

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Note: CRM has been recently superseded by CiscoWorks 2000 Resource Manager Essentials (RME).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.ffff.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.ffff.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.

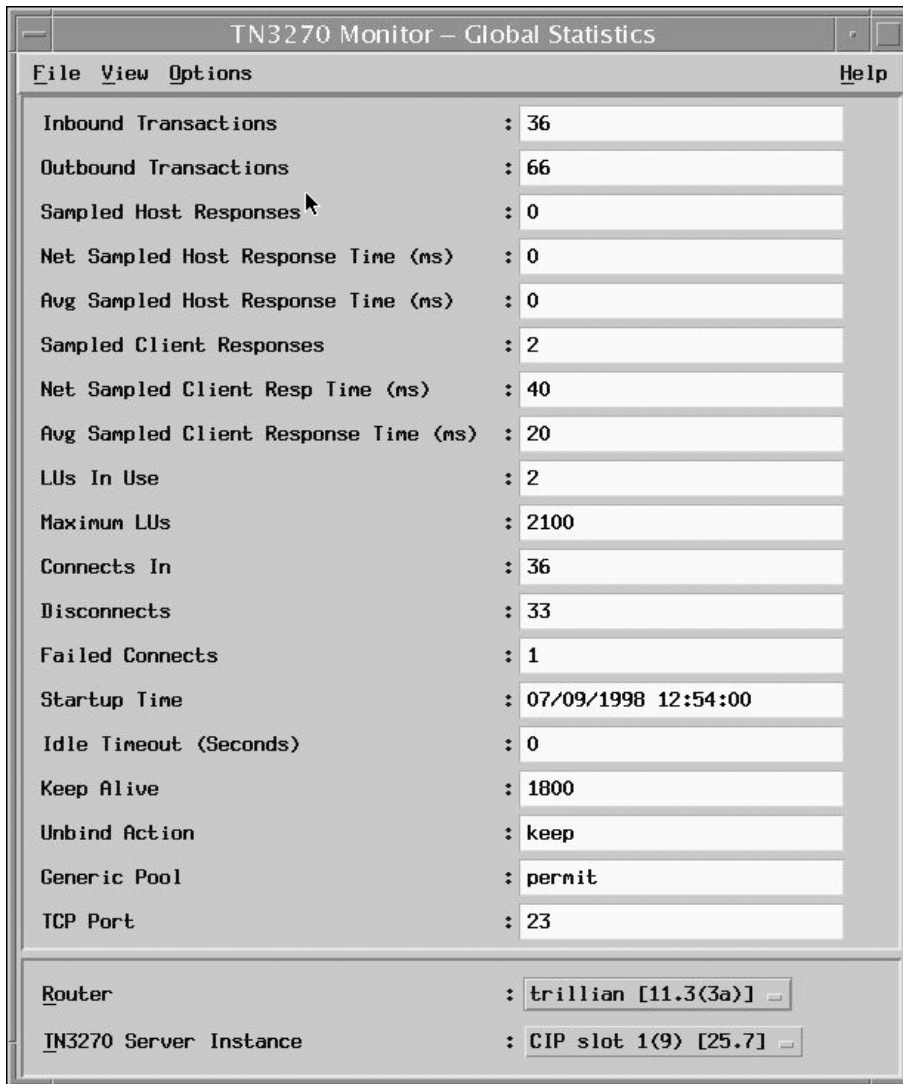
For example, the following is a KORN shell script that invokes TN3270 Monitor for four different TN3270 Server IP addresses. It starts TN3270 Monitor four times and assumes that the SNMP read-only community string is public.

```
#!/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
PUIOE	172.26.20.34	23	active
PUXCPT07	172.26.20.35	23	active
PUXCPA09	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	: PUXCPT07
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
LU 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.

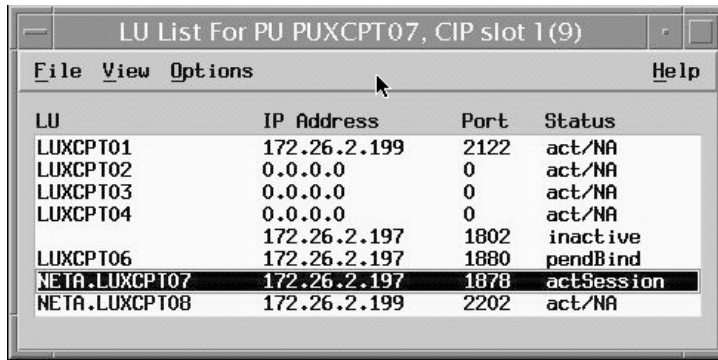
Table 5-7 Statistics on the PU Detail Window

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

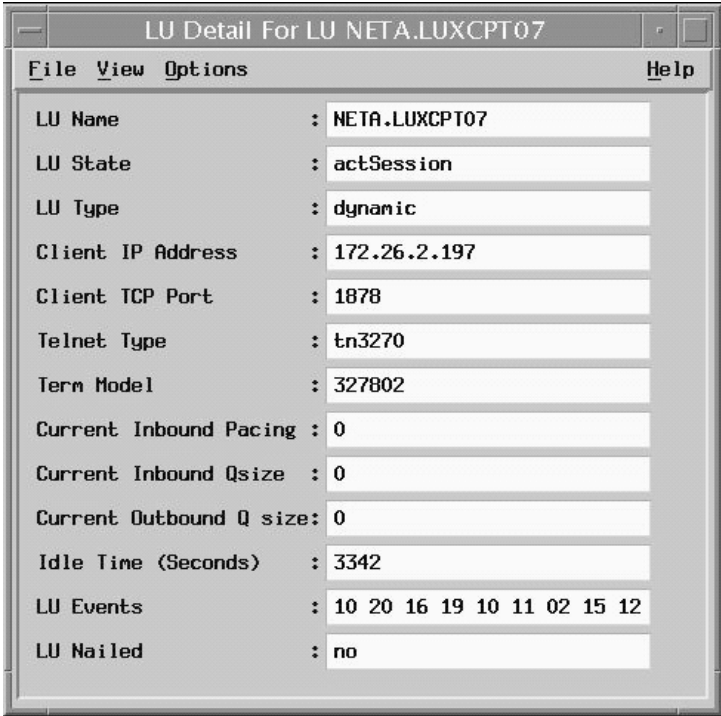


Table 5-8 lists the fields displayed in the LU Detail window.

