Step 1. From the Internetwork Performance Monitor main window, select **Configure>Target**. The IPM:Target window (Figure 5-39) is displayed.

Figure 5-39 IPM:Target Window

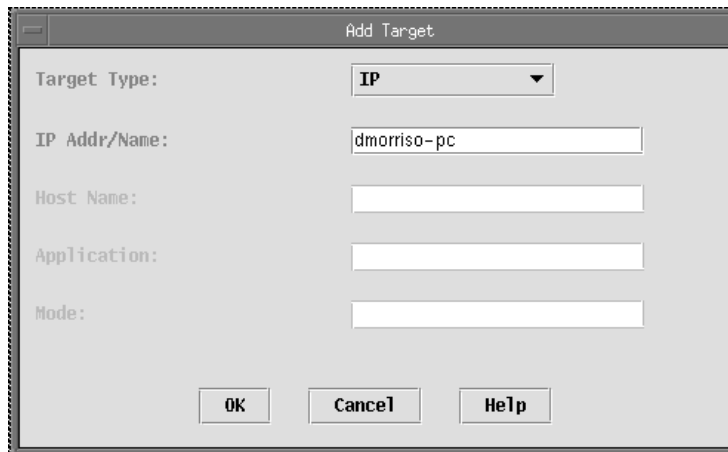


The screenshot shows a window titled "IPM: Target Window" with a menu bar containing "File", "Edit", and "Help". Below the menu bar is a table with three columns: "Host", "Appl.", and "Type". The table contains the following data:

Host	Appl.	Type
171.68.2.54		ICMP_ECHO
172.18.55.169		ICMP_ECHO
172.18.55.170		ICMP_ECHO
172.30.112.66		ICMP_ECHO
172.30.15.29		ICMP_ECHO
172.30.63.13		ICMP_ECHO
172.30.63.14		ICMP_ECHO
CWBR01		SSCP_ECHO
CWBR01	NSPECHO	SNA_ECHO

Step 2. From the IPM:Target window, select **Edit>Add**. The Add Target window (Figure 5-40) is displayed.

Figure 5-40 Add Target Window



The screenshot shows a dialog box titled "Add Target" with the following fields and controls:

- Target Type: A dropdown menu with "IP" selected.
- IP Addr/Name: A text input field containing "dmorriso-pc".
- Host Name: An empty text input field.
- Application: An empty text input field.
- Mode: An empty text input field.
- Buttons: "OK", "Cancel", and "Help" buttons at the bottom.

Step 3. On the Add Target window, enter data in the following fields:

- Target Type—Protocol type to be used with this target. Select **IP**.
- IP Addr/Name—Enter the IP address or host name of the client.

Step 4. Click **OK**.

Next, define a target for the mainframe that uses an IP echo. Repeat Steps 2 through 4. In Step 3, enter the following values:

- Target Type—Protocol type to be used with this target. Select **IP**.
- IP Addr/Name—Enter the IP address or host name of the mainframe.

Finally, define a target for the mainframe that uses an SNA echo. Repeat Steps 2 through 4. In Step 3, enter the following values:

- Target Type—Protocol type to be used with this target. Select **SNA SSCP Echo**.
- Host Name—Enter the host name defined for the SNA PU connection to VTAM.

Configuring an Operation

An IPM operation is an alias for a set of parameters used in measuring response time. You need to configure two operations, one for your IP echo measurements and one for your SNA echo measurements. First, configure the operation for the IP echo measurements. To configure an IPM operation, do the following:

- Step 1. From the Internetwork Performance Monitor main window, select **Configure>Operation**. The IPM: Operation window is displayed.
- Step 2. From the IPM: Operation window, select **Edit>Add**. The IPM: Add Operation window (Figure 5-41) is displayed.

Figure 5-41 IPM-Add Operation Window

The screenshot shows a dialog box titled "IPM: Add Operation". It has three tabs: "Protocol", "Statistics", and "Threshold". The "Protocol" tab is selected. The "Name" field contains "TN3270 IP". The "Description" field contains "IP echo for TN3270 Server". The "Sample Interval" is set to "60" with the unit "Secs". Below these fields are two dropdown menus: "Type" is set to "Path Echo" and "Protocol" is set to "IP Echo". There are two empty text boxes for "Request Size" and "Response Size". Below them is a checkbox labeled "Verify Data" which is unchecked. At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help...".

- Step 3. Enter data in the following fields:
 - Name—Enter a name for this operation. We will call this **TN3270 IP**.
 - Description—Enter **IP Echo for TN3270 Server**.
 - Interval—Use the default of 60 seconds. The valid range is from 10 to 3600 seconds (1 hour).
 - Type—Select **PathEcho**, which causes IPM to use route discovery algorithm to find a path to the destination and perform an echo for each device (hop) in the path.
 - Protocol—Select **IP Echo**.
- Step 4. Click **OK**.

Next, configure the operation for the SNA echo measurements. Repeat Steps 2 through 4. In Step 3, enter the following values:

- Name—Enter a name for this operation. We will call this **TN3270 SNA**.
- Description—Enter **SNA Echo for TN3270 Server**.
- Interval—Use the default of 60 seconds. The valid range is from 10 to 3600 seconds (1 hour).
- Type—Select **PathEcho**.
- Protocol—Select **SNA SSCP Echo**.

