Cisco Reader Comment Card

General Information

1 Years of networking experience _____ Years of experience with Cisco products _____

2 I have these network types: ☐ LAN ☐ Backbone ☐ WAN
☐ Other: _____

3 I have these Cisco products: ☐ Switches ☐ Routers
☐ Other: Specify model(s) _____

4 I perform these types of tasks: ☐ H/W Install and/or Maintenance ☐ S/W Config
☐ Network Management ☐ Other: _____

5 I use these types of documentation: ☐ H/W Install ☐ H/W Config ☐ S/W Config
☐ Command Reference ☐ Quick Reference ☐ Release Notes ☐ Online Help
☐ Other: _____

6 I access this information through: ____% Cisco Connection Online (CCO) ____% CD-ROM
____% Printed docs ____% Other: _____

7 Which method do you prefer? _____

8 I use the following three product features the most:

Document Information

Document Title: CiscoWorks Blue Internetwork Status Monitor Installation Guide

Part Number: S/W Release (if applicable): Version 2

On a scale of 1–5 (5 being the best) please let us know how we rate in the following areas:

_____ The document was written at my technical level of understanding.
_____ The information was accurate.
_____ The document was complete.
_____ The information I wanted was easy to find.
_____ The information was well organized.
_____ The information I found was useful to my job.

Please comment on our lowest score(s):

Mailing Information

Company Name Date

Contact Name Job Title

Mailing Address

City State/Province ZIP/Postal Code

Country Phone ( ) Extension

Fax ( ) E-mail

Can we contact you further concerning our documentation? ☐ Yes ☐ No

You can also send us your comments by e-mail to **bug-doc@cisco.com**, or fax your comments to us at **(408) 527-8089**.

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 4631 SAN JOSE CA

POSTAGE WILL BE PAID BY ADDRESSEE

ATTN DOCUMENT RESOURCE CONNECTION
CISCO SYSTEMS INC
170 WEST TASMAN DRIVE
SAN JOSE CA 95134-9883

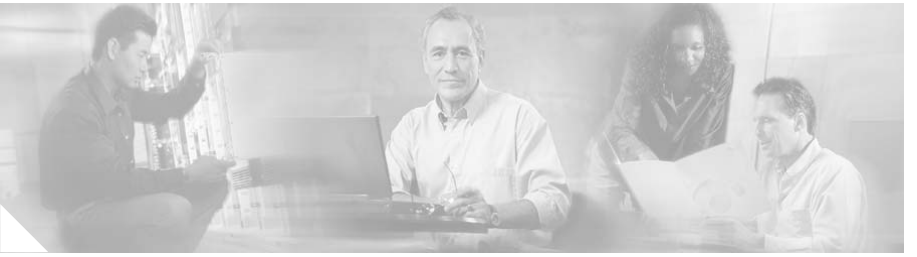
Cisco Systems

CiscoWorks Blue
Internetwork Status Monitor

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

CiscoWorks Blue Internetwork Status Monitor Installation Guide

CONTENTS



About This Guide

This chapter provides information on the following topics:

Document Objectives

This guide describes the tasks and commands necessary to install and configure the CiscoWorks Blue Internetwork Status Monitor (ISM) product.

Audience

This guide is intended for network engineers and Multiple Virtual Storage (MVS) system programmers who are responsible for installing and configuring Cisco resources in a Systems Network Architecture (SNA) environment.

This guide assumes that you are familiar with the basic concepts and terminology used in internetworking and that you understand the network topology and protocols. This guide assumes that a network engineer will install and configure the Cisco resources for use with ISM, and that an MVS system programmer will install and configure ISM on the mainframe.

Document Organization

This guide is divided into the following chapters:

- Chapter 1, “Preparing to Install ISM,” provides introductory information about installing ISM including who should perform the installation, an overview of the installation tasks and system requirements.
- Chapter 2, “Configuring the Mainframe-to-Router Link,” describes the tasks for MVS system programmers and network engineers to properly configure the connection between the mainframe and resources.
- Chapter 3, “Installing ISM,”provides detailed instructions for installing and verifying the installation of ISM on the mainframe.
- Chapter 4, “Migrating from a Prior Release of ISM,” describes the process of moving from the previous release of ISM to the current ISM release. It discusses the benefits of migrating to the most current version, how the ISM data is handled, and how to convert some of your existing ISM configuration and resource data for use in ISM V2.
- Chapter 5, “Configuring ISM,”describes how to start and configure the ISM program for the first time. It provides instructions on enabling the ISM management environment and defining user profiles.
- Chapter 6, “Uninstalling ISM V1R3.0,” describes how to remove ISM V1R3.0 from the mainframe after you have migrated to and tested ISM V2.
- Chapter 6, “Troubleshooting,” describes methods to diagnose mainframe-to-resource link configuration problems and problems discovered during the installation as well as verification of the ISM software.

Document Conventions

The terms *resource* and *router* are used throughout this documentation. To avoid confusion, be aware that all routers are resources, therefore the term *resource* encompasses *router*—whereas the term *router* is specific.

This guide uses basic conventions to represent text and table information.

Command descriptions in this guide use the following conventions:

- Commands and keywords are in **boldface** font.
- Arguments for which you supply values are in *italic* font.
- Elements in square brackets ([ ]) are optional.
- Alternative, but required, keywords are grouped in braces ({ }) and separated by a vertical bar (|).

Examples use the following conventions:

- Terminal sessions and information the system displays are printed in `screen` font.
- Information you enter is in **`boldface screen`** font.
- Variables you enter are printed in *`italic screen`* font
- In examples, an exclamation point (!) at the beginning of a line in a resource configuration indicates a comment line.

In addition, this guide uses the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

Caution Means *reader be careful*. You are capable of doing something that might result in equipment damage or loss of data.

Tip Means *the following are useful tips*.

Related Documentation

For more information about CiscoWorks Blue ISM, refer to the following Cisco publications:

- *CiscoWorks Blue Internetwork Status Monitor User Guide*
- *CiscoWorks Blue Internetwork Status Monitor Data Areas*
- CiscoWorks Blue Internetwork Status Monitor Online Help

For additional information, refer to the following Cisco publications:

- Configuration guides and command references for Cisco router products used at your site
- *Cisco IOS Bridging and IBM Networking Configuration Guide*
- *Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2* and *Volume 2 of 2*
- *Cisco IOS Command Summary*
- *Cisco IOS System Error Messages*
- *Internetworking Terms and Acronyms*

For more information about using IBM's NetView, you can refer to the following NetView publications:

- *NetView Operation*
- *Learning About NetView Operation*
- *NetView Command Summary*

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

The most current Cisco documentation is available on the World Wide Web at the following website:

http://www.cisco.com

Translated documentation is available at the following website:

http://www.cisco.com/public/countries_languages.html

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

Cisco documentation can be ordered in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

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

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

You can access CCO in the following ways:

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

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

Preparing to Install ISM

CiscoWorks Blue Internetwork Status Monitor (ISM) for NetView is a program that runs on a Multiple Virtual Storage (MVS) mainframe using NetView, IBM's network management platform, and manages Cisco routers. ISM bridges the worlds of mainframe network management and management of distributed routers in LAN and WAN topologies.

This chapter provides the following information to help you prepare to install ISM:

Planning Who Should Install ISM

Installing ISM requires that you perform tasks for configuration of the mainframe and router sides of the network environment, in addition to actually installing and enabling the ISM software on the mainframe.

Often in the mixed network environment of mainframes and LANs, an MVS system programmer installs and maintains the mainframe side of the network, while a network engineer manages the routers on the LAN side of the network. In such an environment, the successful installation and operation of ISM requires the close coordination between these job functions at a customer site.

Readers who perform the following job functions are the target audience for this installation guide:

- The MVS or Virtual Telecommunications Access Method (VTAM) system programmer responsible for installing and configuring ISM on the mainframe system.

  ISM works in the VTAM and NetView communications environment. Because the mainframe installation tasks for ISM involve VTAM and NetView integration, a VTAM system programmer installs ISM. However, any MVS system programmer can perform the tasks in coordination with the site's VTAM system programmer.
- The network engineer responsible for installing and configuring the routers to be managed by ISM.

Overview of the Installation Tasks

ISM installation is accomplished in four stages as reflected by the following chapters:

- Configuring the Mainframe-to-Router Link
- Installing ISM
- Migrating from a Prior Release of ISM
- Configuring ISM

Each stage ends with verification of successful completion in order to isolate and troubleshoot problems immediately, if they occur.

This section summarizes the installation tasks. Detailed instructions are provided in subsequent chapters. Use the following list to ensure you perform all the ISM installation steps applicable to your site's environment.

Note Be sure that the mainframe and routers meet the minimum hardware and software requirements to install and operate ISM. See the "System Requirements" section on page 1-4.

Enabling ISM to Monitor Routers

The tasks in this section are the only ones that require the involvement of network engineers responsible for configuring the router. For detailed instructions, see Chapter 2, "Configuring the Mainframe-to-Router Link."

Step 1 Configure a VTAM physical unit (PU) to support the Service Point (SP) for each router to manage using ISM.

Step 2 Configure each router to support the SNA SP you defined in VTAM.

Step 3 Verify that the routers can connect to VTAM and can communicate with NetView using RUNCMDs.

Verifying the NetView Environment

Step 1 Verify the timeout value for RUNCMDs to ensure that the values of the costime and max reply options are set correctly in NetView to support the ISM autotasks.

Step 2 Verify whether NetView supports RUNCMDs to ensure proper configuration of the NetView VTAM definition for LU 6.2 support.

Step 3 Verify the router's mainframe connection.

Step 4 Verify the router connection from NetView to ensure that network devices are configured properly and that the router can attach to the network.

Step 5 Verify the router connection from VTAM to ensure that the router is communicating with the mainframe from VTAM.

Installing ISM

Step 1 Load the ISM software onto the mainframe using either the direct or System Modification Program Extended (SMP/E) installation methods.

Step 2 Update SYS1.PARMLIB to authorize the ISM load library.

Step 3 Update the members of the NetView DSIPARM data set.

Step 4 Install the VTAM XID Configuration Services exit routine.

Step 5 Verify the ISM software installation so ISM can communicate with NetView.

Configuring ISM

Step 1 Configure the ISM management environment.

Step 2 Define the ISM user profiles.

System Requirements

This release of ISM requires the components described below for both the mainframe and router environments. Be sure to note the Cisco IOS software levels required in your routers for the type of router management you want to support.

Mainframe Hardware Requirements

The following hardware is required to install the ISM program on the mainframe:

- Direct access storage in the following amounts, according to the ISM installation method that you select:
  - For the direct installation method, approximately 50 megabytes.
  - For the SMP/E installation method, approximately 70 megabytes.

Note For detailed information about the allocation of storage for the ISM installation files, see Chapter 3, “Installing ISM.”