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	Sev	Event	CIP	PU	LU	Rem IP Address	RPort	Loc IP Address	LPort
07/09/1998 16:01:17	N	LU Disc frn tnet ses	1	PUXCPT07	NETA.LUXCPT08	172.26.2.199	2202		
07/09/1998 15:51:11	N	Tnet sess connected	1	PUXCPT07		172.26.2.197	1880	172.26.20.35	23
07/09/1998 15:50:55	N	LU Disc frn tnet ses	1	PUI0E	LUEEEE04	172.26.2.197	1879		
07/09/1998 15:50:44	N	Tnet sess connected	1	PUI0E		172.26.2.197	1879	172.26.20.34	23
07/09/1998 15:47:42	N	Tnet listen state ch	1					172.26.20.35	23
07/09/1998 15:47:12	T	Static LU activated	1		PUXCPT07 LUXCPT04				
07/09/1998 15:47:12	T	Static LU activated	1		PUXCPT07 LUXCPT03				
07/09/1998 15:47:12	T	Static LU activated	1		PUXCPT07 LUXCPT02				
07/09/1998 15:47:12	T	Static LU activated	1		PUXCPT07 LUXCPT01				
07/09/1998 15:47:12	N	PU state changed	1	PUXCPT07				172.26.20.35	23
07/09/1998 15:47:12	N	PU state changed	1	PUXCPA09				172.26.20.35	23
07/09/1998 15:46:56	U	Link to ILLUS lost	1						
07/09/1998 15:46:56	U	Link lost	1						
07/09/1998 15:46:56	U	Link disc by remote	1						
07/09/1998 15:46:56	U	Conwin Unbrd by ILLUS	1						
07/09/1998 15:46:56	N	Tnet listen state ch	1					172.26.20.35	23
07/09/1998 15:46:56	N	PU state changed	1	PUXCPT07				172.26.20.35	23
07/09/1998 15:46:56	N	PU state changed	1	PUXCPA09				172.26.20.35	23
07/09/1998 15:46:56	U	Conlstr Unbrd by ILLUS	1						
07/09/1998 15:43:16	U	CP Conlstr Unbound	1						
07/09/1998 15:43:16	U	CP Conlstr Unbound	1						
07/09/1998 15:39:00	N	LU-LU sess started	1	PUXCPT07	NETA.LUXCPT07	172.26.2.197	1878	172.26.20.35	23
07/09/1998 15:39:00	T	LU Bind	1	PUXCPT07	NETA.LUXCPT07	172.26.2.197	1878		
07/09/1998 15:38:51	N	Tnet sess connected	1	PUXCPT07	LUXCPT07	172.26.2.197	1878	172.26.20.35	23
07/09/1998 15:38:40	N	LU Disc frn tnet ses	1	PUXCPT07	LUXCPT07	172.26.2.197	1847		
07/09/1998 15:38:29	N	LU-LU sess started	1	PUXCPT07	NETA.LUXCPT08	172.26.2.199	2202	172.26.20.35	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     15     2     1      1
   0  HSSI         6     3     3      3
   3  ISDN         21     3     73     46
   3  Tunnel       6     3     2     4
   2  ATM          21     3     15     15
  14  FastEthernet 6     3     2     2
 158  Serial      21     3     73     15
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 5-10 CMCC Extended Display Panel

```

NSPVCDIS                      CMCC Extended Display                      CNM01  09/10/98
                                TARGET: CNM01  16:03

-----
| Spname | --- | CMCC | --- | Channel | --- | SUB CHANNEL |
| MHONVPU1 | | Slot 3 | | 3/0 | | Mode= CLAW |
-----
                                | Path= 0100 |
                                | Device= 30 |
                                | Sense= 0000 |
                                | Mode= CLAW |
                                | Path= 0100 |
                                | Device= 31 |
                                | Sense= 0000 |
                                | Mode=      |
                                | Path=      |
                                | Device=      |
                                | Sense=      |
-----

Status= ALERT          Status= ACTIV
EXT= CM                Hardware= CIP2
                        Level= 5.0
                        Software= 214.40

                                Press PF11 for
                                More channels.

Tab to a resource name and press enter
to obtain details about the resource.

Action==>
1=HELP 2=MAIN 3=RTN          6=ROLL          11=Channel

```

This panel displays status information for the first interface, interface 0, on the channel connection. In this example, the channel connection is provided by a CIP. The TN3270 Server is always implemented on interface 2 of a CIP or CPA, so to view the status of interface 2, press PF11 twice. The CMCC Extended Display panel (Figure 5-11) for interface 3/2 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= UP  |
-----

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		18:27 09/09/98 UNKNOWN
MHONVPU1	CHANNEL3/1	UP		18:27 09/09/98 UNKNOWN
MHONVPU1	CHANNEL3/2	UP		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
SName: MHONVPU1   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          InDestUnreaches:
  InTimeExcds    : 0          InParmProbs       : 0          InSrcQuenches  :
  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.

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.

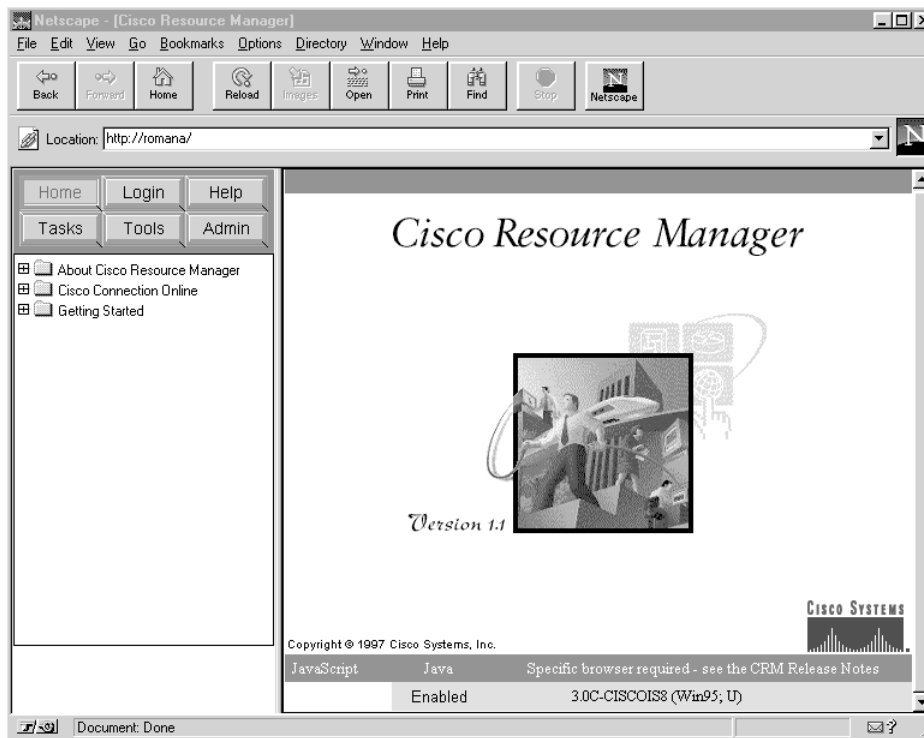
These instructions assume that you have successfully installed Cisco Resource Manager on a UNIX or NT workstation.

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.

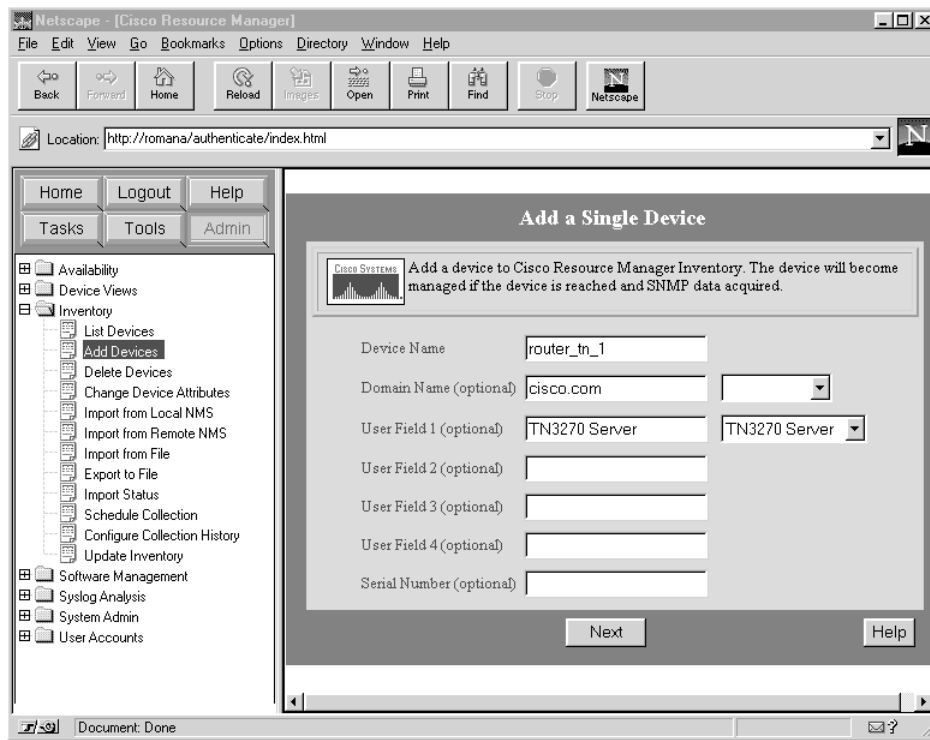
- Step 1. From a Java-compliant Web browser, browse the network management system workstation that is currently running Cisco Resource Manager. In this example, Cisco Resource Manager is running on a workstation named romana. The Cisco Resource Manager main window (Figure 5-18) is displayed.