Configuring Collectors

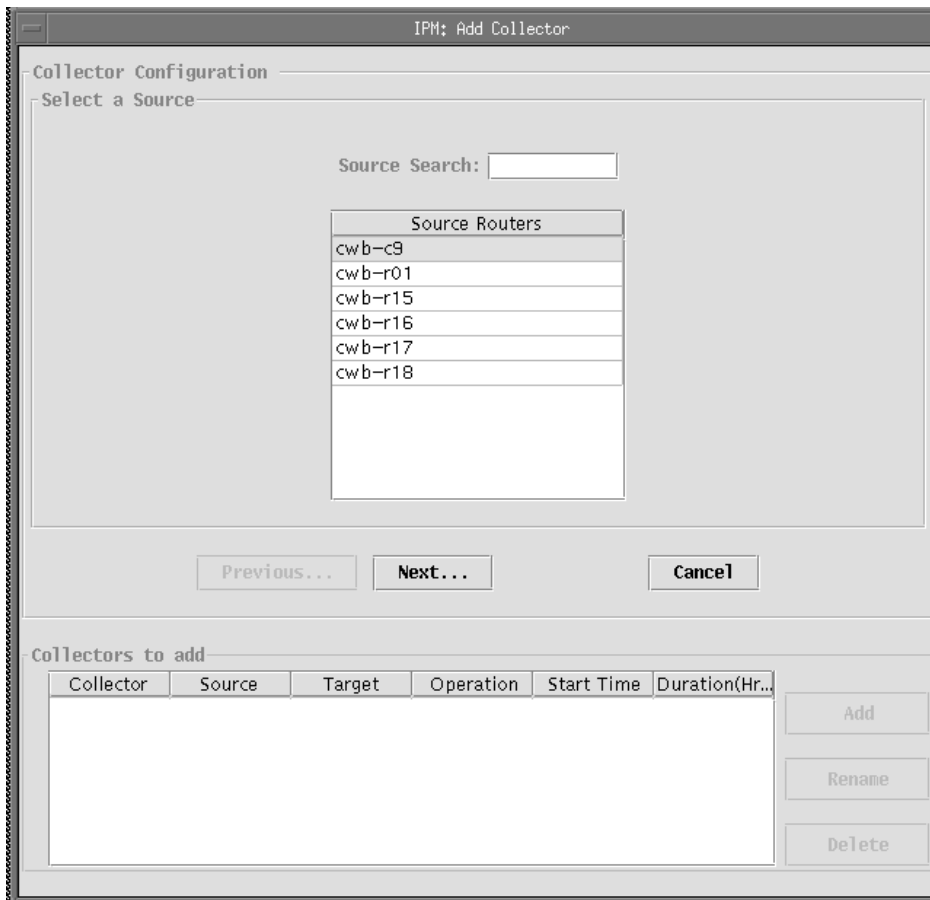
After you configure the IPM SNMP agents, targets, and operations, you can configure a collector, which is a combination of a source, target, and operation. For each collector, you can also specify parameters for gathering statistics, generating event notifications, and scheduling. For more information about these parameters, see the *CiscoWorks Blue Internetwork Performance Monitor User Guide*.

Note: Once you have configured a collector, you cannot change its attributes.

You will need three collectors, one for each measurement that you want to take. First, configure the collector for the measurement from the TN3270 Server Router to the client. To add a new IPM collector, do the following:

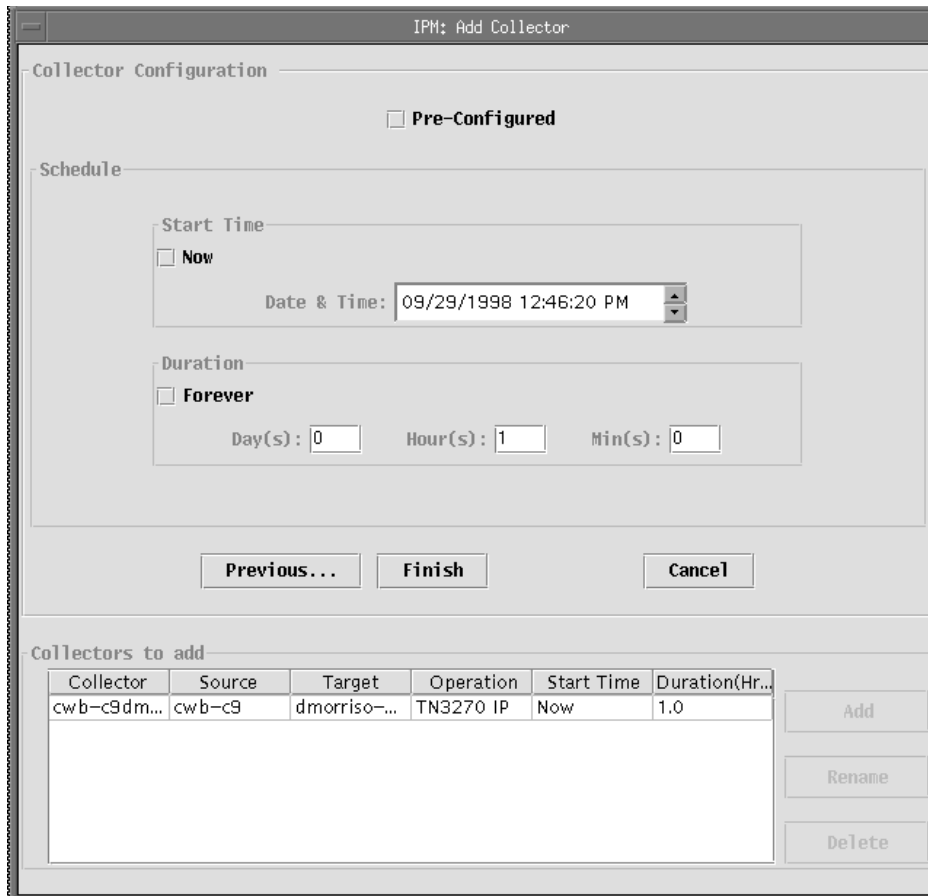
Step 1. From the Internetwork Performance Monitor main window, select **Edit>Add**. The IPM: Add Collector window (Figure 5-42) is displayed.

Figure 5-42 IPM: Add Collector Window



- Step 2. Select a source and click **Next**. The list of targets is displayed.
- Step 3. Select a target and click **Next**. The list of operations is displayed.
- Step 4. Select an operation and click **Next**. The start time and duration are displayed (Figure 5-43).

Figure 5-43 IPM: Add Collector Window (Start Time and Duration)



Step 5. Alter the start time, if desired, or select **Now**. Specify a duration or select **Forever**.