Mainframe Software Requirements

The following operating system and application software is required to install the ISM program on the mainframe:

- OS/390-MVS mainframe running MVS/ESA Version 4.1 or later, OS/390, or z/OS
- SMP/E Release 7 or later (required for SMP/E installation method only)
- TME/10 NetView for OS/390 (Version 1.2 or later)
- VTAM Version 4.1 or later for support of ISM's SNA Session Monitoring application
- Any version of VTAM for support of the other ISM applications

Cisco IOS Software Requirements

Your routers must meet the following Cisco IOS software levels for the type of router management that you want to support in ISM:

- For Remote Source-Router Bridging (RSRB) support, Cisco IOS Release 11.0 or later
- For data-link switching (DLSw+) support, Cisco IOS Release 11.1 or later
- For Cisco mainframe channel connection (CMCC) routing information field (RIF) support, Cisco IOS Release 11.3 or later

Planning the ISM Installation

Before you install the ISM software, complete the following planning tasks:

- Choose the direct or SMP/E method of installing ISM software. The method you choose changes the storage requirements for the installation.
- Review the "Verifying the ISM DASD Storage Requirements" section on page 1-6 to select the appropriate direct access storage device (DASD) locations to accommodate the ISM installation and production files.
- Determine the volume serial numbers of the DASD to use for your ISM installation and production files.

- Determine the high-level qualifier (or prefix) you will use to identify your ISM data sets.

Verifying the ISM DASD Storage Requirements

The following sections will help you determine the amount of ISM DASD storage required for your site's ISM installation:

Installation Storage Requirements

The amount of storage that ISM requires for the installation data sets varies based on the method you use to install the software. The DASD storage requirements for the target libraries shown in Table 1-1, apply to both the direct method and SMP/E method of installation.

Table 1-1 lists the data set name and provides a brief description, along with the minimum storage requirements for the ISM installation target libraries.

Note Through the remainder of this chapter, the file specifications use the variable *prefix* to represent the high-level file qualifier. When you run the jobs in the sample members of the installation data sets, change the occurrences of *prefix* to the high-level qualifier selected for ISM.

Table 1-1 DASD Storage Requirements for Target Libraries

Data Set Name	Description	Space
prefix. NSPI202.NSPNINST	Installation jobs	1 MB
prefix. NSPI202.NSPNLOAD	Load library; command modules and exits	1 MB

Table 1-1 DASD Storage Requirements for Target Libraries (continued)

Data Set Name	Description	Space
prefix. NSPI202.NSPNCLST	CLIST and REXX routines	15 MBs
prefix. NSPI202.NSPNHTML	HTML routines	6 MBs
prefix .NSPI202.NSPNPANL	Presentation panels	4 MBs
prefix .NSPI202.NSPNSAMP	Sample installation and customization procedures	2 MBs

Additional SMP/E Installation Storage Requirements

In addition to the storage requirements for the target libraries, the SMP/E method requires at least 20 additional megabytes for the distribution libraries.

Table 1-2 lists the data set name, a brief description of each data set, and the minimum storage required for the ISM installation distribution libraries when you use SMP/E to install the software.

Table 1-2 DASD Storage Requirements for SMP/E Distribution Libraries

Data Set Name	Description	Storage
prefix. NSPI202.NSPNINST	Installation jobs	1 MB
prefix. NSPI202.ANSPNLOA	Load library; command modules and exits	1 MB
prefix. NSPI202.ANSPNCLS	CLIST and REXX routines	15 MB
prefix. NSPI202.ANSPNHTM	HTML routines	6 MB

Table 1-2 DASD Storage Requirements for SMP/E Distribution Libraries

Data Set Name	Description	Storage
prefix. NSPI202.ANSPNPAN	Presentation panels	4 MB
prefix. NSPI202.ANSPNSAM	Sample installation and customization procedures	2 MB

Production Storage Requirements

Table 1-3 lists the recommended storage requirements for the ISM production members for NetView. The production storage requirements apply to both the direct and SMP/E installation methods.

Table 1-3 ISM Storage Requirements

Name	Storage
NETVIEW.USER.DSICLD (NSPNCLST or ANSPNCLS)	15 MB
NETVIEW.USER.DSICLD (NSPNHTML or ANSPNHTM)	6 MB
NETVIEW.USER.LOADLIB (NSPNLOAD or ANSPNLOA)	1 MB
NETVIEW.USER.CNMPNL1 (NSPNPNLS or ANSPNPAN)	4 MB
NETVIEW.USER.DSIPARM (ISMTBL, ISMDMN, ISMCMD, and ISMOPF)	1 MB

VSAM Storage Requirements

Table 1-4 lists the initial VSAM storage allocations for the data sets that ISM uses. The maximum storage required depends on the number of routers and interfaces monitored and on the ISM functions enabled. Some of the data sets are optional depending on the ISM functions you plan to implement at your site.

The first four required data sets may use 12 MBs of storage. Full implementation of the ISM functions and their corresponding data sets allocates additional storage of 30 MBs.

The VSAM storage requirements in Table 1-4 apply to both the direct and SMP/E installation methods.

Table 1-4 VSAM Storage Requirements

Data Set Name	Description	Storage
prefix. ISMDSA	ISM management data	5 MBs
prefix. ISMDSH	Router and Cisco mainframe channel connection archive data	5 MBs
prefix. ISMDSM	Primary event log data	1 MB
prefix. ISMDSN	Alternate event log data	1 MB
		Total: **12 MBs**
Optional Data Sets		
prefix. ISMDSI	Interface statistics and performance data	5 MBs
prefix. ISMDSC	Router configuration data	5 MBs
prefix. ISMDSR	SNA session data	10 MBs
prefix. ISMDSD	Router memory dump data	5 MBs
prefix. ISMDSW	SNASw statistics and performance data	5 MBs
		Total: **30 MBs**

VSAM Record Requirements for ISM Configuration

Table 1-5 lists the number of VSAM records required for ISM configuration. Use this information to evaluate the size of the VSAM data sets for your site's installation.

Table 1-5 VSAM Record Requirements for ISM Configuration

Record Name	Number of Records
Setup definition	2
Router management	2 per router
Interface management	1 per interface
Operator security	1 per operator
DSPU management	1 per VTAM DSPU
Router statistics	1 header record plus wrap count per router
Interface statistics	1 header record plus wrap count per interface
Interface performance	1 header record plus wrap count per interface
RIF history	1 header record plus wrap count per PU
Router configuration	1 header record plus 1 record per configuration statement
SNASw configuration	1 per SNASw instance
Cisco mainframe channel connection management	1 per Cisco mainframe channel connection
Cisco TN3270 Statistics	1 header record plus wrap count per interface
CMCC statistics	1 header plus wrap count
TN3270 statistics	1 header plus wrap count

ISM Installation File Contents

Table 1-6 describes the format of the files after you receive them from the CCO site.

Table 1-6 ISM Zip File Contents

Name	Record Format	Logical Record Length	Block Size	Distribution Library
NSPI202.SMPMCS.XMIT	FB	80	3120	
NSPI202.F1.XMIT	FB	80	3120	JCLIN
NSPI202.F2.XMIT	U	0	6144	ANSPNLOAD
NSPI202.F3.XMIT	FB	80	3120	ANSPNSAMP
NSPI202.F4.XMIT	FB	80	3120	ANSPNCLST
NSPI202.F5.XMIT	FB	80	3120	ANSPNPANL
NSPI202.F6.XMIT	FB	80	3120	ANSPNHTML
NSPI202.NSPNINST.XMIT	FB	80	3120	ANSPNINST

Getting Started

The installation steps that you perform depend, in part, upon your site's environment and how you plan install this release of ISM.

If your site currently has ISM V1R3.0 installed, read the following chapters:

- Chapter 3, "Installing ISM"
- Chapter 4, "Migrating from a Prior Release of ISM"
- Chapter 5, "Configuring ISM"

If your site does not have any version of ISM installed, read the following chapters:

- Chapter 2, "Configuring the Mainframe-to-Router Link"
- Chapter 3, "Installing ISM"
- Chapter 5, "Configuring ISM"

Configuring the Mainframe-to-Router Link

Before you can use ISM to manage routers on your network, a link must be established between the mainframe and the router for communication. To establish this link, you need to configure both the mainframe and the router sides of the network. Configuring the mainframe-to-router link involves the following tasks:

- Defining a VTAM PU for each router on the mainframe
- Configuring SNA Service Point support on the router

This chapter provides detailed instructions for enabling the link between the mainframe host and a router. This chapter discusses the following topics:

Coordinating the ISM Installation

This chapter explains how to configure the network devices for use with ISM, and how the router configuration correlates to the VTAM PU definition on the mainframe.

To ensure successful configuration of the mainframe-to-router link, the network engineer should coordinate setup of the router configuration with the MVS system programmer responsible for configuring the router's VTAM connection on the mainframe.

For the Network Engineer

This section describes installation information relevant to the network engineer.

- If you have already configured SNA service point support on your routers for ISM V1R3.0, then you do not need to perform any additional configuration on the router.
- If you are installing ISM at your site for the first time, be sure to read the "Preparing to Install ISM" chapter before proceeding.

For the MVS System Programmer

This section describes installation information relevant to the MVS system programmer.

- If you have ISM V1R3.0 installed and are adding new routers to the network, you must define a PU in VTAM. If you do not need to add new routers, skip this chapter, and read Chapter 3, "Installing ISM."
- If you are installing ISM for the first time, you must configure VTAM to define a PU for each router you will be managing from ISM. This step can be performed before you install ISM, to verify that the proper mainframe connections to the router are established.

Configuring a VTAM Connection

Before you can use ISM to view and manage a Cisco router from your NetView console, the router must be connected to the VTAM host through a systems services control point-to-physical unit (SSCP-to-PU) session. This connection is established by defining a PU for each router in the VTAM configuration file.

To define a PU, add the following lines to the VTAM configuration file for each router, and specify the values for the *SERVICE_POINT_NAME*, *idblock number*, and *id number* arguments for each router. These arguments must correspond to the values specified in the configuration of the router.

Note Dynamic PU allocation is not supported by ISM.

Table 2-1 defines each of the VTAM arguments. For information about how these arguments correspond to the router configuration, see "Correlating the Router and VTAM Configuration Information" section on page 2-9.

The PU type, ID block, and ID number arguments are the most important arguments in the sample VTAM definition. The other arguments are given as an example only, and are not required.

Table 2-1 VTAM Configuration File Arguments

Argument	Description
SERVICE_POINT_NAME	Service point name of the router (1 to 8 characters).
idblock number	Identification number sent to the host when a connection is being established. The *idblock number* corresponds to the first 3 hexadecimal digits of the router exchange identification (XID) number.
id number	Unique number that identifies the router. The *id number* corresponds to the last 5 hexadecimal digits of the router's XID number.

Configuring the Router

In addition to configuring a VTAM connection for each router, you must configure the router to support communication with ISM. To ensure that the router is properly configured, perform the tasks in the following sections:

- Configuring and Connecting the Router to the Network, page 2-4
- Specifying the Router Name and Enable Password, page 2-4
- Configuring SNA Service Point Support, page 2-5

Configuring and Connecting the Router to the Network

Be sure to enable the router according to the instructions provided in the documentation that came with your router. Verify that the router is configured and connected to the network.

For detailed information about configuring and connecting Cisco routers, refer to the "Related Documentation" section on page -xii.

Specifying the Router Name and Enable Password

Use the **dspu/sna host** and **enable password** commands in the configuration file of each router to specify the router name and password-protected security level for the router. These parameters are used in the implementation of ISM.