Figure 5-18 Cisco Resource Manager Main Window



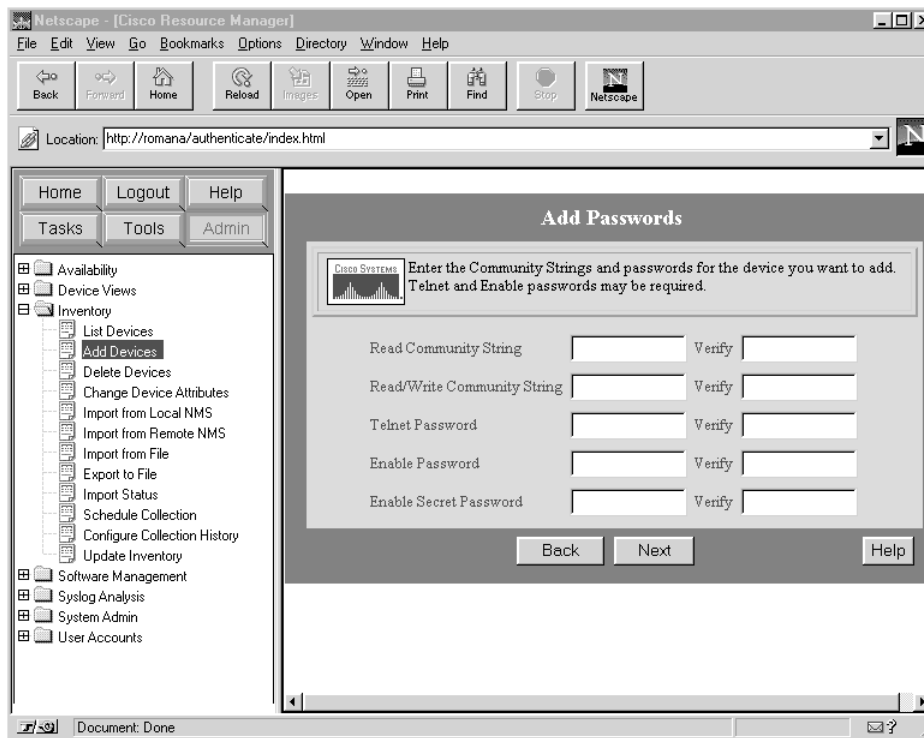
- Step 2. Click Login and log in with administrator privileges. The Cisco Resource Manager default user name and password are admin.
- Step 3. Add all of the routers running the TN3270 Server by doing the following:
 - Click Admin.
 - Click the Inventory folder.
 - Click Add Devices. The Add a Single Device window (Figure 5-19) is displayed.

Figure 5-19 Add a Single Device Window



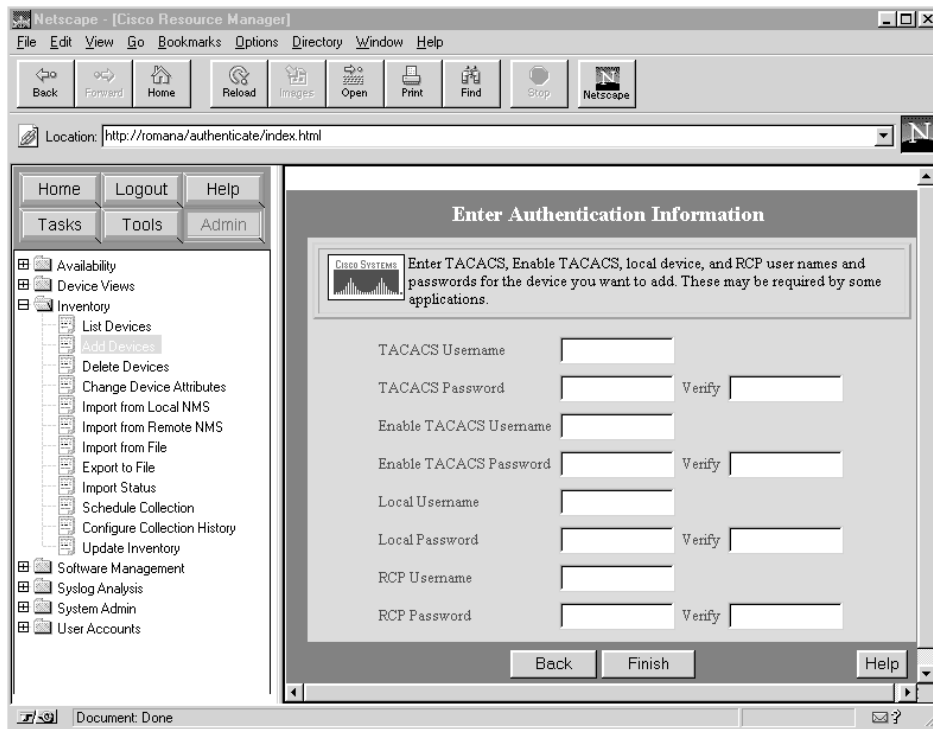
- Enter the IP address or host name of a router running TN3270 Server. The IP address should be the address used by TN3270 clients to connect to the TN3270 Server on that router.
- In the User Field 1 field, enter TN3270 Server to identify this router as running the TN3270 Server.
- Click Next. The Add Passwords window (Figure 5-20) is displayed.

Figure 5-20 Add Passwords Window



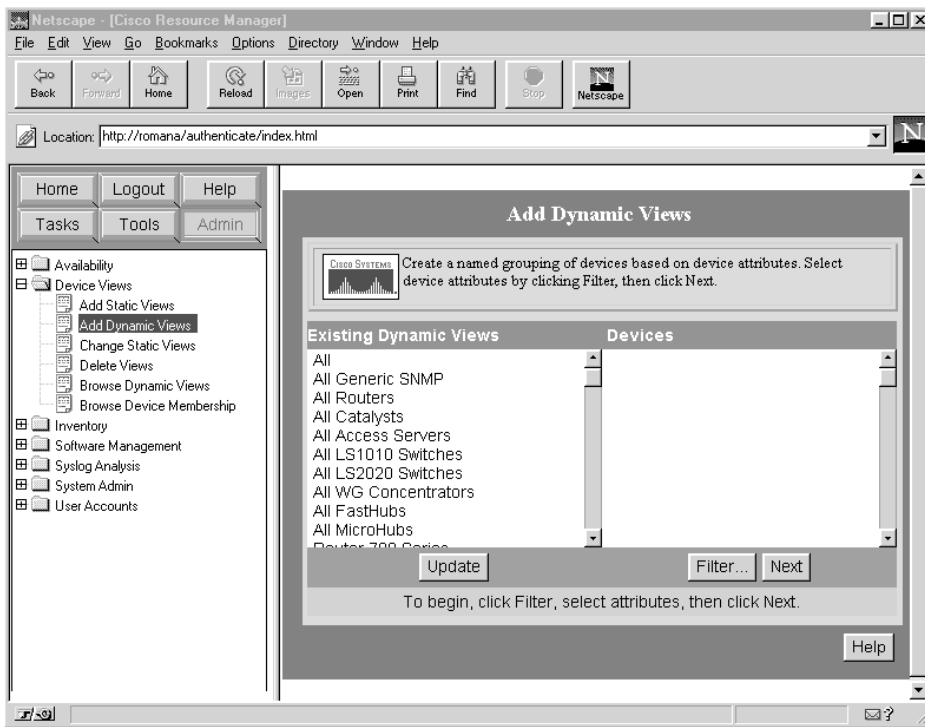
- Enter the Read and Read/Write community strings that are configured for the router.