Step 6. Click **Finish**.

Next, configure a collector for the IP measurement from the TN3270 Server router to the mainframe. Finally, configure a collector for the SNA measurement from the TN3270 Server router to the mainframe.

Viewing Response Time Data

After you have configured the collectors, let them run for a few hours to collect a sampling of response-time data. You can then view the results of the collectors to isolate the network bottleneck. First, display the response times for the path from the TN3270 Server router to the client. To view response-time data, do the following:

- Step 1. From the Internetwork Performance Monitor main window, select the collector to be viewed.
- Step 2. From the menu bar, select **View>Display Results**. The IPM Display Time Filter window is displayed.
- Step 3. When this window is displayed, it already contains the starting and ending times for the collector. Click **OK** to view the results. The IPM Display window is displayed. No data is displayed yet, but the window shows you the paths found from the source to the target. Each icon in the upper-left corner of this window represents a different path.
- Step 4. Select one of the path icons to see all the hops for that path and then select one of the hops. The response-time statistics for that hop are displayed.

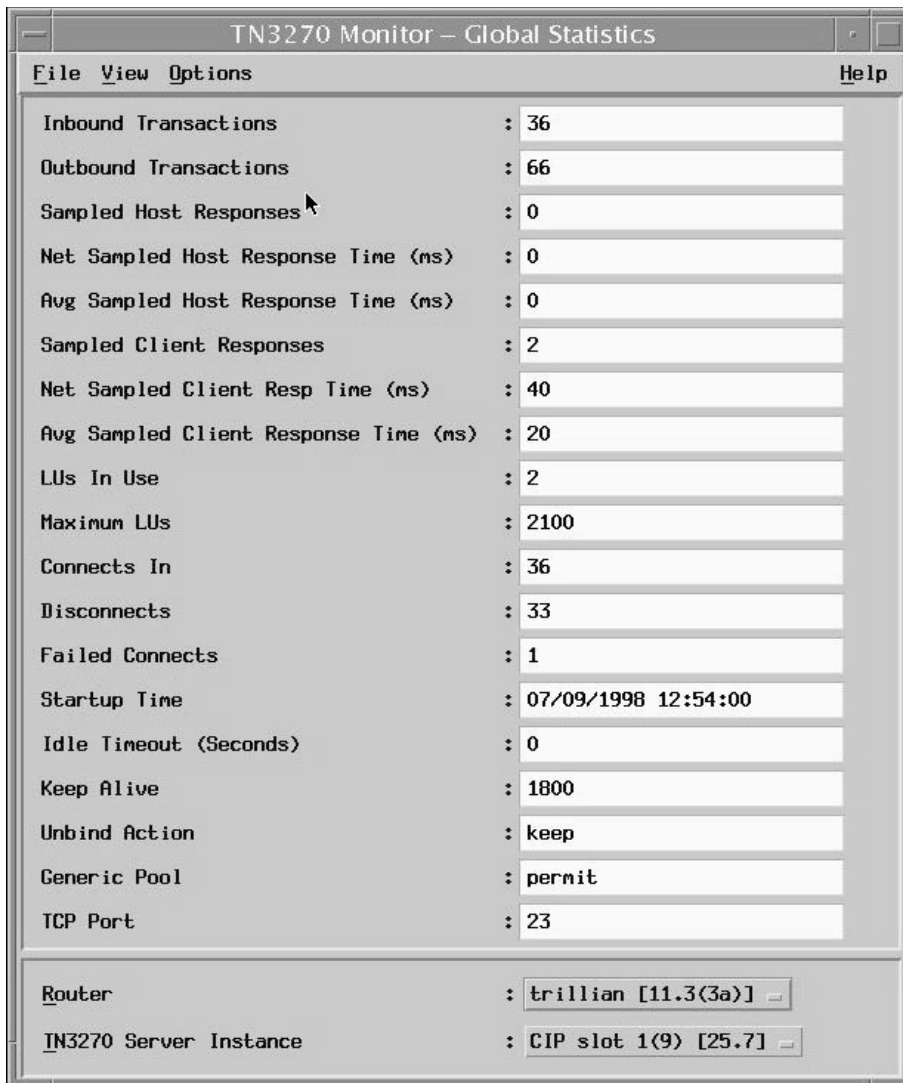
TN3270 Monitor

TN3270 Monitor also provides information about response times based on a sampling of host and client responses. The client data is only meaningful if you have configured the timing mark in the TN3270 Server. To configure the timing mark, access the command line of the TN3270 Server router and issue the **timing-mark** command in TN3270 configuration mode, as shown below:

```
router(cfg-tn3270)#timing-mark
```

To view the response-time data gathered by TN3270 Monitor, initiate the program to monitor the desired router. The Global Statistics window (Figure 5-44) is displayed.

Figure 5-44 Global Statistics Window



The screenshot shows a window titled "TN3270 Monitor - Global Statistics" with a menu bar containing "File", "View", "Options", and "Help". The main area displays a list of statistics in a two-column format. At the bottom, there are two dropdown menus for "Router" and "TN3270 Server Instance".

Inbound Transactions	: 36
Outbound Transactions	: 66
Sampled Host Responses	: 0
Net Sampled Host Response Time (ms)	: 0
Avg Sampled Host Response Time (ms)	: 0
Sampled Client Responses	: 2
Net Sampled Client Resp Time (ms)	: 40
Avg Sampled Client Response Time (ms)	: 20
LUs In Use	: 2
Maximum LUs	: 2100
Connects In	: 36
Disconnects	: 33
Failed Connects	: 1
Startup Time	: 07/09/1998 12:54:00
Idle Timeout (Seconds)	: 0
Keep Alive	: 1800
Unbind Action	: keep
Generic Pool	: permit
TCP Port	: 23
Router	: trillian [11.3(3a)]
TN3270 Server Instance	: CIP slot 1(9) [25.7]

This window includes the following fields:

- **Sampled Host Responses**—Number of inbound transactions examined for performance statistics, such as response time.
- **Net Sampled Host Response Time**—For each sampled Inbound Transaction, the amount of time that passes between when the RU chain is sent from the router and when a response is received from the host is measured. The total of all times measured for all the Inbound Transactions is the Net Sampled Host Response Time.
- **Avg Sampled Host Response Time**—Average Sampled Host Response Time in deciseconds (10 ms).
- **Sampled Client Responses**—Number of Outbound Transactions monitored for response time calculations.
- **Net Sampled Client Resp Time**—For each sampled Outbound Transaction, the amount of time that passes between when the timing mark is sent to the client and a response is received from the client is measured. The total time measured for all the Outbound Transactions is the Net Sampled Client Resp Time.
- **Avg Sampled Client Response Time**—This is the average Sampled Client Response Time in deciseconds (10 ms).

