

Using CMCC Network Management Tools

This chapter describes the tools available to manage Cisco channel-attached routers, CMCCs, and Cisco router and switch networks used in your data center solutions. It describes the main network management tools and compares these tools to those commonly used to manage an NCP.

This chapter includes the following information:

- CiscoWorks Blue suite of products
- Comparing a channel-attached router equipped with a CIP to an IBM 3745 with the NCP
- Configuring the router for host management

CiscoWorks Blue Suite of Products

CiscoWorks Blue is a suite of network management products that support management of integrated SNA and router networks. The key products in this suite include:

- Internetwork Status Monitor (ISM)
- CiscoWorks Blue SNA View
- CiscoWorks Blue Maps

These tools speed problem identification, simplify problem isolation, and enable trend analysis. The tools simplify event correlation by consolidating the SNA perspective and the router perspective onto a single console of your choice. In addition to these tools, you can use **show** commands to query CMCC traffic statistics, memory utilization, and cycle utilization. A summary of each product follows.

Internetwork Status Monitor

CiscoWorks Blue ISM for the S/390 provides management and visibility of Cisco devices from the mainframe. Cisco has provided mainframe management of routers since 1996. Powerful features, including a new Web interface, support of Simple Network Management Protocol (SNMP), monitoring of Cisco TN3270 Servers, systems management facility (SMF) logging of events and statistics, and several other usability enhancements provide mainframe operators with the full visibility of Cisco routers, switches, interfaces, and CMCCs from a single mainframe console. By enhancing the NetView management platform, ISM leverages investments in mainframe networks and systems management and provides a reliable, scalable solution for managing Cisco devices.

Note: ISM Version 2.0 works only with IBM's Tivoli NetView for OS/390 (NetView). Earlier releases of ISM also worked with Sterling's SOLVE:Netmaster, which is now Computer Associates' NetworkIT NetMaster. This document discusses the functionality of the latest release, ISM Version 2.0. However, much of the information also applies to the earlier releases.

Protecting Your Investment

ISM gives the data center visibility into the Cisco network while protecting investments in mainframe software and management skills. ISM eliminates the need to use TCP/IP on the host for management, as well as the need to purchase UNIX- or Windows-based software for basic router management. Because ISM uses many of the NetView functions to deliver router management, no retraining or SNMP knowledge is required. Familiar operator consoles with common function keys, help panels, event displays, and network logs help traditional MVS network operators ease their way into distributed network management. For enhanced management, ISM provides SNMP capability in addition to the use of RUNCMDs.

Providing Proactive Network Management

ISM logs a variety of key data for historical and trend analysis, allowing network administrators to manage the network with:

- CMCC performance monitoring data
- Router and interface statistics
- Data from monitoring of Cisco routers, switches, TN3270 Servers, and LocalDirector
- Interface load statistics
- Resource and interface performance monitoring data
- Configuration archiving

By collecting performance data from the network and analyzing historical trends, a network manager can often uncover and avoid problems before they occur. Alerts can be created when CPU or memory thresholds are exceeded on routers and CMCCs.

Providing Increased Productivity and High Availability

Quick, efficient problem resolution translates into higher productivity from network operators and higher availability of your network. ISM provides an array of features that enable operators to rapidly identify, diagnose, and correct problems within the network, including:

- Status-at-a-glance displays for Cisco routers, switches, CMCCs, TN3270 Servers, and interfaces
- Detailed status displays for quick problem diagnosis
- Web interface in addition to 3270 displays
- SMF logging of events and statistics
- Correlation of events
- Integrated command menu for most commonly used commands
- Command-line interface (CLI)
- CMCCs and DSPU management functionality
- Resource grouping to easily facilitate operator's span of control
- Device-specific network management vector transports (NMVTs) for managing Cisco routers
- RIF information displays

Enabling Quick Detection and Correction

Using Web browser or traditional 3270 displays, ISM displays a summary screen of all routers being managed via the service point function or SNMP. Routers are color-coded to indicate their status such as up, down, connect, or performance degraded. Using detailed status displays, operators can quickly diagnose problems by displaying flags next to the troubled router, indicating the nature of the problem. Events forwarded to the mainframe by Cisco resources are correlated with the managed routers, allowing operators to easily select the alerts that apply to a particular router.