- Enter the Telnet and Enable passwords for the router.
- Click Next. The Enter Authentication Information window (Figure 5-21) is displayed. If you are using TACACS, enter that information in this window.

Figure 5-21 Enter Authentication Information Window



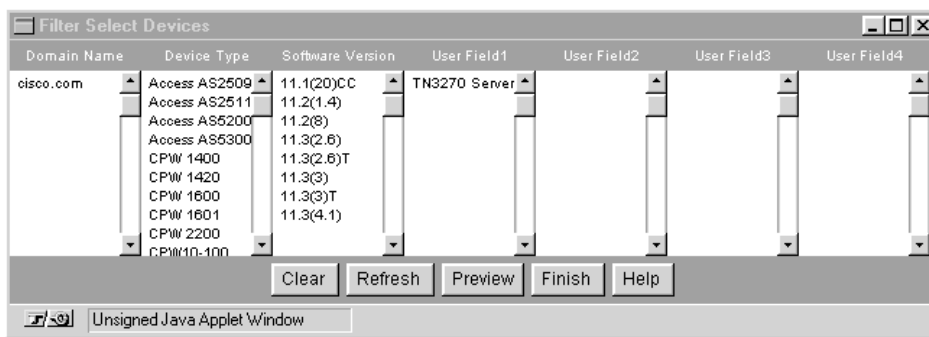
- Click Finish to add the router to the Cisco Resource Manager database.
 - Repeat this process for each router that is running the TN3270 Server.
- Step 4. Configure a Dynamic Device View for all routers running TN3270 Server by doing the following:
- Click Admin.
 - Click the Device Views folder.
 - Click Add Dynamic Views. The Add Dynamic Views window (Figure 5-22) is displayed.

Figure 5-22 Add Dynamic Views Window



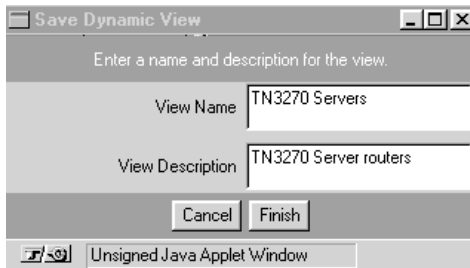
- Click Filter. The Filter Select Devices window (Figure 5-23) is displayed.

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

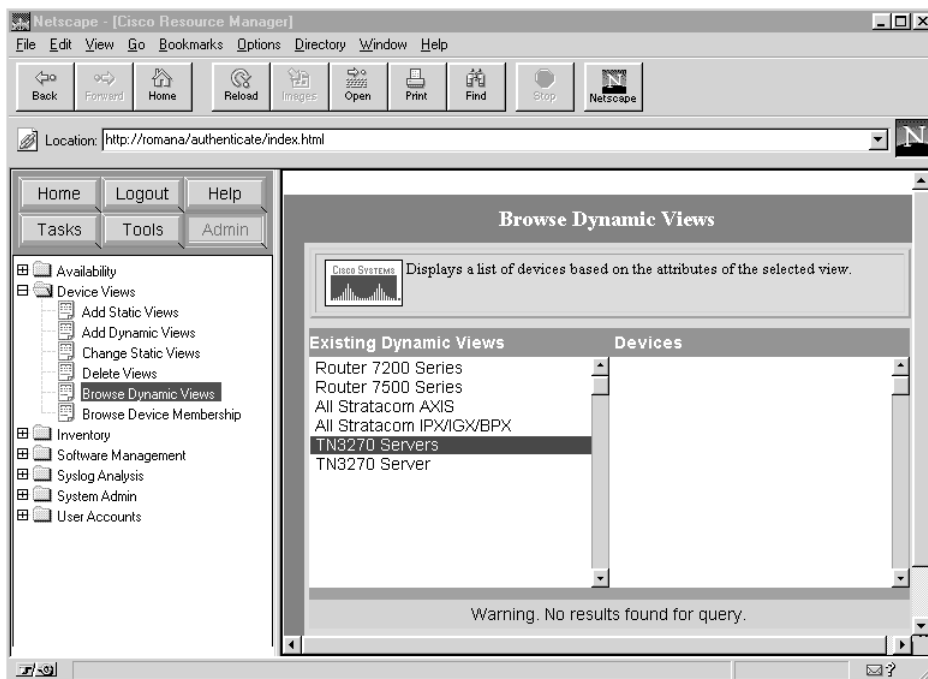


- In the View Name field, enter TN3270 Servers and in the View Description field, enter a brief description of the view.
- Click Finish. This process defines a group of routers entitled TN3270 Servers to the Cisco Resource Manager database.

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.

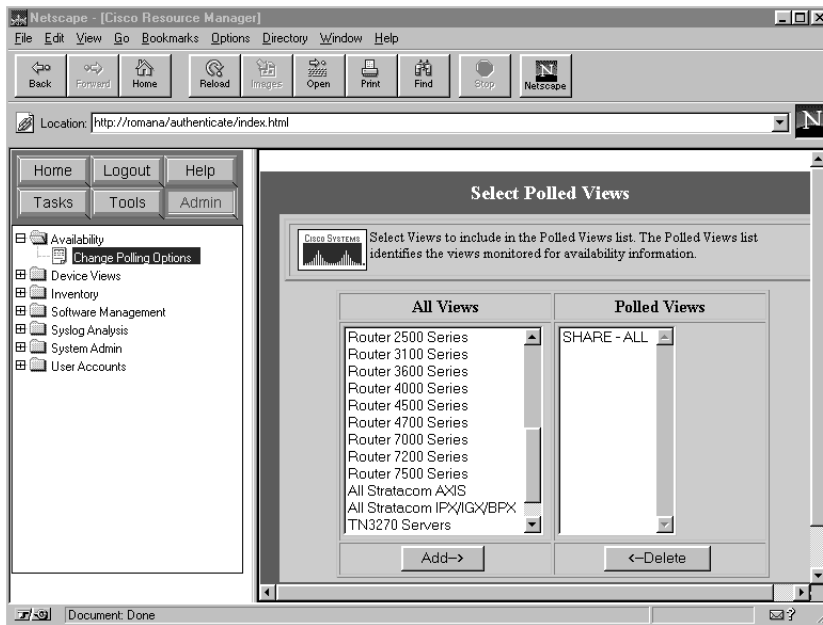
Figure 5-25 Browse Dynamic Views



Step 6. Configure Availability Polling of your routers by doing the following:

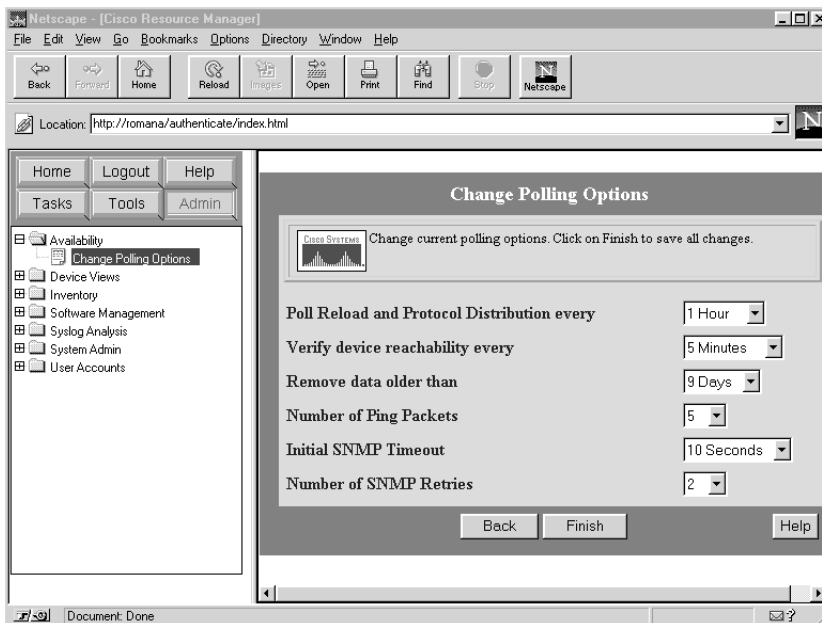
- Click Admin.