Managing from the Mainframe

Although ISM does not provide specific response-time data, it will alert you to a degraded state in a router if it receives an NMVT indicating a change in the response time by changing the color of the router to pink on the ISM Router Status panel.

Once you have defined your group of TN3270 Server routers, to monitor the status of the defined group, do the following:

- Step 1. On the IMS main menu, place your cursor beside MGR and press **Enter**. The Router Status panel is displayed.
- Step 2. In the Group/Router/Alias field, type TN3270 and press **Enter**. The Router Status panel (Figure 5-45) is displayed again, but this time contains only the routers defined as part of the TN3270 group.

Figure 5-45 Router Status Panel

```
NSPVMGRF Router Status Routers: 40 CNM01 09/15/98
Group/Router/Alias: TN3270 1 to 6 Target: CNM01 17:17
SPname SPname SPname SPname SPname SPname SPname SPname
CWBC01
CWBC07
MHONVPU1
MHONVPU2

NSP1186I Position cursor on resource and press PF5 to diagnose status.
==>
1=HELP 2=MAIN 3=RTN 5=DIAG 6=ROLL 9=DETAIL 10=MENU 12=RESET
```

The routers should be displayed in green. If a response time problem is detected, the color of the router will change to pink.

Monitoring TN3270 Server Performance

In addition to network response time, other factors can impact the performance of the TN3270 session. Performance problems are typically related to memory and CPU utilization issues.

Managing from the Workstation

TN3270 Monitor allows you to view events logged for a TN3270 Server. If you detect a performance problem with the server, you can use the TN3270 Monitor to locate events that indicate the nature of the performance problem. One of these events is “No memory for lu alloc”.

While in the TN3270 Monitor Events window, you can search for events that meet certain criteria. For example, to perform a search for all events related to memory problems, do the following:

- Step 1. Select **View>Search**. The Search window is displayed.
- Step 2. In the Search for field, specify **Event contains memory**.
- Step 3. By default, the search is performed against only the events currently listed in the TN3270 Monitor window. To perform a search against all events received from the router, click the button beside Search Current View, and select **Search Event Log** from the drop-down list.
- Step 4. Click **Search**. The results of the search are displayed in the Search window. This window is not dynamic. It lists only the events that match the criteria at the time the search was performed.

- Step 5. To apply the search results to the events window, select the events in the Search window that you would like to highlight in the filtered view. You can click on individual events or click **Select All** to select all the events.
- Step 6. Click **Apply** to highlight the same events in the filtered view.

Managing from the Mainframe

ISM alerts you to changes in router performance by changing the color of the router name as displayed on the ISM Router Status panel. You can use other ISM panels to determine the nature of the performance problem.

Once you have defined your group of TN3270 Server routers, to monitor the status of the defined group, do the following:

- Step 1. On the IMS main menu, place your cursor beside MGR and press **Enter**. The Router Status panel (Figure 5-46) is displayed.
- Step 2. In the Group/Router/Alias field, type TN3270 and press **Enter**. The Router Status panel is displayed again, but this time contains only the routers defined as part of the TN3270 group.

Figure 5-46 Router Status Panel

```

NSPVMGRF   Router Status           Routers: 40           CNM01   09/15/98
Group/Router/Alias: TN3270         1 to 6           Target: CNM01   17:17
SPname     SPname     SPname     SPname     SPname     SPname     SPname     Spname
CWBC01
CWBC07
MHONVPU1
MHONVPU2

NSP1186I Position cursor on resource and press PF5 to diagnose status.
==>
1=HELP 2=MAIN 3=RTN 5=DIAG 6=ROLL           9=DETAIL 10=MENU 12=RESET

```

The routers should be displayed in green. If a performance problem is detected, the color of the router will change to yellow.

- Step 3. Press **PF9**. The Router Status Extended panel (Figure 5-47) is displayed.

Figure 5-47 Router Status Extended Panel

```

NSPVMGRX      NSPMGR3 - Router Status Extended          CNM55  09/29/98
Group/Router/Alias:          Routers: 41          Target: CNM55  10:03
SPname   Status   Xtended   Operator Router Hostname   Operation Group(s)
$X0002E4  NOMON
$X0002E5  NOMON
CWBC01   PERF     T         cwbc01  cwbc-c1  TEST15
CWBC02   PERF     TLE      cwbc02  cwbc-c2  TEST8
CWBC03   ACTIV
CWBC04   PERF     LT       cwbc04  cwbc-c4  TEST1
CWBC05   NOMON
CWBC06   INOP
CWBC07   ACTIV
CWBC08   ACTIV
CWBC09   ALERT
CWBC10   CONCT
CWBC11   ACTIV
CWBC12   CONCT
CWBR11   CONCT
CWBR12   CONCT
CWBR13   CONCT
CWBR14   CONCT
NSP1186I Position cursor on resource and press PF5 to diagnose status.
==>
1=HELP 2=MAIN 3=RTN 5=DIAG 6=ROLL          8=FWD 9=RESETOP 10=MENU

```

For routers that are experiencing performance problems, the Status column will display PERF. The Xtended column then contains one or more letters that indicate the nature of the problem. Possible values are:

- P—A router memory or CPU usage problem
- Q—A CMCC memory or CPU usage problem
- Other letters indicate the type of interface that is experiencing a problem:
 - A—Async
 - M—ATM
 - C—Channel
 - E—Ethernet
 - D—FastEthernet
 - F—FDDI
 - H—HSSI
 - B—ISDN
 - L—Loopback
 - S—Serial
 - T—Tokenring
 - U—Tunnel

Step 4. Place your cursor on the desired router and press **PF5**. The resulting panel depends on the nature of the performance problem.