Integrating with Mainframe Problem Diagnosis

The ISM management software works in conjunction with the service point feature implemented in the Cisco IOS Software or SNMP agent support implemented in a Cisco device. This combination allows native management of the router from mainframe-based applications and generates NMVTs that are specific to resources and downstream devices. The alerts created in this manner are included in Network Problem Determination Aid (NPDA) displays in NetView. The NMVT alerts use standard code points and require no changes to VTAM or NetView. Automated responses to these alerts can be created in the same manner as any other NMVT generic alert. Figure 7-1 shows the ISM Main Menu Panel in a mainframe environment.

Figure 7-1 ISM Main Menu Panel in a Mainframe Environment

```

NSPVMRI4      Internetwork Status Monitor (ISM) V2      CNM56  08/24/00
                                                    16:15
Options      Description
+  SUM      ISM Status Summary
+  ISMR     Resource Manager:
Applications
+  MGR      Resource Status Display
+  INT      Interface Status Display. A=Async B=ISDN C=Channel  Type:
           D=FastEthernet E=Ethernet F=FDXI G=GigaBit H=HSSI I=CLAW
           L=Loopback M=ATM N=MPC S=Serial T=Tokenring U=Tunnel
+  DSPU     DSPU Monitor
+  CMCC     Cisco Mainframe Channel Connection (CMCC) Monitor
+  TN32     Cisco TN3270 Monitoring Operations

+  SNR      Session Monitoring  PU:      MAC:
+  LOG      Activity Log
+  HELP     Command Descriptions.
ISM Last Initialized: 08/24/00 10:58 ISHMGR
NSP1140I Tab to desired selection and press enter.
Action=>
1=HELP 2=MAIN 3=RTN      6=ROLL      8=ADMIN
  
```

Figure 7-2 shows the Web-based ISM Main Screen, which you can access from your Web browser.

Figure 7-2 Web-Based ISM Main Menu Screen



CiscoWorks Blue SNA View

Many organizations are in transition from a native SNA environment (SDLC protocols over slow-speed links or Token Ring) to a mixed SNA/IP environment. Problem determination in this mixed, multiproduct environment can be very difficult with inadequate tools for diagnosis. When an end user calls in with a network problem, it can take a long time to identify the root cause of the problem, which delays resolution.

CiscoWorks Blue SNA View provides an easy-to-use, Web-based interface that takes whatever information an end user can provide and quickly highlights the likely cause of the problem. It integrates with other problem-solving tools such as Tivoli NetView for OS/390, CiscoWorks2000, and Cisco TN3270 Monitor. This integration allows the help desk operator to perform first-level diagnosis on network problems and results in faster problem resolution for your end users.

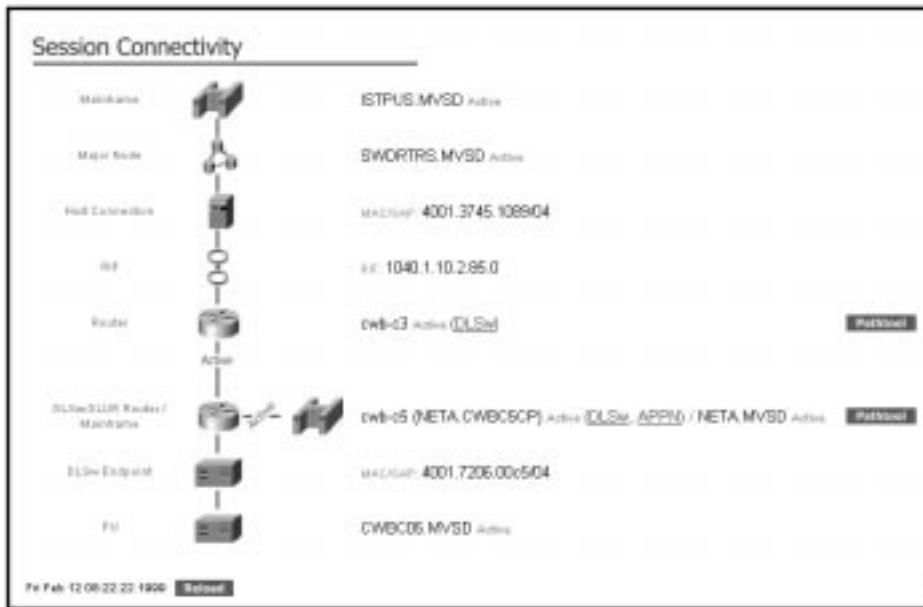
SNA View extends the capabilities of the CiscoWorks Blue family of network management applications to include correlation and control for the integrated SNA and TCP/IP network. By interacting with the mainframe, SNA View collects PU and LU information and correlates it with information gathered from Cisco devices and Cisco TN3270 Servers. The SNA View operator accesses this information by providing filtering criteria. The filtering criteria can include items such as:

- PU or LU name (or wild-card name)
- IP address (or wild-card address)
- MAC address (or wild-card address)
- Status filter
- Protocol filter (APPN, DLSw, TN3270, and RSRB)
- PU 4 name

SNA View searches its database of SNA sessions and provides a list of sessions that match the filter criteria. The operator can select any of these sessions to receive a graphical end-to-end Session Connectivity Display.

The Session Connectivity Display shows each of the devices that participates in the end user's session and provides status information for each of the devices. The operator can select any of the devices in the session and can optionally "hotlink" to other network management tools depending on the type of device. For SNA resources, such as FEPs or links, the operator can hotlink to the HTML version of Tivoli NetView for OS/390. For Cisco devices, the operator can hotlink to CiscoWorks2000 or CiscoView. If the session is using DLSw, APPN, or RSRB protocols, the UNIX operator can hotlink into the Web-based versions of CiscoWorks Blue Maps. If the session is using TN3270, the UNIX operator can access the Cisco TN3270 Monitor application. Figure 7-3 shows an example of a Session Connectivity Display.

Figure 7-3 Session Connectivity Display



CiscoWorks Blue Maps

CiscoWorks Blue Maps monitors the physical and logical relationships between Cisco routers that support SNA protocols. Maps shows you the status of your combined SNA and IP network through the use of UNIX-based topographical maps and Web-based displays. These displays allow your help desk operators and network administrators to immediately identify problems and to begin problem resolution before end users realize that there is a problem. In addition, Maps correlates information gathered from Cisco routers with information gathered from one or more VTAM domains, enabling the management of PU and LU sessions from within the graphical displays.

Network managers need the right tools for the right job, and troubleshooting a problem within DLSw, APPN, or RSRB networks can be a complex task without those tools. First, you would need to identify the connectivity of a PU or LU to the router supporting that device. Then, you would telnet into that router and issue a series of CLI commands in order to display the circuits and sessions that are passing through the router. After that, you would write the results down, or try to remember them as you telnet from the original router to the router at the other end of the connection. After telneting into the peering router, you would need to issue another set of CLI commands (remembering the correct parameters) and process the results of those commands in order to draw a mental map of the connectivity. Finally, when you had determined the correct path for the connectivity of the session, you would gather data for problem resolution, if you could remember the format of the commands and could interpret the results of those commands. This is quite a laborious process.

Cisco has made all of this easier for you with Maps. It simplifies the process of managing DLSw, APPN, and RSRB networks by monitoring the physical and logical relationships between the Cisco and non-Cisco routers that are supporting these SNA protocols. Maps is an easy-to-use, cost-effective solution that automatically discovers the DLSw, APPN, or RSRB routers and uses information in Management Information Bases (MIBs) to draw a topology map of the protocols. This map shows the physical and logical rings that connect the devices, and the routers are color-coded according to the health of the SNA protocol, providing status information at

a glance. Additional information is just a mouse-click away, providing quick access to detailed status of peer connections, traffic statistics, and error statistics. No longer do you need to remember protocol-specific CLI commands or learn MIB values.

Cisco has provided seamless integration of Maps with CiscoView and the Path Tool application, providing the ability to gather detailed information about the health of the device, such as the status of interfaces, ports, and the IP connectivity between resources. Maps goes that extra step by correlating PU and LU information from VTAM to provide end-to-end dependency views, showing how your end user's sessions traverse your IP environment—an essential picture for diagnosing problems.

As network managers are moving rapidly to support Web technologies and Internet standards as the basis for the next generation of enterprise management solutions, Maps has embraced the “management intranet” by providing a Web-based interface. Maps can be integrated into the CiscoWorks2000 framework, providing a “portal” of management applications utilizing the power of Web technologies in solving management problems.