Router Name

The name that you specify for the router in the **dspu/sna host** command is used when you configure SNA service point support in the router and also when you configure the VTAM connection.

For more information about using this command, see the *Cisco IOS Configuration Fundamentals Configuration Guide*.

Enable Password

The **enable password** command controls access to various privilege levels on the router. When **enable password** is enabled in the configuration file of the router, ISM recognizes this level of security and prompts the user to specify the password to execute any enable-mode commands from ISM.

Note ISM also supports Terminal Access Controller Access Control System (TACACS) security in the router. Your router configuration may vary if TACACS is implemented.

To specify the privilege level and password that you would type to enter enable mode on the router, use the following command:

enable password [**level** *level*]{*password* | *encryption-type encrypted-password*}

For more information about using this command, see the *Cisco IOS Security Command Reference*.

Configuring SNA Service Point Support

To configure SNA service point support on the router, you need to add Cisco IOS software **sna host** commands to the configuration file of your router. The specific commands you add will depend on the type of connection you wish to establish. For detailed information on configuring SNA service point support and the Cisco IOS software command for your interface type, refer to the *Cisco IOS Bridging and IBM Networking Configuration Guide* and *Command Reference* publications.

The following procedure shows the basic steps to define SNA service point support for Ethernet and Token Ring connections. Again, the actual commands you use will depend on the type of connection you wish to establish. If you want to view some specific configuration examples, see the "Router Configuration Samples" section on page 2-6.

Perform the following tasks to define SNA service support for Ethernet and Token Ring:

Step 1 Define a link to an SNA host in global configuration mode using the **sna host** command.

The following example shows the syntax of the **sna host** command for Token Ring, Ethernet, FDDI, RSRB, or virtual data-link control (VDLC) connections:

sna host *host-name* **xid-snd** *xid* **rmac** *remote-mac* **rsap** *remote-sap* **lsap** *local-sap* **focalpoint**

Note Be sure to specify the *focalpoint* argument when you define the SNA link. Accept only the default values for the other options (such as retries) in the **sna host** command. If you specify any other values for these options, the router connection to ISM may not work properly. The *focalpoint* argument in the router configuration file is not related to ISM's Focal Point application.

Step 2 Enable the local service access point (SAP) on the interface when you are in interface configuration mode, using the command syntax:

sna enable-host lsap *lsap-address*

Step 3 Start an outgoing connection when you are in interface configuration mode, using the command syntax:

sna start *host-name*

For more information about these commands and their options, see the *Cisco IOS Bridging and IBM Networking Command Reference*.

Router Configuration Samples

This section provides five samples of the SNA Service Point configuration in a router configuration file. The following samples are provided:

Configuration Through a Local Ring to an IBM 3745 Token Ring Interface Connector

The following example shows the lines that would appear in the configuration file of a router with an interface configured through a local ring to 3745 Token Ring Interface Connector:

```
sna host CWBC02 xid-snd 05dcc002 rmac 4001.3745.1088 rsap 4 lsap 4 focalpoint
!
interface TokenRing0/1
 ip address 172.18.9.129 255.255.255.240
 ring-speed 16
 sna enable-host lsap 4
 sna start CWBC02
```

Configuration for a DSPU with RSRB on a CMCC

The following example shows the lines that would appear in the configuration file of a router combining a Cisco mainframe channel connection with an interface configured for RSRB:

```
dspu rsrb 325 1 900 4000.7000.0001
dspu rsrb enable-host lsap 4
!
dspu host CWBC01 xid-snd 05dcc001 rmac 4000.3333.4444 rsap 4 lsap 4 focalpoint
!
dspu rsrb start CWBC01
!
interface Channel4/1
```

```
 no ip address
 no keepalive csna C010 C0
!
interface Channel4/2
 ip address 172.18.9.145 255.255.255.240
 no keepalive
 lan TokenRing 0
 source-bridge 28 1 900
 adapter 4 4000.3333.4444
```

Configuration for DSPU with RSRB

The following example shows the lines that would appear in the configuration file of a router with an interface configured for DSPU with RSRB:

```
source-bridge ring-group 600
source-bridge remote-peer 600 tcp 172.18.9.19
!
dspu host CWBC09 xid-snd 05dcc009 rmac 4001.3745.1089 rsap 4 lsap 4 focalpoint dspu pool
lupool host CWBC09 lu 2 16
!
dspu pu DSPUPC8 xid-rcv 05dcca18
dspu lu 2 9 pool lupool
!
interface TokenRing0
 ip address 172.18.9.19 255.255.255.240
 ring-speed 16
 multiring all
 source-bridge 85 3 600
 dspu enable-host lsap 4
 dspu start CWBC09
```

Configuration for RSRB with a Loopback

The following example shows the lines that would appear in the configuration file of a router with RSRB and an interface configured with loopback:

```
!
source-bridge ring-group 600
source-bridge remote-peer 600 tcp172.18.10.97
source-bridge remote-peer 600 tcp172.18.10.98
!
sna rsrb 1011 3 600 4000.ffff.00cb
sna rsrb enable-host lsap 4
!
```

```
sna host CWBC0B xid-snd 05dcc00b rmac 4001.3745.1089 rsap 4 lsap 4 focalpoint sna rsrb
start CWBC0B
!
interface Loopback0
 ip address 172.18.10.97 255.255.255.252
!
```

Configuration for DLSw+ Using Virtual Data-Link Control

The following is an example of the lines that would appear in the configuration file of a router using virtual data-link control over DLSw+:

```
source-bridge ring-group 99
dlsw local-peer peer-id 172.18.16.2
dlsw remote-peer 0 tcp 172.18.16.1
!
sna vdlc 99 4000.4500.01f0
sna vdlc enable-host lsap 12
!
sna host HOST-B xid-snd 065bbbb0 rmac 4000.7000.01f1 rsap 4 lsap 12 focalpoint
!
sna vdlc start HOST-B
!
interface serial 3
    description IP connection to dspu7k
    ip address 172.18.16.2 255.255.255.0
    clockrate 4000000
!
```

Correlating the Router and VTAM Configuration Information

The router's service point name and the XID number must correspond in both the router and VTAM configurations to successfully establish a link between the router and the SNA host. It is important that the network engineer and the MVS system programmer communicate for proper setup of these two configurations.

The following example shows the format of a Cisco IOS software **sna host** command that you use to configure the router for SNA Service Point support:

sna host *host_name* **xid-snd** *xid* **rmac** *remote_mac* **[rsap** *rsap_addr***] [lsap** *local_sap***] [focalpoint]**

The values for the *host_name* and *xid* in the router configuration correspond to the VTAM PU definition in the following way:

- The *SERVICE_POINT_NAME* argument shown in the VTAM PU definition is the name of the router configured the in *host* argument of the **sna host** command.
- The *idblock number* and *id number* arguments shown in the VTAM PU definition are components of the router XID number that you specify as the value for *xid* in the **xid-snd** argument of the **sna host** command.

  For example, if the router XID is 05D00001, you specify an *idblock number* of 05D and an *id number* of 00001 in the VTAM PU definition. You specify a value of 05D00001 in the **xid-snd** argument of the **sna host** command.

Example

The following example shows a VTAM configuration file which was configured for connection to a router with the hostname *GLENDUSK* and XID of *05DBB000*:

```
SWDRTRS VBUILD TYPE=SWNET
GLENDUSK        PU      ADDR=01,                x
                        PUTY PE=2,              x
                        IDBLK=05D,              x
                        IDNUM=BB000,            x
                        DISCNT=(NO),            x
                        ISTATUS=ACTIVE,         x
                        MAXDATA=521,            x
                        IRETRY=YES,             x
                        MAXOUT=7,               x
                        PASSLIM=5,              x
                        MAXPATH=4
```

The following is the **sna host** command for this router's configuration:

```
sna host glendusk xid-snd 05dbb00 rmac 4001.3745.1088 rsap 4 lsap 4
focalpoint
```

For more information about the **sna host** command, see the *Cisco IOS Bridging and IBM Networking Command Reference*.

Verifying the NetView Environment

This section describes the following procedures, which are used to verify that NetView is properly configured to support the service point in the router:

- Verifying the Timeout Value for RUNCMDs
- Verifying if NetView Supports RUNCMDs

Verifying the Timeout Value for RUNCMDs

This section describes the procedure to verify the values of the **costime** and **maxreply** options are set correctly in NetView to support the ISM autotasks.

The **costime** option specifies the amount of time (in seconds) that ISM waits before detecting that a timeout of the RUNCMD has occurred. The ISM autotasks will wait for a RUNCMD to complete, and all other ISM processing stops until it is done. This may result in ISM pausing for long periods waiting for a response from a RUNCMD.

The **maxreply** option specifies the amount of time (in seconds) that NetView waits before detecting that a timeout of the RUNCMD has occurred. If the value is 86400, NetView will timeout the RUNCMD after 24 hours have passed.

When a **RUNCMD** times out, ISM places the router in an inoperable (INOP) state until an operator resets the router's status.

Note When **costime** defaults to the value of maxreply, only costime should be changed.

To verify the value for the **costime** option and change it if necessary, complete the following steps:

Step 1 From a NetView command prompt, type the command **list defaults** and press **Enter**.

Note the value for the **costime** argument. A value of 120 seconds is suggested for the **costime** argument.

Step 2 To change the value of the **costime** argument, complete one of the following tasks:

- To dynamically change the value of the **costime** argument without restarting NetView, type **defaults costime=120** from the NetView command prompt.
- To permanently specify the costime argument in NetView, modify the NetView production CLIST (the default CLIST is CNME1035) to specify the command **defaults costime=120**. If you are running Tivoli NetView for z/OS Version 5 or later, specify "DEFAULTS.COSTIME=120" in CNMSTYLE.

Note The default CLIST for NetView 1.3 is CNME1034.

Verifying if NetView Supports RUNCMDs

This section describes the procedure that verifies proper configuration of the NetView VTAM definition for LU 6.2 support. Although the router rejects NetView's initial LU 6.2 commands, NetView's response is to use the DSIGDS or CNMxxGDS task to send RUNCMDs, which are supported by the router. LU 6.2 support must be configured in VTAM so that NetView uses the DSIGDS task, which allows communication with the router.

To verify NetView's RUNCMD support, browse the VTAM definition for NetView and verify that your site's NetView application major node contains the following information in the second and third lines:

```
CNM01    APPL AUTH=(VPACE,ACQ,PASS),PRTCT=CNM01
                MODETAB=AMODETAB,DLOG MOD=DSIL6MOD
                APPC=YES,PARSESS=YES,
                DMINWNL=4,DMINWNR=4,DSESLIM=8,VPACING=10,
                AUTOSES=2
*               STATOPT='NETVIEW'
```

Verifying the Router's Mainframe Connection

Once you have configured a VTAM connection for each router and verified that the configuration and SNA service point support have been properly defined, you can test the router's configuration from NetView and VTAM. This is the first level of installation verification for ISM.

To diagnose the error if the verification procedures indicate a problem with the link, see Chapter 6, "Troubleshooting."