- If the Xtended column contains a P, the Router Performance History panel (Figure 5-48) is displayed and the problem data is highlighted.

Figure 5-48 Router Performance History Panel

NSPVRHIA		Router Performance History					CNM55	09/29/98
RTR Name: CWBC01							Target: CNM55	10:36
Date	Time	CPU Utilization (95%)			Memory Usage (10%)		(*)=Thresholds	
		5 Sec	1 Min	5 Min	TOTAL:	USED:	FREE:	
09/29/98	10:29	5%/4%	7%	7%	54633684	3016896	51616788	
09/29/98	10:14	4%/3%	7%	8%	54633684	3016728	51616956	
09/29/98	09:59	17%/3%	9%	8%	54633684	3009508	51624176	
09/29/98	09:44	6%/3%	9%	8%	54633684	3009508	51624176	
09/29/98	09:29	4%/3%	6%	7%	54633684	3009508	51624176	
09/29/98	09:14	5%/4%	8%	7%	54633684	3009472	51624212	
09/29/98	08:59	4%/3%	7%	7%	54633684	3009508	51624176	
09/29/98	08:44	4%/3%	8%	8%	54633684	3009508	51624176	
09/29/98	08:29	4%/3%	7%	7%	54633684	3009508	51624176	
09/29/98	08:14	5%/4%	6%	7%	54633684	3009472	51624212	
09/29/98	07:59	6%/4%	8%	7%	54633684	3009508	51624176	
09/29/98	07:44	5%/4%	7%	7%	54633684	3009508	51624176	
09/29/98	07:29	36%/3%	8%	7%	54633684	3009508	51624176	
09/29/98	07:14	4%/4%	7%	7%	54633684	3009472	51624212	
09/29/98	06:59	5%/4%	7%	7%	54633684	3009508	51624176	
09/29/98	06:44	5%/4%	8%	8%	54633684	3009508	51624176	
09/29/98	06:29	4%/3%	7%	7%	54633684	3009508	51624176	

==>

1=HELP 2=MAIN 3=RTN 6=ROLL 8=FWD 10=CPU 11=MEM

If you press **PF11**, the Router Command Interface panel (Figure 5-49) with the **show process mem** command is displayed.

Figure 5-49 Router Command Interface Panel with show process mem Command

```

NSPVCMDA          Router Command Interface          CNM55   09/29/98
SPname: CWBC01    Log:( NO | YES ) NO             Target: CNM55   10:39
Hostname= cwb-cl> Password:
  show process mem

Total: 54633684, Used: 3016896, Free: 51616788
PID  TTY  Allocated      Freed      Holding    Getbufs    Retbufs Process
  0   0    185176         1236       2412852    0           0 *Init*
  0   0      612         26191796    612        0           0 *Sched*
  0   0  173321672     159255952   3528       386140      0 *Dead*
  1   0      256          256         1720        0           0 Load Meter
  2   0  241690312     241510540  162204      0           0 Exec
  3   0      0            0           2720        0           0 Check heaps
  4   0    30004         0           2812       10140      0 Pool Manager
  5   0      256          256         2720        0           0 Timers
  6   0    10380         0           13100       0           0 CXBus hot stal
  7   0      304          0           3024        0           0 IPC Zone Manag
  8   0      0            0           2720        0           0 IPC Realm Mana
  9   0   13240576      952         3248        0           0 IPC Seat Manag
 10  0      1512         1219128     4152        0           0 ARP Input

==>
1=HELP 2=MAIN 3=RTN 5=COPY 6=ROLL          8=FWD          11=RIGHT 12=RECALL

```

- If the Xtended column contains a Q, the CMCC History panel (Figure 5-50) is displayed and the problem data is highlighted.

Figure 5-50 CMCC History Panel

NSPVCCHIA		CMCC History				CNM55 09/29/98		
RTR Name: CWBC01		Slot: 3				TARGET: CNM55 10:33		
Date	Time	Memory (10%)	CPU Utilization (75%)			DMA Utilization		
		dram	1 Min	5 Min	60 Min	1 Min	5 Min	60 Min
09/29/98	10:29	53909712/64M	1%	0%	0%	1%	0%	0%
09/29/98	10:14	53909712/64M	1%	0%	0%	1%	0%	0%
09/29/98	09:59	53909712/64M	1%	0%	0%	1%	0%	0%
09/29/98	09:44	53909712/64M	1%	0%	0%	1%	0%	0%
09/29/98	09:29	53909712/64M	1%	0%	0%	1%	0%	0%
09/29/98	09:14	53909712/64M	1%	0%	0%	1%	0%	0%
09/29/98	08:59	53909712/64M	1%	0%	0%	1%	0%	0%
09/29/98	08:44	53909712/64M	1%	0%	0%	1%	0%	0%
09/29/98	08:29	53909712/64M	1%	0%	0%	1%	0%	0%
09/29/98	08:14	53909712/64M	1%	0%	0%	1%	0%	0%
09/29/98	07:59	53909712/64M	1%	0%	0%	1%	0%	0%
09/29/98	07:44	53909712/64M	1%	0%	0%	1%	0%	0%
09/29/98	07:29	53909712/64M	1%	0%	0%	1%	0%	0%
09/29/98	07:14	53909712/64M	1%	0%	0%	1%	0%	0%
09/29/98	06:59	53909712/64M	1%	0%	0%	1%	0%	0%
09/29/98	06:44	53909712/64M	1%	0%	0%	1%	0%	0%
09/29/98	06:29	53909712/64M	0%	0%	0%	1%	0%	0%

==> MORE=>

1=HELP 2=MAIN 3=RTN 5=CURRENT 6=ROLL 8=FWD 11=RIGHT

- If the Xtended column contains any other letters, the appropriate interface panel is displayed.