Comparing a Channel-Attached Router Equipped with a CIP to an IBM 3745 with the NCP

This section compares the network management tools that IBM provides for the NCP with those available for a similar CMCC/router configuration. The following functions are examined:

- Alerts
- Statistics
- Console support
- Trace/debug
- Connectivity test
- Memory display/dump
- Recovery
- Performance monitoring
- Configuration management
- Router configuration for host management

Generating Alerts

Both the NCP and the CMCC (via the service point) provide alerts when a resource fails.

Alerts are either generated by or passed through the NCP to VTAM. In VTAM, the alerts are forwarded to NetView. The NCP generates alerts for all the resources it manages and forwards the alerts it receives from an external resource. The NCP does not create traps or support SNMP.

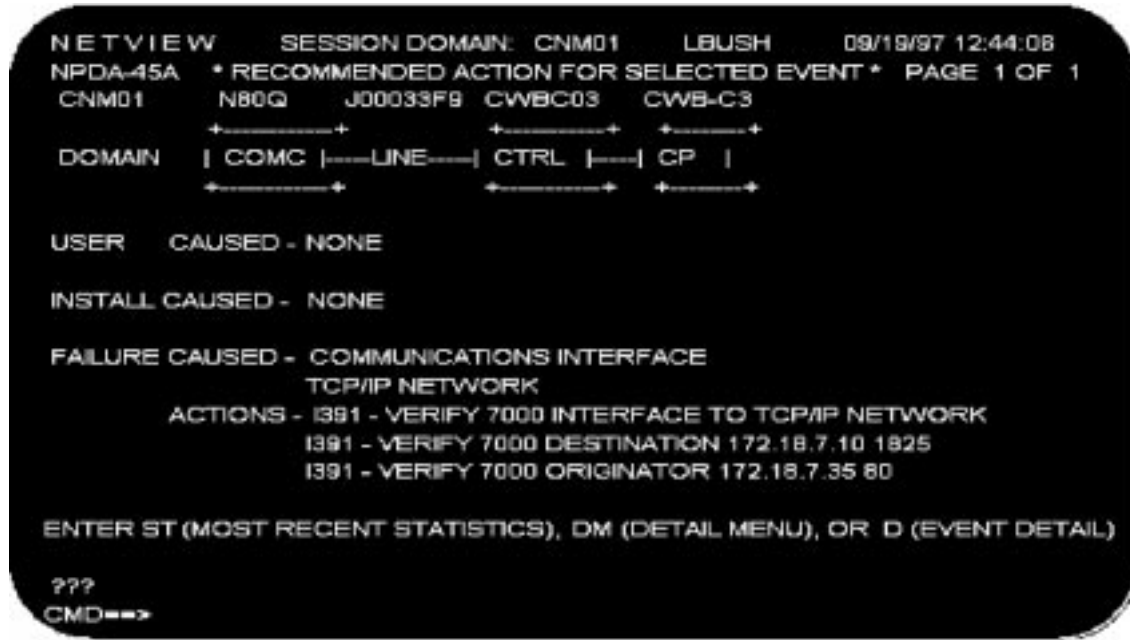
The CMCC/router provides alerts for SNA resources and convert some traps to alerts. It also creates traps for all the alerts. Table 7-1 compares the NCP and CMCC alerts. In the case of switched SNA resources operating on a router SDLC interface, alerts are generated for all SDLC-related errors.

Table 7-1 Comparison of Alert Support for the NCP and the CMCC

Alert Support Comparison	NCP	CMCC
Local Interface Failure	Yes	Yes
Downstream Alerts	Yes	Limited
Resolved Alerts	No	Possible (ISM with Syslog)
Threshold	Slowdown	Possible (ISM)

When VTAM initiates intensive-mode recording (IMR), the NCP can generate alerts for soft errors. Figure 7-4 shows an example of an alert received from a router.

Figure 7-4 NetView Alert Screen



Collecting Statistics

NCP provides statistics for all links, lines, and PUs. NetView has the ability to log the statistics to SMF. NCP provides statistics for the following conditions:

- When the NCP is shut down normally
- When a resource fails or is made inactive
- When a counter that relates to the interface is filled, such as traffic or soft errors

Table 7-2 summarizes the statistical features of the NCP and the CMCC.