Verifying the Router Connection from NetView

Use the following procedure to verify that the network devices are configured properly and that the router can attach to the network:

Step 1 From a NetView command prompt, issue the following command for each router, where *router_name* is the hostname and service point name of the router that you are verifying:

DIS *router_name*

If properly configured and connected, the router status displays an active (ACTIV) status. If the router does not display an active status, either it is not successfully configured, and therefore is not attached to the network, or the service point is not defined correctly. To further diagnose the problem, see Chapter 6, "Troubleshooting."

Step 2 Repeat Step 1 for each router that you plan to monitor using ISM.

Testing with NetView RUNCMDs

ISM uses NetView's RUNCMD facility to support communication between ISM and the router. To verify that the router can communicate with NetView using RUNCMDS, use the following procedure:

Step 1 From a NetView console, type the following command:

RUNCMD SP=*router_name***,APPL=console,CLISTVAR=no show** ?

Where:

SP=*router_name*	Specifies the name of the service point to execute the command. This is the name of the router and the service point name that you configured in VTAM.
APPL=*applname*	Specifies the name of the link connection subsystem manager to execute the command. This is the service point application name. This example specifies **console.**
CLISTVAR={Y/N}	Specifies whether replies are saved in command list variables. This example specifies **no**.
show ?	The command that the router should execute. The **show ?** command produces a list of the supported **show** commands for the router.

Step 2 Verify that you receive a list of the commands supported by that router. To further diagnose the problem if you receive a response indicating a router problem (such as not defined to VTAM, not active, disabled service point, or RUNCMD timeout), see Chapter 6, "Troubleshooting." .

Verifying the Router Connection from VTAM

You can verify communication between the router and the mainframe from VTAM, using the following procedure:

Step 1 From the MVS console, issue the following command for each router name, where *router_name* is the hostname and service point name of the router you are verifying:

d net,ID=*router_name***,E**

Step 2 Repeat Step 1 for each router you plan to monitor using ISM.

Configuring SNMP on a Target Router

Before ISM uses SNMP to monitor Cisco routers, you must enable SNMP within a target router. ISM uses the community name to obtain variables. By default, ISM uses "public" as the community name. When defining a router to ISM, the community name can be changed for a single router or all routers.

To enable SNMP on a router, add a statement to your configuration as follows:

```
snmp-server community public RO
```

If you want to send SNMP traps to a host where ISM resides, complete the following steps:

Step 1 Add a statement for a router to your configuration as follows:

```
snmp-server host 172.18.55.14 public
```

This is another example of sending SNMP traps to a host where ISM resides.

```
snmp-server community public RO
snmp-server packetsize 8192
snmp-server queue-length 30
snmp-server enable traps snmp
snmp-server enable traps channel
snmp-server enable traps isdn call-information
snmp-server enable traps config
snmp-server enable traps envmon
snmp-server enable traps bgp
```

```
snmp-server enable traps frame-relay
snmp-server enable traps syslog
```

Step 2 Add statements for each host that is to monitor the router, as follows:

```
snmp-server host 172.18.55.14 traps public
snmp-server host 172.18.55.15 traps public
```

Defining SNMP in Cisco Routers

To specify the recipient of an SNMP notification operation, use the **snmp-server host global** configuration command.

snmp-server host *host* **[traps | informs] [version {1 | 2c}]**
community-string [udp-port *port*] [*notification-type*]

To remove a specified host use the **no** form of this command.

no snmp-server host *host* **[traps | informs]**

The following table lists the syntax and a description for each command:

Syntax	Description
host	Name or Internet address of the host.
traps	Send SNMP traps to this host. This is the default.
informs	Send SNMP informs to this host.
version	Version of the Simple Network Management Protocol (SNMP) used to send the traps.
1	SNMPv1. This option is not available with informs
2c	SNMPv2C.
community-string	Password-like community string sent with the notification operation.

Syntax	Description
udp-port *port*	UDP port of the host to use. The default is 162.
notification-type	Notification Type to be sent to the host. If no type is specified, all notifications are sent. The notification type includes one or more of the following keywords: • **bgp**—Sends Border Gateway Protocol (BGP) state change notifications. • **config**—Sends configuration notifications. • **dspu**—Sends downstream physical unit (DSPU) notifications. • **entity**—Sends Entity MIB modification notifications. • **envmon**—Sends Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded. • **frame-relay**—Sends Frame Relay notifications. • **isdn**—Sends Integrated Services Digital Network (ISDN) notifications. • **llc2**—Sends Logical Link Control, type 2 (LLC2) notifications. • **rptr**—Sends standard repeater (hub) notifications. • **rsrb**—Sends remote source-route bridging (RSRB) notifications. • **rtr**—Sends response time reporter (RTR) notifications. • **sdlc**—Sends Synchronous Data Link Control (SDLC) notifications. • **sdllc**—Sends SDLLC notifications. • **snmp**—Sends Simple Network Management Protocol (SNMP) notifications defined in RFC 1157. • **stun**—Sends serial tunnel (STUN) notifications. • **syslog**—Sends error message notifications (Cisco Syslog MIB). Specifies the level of messages to be sent with the logging history level command. • **tty**—Sends Cisco enterprise-specific notifications when a Transmission Control Protocol (TCP) connection closes. • **x25**—Sends X.25 event notifications.

Defaults

The **snmp-server host** command is disabled by default. No notifications are sent.

If you enter this command with no keywords, the default is to send all trap types to the host. No informs will be sent to this host.

If no version keyword is present, the default is version 1. If no traps or informs keyword is present, traps are enabled.

The **no snmp-server host** command with no keywords will disable traps, but not informs. In order to disable informs, use the **no snmp-server host informs** command.

This command first appeared in Cisco IOS Release 10.0.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received.

However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response PDU. If the sender does not receive a response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination.

However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once, while an inform may be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. In order to configure the router to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no keywords, all trap types are enabled for the host. In order to enable multiple hosts, you must issue a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overrides the previous command. Only the last **snmp-server host** command will be in effect. For

example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command will replace the first.

The **snmp-server host** command is used in conjunction with the **snmp-server enable** command. Use the **snmp-server enable** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable** command and the **snmp-server host** command for that host must be enabled.

However, some notification types cannot be controlled with the **snmp-server enable** command. For example, some notification types are always enabled. Other notification types are enabled by a different command. For example, the linkUpDown notifications are controlled by the **snmp trap link-status** command. These notification types do not require an **snmp-server enable** command.

A notification-type option's availability depends on the router type and Cisco IOS software features supported on the router. For example, the envmon notification-type is available only if the environmental monitor is part of the system.

SNMP Trap Examples

The following example sends the SNMP traps defined in RFC 1157 to the host specified by the name myhost.cisco.com. The community string is defined as comaccess:

```
snmp-server enable traps
snmp-server host myhost.cisco.com comaccess snmp
```

The following example sends the SNMP and Cisco environmental monitor enterprise-specific traps to address 172.30.2.160:

```
snmp-server enable traps
snmp-server host 172.30.2.160 public snmp envmon
```

The following example enables the router to send all traps to the host myhost.cisco.com using the community string public:

```
snmp-server enable traps
snmp-server host myhost.cisco.com public
```

The following example will not send traps to any host. The BGP traps are enabled for all hosts, but only the ISDN traps are enabled to be sent to a host:

```
snmp-server enable traps bgp
snmp-server host bob public isdn
```

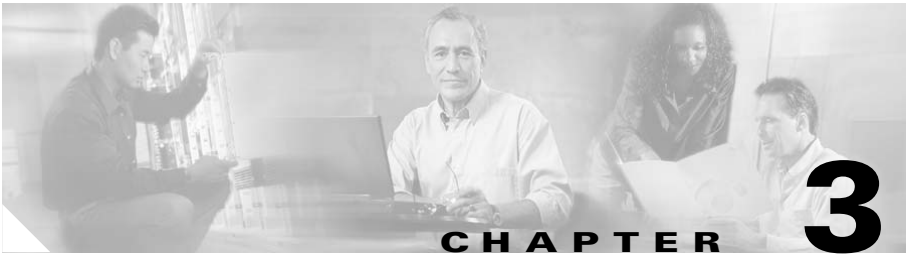
The following example enables the router to send all inform requests to the host myhost.cisco.com using the community string public:

```
snmp-server enable traps
snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

You can use the master indexes or search online to find documentation for the following related commands:

- **snmp-server host**
- **snmp-server informs**
- **snmp-server trap-source**
- **snmp-server trap-timeout**



CHAPTER 3

Installing ISM

This chapter provides detailed instructions for installing and verifying ISM. It includes the following sections:

This chapter assumes you have read Chapter 1 and performed the tasks described in Chapter 2, “Configuring the Mainframe-to-Router Link.”

To install ISM, complete the following steps:

Step 1 The ISM licensing scheme enables Cisco to distribute ISM via the CCO website. To enable ISM licensing, request a license key through Cisco's online ordering system.

The ordering system prompts you for a CPU serial number and for the type of license you want, either permanent or evaluation. Evaluation licenses are good for between 30 and 120 days.

The ordering system e-mails you the terms of your license and a 40-byte license key, similar to the following sample key:

```
301B2D301B203C383D11C1EA4CC0EE41CEC8CDE1
```

Make a note of this license key. You will use it in the "Updating the DSIPARM Members" section on page 3-20.

During initialization, ISM reads the license key, verifies the CPU serial number, and checks the license key expiration date. If the CPU serial numbers do not match, or if the license key has expired, ISM halts initialization. If the license key has less than 30 days left before expiring, ISM completes initialization and issues a reminder that a new license is required.

Step 2 Download the ISM installation data set.

Step 3 Install the ISM program using either the direct method or SMP/E method.

Step 4 Authorize the ISM load library, prefix.NSPI202.NSPNLOAD.

Step 5 Allocate the VSAM data sets.

Step 6 Update VTAM:

- Make sure you are *not* filtering message IST590I from reaching ISM
- If desired, install the VTAM exit when implementing the SNA session monitoring application of ISM

Step 7 Install and configure SNMP (Optional).

Step 8 Update NetView by performing the following tasks:

- Update the NetView procedure
- Update the DSIPARM members
- Optionally integrate ISM with NetView's STATMON utility
- Update the DSIPRF profiles

Step 9 Verify the installation.

Downloading the ISM Installation Data Set

This section describes how to install ISM. It includes the following sections:

Downloading and Running NSPI202.EXE

All the files required to install ISM are packaged in a self-extracting WINZIP file named NSPI202.EXE, which you can download from the following location:

- http://www.cisco.com/cgi-bin/tablebuild.pl/ism-v2

Step 1 Download NSPI202.EXE to a PC using binary mode. (The files contained in NSPI202.EXE are in EBCDIC format. Transferring the files in binary mode ensures correct character translation.)

Step 2 Double-click on NSPI202.EXE. The WINZIP self-extractor dialog appears.

Step 3 Enter the name of the directory in which you want to store the extracted files.

Step 4 Click **Unzip**. The following eight files are extracted and stored in the specified directory:

- NSPI202.NSPNINST.XMIT
- NSPI202.F1.XMIT
- NSPI202.F2.XMIT
- NSPI202.F3.XMIT
- NSPI202.F4.XMIT
- NSPI202.F5.XMIT
- NSPI202.F6.XMIT
- NSPI202.SMPMCS.XMIT

These files now are converted to XMIT format using the TSO Transmit facility.

Sending the Installation Files to the Host

Send the extracted files to the OS/390 host. Transfer the eight files to the OS/390 host using binary mode. Set the OS/390 host FTP SITE options as follows:

LRECL=80 BLOCKSIZE=3120 RECFM=FB CYLINDERS PRIMARY=1 SECONDARY=1

The following example shows a sample FTP session for sending the files to the OS/390 host:

```
ftp mvshost.com
user: ibmuser
password: xxxxxxxx
bin
quote site lrecl=80 blocksize=3120 recfm=fb cylinders primary=1
secondary=1
put nspi202.nspninst.XMIT
quote site lrecl=80 blocksize=3120 recfm=fb cylinders primary=1
secondary=1
put nspi202.f1.XMIT
quote site lrecl=80 blocksize=3120 recfm=fb cylinders primary=1
secondary=1
put nspi202.f2.XMIT
```

```
quote site lrecl=80 blocksize=3120 recfm=fb cylinders primary=2
secondary=1
put nspi202.f3.XMIT
quote site lrecl=80 blocksize=3120 recfm=fb cylinders primary=9
secondary=1
put nspi202.f4.XMIT
quote site lrecl=80 blocksize=3120 recfm=fb cylinders primary=4
secondary=1
put nspi202.f5.XMIT
quote site lrecl=80 blocksize=3120 recfm=fb cylinders primary=3
secondary=1
put nspi202.f6.XMIT
quote site lrecl=80 blocksize=3120 recfm=fb cylinders primary=1
secondary=1
put nspi202.smpmcs.XMIT
quit
```

Receiving the Installation Files

The Receive TSO option converts the sequential data sets that you sent to the OS/390 host into PDS format. You do not need to pre-allocate the data sets. Follow these steps to receive the installation files:

Step 1 After you transfer the files to the host, use TSO option 3.4 to list the eight data sets. Your list should resemble the following list, except for the *userid* and *volume*:

```
Menu Options View Utilities Compilers Help
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
DSLIST - Data Sets Matching xxxx.NSPW* Row 1 of 6
Command ===> Scroll ===> PAGE
Command - Enter "/" to select action Message Volume
------------------------------------------------------------------------
xxxx.NSPI202.NSPNINST.XMIT SMSC1F
xxxx.NSPI202.F1.XMIT  SMSC1F
xxxx.NSPI202.F2.XMIT SMSC1F
xxxx.NSPI202.F3.XMIT SMSC1F
xxxx.NSPI202.F4.XMIT SMSC1F
xxxx.NSPI202.F5.XMIT SMSC1F
xxxx.NSPI202.F6.XMIT  SMSC1F
xxxx.NSPI202.SMPMCS.XMIT  SMSC1F
**************************** End of Data Set list **************
```

Step 2 At the beginning of the first line of the list, enter **Receive inds(/)** as shown below:

```
Command - Enter "/" to select action Message Volume
```

```
------------------------------------------------------------------------------
receive inds(/).XMIT  SMSC1F
xxxx.NSPI202.F1.XMIT SMSC1F
xxxx.NSPI202.F2.XMIT  SMSC1F
xxxx.NSPI202.F3.XMIT SMSC1F
xxxx.NSPI202.F4.XMIT SMSC1F
xxxx.NSPI202.F5.XMIT SMSC1F
xxxx.NSPI202.F6.XMIT SMSC1F
xxxx.NSPI202.SMPMCS.XMIT  SMSC1F
***************************** End of Data Set list ****************************
```

The following message is displayed:

```
Enter restore parameters or 'DELETE' or 'END'
```

The first data set is restored.

Step 3 Press **Enter**.

Step 4 At the beginning of the second line of the list, enter an equal sign (**=**) to repeat the previous command, and press **Enter**. The second data set is restored.

Step 5 Repeat Step 4 to restore the remaining six data sets.

Step 6 Press **PF3**, then press **Enter** to list the sixteen data sets (the eight sequential data sets and the eight PDS data sets). Your list should resemble the following:

```
DSLIST - Data Sets Matching HAL1.NSPW* Row 1 of 17
Command ===> Scroll ===> PAGE
Command - Enter "/" to select action Message Volume
------------------------------------------------------------------------------
xxxx.NSPI202.NSPNINST SMSC18
xxxx.NSPI202.NSPNINST.XMIT  SMSC1F
xxxx.NSPI202.F1  SMSC18
xxxx.NSPI202.F1.XMIT  SMSC1F
xxxx.NSPI202.F2  SMSC18
xxxx.NSPI202.F2.XMIT  SMSC1F
xxxx.NSPI202.F3  SMSC18
xxxx.NSPI202.F3.XMIT  SMSC1F
xxxx.NSPI202.F4  SMSC18
xxxx.NSPI202.F4.XMIT  SMSC1F
xxxx.NSPI202.F5  SMSC18
xxxx.NSPI202.F5.XMIT  SMSC1F
xxxx.NSPI202.F6  SMSC18
xxxx.NSPI202.F6.XMIT  SMSC1F
xxxx.NSPI202.SMPMCS  SMSC18
xxxx.NSPI202.SMPMCS.XMIT  SMSC1F
***************************** End of Data Set list ****************************
```

Contents of the Installation Data Set

Table 3-1 describes the members in the installation data set, *prefix*.NSPI202.NSPNINST. If you are installing ISM directly, use only the COPYISM member. The remaining members are used for an SMP/E installation of ISM.

Table 3-1 ISM Installation Data Set Contents

Member	Description
ALLOC	SMP/E allocate target and distribution files job.
ALLOCSMP	SMP/E allocate SMP work and temporary files job.
COPYISM	Direct installation procedure to copy installation files from tape to DASD.
ISMACCPT	SMP/E procedure to accept ISM.
ISMAPPLY	SMP/E procedure to apply ISM.
ISMCSI	SMP/E procedure to create and initialize ISM CSI files.
ISMRECV	SMP/E procedure to receive ISM.
ISMREJCT	SMP/E procedure to reject ISM.

Choosing an ISM Installation Method

You can install the ISM program using either the direct method, or the SMP/E, but first run *prefix*.NSPI202.NSPINST, to unload the ISM installation data set.

Note When you run any of the sample ISM installations described in this chapter, make sure you follow the instructions specific to each job to customize the JCL for your installation.

Installing ISM Directly

If you chose the direct method, run the sample job provided in the COPYISM member of the installation data set, prefix.NSPI202.NSPINST.

COPYISM copies the following ISM data sets from the Relfiles to DASD:

- *prefix*.NSPI202.NSPNLOAD
- *prefix*.NSPI202.NSPNCLST
- *prefix*.NSPI202.NSPNHTML
- *prefix*.NSPI202.NSPNPANL
- *prefix*.NSPI202.NSPNSAMP

Example

The following example is an excerpt of the COPYISM sample JCL to install ISM directly. Follow the directions to unload the data set. The remaining statements of the COPYISM job are similar and unload the rest of the ISM installation data sets.

```
//COPYISM JOB ('ACCOUNTING INFO'),PGMRNAME,MSGLEVEL=(1,1),
//            MSGCLASS=A,CLASS=A,TIME=5
//*
//*****************************************************************
//*                                                               *
//*  ISM 2    COPY PROCEDURE                                      *
//*                                                               *
//*  THIS JOB WILL COPY THE ISM INSTALLATION DATASETS FROM        *
//*  THE DISTRIBUTION files TO DASD.  MODIFY THIS JOB ACCORDING   *
//*  TO THE FOLLOWING INSTRUCTIONS, THEN SUBMIT THE JOB.          *
//*                                                               *
//*  1) CHANGE THE JOB CARD FOR YOUR SITE.                        *
//*                                                               *
//*  2) CHANGE ALL OCCURRENCES OF "prefix" TO YOUR                *
//*     PRODUCTION DATASETS' HIGH-LEVEL QUALIFIER.                *
//*                                                               *
//*  3) CHANGE ALL OCCURRENCES OF "volser" TO YOUR OUTPUT DASD    *
//*     VOLUME SERIAL NUMBER.                                     *
//*                                                               *
//*  4) CHANGE ALL OCCURRENCES OF "relhlq" TO THE HIGH-LEVEL      *
//*     QUALIFIER YOU RECIEVED THE RELFILES UNDER.                *
//*                                                               *
//*  5) CHANGE ALL OCCURRENCES OF "sysunit" TO THE UNIT TYPE OF   *
//*     YOUR OUTPUT DASD DRIVE.                                   *
//*                                                               *
//*****************************************************************
//*
//*
//LOAD1    EXEC PGM=IEBCOPY
//SYSPRINT DD SYSOUT=*
```