You can also configure ISM to generate an alert if certain performance thresholds are exceeded. To configure the performance thresholds, do the following:

- Step 1. On the ISM main panel, select **CMCC**. The CMCC Monitoring Options panel is displayed.
- Step 2. Select **List** to display all of the CMCC routers that ISM has discovered. The Cisco Mainframe Channel Connections panel is displayed.
- Step 3. Place your cursor beside the desired router and press **PF9**. The ISM CMCC Administration panel (Figure 5-51) is displayed.

Figure 5-51 ISM CMCC Administration Panel

```
NSPVCDEF          ISM CMCC Administration          CNM55  09/29/98
                  TARGET: CNM55  11:18

Router Name: CWBC01      CMCC Slot: 3      Related Channels:  3/0  3/1  3/2

Current Status:  ACTIV      Last Status Change:  08:00  09/28/98  UNKNOWN

CMCC Version:  CIP 4.132 210.40

Overrides:  C=75
CPU Threshold: 75      Memory Threshold:      Archive:

Monitor Mode ( YES | NO ): YES

Delete history and performance records ( NO | YES ): NO

Change Type ( 2: Update, 3: Delete ): 2
Action Type ( 1: Next Initialization, 2: Current, 3: or Both): 3

  NSP1037I Make changes and press Enter to validate.
Action==>
1=HELP 2=MAIN 3=RTN 4=UPDATE 6=ROLL          9=DEBUG
```

You can alter the CPU and memory thresholds. Then, when the threshold is exceeded, ISM generates an alert.

Glossary

3270 data stream—A type of data stream developed by IBM for use with communication between mainframe applications and end users. The data stream includes control characters that instruct the receiving device how to format or display the information. The control characters allow the application to use the entire screen, as opposed to a single command line, to display information in and receive input from various areas of the screen, called partitions.

ACTLU—(activate logical unit) In SNA, a command used to start a session on a logical unit.

ACTPU—(activate physical unit) In SNA, a command used to start a session on a physical unit.

APAR—(authorized program analysis report) Problem tracking mechanism used by IBM.

APPN—(Advanced Peer-to-Peer Networking) Enhancement to the original IBM SNA architecture. APPN handles session establishment between peer nodes, dynamic transparent route calculation, and traffic prioritization for APPC traffic.

ARP—(Address Resolution Protocol) An Internet protocol used to map an IP address to a MAC address. Defined in RFC 826.

Bus-and-tag—IBM channel, developed in the 1960s, incorporating copper multiwire technology. Replaced by the ESCON channel.

channel-attached router—Any Cisco router that is connected to a mainframe via a channel connection using either the CIP or CPA.

CICS—(Customer Information Control System) IBM application subsystem allowing transactions entered at remote terminals to be processed concurrently by user applications.

CIP—Channel Interface Processor.

Client—(also referred to as an end client or TN3270 client) The remote users that access the TN3270 Server.

CMCC—(Cisco Mainframe Channel Connection) Any of the Cisco router CIP and CPA feature cards (interface processors or port adapters) that allows a user to establish a channel connection between the router and a mainframe.

CMOS—Complementary Metal Oxide Semiconductor.

CoS—(class of service) An indication of how an upper-layer protocol requires a lower-layer protocol to treat its messages. In SNA subarea routing, CoS definitions are used by subarea nodes to determine the optimal route to establish a given session. A CoS definition comprises a virtual route number and a transmission priority field. Also called ToS.

CP—(control point) In SNA networks, element that identifies the APPN networking components of a PU 2.1 node, manages device resources, and provides services to other devices. In APPN, CPs are able to communicate with logically adjacent CPs using CP-to-CP sessions.

CPA—Channel Port Adapter.

CSNA—Cisco SNA.

DDDLU—(Dynamic Definition of Dependent LU) A feature of VTAM that allows LUs to be created as needed and not be predefined under a switched PU. The CIP TN3270 Server supports DDDLU.

DHCP—(Dynamic Host Configuration Protocol) A mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.

Direct PU—A PU type 2 that has its own LLC2 link to the owning VTAM. Several direct PUs can share a local SAP, but each must have a unique local/remote MAC/SAP quadruple.

DLSw—(data-link switching) An interoperability standard, described in RFC 1434, that provides a method for forwarding SNA and NetBIOS traffic over TCP/IP networks using data-link layer switching and encapsulation. DLSw uses SSP instead of SRB, eliminating the major limitations of SRB, including hop-count limits, broadcast and unnecessary traffic, timeouts, lack of flow control, and lack of prioritization schemes.

DLU—(dynamic LU) An LU that is dynamically created using DDDLU.

DLUR—(Dependent LU Requester) A feature of APPN that allows traditional 3270 traffic to be routed over the APPN network. The DLUR feature in the CIP creates an LU 6.2 session (pipe) with DLUS (Dependent LU Server) in VTAM (VTAM V4R2 or higher). DLUR is defined as a separate switched PU to VTAM. All 3270 session control traffic (SSCP-to-PU and SSCP-to-LU) flows over this DLUR-DLUS pipe. Session data traffic, however, can be routed directly from LU to LU using APPN routing. The CIP DLUR is implemented as an APPN end node (EN).

DLUR PU—A PU 2 that uses the DLUR-DLUS pipe to send and receive all session control traffic. It does not use its own source SAP because it uses the DLUR SAP. Similarly, it does not have its own LLC session to the mainframe gateway because it rides on top of the DLUR LLC link.

DLUS—(Dependent LU Server) The server half of the Dependent LU Requester/Server enhancement to APPN. The DLUS component provides SSCP services to DLUR nodes over an APPN network.

DNS—(Domain Name System) The system used in the Internet for translating names of network nodes into addresses.

DRP—(Director Response Protocol) A protocol used by the DistributedDirector feature in IP routing.