- Click the Availability folder.
- Click Change Polling Options. The Select Polled Views window (Figure 5-26) is displayed.

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

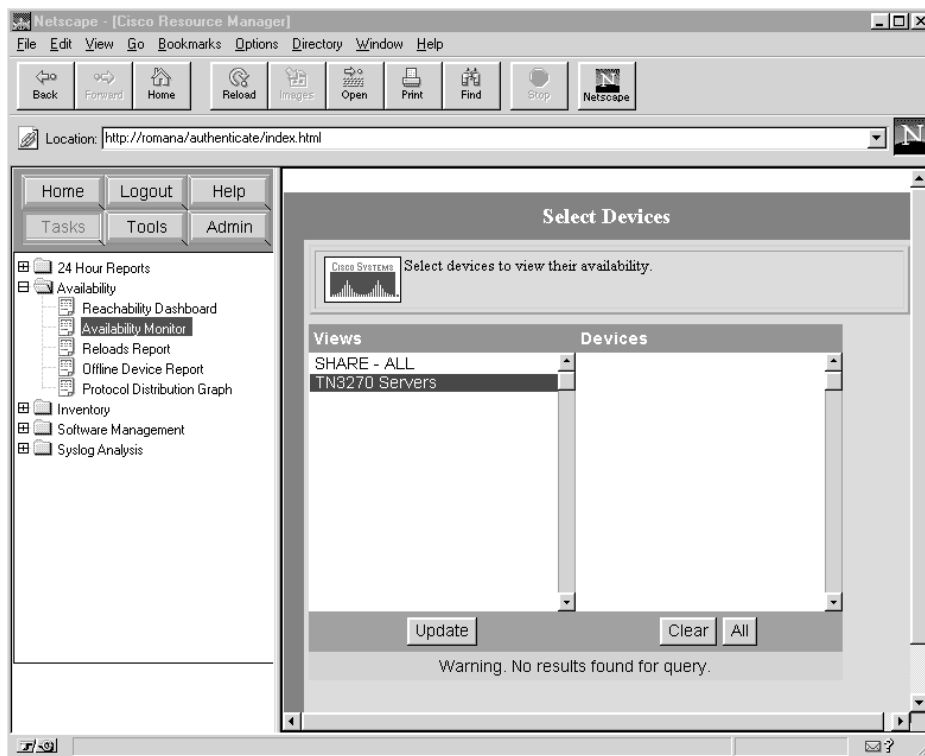
Use the Availability Monitor to continuously check selected devices. You can view device reachability status and response time. Availability Monitor information is updated at half the SNMP polling rate. For example, if your SNMP polling interval is set to 10 minutes, the Availability Monitor is updated 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

Device Name	Last Response	Device Reachability (%)	Response Time (ms)	Interface Status
↘ bottlebrush	Jul 31 1998 09:43:11	0	N/A	Unknown
↗ banksia	Sep 28 1998 15:08:12	100	17	
↗ flametree	Sep 28 1998 15:08:12	100	16	
↗ gumtree	Sep 28 1998 15:08:12	100	15	
↗ ironbark	Sep 28 1998 15:08:12	100	2	
↗ jarrah	Sep 28 1998 15:08:12	100	2	
↗ kangeroopaw	Sep 28 1998 15:08:12	100	11	
↗ karri	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

The screenshot shows a web browser window titled "Interface Details - jarrah" with a menu bar (File, Edit, View, Go, Bookmarks, Options, Directory, Window, Help) and buttons for Back, Close, Save As, and a CSV Format dropdown. The main content is a table with the following data:

Interface	Update Time	Operational Status	Admin Status	Speed (bps)	Physical Address	Network Address
Ethernet0/0/0	Sep 28 1998 15:16:16	down	down	10000000	00:60:3e:27:4e:00	Unknown
Ethernet0/0/1	Sep 28 1998 15:16:16	up	up	10000000	00:60:3e:27:4e:01	172.26.2.52
Ethernet0/0/2	Sep 28 1998 15:16:16	down	up	10000000	00:60:3e:27:4e:02	172.26.50.202
Ethernet0/0/3	Sep 28 1998 15:16:16	down	down	10000000	00:60:3e:27:4e:03	Unknown
TokenRing0/1/0	Sep 28 1998 15:16:16	up	up	16000000	00:06:7c:e4:72:10	172.26.50.1
TokenRing0/1/1	Sep 28 1998 15:16:16	up	up	16000000	00:06:7c:e4:72:90	172.26.50.9
TokenRing0/1/2	Sep 28 1998 15:16:16	down	down	16000000	00:06:7c:e4:72:50	Unknown
TokenRing0/1/3	Sep 28 1998 15:16:16	down	down	16000000	00:06:7c:e4:72:d0	Unknown
Channel3/0	Sep 28 1998 15:16:20	down	up	98304000	Unknown	Unknown
Channel3/2	Sep 28 1998 15:16:20	up	up	98304000	Unknown	Unknown