Table 7-2 Statistics Summary

Statistics Summary	NCP	CMCC
End of Day (EOD)	Yes	No
Threshold	Yes	No
Solicited	No	Yes (ISM)
Archived	Yes (NPDA)	Yes (ISM)

Figure 7-5 shows an example of a statistical record for an NCP managed resource.

Figure 7-5 Statistical Record for an NCP-Managed Resource

```

NET VIEW      SESSION DOMAIN: CNM01      LBUSH      09/19/97 12:45:06
NPDA-45A * RECOMMENDED ACTION FOR SELECTED EVENT * PAGE 1 OF 1
CNM01      N80Q      L0304      P0304A
           +-----+           +-----+
DOMAIN     | COMC |---LINE---| CTRL |
           +-----+           +-----+

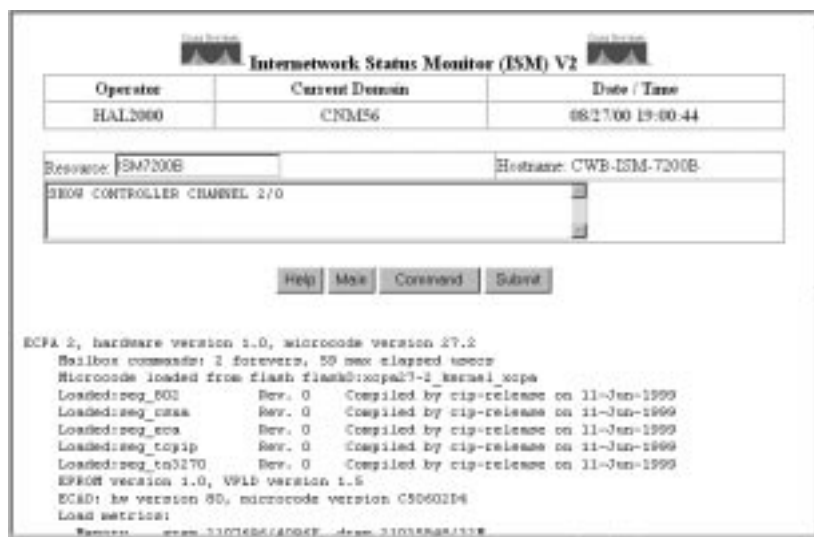
          STAT TOTAL      TOTAL E/T RATIO  TRANSMISSIONS  RECEIVES
DATE/TIME TYPE TRAFFIC  TEMPS  SET  CALC  TRAFFIC  TEMPS  TRAFFIC  TEMPS
05/01 16:48 DACT    6953      1   3.0  0.0   6953      0      0      0

ENTER EV (EVENT)

???
```

ISM can collect statistics based on user-defined intervals. Also, ISM can collect and archive router CPU and memory utilization data. Interface statistics can be collected and archived. ISM monitors the CIP, CPU, and memory, and monitors and archives channel statistics. Figure 7-6 shows an example of records collected for an ISM-managed interface.

Figure 7-6 Web-Based Statistical Record Collected for an ISM-Managed Interface



Providing Console Support

The FEP allows attachment of a console used for service support of the FEP. The console (MOSS) has limited functionality with the FEP and is not supported by NCP. Console users must have technical expertise because the console is primarily used to display and alter storage on the FEP.

The CMCC/router offers various options:

- A terminal can be attached to the router console interface
- A terminal can be attached via a Telnet session
- NetView can be attached as a console when the service point function is implemented in the router

The console support for the router allows operators to perform router functions, as listed in Table 7-3. The MOSS console is usually located next to the FEP, and access to the console is usually restricted. The console support for the router is local or remote and has security features to control access and command level.

Table 7-3 Console Support

Console Support	NCP	CIP/Router
Console	Yes (MOSS)	Yes
Telnet Access	No	Yes
NetView Access	Yes	Yes (RUNCMD)

Providing Trace and Debug Facilities

VTAM provides trace facilities that you can use to trace either the NCP or the CMCC. NCP has a line trace that is initiated from VTAM. The output is sent back to VTAM and recorded using the Generalized Trace Facility (GTF). A VTAM buffer trace is available for any resource that is known to VTAM. Table 7-4 contrasts the trace/debug support of the NCP and CMCC/router.