EN—(end node) An APPN end system that implements the PU 2.1, provides end-user services, and supports sessions between local and remote CPs. ENs are not capable of routing traffic and rely on an adjacent NN for APPN services.

ESCON—(Enterprise Systems Connection) IBM's fiber optic serial channel for attaching mainframes to peripherals such as storage devices, backup units, and network interfaces. This channel incorporates fiber channel technology. The ESCON channel replaces the bus-and-tag channel.

FEP—(front-end processor) A device or board that provides network interface capabilities for a networked device. In SNA, an FEP is typically an IBM 3745 device.

HSRP—(Hot Standby Router Protocol) A protocol that provides high network availability and transparent network topology changes. HSRP creates a Hot Standby router group with a lead router that services all packets sent to the Hot Standby address. The lead router is monitored by other routers in the group, and if it fails, one of these standby routers inherits the lead position and the Hot Standby group address.

ICN—Interchange node.

IMS—(Information Management System) A database/data communication (DB/DC) system from IBM that is used to manage complex databases and networks.

INCLUD0E—A feature of VTAM that allows the actual LU to be sent in the ACTLU. Normally, for direct PUs, the LOCADDR number (2 hexadecimal characters) is sent to the CIP with the ACTLU. However, if a parameter called INCLUD0E=YES is coded on the PU statement, then VTAM also sends the actual LU name to the channel-attached router with the ACTLU. INCLUD0E is not relevant to DLUR PUs because DLUS sends the LU name to the channel-attached router by default. INCLUD0E was first supported by XCA in VTAM 4.4 (plus PTFs). If the Direct PU connects to VTAM via an FEP, then the FEP also needs to support INCLUD0E.

IPM—(Internetwork Performance Monitor) A Cisco workstation-based network management product that provides data about response times between devices.

ISM—(Internetwork Status Monitor) A Cisco mainframe-based network management product that allows users to manage their Cisco routers from their mainframe network management application (NetView for OS/390 or SOLVE:Netmaster).

ISP—(Internet Service Provider) A company that provides Internet access to other companies and individuals.

JES—(job entry subsystem) An IBM licensed program that receives jobs into the system and processes all output data produced by the jobs.

LEN node—(low-entry networking node) In SNA, a PU 2.1 that supports LU protocols, but whose CP cannot communicate with other nodes. Because there is no CP-to-CP session between a LEN node and its NN, the LEN node must have a statically defined image of the APPN network.

LLC—(Logical Link Control) Higher of the two data link layer sublayers defined by the IEEE. The LLC sublayer handles error control, flow control, framing, and MAC-sublayer addressing. The most prevalent LLC protocol is IEEE 802.2, which includes both connectionless and connection-oriented variants.

LOCADDR—Local address.

LPAR—Logical partition.

LPD—(line printer daemon) The protocol used to send print jobs between UNIX systems.

LU—(logical unit) A type of addressable unit in an SNA network. The LU is the port through which the end user accesses both the SSCP provided services, and communicates with other LUs at other nodes.

LU nailing—A method by which you can associate a client's connection request with a specific LU.

LSAP—(link service access point) In the IBM Token Ring network, the logical point at which an entity in the logical link control sublayer provides services to the next higher layer.

MAC—(Media Access Control) Lower of the two sublayers of the data link layer defined by the IEEE. The MAC sublayer handles access to shared media, such as whether token passing or contention will be used.

MVS—(Multiple Virtual Storage) Operating system for IBM mainframes.

NAU—(network addressable unit) An SNA term to describe the three entities which are addressable in an SNA network: SSCP, PU and LU.

NCP—(Network Control Program) In SNA, a program that routes and controls the flow of data between a communications controller (in which it resides) and other network resources.

NMVT—(Network Management Vector Transport) An SNA message consisting of a series of vectors conveying network management information.

NN —(network node) An SNA intermediate node that provides connectivity, directory services, route selection, intermediate session routing, data transport, and network management services to LEN nodes and ENs. The NN contains a CP that manages the resources of both the NN and those of the ENs and LEN nodes in its domain. NNs provide intermediate routing services by implementing the APPN PU 2.1 extensions.

Non-E Client—An end-user workstation, usually a PC, that is running TN3270 client software that does not support the functions of TN3270E.

OSPF—(Open Shortest Path First) Link-state, hierarchical IGP routing algorithm proposed as a successor to RIP in the Internet community. OSPF features include least-cost routing, multipath routing, and load balancing. OSPF was derived from an early version of the IS-IS protocol.

PLU—(primary logical unit) In SNA, the LU that sends the Bind to activate a session with its partner LU.

PU—(physical unit) A type of addressable unit in an SNA network. Each node in the network has a PU, which provides services to control the physical configuration and the communication system resources associated with the node, and also to collect maintenance and operational statistics.

PSID—(product-set identification) In SNA, a technique for identifying the hardware and software products that implement a network component.

PTF—(program temporary fix) Interim program fixes offered by IBM.

QLLC—(Qualified Logical Link Control) Data link layer protocol defined by IBM that allows SNA data to be transported across X.25 networks.

QoS—Quality of Service.

RMAC—Remote MAC.

RSAP—Remote SAP.

RSRB—(remote source-route bridging) A method of encapsulating SRB traffic over WAN links.

RTR—(response-time reporter) A feature of Cisco IOS software that provides round trip time measurements between devices.

SAP—(service access point) A logical address that allows a system to route data between a remote device and the appropriate communications support.

SLU—(secondary logical unit) In SNA, the LU that contains the secondary half-session for a particular LU-to-LU session. An LU can contain secondary and primary half-sessions for different active LU-to-LU sessions.

SNA—(Systems Network Architecture) An architecture designed by IBM to provide a unified systems design for their communication network products.

SNAP—(Subnetwork Access Protocol) Internet protocol that operates between a network entity in the subnetwork and a network entity in the end system. SNAP specifies a standard method of encapsulating IP datagrams and ARP messages on IEEE networks. The SNAP entity in the end system makes use of the services of the subnetwork and performs three key functions: data transfer, connection management, and QoS selection.