Loopback0	Sep 28 1998 15:16:20	up	up	4294967295	Unknown	172.26.50.240

Generated: Mon Sep 28 15:17:08 1998
Cisco Systems, Inc. ©
Document: Done

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

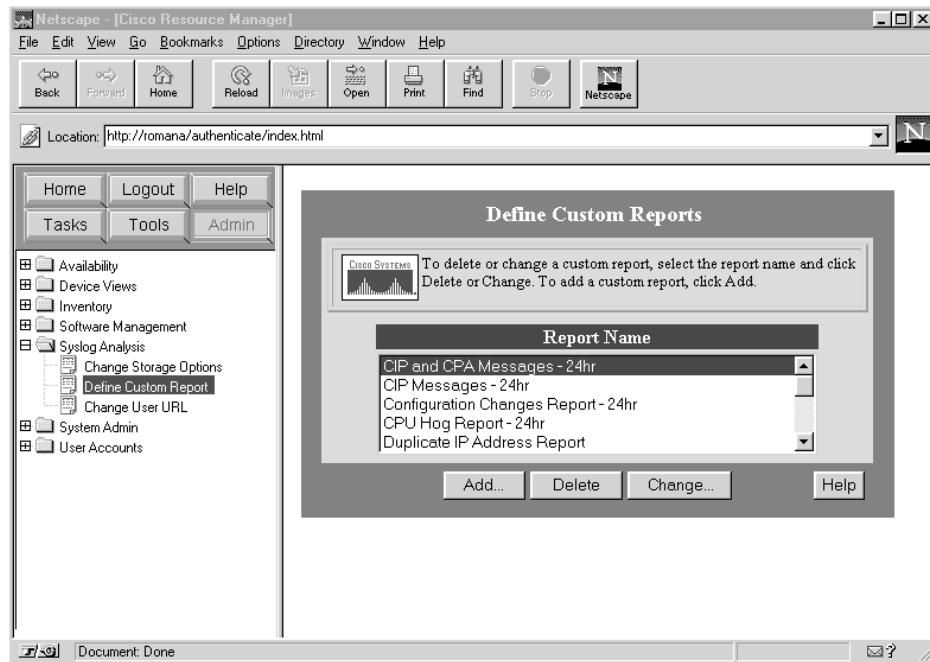
The TN3270 Server identifies error and informational messages using the SYSLOG facility. These messages are the best way for TN3270 Server software to notify the network operator that there is an operational or configuration error. Explanations and recommended corrective actions for all TN3270 Server 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:

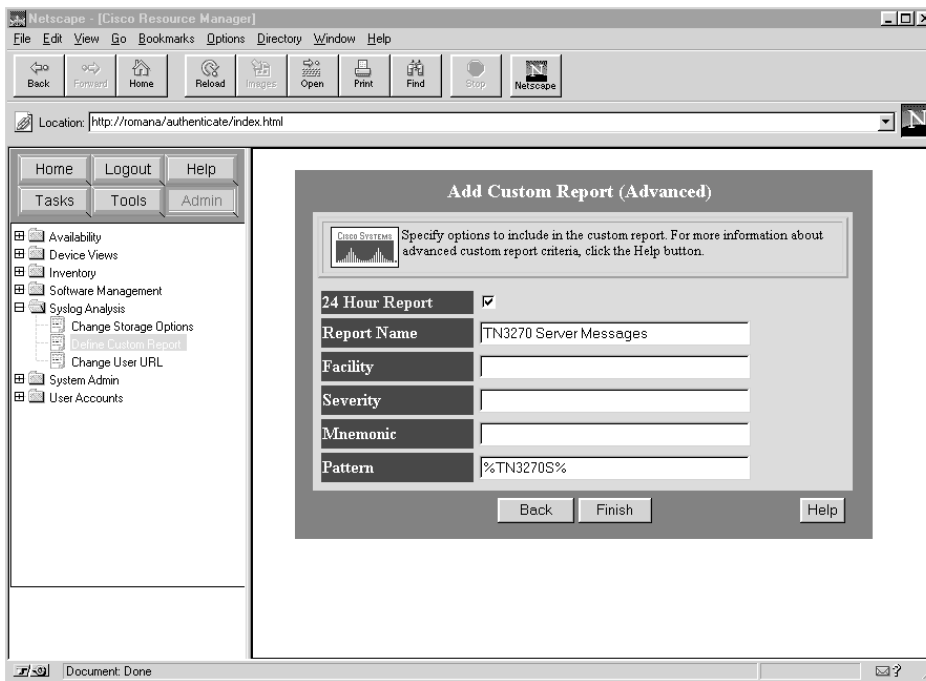
- Step 1. On the Cisco Resource Manager main window, click Admin.
- Step 2. Click the Syslog Analysis folder.
- Step 3. Click Define Custom Report. The Define Custom Reports window (Figure 5-31) is displayed.

Figure 5-31 Define Custom Reports Window



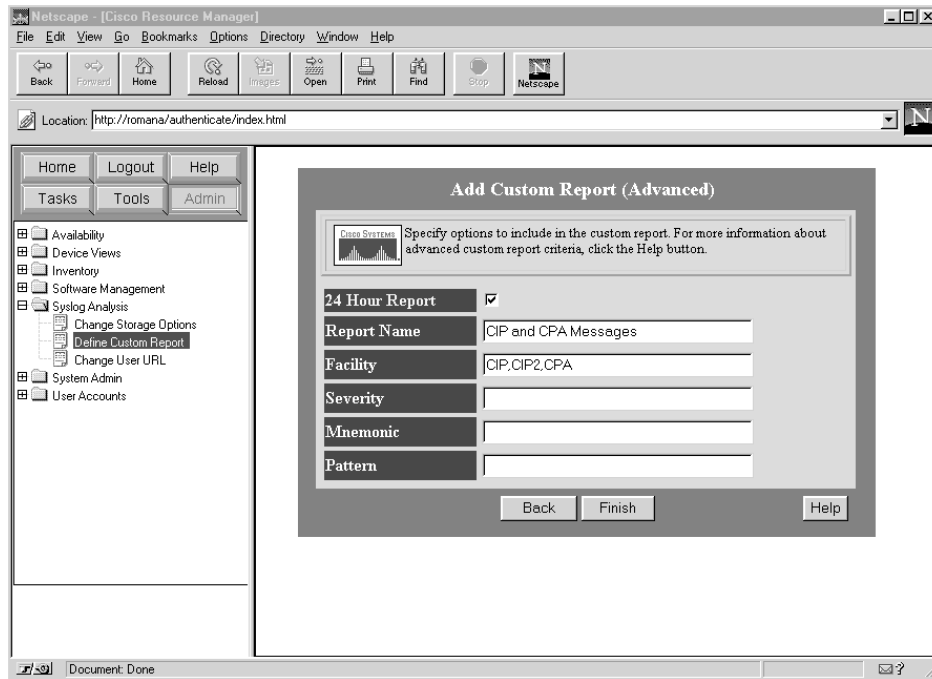
- Step 4. Click Add. The Add Custom Report window is displayed.
- Step 5. Click Advanced. The Add Custom Report (Advanced) window (Figure 5-32) is displayed.

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

Router	Interface	Status	Encaps	Last Change	Previous
CWBC01	CHANNEL3/0	UP		14:31 09/15/98	UNKNOWN
CWBC01	CHANNEL3/1	UP		14:31 09/15/98	UNKNOWN
CWBC01	CHANNEL3/2	UP		14:31 09/15/98	UNKNOWN
CWBC01	CHANNEL4/0	UP		14:31 09/15/98	UNKNOWN
CWBC01	CHANNEL4/1	UP		14:31 09/15/98	UNKNOWN
CWBC01	CHANNEL4/2	UP		14:31 09/15/98	UNKNOWN
CWBC07	CHANNEL3/0	UP		14:32 09/15/98	UNKNOWN
CWBC07	CHANNEL5/0	UP		14:32 09/15/98	UNKNOWN
MHONVPU1	CHANNEL3/0	DOWN		14:34 09/15/98	UNKNOWN
MHONVPU1	CHANNEL3/1	UP		14:34 09/15/98	UNKNOWN
MHONVPU1	CHANNEL3/2	UP		14:34 09/15/98	UNKNOWN
MHONVPU1	CHANNEL3/2.1	UP		16:45 09/15/98	INVALID
MHONVPU1	CHANNEL3/2.10	UP		16:45 09/15/98	INVALID
MHONVPU1	CHANNEL3/2.2	UP		16:45 09/15/98	INVALID
MHONVPU1	CHANNEL3/2.20	UP		16:45 09/15/98	INVALID
MHONVPU1	CHANNEL3/2.5	UP		16:45 09/15/98	INVALID
MHONVPU1	CHANNEL3/2.9	UP		16:45 09/15/98	INVALID
MHONVPU2	CHANNEL5/0	UP		14:34 09/15/98	UNKNOWN

NSPVIDI3 Interfaces Type= C Channel CNM01 09/15/98
 Number of Interfaces: 19 Filter: Target: CNM01 17:12
 ==>
 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.