Table 7-4 Trace/Debug Facilities for the NCP and CMCC/Router

Trace/Debug	NCP	CMCC/Router
Data Trace	Yes (VTAM)	Yes (VTAM)
Line Trace	Yes (VTAM)	No (See debug)
Packet Trace	No	Yes (DEBUG)

The router provides debug facilities that allow detailed problem determination. In most cases, the debug facility requires an authorized operator. Cisco recommends that you perform the trace type of debug operations through a Telnet session rather than across the service point interface.

The Cisco IOS Software provides extensive debug facilities. For more detail, see the documentation under the appropriate Cisco IOS release at www.cisco.com/univercd/cc/td/doc/product/software/index.htm.

Performing Connectivity Tests

The connectivity test allows you to verify a remote connection. In SNA networks, NPDA provides functions that allow you to verify a remote connection. The LPDA function was added to support modems that have the LPDA feature.

The router allows you to ping a remote resource, if it has an IP address. IPM can perform connectivity tests and report exceptions. You can also create connectivity features in ISM that direct specific routers to perform a connectivity test.

Displaying and Dumping Memory

VTAM provides two types of facilities to obtain memory information from the NCP, which are discussed in the following sections.

Displaying Storage Information

Use the following command to obtain storage information from the NCP:

```
DISPLAY NET ,NCPSTOR ,ID=&NCP ,ADDR=&ADR ,LENGTH=&LEN
```

NetView provides a CLIST (NCPSTOR) to simplify the use of this command:

```
NCPSTOR NCP572P ,260
```

The NCP displays the following responses:

```
IST097I NCPSTOR ACCEPTED
IST244I NCP STORAGE FOR ID = NCP572P
IST245I 000260 81C2282F 104828AE 415CF00F 991528B3
IST245I 000270 0108E1F0 80804154 A821D410 25B9F2A0
```

Dumping an Active NCP

Use the following command to dump router memory from the NCP:

```
MODIFY NET ,DUMP ,&OPTIONS
```

NetView provides a CLIST (NCPDUMP) to simplify the use of the command:

```
NCPDUMP NCP1 ,DYNA ,PDS=NCPDUMP
```

Cisco routers can display router memory statistics. For more detail, see the documentation under the appropriate Cisco IOS release at www.cisco.com/univercd/cc/td/doc/product/software/index.htm.

Recovering the Interface

When an NCP fails or an interface on an NCP fails, you must add automation routines to perform the recovery. Without automation routines, the interface remains inactive and the NCP will not try to recover the interface.

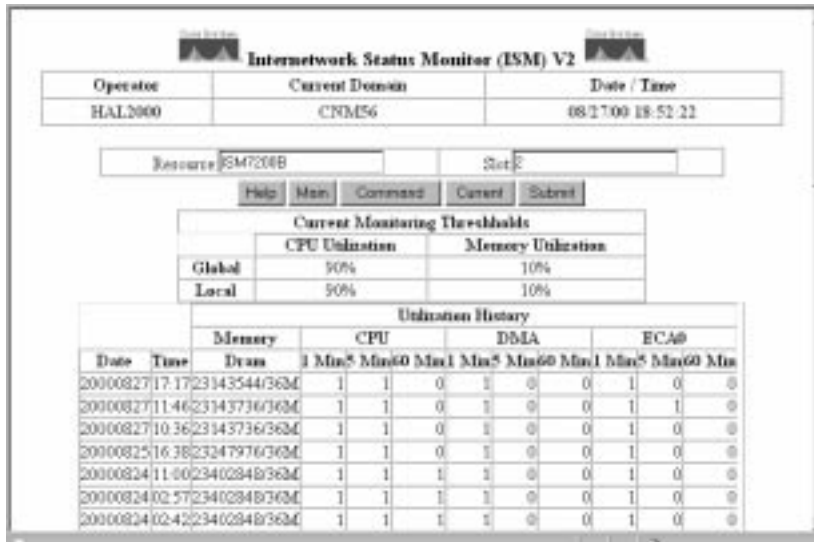
On the Cisco router, interfaces attempt to recover unless they are administratively down. However, you must add automation routines in NetView to recover the channel when the CMCC is reloaded.

Monitoring Performance

Performance monitoring determines whether the performance of the FEP and interface is acceptable. Also, monitoring is performed for planning purposes. In most environments, products such as NETSPY or NPM are used to monitor performance.