SNMP—(Simple Network Management Protocol) Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

SRB—(source-route bridging) Method of bridging originated by IBM and popular in Token Ring networks. In an SRB network, the entire route to a destination is predetermined, in real time, prior to the sending of data to the destination.

SR/TLB—(source-route translational bridging) Method of bridging where source-route stations can communicate with transparent bridge stations with the help of an intermediate bridge that translates between the two bridge protocols.

Static LU—An LU that is hard-coded in the VTAM PU definition in the switched major node. When the PU is activated, VTAM activates the static LUs by sending an ACTLU to the channel-attached router for each statically defined LOCADDR.

SSCP—(system services control points) A type of addressable unit in an SNA network. The SSCP provides services to manage the network and respond to network requests from network operators and terminal operators.

SSCPFM—(system services control point format) A parameter of the LUGROUP major node that specifies the data stream format to be used for communication between the client and the mainframe.

switched PU—An SNA physical unit that is defined in a VTAM switched major node. All TN3270 Server PUs are switched PUs.

SWMN—(switched major node) In VTAM, a major node that contains minor nodes that are PUs and LUs attached by switched Synchronous Data Link Control (SDLC) links.

TACACS—(Terminal Access Controller Access Control System) Authentication protocol, developed by the DDN community, that provides remote access authentication and related services, such as event logging. User passwords are administered in a central database rather than in individual routers, providing an easily scalable network security solution.

TN3270E client—A workstation that is running TN3270 client software that supports RFC 2355 functions. These functions include the ability to request a specific LU name and support for printers (LU 1 and LU 3) in addition to LU 2 support.

TN3270 Server—The channel-attached router function that converts TN3270 traffic into native SNA upstream to the host and converts native SNA to TN3270 traffic going back to the client.

ToS—Type of service.

TTL—Time-to-Live.

USSTAB—(unformatted system services tables) A parameter of the LUGROUP major node that specifies which table to use for determining the definitions of operator messages and certain commands.

VTAM—(Virtual Telecommunications Access Method) Set of programs that control communication between LUs. VTAM controls data transmission between channel-attached devices and performs routing functions.

XID—(eXchange IDentification) A command that is sent from one communication node to another to establish a communication link between the two nodes and to exchange node configuration parameters. IBM has defined four formats for XIDs: formats 0, 1, 2, and 3. These formats are used between different types of nodes. But all of these formats share a common identification field consisting of an IDBLK and IDNUM.

XCA—External Communications Adapter.

References

This appendix contains lists of helpful reference documents.

Compliant RFCs

The RFCs that are used to define TN3270 are RFC 1576, RFC 1646, and RFC 2355.

- **RFC 1576**—This document describes the existing implementation for transferring 3270 display terminal data using currently available Telnet capabilities. The name traditionally associated with this implementation is TN3270. Information is provided to aid in the implementation of TN3270 servers and client terminal emulators. The following areas pertaining to TN3270 implementations are presented in this document:
 - Telnet options negotiated to transition from a NVT ASCII state to a TN3270 state ready to process incoming 3270 data stream commands
 - Method for sending and receiving 3270 data
 - Method of handling the special keys, known as SYSREQ and ATTN, using current available Telnet commands
- **RFC 1646**—This document describes protocol extensions to TN3270 for printer support. There are two extensions outlined in this document. The first defines a way for a TN3270 client to request a specific device (LUname) from a TN3270 server. The second extension specifies how a TN3270 printer device can be requested by a TN3270 client and the manner in which the 3270 printer status information can be sent to the TN3270 server.
- **RFC 2355**—This document describes a protocol that more fully supports 3270 devices than the existing TN3270 practices. Specifically, it defines a method of emulating both the terminal and printer members of the 3270 family of devices via Telnet; the Telnet client is able to request that it be assigned a specific device-name (also referred to as “LU name” or “network name”). Finally, it adds support for a variety of functions such as the ATTN key, the SYSREQ key, and SNA response handling.

Cisco Documentation

This section lists Cisco documents that contain additional information about the products and features described in this document. All documents listed in this section can be found on CCO.

The following Cisco IOS software documents contain additional information about configuring the router features described in this document:

- *Bridging and IBM Networking Configuration Guide*
- *Bridging and IBM Networking Command Reference*
- *MIB Quick Reference*
- *System Error Messages*

The following documents contain additional information about the TN3270 clients described in this document:

- *WebConnect Pro Installation Guide Version 3.5*
- *WebConnect Pro User Guide Version 3.5*

The following Cisco documents contain additional information about the network management products described in this document:

- *CiscoWorks Blue Maps Installation and User Guide*
- *Internetwork Status Monitor Installation Guide*
- *Internetwork Status Monitor User Guide*
- *CiscoWorks Blue Internetwork Performance Monitor User Guide*
- *Cisco Resource Manager 1.1 Installation Guide for Solaris*
- *Cisco Resource Manager 1.1 Installation Guide for Windows NT*
- *Learning to Use Cisco Resource Manager 1.1*

The following Cisco documents contain chassis-specific hardware configuration or troubleshooting information:

- *Cisco 7000 Hardware Installation and Maintenance*
- *Cisco 7010 Hardware Installation and Maintenance*
- *Cisco 7505 Hardware Installation and Maintenance*
- *Cisco 7507 Hardware Installation and Maintenance*
- *Cisco 7513 Hardware Installation and Maintenance*
- *Cisco 7202 Hardware Installation and Maintenance*
- *Cisco 7204 Hardware Installation and Maintenance*
- *Cisco 7206 Hardware Installation and Maintenance*

The following Cisco documents contain information about the CIP and CPA:

- *Channel Interface Processor (CIP) Installation and Configuration*
- *Channel Interface Processor Microcode Release Note and Microcode Upgrade Requirements*
- *PA-IC-E ESCON Channel Port Adapter Installation and Configuration*
- *Channel Port Adapter Microcode Release Note and Microcode Upgrade Requirements*