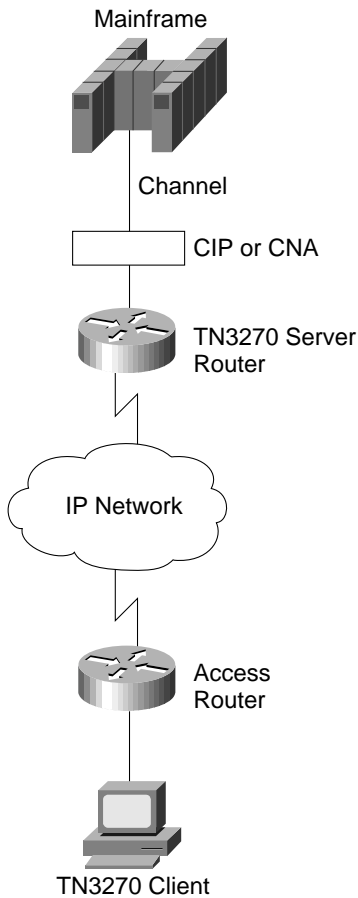
TN3270 Server configuration problems can be diagnosed from ISM using the Router Command Interface panel as described in Viewing TN3270 Server Configuration and Statistics. These commands display overall TN3270 Server configuration parameters, as well as list all defined PUs and LUs.

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:

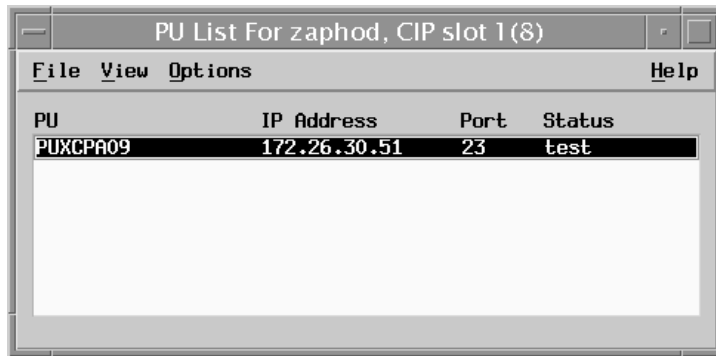
- Mainframe
- Connectivity between the mainframe and the TN3270 Server router
- CMCC (CIP or CPA)
- TN3270 Server software running on the CIP or CPA
- TN3270 Server router
- Connectivity between the TN3270 Server router and the access router, which is the IP network cloud in Figure 5-37
- Connectivity 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).

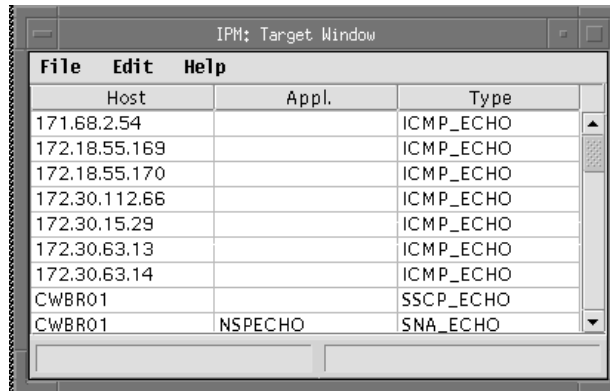
In this section, we assume that you have already defined the router on which the TN3270 Router is running as an IPM Source. For more information about defining IPM sources, see the *CiscoWorks Blue Internetwork Performance Monitor User's Guide*.

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

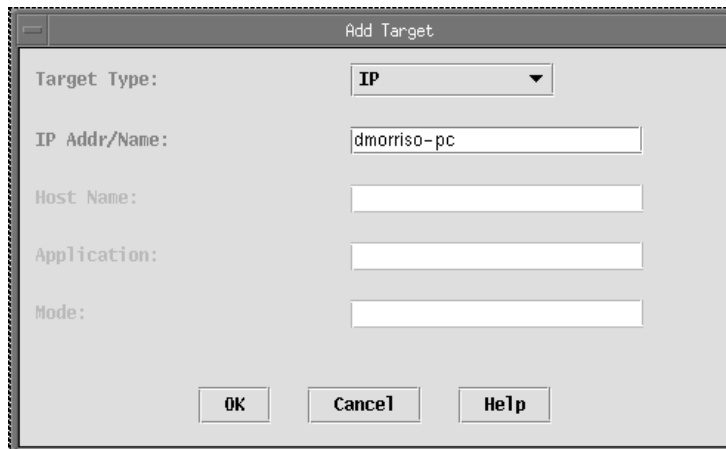


The screenshot shows a window titled "IPM: Target Window" with a menu bar containing "File", "Edit", and "Help". Below the menu bar is a table with three columns: "Host", "Appl.", and "Type". The table contains the following data:

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".

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:

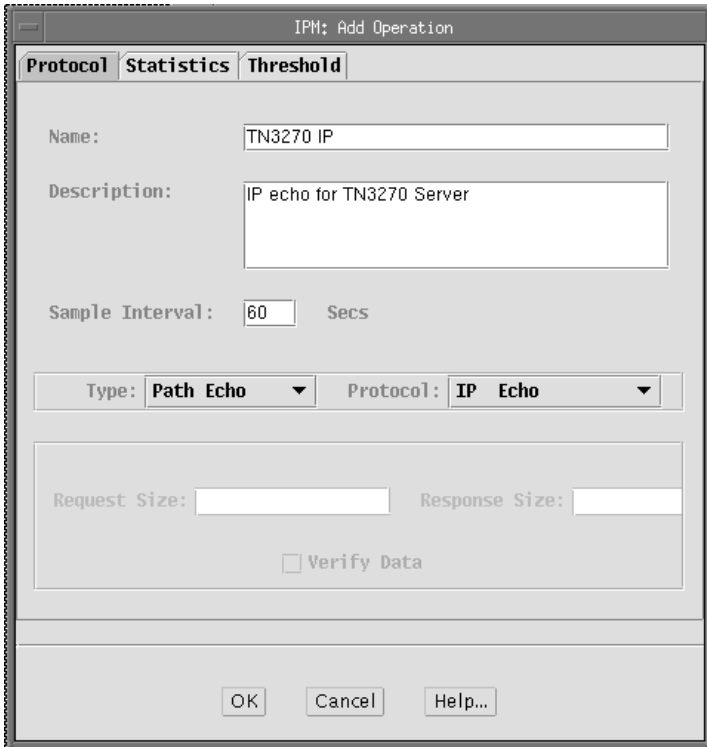
- Target Type—Protocol type to be used with this target. Select SNA SSCP Echo.
- Host Name—Enter the host name defined for the SNA PU connection to VTAM.