With the router, you can use the **show** commands to monitor buffer utilization, memory utilization, or CPU. Figure 7-7 shows an example of router performance data archived by ISM.

Figure 7-7 SM Router CPU/Memory Utilization Data



Configuration Management

Except for dynamically adding lines, and PUs and LUs, NCP configurations must be assembled and loaded to add new features. This compilation is performed at the mainframe. A copy of the source is passed to VTAM so that it knows what has been generated in the NCP.

For the CMCC/router environment, VTAM does not need to know what is configured in the router. However, you must define a TYPE=XCA major node that identifies the channel the CMCC is using. All resources connecting to VTAM via the CMCC must be defined in a TYPE=SWNET. NCPs are loaded via the host channel. Routers are loaded from an FTP server.

ISM allows you to archive the router configuration in the mainframe. ISM also has the capability to discover and monitor all interfaces configured in the router.

Configuring the Router for Host Management

XCA Major Node

```
*DDDLU LUGROUP FOR TN3270
*
*DATE CHANGED   WHO       WHAT
*-----
*****
XCAPUGEN        VBUILD  TYPE=XCA
X31PR04         PORT    MEDIUM=RING, ADAPNO=4, SAPADDR=4, CUADDR=8C0, TIMER=90
X31PR04         PORT    MEDIUM=RING, ADAPNO=4, SAPADDR=4, CUADDR=8C0, TIMER=90, X
                TGP=TRING16M, VNNAME=NETA.CNNNET1, VNGROUP=CNNGRP1
CNNGRP1         GROUP   DIAL=YES, ISTATUS=ACTIVE, ANSWER=ON, CALL=INOUT, X
AUTOGEN=(100,L,P)
GRP390T5        GROUP   DIAL=NO
LN390T5         LINE    USER=SNA, ISTATUS=ACTIVE
P390T5          PU      MACADDR=400170000390, TGN=1, SAPADDR=04, SUBAREA=39, X
                PUTYPE=5, ISTATUS=ACTIVE
```

Switched Major Node Definition

```
*SWDRTRS VBUILD TYPE=SWNET
*****
* SW MAJ NODE FOR LAB AND RUNCMD TESTING OF ROUTERS
*
* LAB TEST ROUTER CWBC01
*
* CWBC01 PU ADDR=01, X
          PUTYPE=2, X
          IDBLK=05D,X
          IDNUM=CC001,X
          DISCNT=(NO), X
          ISTATUS=ACTIVE,X
          MAXDATA=521,X
          IRETRY=YES, X
          MAXOUT=7, X
          PASSLIM=5,X
          MAXPATH=4Router Configuration (Partial)
Building configuration...
Current configuration:
!
version 11.2
service udp-small-servers
service tcp-small-servers
!
hostname cwb-cl
!
boot system flash slot0:c7000-js-mz
boot system mzalocc/c7000-j-mz 171.69.160.22
enable password -- suppressed --
!
microcode CIP flash slot0:cip208-0_kernel_hw4
microcode reload
ip subnet-zero
ip domain-name cisco.com
ip name-server 171.69.160.21
ip name-server 171.68.10.70
ip accounting-list 0.0.0.1 255.255.255.0
source-bridge ring-group 900
source-bridge remote-peer 900 tcp 172.18.9.17
source-bridge remote-peer 900 tcp 172.18.9.145
dlsw local-peer peer-id 172.18.9.161 promiscuous
!
> DSPU is required for focal point connection via the CIP.
dspu rsrp 325 1 900 4000.7000.0001
dspu rsrp enable-host lsap 4
!
dspu host CWBC01 xid-snd 05dcc001 rmac 4000.3333.4444 rsap 4 lsap 4 focalpoint
!
dspu rsrp start CWBC01
!
interface Tunnel0
no ip address
!
interface Ethernet1/0
no ip address
shutdown
no mop enabled
!
```



```
interface Ethernet1/1
description ethernet to hub 2
no ip address
shutdown
no mop ena
bled
!
interface Ethernet1/2
no ip address
shutdown
no mop enabled
!
interface Ethernet1/3
no ip address
ip accounting output-packets
ip accounting access-violations
shutdown
> Listing terminated
```