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



- 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

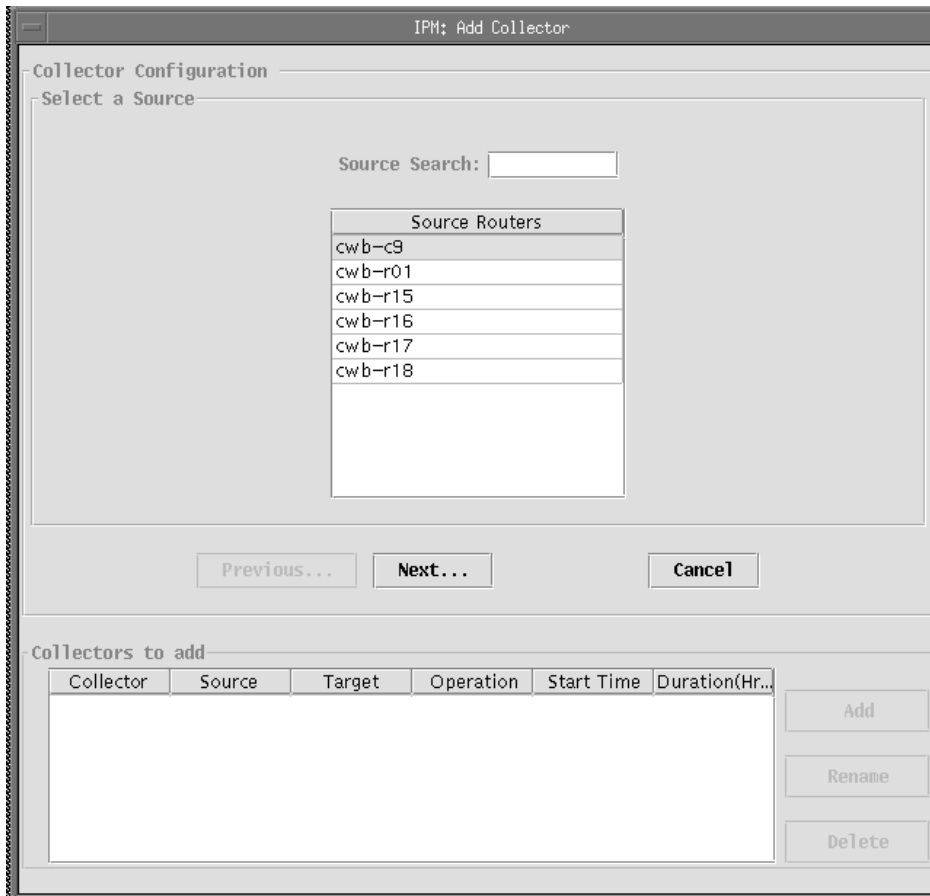
After you configure the IPM SNMP agents, targets, and operations, you can configure a collector, which is a combination of a source, target, and operation. For each collector, you can also specify parameters for gathering statistics, generating event notifications, and scheduling. For more information 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:

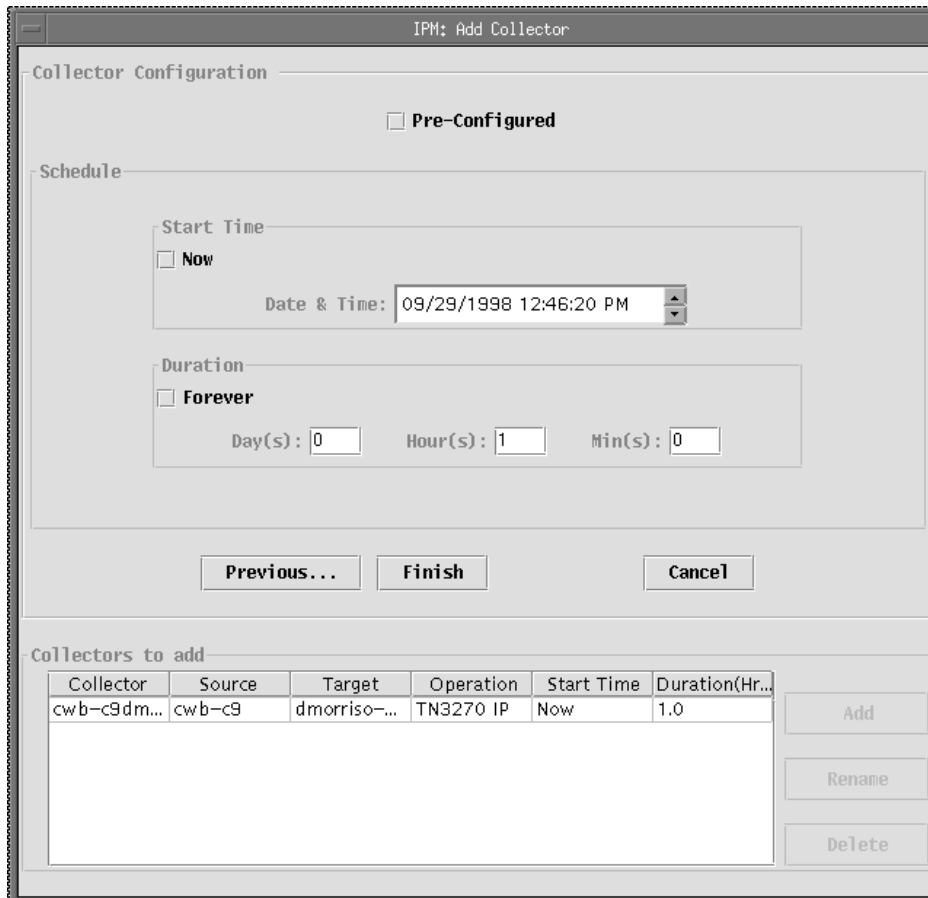
- Step 1. From the Internetwork Performance Monitor main window, select Edit>Add. The IPM: Add Collector window (Figure 5-42) is displayed.

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.

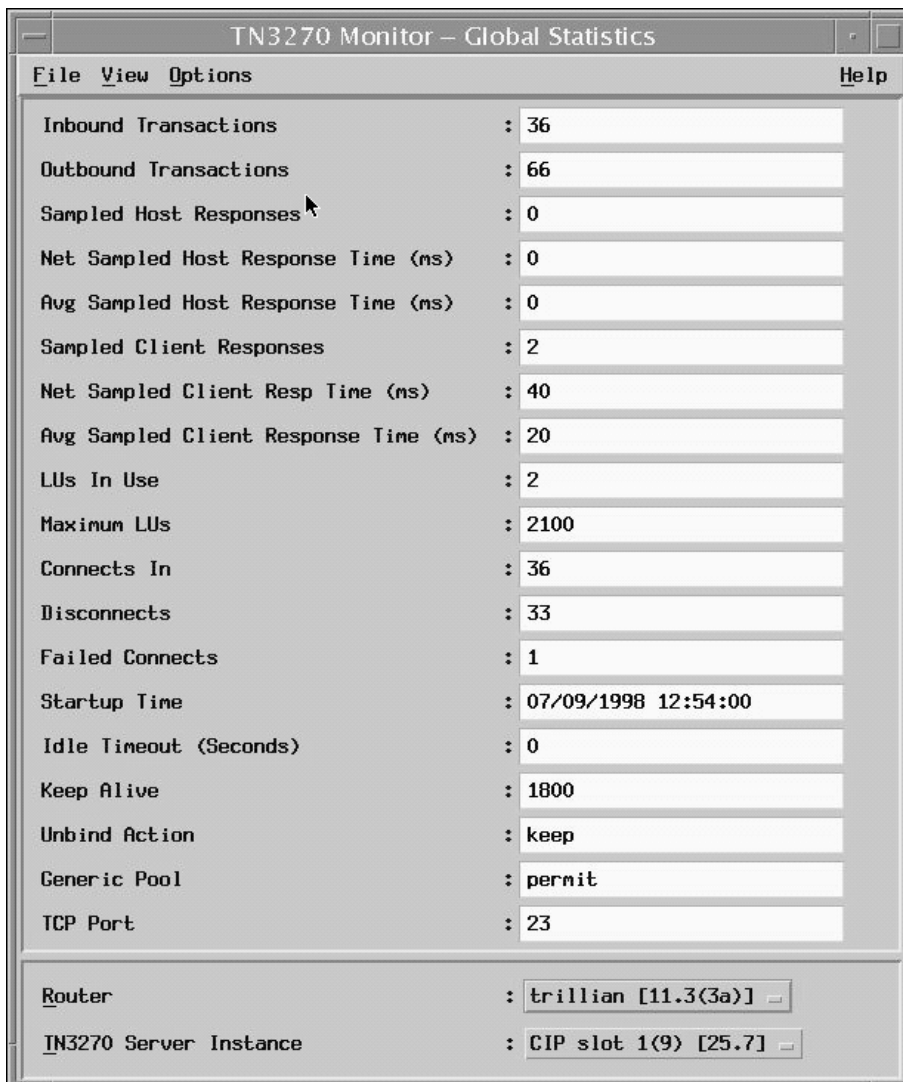
TN3270 Monitor

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



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      NSPMGRT3 - 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  cwbc01      TEST15
CWBC02      PERF    TLE        cwbc02  cwbc02      TEST8
CWBC03      ACTIV
CWBC04      PERF    LT         cwbc04  cwbc04      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.