```
//SYSUT3   DD UNIT=SYSDA,SPACE=(CYL,(1,1))
//SYSUT4   DD UNIT=SYSDA,SPACE=(CYL,(1,1))
//*
//ILOAD    DD DISP=SHR,DSN=relhlq.NSPI202.F2
//OLOAD    DD DSN=prefix.NSPI202.NSPNLOAD,
//            UNIT=sysunit,VOL=SER=volser,
//            DISP=(NEW,CATLG),DCB=(RECFM=U,
//            BLKSIZE=6144),SPACE=(CYL,(1,1,25))
//*
//ISAMP    DD DISP=SHR,DSN=relhlq.NSPI202.F3
//OSAMP    DD DSN=prefix.NSPI202.NSPNSAMP,
//            UNIT=sysunit,VOL=SER=volser,
//            DISP=(NEW,CATLG),DCB=(RECFM=FB,LRECL=80,
//            BLKSIZE=3120),SPACE=(CYL,(1,1,25))
//*
//ICLIST   DD DISP=SHR,DSN=relhlq.NSPI202.F4
//OCLIST   DD DSN=prefix.NSPI202.NSPNCLST,
//            UNIT=sysunit,VOL=SER=volser,
//            DISP=(NEW,CATLG),DCB=(RECFM=FB,LRECL=80,
//            BLKSIZE=3120),SPACE=(CYL,(10,1,99))
//*
//IHTML    DD DISP=SHR,DSN=relhlq.NSPI202.F5
//OHTML    DD DSN=prefix.NSPI202.NSPNHTML,
//            UNIT=sysunit,VOL=SER=volser,
//            DISP=(NEW,CATLG),DCB=(RECFM=FB,LRECL=80,
//            BLKSIZE=3120),SPACE=(CYL,(5,1,50))
//*
//IPANEL   DD DISP=SHR,DSN=relhlq.NSPI202.F6
//OPANEL   DD DSN=prefix.NSPI202.NSPNPANL,
//            UNIT=sysunit,VOL=SER=volser,
//            DISP=(NEW,CATLG),DCB=(RECFM=FB,LRECL=80,
//            BLKSIZE=3120),SPACE=(CYL,(3,1,99))
//*
//SYSIN    DD *
LOAD     COPYMOD INDD=ILOAD,OUTDD=OLOAD
SAMP     COPY    INDD=ISAMP,OUTDD=OSAMP
CLIST    COPY    INDD=ICLIST,OUTDD=OCLIST
HTML     COPY    INDD=IHTML,OUTDD=OHTML
PANEL    COPY    INDD=IPANEL,OUTDD=OPANEL
```

Installing ISM Using SMP/E

Use the following procedure to install ISM in a zone other than the MVS zone on your mainframe using SMP/E:

Step 1 Use the sample SMP/E member named ALLOC, in *prefix*.NSPI202.NSPNINST, to allocate your target and distribution libraries.

Step 2 Submit the SMP/E member named ALLOCSMP located in the *prefix*.NSPI202.NSPNINST data set. This job allocates and initializes SMP work and temporary files.

Step 3 Edit and submit the SMP/E member named ISMCSI in the *prefix*.NSPI202.NSPNINST data set. This job allocates and initializes the SMP CSIs.

Step 4 Edit the *prefix*.NSPI202.SMPMCS data set, changing the value of ++VER(Z038) to the preferred zone.

Step 5 Submit the SMP/E member named ISMRECV, in the *prefix*.NSPI202.NSPNINST data set, to receive ISM.

Step 6 Use the sample SMP/E member named ISMAPPLY, in *prefix*.NSPI202.NSPNINST, to apply ISM.

Step 7 Use the sample SMP/E member named ISMACCPT, in *prefix*.NSPI202.NSPNINST, to accept ISM.

Note ISM can be installed into an existing SMP/E zone. If you prefer to install ISM into an existing zone, omit steps 2 and 3 (ALLOCSMP and ISMCSI).

Authorizing the ISM Load Library

After installing the ISM program files, authorize the library *prefix*.NSPI202.NSPNLOAD by adding it to SYS1.PARMLIB or by copying it to one of your site's authorized user libraries. This allows ISM to process some authorized commands and perform security checks.

To authorize the ISM load library, complete the following steps:

Step 1 Add the data set *prefix*.NSPI202.NSPNLOAD and its DASD volume name to your list of authorized program facility (APF) authorized data sets in SYS1.PARMLIB(IEAAPFxx) or SYS1.PARMLIB(PROGxx).

Step 2 Reload (IPL) MVS if necessary. If your system is enabled to use dynamic APF services, you can avoid reloading MVS by using the **SETPROG** command to dynamically update the APF list. See the *Initialization and Tuning Reference* manual for your MVS/ESA system for more information about authorizing data sets.

Allocating the VSAM Data Sets

There are six jobs to run when allocating the VSAM data sets that ISM uses. Two are required and four are optional, depending upon the ISM functions you plan to implement.

Member	Description
ISMALLAH (Required)	Allocates the ISM management data set (ISMDSA) and resource and Cisco mainframe channel connection archive data set (ISMDSH).
ISMALLMN (Required)	Allocates the ISM primary event log (ISMDSM) and alternate event log (ISMDSN).
ISMALLI (Required)	Allocates the interface statistics and performance data set (ISMDSI).
ISMALLC (Optional)	Allocates the resource configuration data set (ISMDSC).
ISMALLR (Optional)	Allocates the SNA session archive data set (ISMDSR).

Member	Description
ISMALLD (Optional)	Allocates the router memory dump data set (ISMDSD).
ISMALLW (Optional)	Allocates the SNASw statistics and perfomance data set (ISMDSW).

For storage requirements see Table 1-4 on page 1-9.

To allocate the VSAM data sets, modify and run each member (located in *prefix*.NSPI202.NSPNSAMP) described in Table 1-5 on page 1-10.

Note All but two of the VSAM-keyed sequence data sets have a record size of 230 with a key of 24. The resource configuration (ISMDSC) and router memory dump (ISMDSD) data sets use a key of 28 and record size of 128.

Updating VTAM

The following sections describe the updates required in VTAM to support ISM:

- Verifying VTAM Message Support, page 3-12
- Supporting SNA Session Monitoring, page 3-12

Verifying VTAM Message Support

The ISM program must receive the IST590I VTAM message over the PPI or PPO interface. *Do not* block the message from reaching NetView.

Supporting SNA Session Monitoring

If you plan to use the SNA session monitoring application in ISM, you must install the functional VTAM XID configuration services exit routine called NSPEMGR, which is provided by the ISM program. The NSPEMGR routine calls a service

routine that writes a message (NSP2015I) containing Media Access Control (MAC), SAP, and RIF data (when available) each time a switched PU connects into the network.

If you are not using your own ISTEXCCS exit routine, install the ISM version, as described in the section "Installing the VTAM XID Exit Routine" section on page 3-13.

If you have your own ISTEXCCS exit routine, or have installed the CiscoWorks Blue SNA View exit, call the Cisco Customer Technical Assistance Center (TAC) for instructions on modifying your existing routine to work with ISM.

Overview of the VTAM XID Exit Routine

The VTAM exit NSPEMGR is driven under a VTAM subtask when VTAM initializes or when activated by a **F NET,EXIT,ID=ISTEXCCS,OPT=ACT** command. When this command is issued, the exit is driven with a BEGIN vector allowing the exit to do any required initialization. It allocates two bytes of memory required for sending information back to VTAM in a BUILD vector. The exit then opens the primary and backup VSAM datasets.

Finally, the BEGIN vector is modified to indicate to VTAM that the exit should be called when VTAM receives an XID for defined PUs. When VTAM receives an XID for a defined PU the exit is once again invoked. The exit is given information about the PU including the PU name, local and remote MAC and SAP addresses for the PU session, the IDBLK/IDNUM for the PU, and finally RIF data if present. All of this data is written to a message (NSP2015I) containing MAC, SAP, and RIF data (when available), each time a switched PU connects to the network. The exit then returns a BUILD vector indicating that VTAM should allow the connection.

At VTAM termination, or when the exit is deactivated using the **F NET,EXIT,ID=ISTEXCCS,OPT=INACT** command, the exit is driven with the END vector. At this point the exit frees the allocated memory.

This process should produce minimal impact to VTAM connection performance.

Installing the VTAM XID Exit Routine

If you are not using your own ISTEXCCS exit routine, you can install the ISM VTAM XID exit routine distributed with your ISM installation files.

To install the ISM VTAM exit routine, complete the following steps:

Step 1 Copy the member named NSPEMGR from the *prefix*.NSPI202.NSPNLOAD data set, to SYS1.VTAMLIB.

Step 2 Use the sample member ISMMPF provided in the *prefix*.NSPI202.NSPNSAMP data set to update the MVS system's MPF table in SYS1.PARMLIB. This allows the ISM message NSP2015I, created by the VTAM exit, to be automated by NetView:

```
NSP*,AUTO(YES),RETAIN(NO),SUP(NO) /* GENERIC ENTRY */
```

Step 3 To verify that the VTAM XID exit is installed properly, run the following VTAM command:

F NET,EXIT,ID=ISTEXCCS,OPT=ACT,MODULE=NSPEMGR

When message NSP2015I is returned to the console, the exit is working correctly.

Step 4 After verifying that the VTAM XID exit executed properly, rename the NSPEMGR member to ISTEXCCS in SYS1.VTAMLIB.

Reassembling the VTAM XID Exit Routine

If you contacted the Cisco TAC for instructions and were told that you need to reassemble and link-edit the VTAM XID exit, complete the following steps:

Step 1 Modify the sample member NSPECCSL provided in the *prefix*.NSPI202.NSPNSAMP data set as required for your site's exit name.

Step 2 Modify the sample member ASMEMGR provided in the *prefix*.NSPI202.NSPNSAMP data set according to your site's requirements as specified in the beginning of the sample job. Be sure to assemble and link-edit the NSPEMGR exit into an authorized user library which is concatenated to SYS1.VTAMLIB (specified in the SYSLMOD statement).

Installing and Configuring SNMP

This section describes the process of installing and enabling SNMP on your mainframe and on the SNMP resources you want to manage. It includes the following sections:

Software Requirements for SNMP

The data sets described in this chapter are provided by IBM TCP/IP for MVS/ESA 3.2.0. The platform supported for using SNMP on the mainframe is *Tivoli's TME10 NetView for OS/390 version 1, Release 2.*

Data Sets Provided by IBM's TCP/IP

Table 3-2 lists the data sets created when you install IBM's TCP/IP on the mainframe.

Table 3-2 IBM TCP/IP Data Sets

Data set Name	Contents
prefix.SEZAINST	Procedures, instructions, and MIB table
prefix.SEZADSIM	SNMP messages
prefix.SEZADSIP	SNMPARMS
prefix.SEZANPNL	SNMP panels
prefix.SEZADSIL	SNMP load modules
prefix.SEZANCLS	CLISTs and code point tables

Because the environment to be managed from NetView is known, ISM can improve response times and reduce TCP/IP overhead by doing some of the conversions in NetView.

To improve the performance of SNMP management of Cisco devices from the mainframe, ISM does the following:

- Queries hosts using their IP address
- Uses ASN.1 notation in SNMP commands

Installing SNMP on the Mainframe

To install SNMP on the mainframe, complete the following tasks:

- Adding SNMP Configuration Statements to TCP/IP Profile Data Set, page 3-16
- Identifying SNMP Port Numbers, page 3-17
- Configuring the SNMP Query Engine, page 3-18

For additional information on installing SNMP, refer to your SNMP product documentation.

Adding SNMP Configuration Statements to TCP/IP Profile Data Set

To modify the *prefix*.PROFILE.TCPIP data set to include SNMP configuration statements, complete the following steps:

Step 1 To start the SNMP query engine (SNMPQE) and SNMP agent (SNMPD) address spaces simultaneously with the TCPIP address space, include SNMPQE and SNMPD in the AUTOLOG statement, as shown below:

```
AUTOLOG
  SNMPQE            ; SNMP Query Engine
  SNMPD             ; SNMP Agent
ENDAUTOLOG
```

Step 2 SNMP uses raw sockets for the SNMP PING functions and for the Distributed Program Interface (DPI). To allow the SNMPQE and the SNMPD to create raw sockets, add SNMPQE and SNMPD to the OBEY statement, as follows:

```
OBEY
```

```
  IBMUSER SNMPD SNMPQE
ENDOBEY
```

Or create an equivalent RACF profile.

Step 3 SNMP requires that port 161 be reserved for all messages sent to the MVS agent, and that port 162 be reserved for SNMP messages that report traps to the MVS client. Make sure that the following statements are part of the *prefix*.PROFILE.TCPIP data set:

```
PORT
  161 UDP SNMPD     ; SNMP Agent
  162 UDP SNMPQE    ; SNMPQE Agent
```

Step 4 Add a statement similar to the following example to identify the contact person for this managed node:

```
SYSCONTACT
  Mickey Mouse, extension 1234
ENDSYSCONTACT
```

SYSCONTACT is the MIB II variable that identifies the contact person for this managed node.

Step 5 Add a statement similar to the following example to identify the physical location of this managed node:

```
SYSLOCATION
  123 North Main Street
  Anytown, NC 99999
ENDSYSLOCATION
```

SYSLOCATION is the MIB II variable that identifies the physical location of this managed node.

Identifying SNMP Port Numbers

The SNMP agent, SNMPD, uses the *prefix*.ETC.SERVICES data set to determine its port numbers. To identify the SNMP port numbers, modify the *prefix*.ETC.SERVICES data set to add the following statements:

```
snmp       161/udp     # snmp request port
snmp-trap  162/udp     # snmp monitor trap port
```

The entries in *prefix*.ETC.SERVICES data set are case sensitive and column sensitive. They must be in lowercase and begin in column one.

Configuring the SNMP Query Engine

To configure the SNMP query engine, follow these steps:

Step 1 Update the SNMP query engine using the *prefix*.SEZAINST(SNMPPROC) data set.

Step 2 Create the MIB data set by creating a MIBDESC. To create a MIBDESC, enter the following command from option 6 of the TSO:

Receive inds ('prefix.NSPI202.NSPNSAMP(MIBDESC)')

This creates a data set userid TCPIP1.MIBDESC.DATA. You can replace the existing TCP.MIBDESC.DATA data set with this data set.

Step 3 To enable the optional data set for NLS support, use the *prefix*.SEZAINT(MSSNMP) data set. This data set specifies the SNMP message repository.

Step 4 To explicitly identify the data set used to obtain the TCPIP.DATA parameters, use the *prefix*.SEZAINST(TCPDATA) data set.

Updating NetView

This section describes the following procedures for modifying NetView data sets:

Updating the NetView Procedure

This sample procedure specifies the ISM load library, CLIST library, panel library, and VSAM data sets which must be updated in your sites's NetView procedure.

To update your existing NetView procedure, perform the following steps:

Step 1 Update the data set high-level qualifiers in the sample JCL provided in member ISMPROC of the prefix.NSPI202.NSPNSAMP library for the following DD names, according to your site's ISM implementation.

The following data sets are required:

- STEPLIB—Specifies the ISM load library
- DSICLD—Specifies the ISM CLIST library and ISM HTML procedure library
- CNMPNL1—Specifies the ISM panels library
- NSPDSA—Specifies the ISM configuration data set
- NSPDSH—Specifies the resource history data set
- NSPDSM—Specifies the ISM primary event log
- NSPDSN—Specifies the ISM alternate event log
- NSPDSI—Specifies the resource interface statistics and performance data set

The following data sets are optional:

- NSPDSR—Specifies the ISM SNA session archive data set
- NSPDSC—Specifies the resource configuration data set
- NSPDSD—Specifies the router memory dump data set
- NSPDSW—Specifies the SNASw statistics and performance data set.

Step 2 Add modified statements from the ISMPROC sample to the NetView procedure. The following example shows an updated NetView procedure with the DD statements to support ISM.

```
//STEPLIB  DD   ---------------------------
//         DD   DISP=SHR,DSN=prefix.NSPNLOAD      ISM LOAD LIBRARY
//*
//DSICLD   DD   ------------------------
//         DD   DSN=SHR,DSN=prefix.NSPNCLST       ISM CLISTS
//         DD   DSN=SHR,DSN=prefix.NSPNHTML      ISM HTML PROCEDURES
```

```
//*
//CNMPNL1  DD   --------------------------
//         DD   DSN=SHR,DSN=prefix.NSPNPANL       ISM PANELS
//*
//* ISM VSAM DATA BASES
//* ISM V1R3 CONFIG DATA BASE
//NSPDSA   DD   DSN=prefix.NSPDSA,
//         DISP=SHR,AMP=AMORG
//* ISM V1R3 ROUTER HISTORY DATA BASE
//NSPDSH   DD     DSN=prefix.NSPDSH,
//         DISP=SHR,AMP=AMORG
//* ISM V1R3 DATA BASE FOR ISM EVENTS
//NSPDSM   DD   DSN=prefix.NSPDSM,
//         DISP=SHR,AMP=AMORG
//NSPDSN   DD   DSN=prefix.NSPDSN,
//         DISP=SHR,AMP=AMORG
//* ISM INTERFACE DATA BASE
//NSPDSI DD     DSN=prefix.NSPDSI,
//         DISP=SHR,AMP=AMORG
//* ISM V1R3 SESSION DATA
//NSPDSR DD     DSN=prefix.NSPDSR,
//         DISP=SHR,AMP=AMORG
//* ISM  V1R3 DATA BASE FOR ROUTER CONFIGURATIONS
//NSPDSC DD     DSN=prefix.NSPDSC,
//         DISP=SHR,AMP=AMORG
//* ISM  V1R3 DATA BASE FOR ROUTER MEMORY DUMPS
//NSPDSD DD     DSN=prefix.NSPDSD,
//         DISP=SHR,AMP=AMORG
//* ISM V2R2 DATA BASE FOR SNASW
//NSPDSW DD     DSN=prefix.NSPDSW,
//    DISP=SHR,AMP=AMORG
```

Updating the DSIPARM Members

This section describes the updates required to enable the following ISM functions in the NetView user DSIPARM data set:

- ISM commands
- SNMP commands
- ISM VSAM tasks
- SNMP task
- ISM automation operators

- SNMP automation operators
- ISM automation table entries
- SNMP automation table entries
- ISM licensing

If you are using a release of NetView that does not use CNMSTYLE, complete the following steps to update the members of the NetView DSIPARM user data set to support ISM.

Step 1 Copy the following members from the prefix.NSPI202.NSPNSAMP data set to the NetView DSIPARM user data set:

- ISMCMD2—ISM Version 2 commands
- ISMCNM2—ISM STATMON Interface
- ISMDMN2—ISM Tasks
- ISMLICSE—ISM licensing information
- ISMOPF2—ISM Autotasks
- ISMTBL2—ISM automation table entries
- NSPDSA—ISM VSAM task member for ISM control files
- NSPDSC—ISM VSAM task member for resource configurations
- NSPDSD—ISM VSAM task member for resource dumps
- NSPDSH—ISM VSAM task member for resource, TN3270, and CMC statistics
- NSPDSI ISM—VSAM task member for interface statistics
- NSPDSM ISM—VSAM task member for event data base (1 of 2)
- NSPDSN ISM—VSAM task member for event data base (2 of 2)
- NSPDSR ISM—VSAM task member for interface statistics
- NSPDSW ISM—VSAM taskl member for SNASw

Step 2 Enable the ISM commands by adding a %INCLUDE ISMCMD2 statement to the DSICMD or DSICMDU member.

Step 3 Enable the ISM VSAM tasks by adding a %INCLUDE ISMDMN2 statement to the DSIDMN or DSIDMNU member.

Step 4 Enter your license key (see Step 1 on page 3-2) in member ISMLICSE. The ISMLICSE member has the following format:

```
ISMLICENSE=301B2D301B203C383D11C1EA4CC0EE41CEC8CDE1
```

The ISMLICSE member can contain comments, identified by an asterisk (*) in column 1. You can include multiple ISMLICENSE entries in the ISMLICSE member, but ISM recognizes only the first.

Step 5 Enable the ISM automation operator profiles by adding a %INCLUDE ISMOPF2 statement to the DSIOPF or DSIOPFU member. The operators defined in ISMOPF2 might have to be added to the s security system for your site.

Step 6 Enable the ISM automation table entries by adding a %INCLUDE ISMTBL2 statement to the current production version of the NetView automation table (such as DSITBL01).

Step 7 If you are running a release of NetView that uses CNMSTYLE, copy member ISMSTGEN from prefix.NSPI202.NSPNSAMP to DSIPARM(CNMSTGEN) to define the ISM VSAM tasks, SNMP, etc. Update the member with the name of your TCP/IP task and VTAM network id.

Step 8 Ensure that the ISM tasks have the authority to issue AUTOTASK, PURGE, RESETDB, START TASK, and STOP commands. The data set prefix.NSPI202.NSPNSAMP(ISMSCAT2) contains a sample ISMSCAT2 member.

Note To integrate ISM commands in the STATMON utility, update and restart NetView, then complete the tasks described in the "Integrating ISM with STATMON" section on page 3-28.

Caution Do not install both ISM V2 and ISM V1R3.0 in NetView. The combination of these systems causes ISM compatibility issues.

Using ISM SNMP Support

To use ISM SNMP support, complete the following steps:

Step 1 Copy the following members from prefix.NSPI202.NSPNSAMP data set to NetView DSIPARM user data set:

- SNMPDMN—SNMP task member
- SNMPOPF—SNMP Autotasks
- SNMPARMS—SNMP task member
- SNMPTBL—SNMP automation table entries

Step 2 Enable the SNMP IUCV task by adding a %INCLUDE SNMPDMN statement to the DSIDMN or DSIDMNU member.

Step 3 Enable the SNMP automation operator profiles by adding a %INCLUDE SNMPOPF statement to the DSIOPF or DSIOPFU member. The operators defined in SNMPOPF might have to be added to your site's security system.

Step 4 Enable the SNMP automation table entries by adding a %INCLUDE SNMPTBL statement to the current production version of the NetView automation table (such as DSITBL01).

Updating DSIPRF Profiles

This section describes the NetView user DSIPRF data set updates. These updates enable the ISM profiles used by the following ISM automation tasks:

- ISMPROFI—Profile for ISMMGRS (ISM refresh autotask) and ISMMGRI (Interface monitoring autotask)
- ISMPROF1—Profile for ISMMGR (ISM primary automation manager)
- ISMPROF2—Profile for NSPMGRM (ISM message automation autotask)
- ISMPROF3—Profile for additional managers (such as ISMMGRA and ISMMGRB)
- ISMPROFS—Profile for SNA Session monitor autotask ISMEXIT
- ISMPROFW—Profile for the SNASw monitor autotask SNASWMON

To update the members of the NetView DSIPRF user data set to support SNMP, copy the following members from prefix.NSPI202.NSPNSAMP to the DSIPRF user data set.

- SNMPPRF1—Profile for primary SNMP autotask
- SNMPPRF2—Profile for SNMP automation autotask

Configuring NetView to Initialize ISM

To start NetView and ISM together, add the following autotask command to the site's production NetView initialization CLIST:

AUTOTASK OPID=ISMMGR

or add to CNMSTYLE

AUTOTASK.ISMMGR.CONSOLE=*NONE*

This command is included in the sample CNMSTGEN.

The ISM program uses autotasks for the following:

- ISMMGR—Primary ISM manager
- ISMMGRM—Automates actions when messages are received
- ISMMGRS—Creates the data used for the ISM status summary display
- ISMMGRI—Collects statistics from interfaces
- SNASWMON—Monitors and collects SNASw
- ISMEXIT—SNA Session Monitor dispatcher task
- ISMEXIT1-9—SNA Session Monitor tasks

The following autotasks are provided by ISM for SNMP management:

- SNMPMGRI—Primary SNMP manager
- SNMPOPER—Autotask used to automate actions when SNMP messages are received

Note If you are using Tivoli NetView 1.2, the CLIST is usually CNME1035. In Tivoli NetView 1.3, the CLIST is CNME1034. In Tivoli NetView 1.4, ISMMGR is started from CNMSTGEN.

Configuring the Standard Interface as an SNMP Monitor

This section describes how to customize NetView to support SNMP. For specific details on installing SNMP, refer to the IBM publication, *eNetwork CS IP Configuration Guide*.

To customize NetView to support SNMP, follow these steps:

Step 1 Add the SNMP task using the following statement in DSIDMNxx:

```
SNMP TASK     MOD=SNMPIUCV,TSKID=SNMPIUCV,PRI=5,INIT=Y
```

SNMPIUCV is the NetView optional task that handles IUCV communication between the NetView program and the SNMP query engine. SNMPIUCV resides in the *prefix*.SEZADSIL data set.

The SNMPIUCV task tries to connect through IUCV to the SNMP query engine. If the task fails, it tries to reconnect as specified by the SNMPQERT keyword in the SNMPARMS member of the *prefix*.SEZADSIP data set. The retry default is every 60 seconds.

Step 2 Add the SNMP command using the following statement:

```
SNMP CMDMDL MOD=SNMP,ECHO=Y,TYPE=R,RES=Y
```

SNMP is the command processor that allows NetView operators and CLISTs to issue SNMP commands. SNMP resides in the *prefix*.SEZADSIL data set. This data set should be concatenated to the STEPLIB DD statement in the NetView start procedure.

Step 3 Add the SNMP parameters (SNMPARMS) data set. The contents of this data set are shown below:

```
Member name: SNMPARMS
*
* SNMPQE SNMPQE     * Userid of SNMP Query Engine
  SNMPQE OESNMQD1   * Userid of SNMP Query Engine
  SNMPQERT 60       * Retry time (seconds) for IUCV CONNECT
  SNMPRCNT 2        * Retry count for sending SNMP requests
  SNMPRITO 10       * Retry initial timeout (10ths of a second)
  SNMPRETO 2        * Retry backoff exponent
                    (1=linear,2=exponential)
  SNMPMMLL 80       * Line length for Multiline Messages 38/44
```

Step 4 Add SNMP messages to DSIMSG as follows:

```
DSIMSG      prefix.SDSIMSG1
            prefix.SEZADSIM
```

The SNMP messages reside in the prefix.SEZADSIM data set as DSISNM*nn*, where *nn* is the number of the member. The valid message members are DSISNM00 through DSISNM055, DSISNM10, DSISNM12, and DSISNM99. The data set containing these members should be added to the DSIMSG DD statement in the NetView start procedure.

Step 5 Add the SNMP CLISTs to NetView by creating two data sets using the following command. Then copy the IBM-provided members into these data sets.

```
DSICLD      prefix.USER.SEZANCLS
            prefix.DSICLD
```

Step 6 Add the SNMP panels to NetView by creating two data sets using the following command, then copy the IBM-provided members into these data sets.

```
CNMPNL1     prefix.USER.SEZANPNL
            prefix.CNMPNL1
```

Step 7 Make the SNMPIUCV modules available to NetView using either steplib or by adding to the linklist.

Step 8 Add the SNMP automation table by modifying the NetView automation table to include the SNMPAUTO (*prefix*.SEZANCLS(SNMPAUTO)) data set.

Step 9 Add at least two autotasks to support the SNMP data set with the following functions:

- Initialize the SNMP manager and execute the timers associated with the active monitoring of target hosts.
- Recover the connection between NetView and TCP/IP to automate the trap to alert conversion.

Verifying SNMP on the Mainframe

To verify that SNMP is correctly installed on the mainframe, use the **snmp ping** command to test the connection to an existing device. At the NetView command prompt, issue the following command:

snmp ping *ip_address*

Where *ip_address* is the IP address of a device that you know is running and is SNMP-enabled.

If SNMP is correctly installed and is currently active, you get a response time message. Otherwise, you get an error message notifying you that SNMP is not installed or is not active.

To verify that the SNMP command is available from NetView use the **dispmod snmp** command. At the NetView command prompt, issue the following command:

dispmod snmp

If the SNMP command is available from NetView, you get the following response.

```
CNM263I MODULE   LENGTH CSECT    DATE     PTF      EPA      AM ATTR
CNM263I SNMP     0011E8 SNMPSNMP 12/09/97 ------- -------- 31
CNM265I END OF DISPLAY
```

To verify that the SNMPIUCV task is available from NetView, use the **dispmod snmpiucv** command. At the NetView command prompt, issue the following command:

dispmod snmpiucv

If the SNMPIUCV task is available from NetView, you get the following response:

```
CNM263I MODULE   LENGTH CSECT    DATE     PTF      EPA      AM ATTR
CNM263I SNMPIUCV 002E40 SNMPIUCV 12/09/97 ------- -------- 31
CNM265I END OF DISPLAY
```

Restarting NetView

After you update the NetView procedure, the DSIPARM data set, and the DSIPRF data set to enable NetView to initialize ISM, restart NetView to install all of the modifications.

When you restart NetView, the ISMMGR autotask begins, which initiates ISM. If you need to stop the autotask while NetView is running, you can use the **isminit reset** command.

Integrating ISM with STATMON

As an option, after you updated NetView for ISM and restarted NetView, you can integrate ISM with STATMON.

You can add ISM commands to the Command Menu in STATMON (Figure 3-1) by updating the DSICNM member in your NetView DSIPARM user data set. When you integrate the following ISM commands, you can go directly to certain areas of the ISM program from STATMON:

- ISMCMD—ISM full-screen resource panel
- ISM—Main menu
- ISMR—Resource menu
- ISMSUM—Status summary
- ISMMGR—List ISM resources

To integrate the ISM commands on the STATMON Command Menu, follow these steps:

Step 1 Enter Edit mode for the **DSICNM** member of your DSIPARM data set.

Step 2 Copy member ISMCNM2 from prefix.NSPI202.NSPNSAMP after the C STATS statement.

Step 3 To enable the commands on the menu, type the following commands from a NetView command prompt and press **Enter**:

STOPCNM STATMON

STARTCNM STATMON

Figure 3-1 STATMON Menu with ISM Commands

Verifying the ISM Installation

After you complete all installation tasks and update and restart NetView, make sure the installation was successful by completing the following verification tasks:

Verifying the ISM Commands from NetView

The following procedure verifies that the ISM commands have been added to the NetView procedure:

Step 1 From a NetView command prompt, type the following command and press **Enter**:

DISPMOD NSPDS

Step 2 Verify that the following text is displayed after you enter the DISPMOD NSPDS command. The data on the second line of the display might vary depending upon your maintenance level.

```
CNM263I MODULE   LENGTH CSECT    DATE     PTF     EPA      AM ATTR
CNM263I NSPDS    000BC0 -------- -------- ------- 0004E440 24 RN RU
CNM265I END OF DISPLAY
```

Verifying the Operation of the ISM Tasks

This section describes the procedure to verify that the ISM tasks have been started and that member ISMDMN is included in NetView. It also verifies that the task member statements for each of the VSAM tasks are located in the NetView DSIPARM.

To verify that the ISM tasks are working properly, complete the following steps:

Step 1 From a NetView command prompt, type the following command and press **Enter**:

LIST NSPDSA

Step 2 Verify the following text after you enter the **LIST NSPDSA** command:

```
* CNM56    LIST NSPDSA
- CNM56    TYPE: OPT TASKID: NSPDSA   TASKNAME: NSPDSA   STATUS:
ACTIVE
- CNM56    MEMBER: NSPDSA
- CNM56    PRIMARY:NSPDSA   STATUS:ACTIVE   SECONDARY:NONE
STATUS:INACTIVE
- CNM56    LOADMOD: DSIZDST
- CNM56    Task Serial:  13
```

```
- CNM56    Messages  Pending:  0  Held:  0
- CNM56    END OF STATUS DISPLAY
```

If this text does not appear, see Chapter 6, "Troubleshooting."

Step 3 Repeat Steps 1 and 2 with the following commands and verify that a corresponding display for each task appears:

- LIST NSPDSC
- LIST NSPDSD
- LIST NSPDSH
- LIST NSPDSI
- LIST NSPDSM
- LIST NSPDSN
- LIST NSPDSR
- LIST NSPDSW

Verifying the ISM Commands and Panels

This section describes the procedure to verify that the ISMCMD member has been included in NetView. To verify that the ISM commands and panels are available, complete the following step:

Step 1 From a NetView command prompt, type the following command and press **Enter**:

BR ISM

Verify the NSPMAIN4 CLIST is displayed, as shown in Figure 3-2.

Figure 3-2 Verify ISM Clist Installation

Verifying the ISM Autotasks

Complete the following steps to verify that the ISMOPF member has been included in NetView:

Step 1 From a NetView command prompt, type the following command and press **Enter**:

LIST ISMADMIN

Step 2 Verify that the following message is displayed after you enter the LIST ISMADMIN command:

```
DSI008I 'ISMADMIN' NOT ACTIVE
```

If the message "DSI077A 'ISMADMIN' STATION NAME UNKNOWN" appears, then the ISM autotask has not been included in NetView. See the "ISM Task Not Known to NetView" section under the "Troubleshooting ISM Installation Problems" section in Chapter 6, “Troubleshooting.”

Verifying the ISM VSAM Commands

Complete the following steps to verify that the ISM VSAM commands are working correctly:

Step 1 From a NetView command prompt, type the following command and press **Enter**:

NSPDS A UPD ISMTEST THIS IS A TEST

Step 2 Verify that the following messages are displayed:

```
NSP1910I REQUEST HAS BEEN QUEUED
NSP1900I ISMTEST INSERTED
```

Step 3 Repeat Step 1 replacing ISMTEST with **ISMTEST1**.

Step 4 Type the following command and press **Enter** to display the ISMTEST record:

NSPDS A REDK ISMTEST

Step 5 Verify that the following messages are displayed:

```
NSP1910I REQUEST HAS BEEN QUEUED
NSP1900I ISMTEST THIS IS A TEST
```

Step 6 Type the following command and press **Enter** to display the records:

NSPDS A LIST ISMTEST ISMTEST1

Step 7 Verify that the following messages are displayed:

```
NSP1910I REQUEST HAS BEEN QUEUED
NSP1900I ISMTEST THIS IS A TEST
NSP1900I ISMTEST1 THIS IS A TEST
NSP1901I END OF LISTING
```

Step 8 Type the following command and press **Enter** to remove the records from the database:

NSPDS A KEYD ISMTEST ISMTEST1

Step 9 Verify that the following messages are displayed:

```
NSP1910I REQUEST HAS BEEN QUEUED
NSP1900I ISMTEST ERASED
NSP1900I ISMTEST1 ERASED
NSP1901I TOTAL RECORDS ERASED = 2
```

Planning the Next Steps

The following sections describe the next steps you should perform to install ISM according to your site's current configuration.

- If you are an existing ISM V1R3.0 site and you have completed the installation and verification procedures, you are ready to convert your files. Proceed with the tasks in Chapter 4, “Migrating from a Prior Release of ISM.”
- If this is the first time for ISM to be installed at your site and you have completed the installation and verification procedures, you are ready to configure the ISM program to manage your resources. Proceed with the tasks in Chapter 5, “Configuring ISM.”

Migrating from a Prior Release of ISM

ISM V2R2 does not coexist with ISM releases prior to V2R0. If your site uses ISM Release V1R3.0, you can migrate existing mainframe definitions and user profiles to ISM V2R2.

This chapter includes the following sections:

Migrating from ISM V2R0

The configuration files for ISM V2R2 and V2R0 are upward compatible.

You can use your ISM V2R0 VSAM files with ISM V2R2.

Note If you update the ISM setup for V2R2, then revert to ISM V2R0 and update the setup, you will lose your settings that are new in ISM V2R2.

Migrating from ISM V1R3.0

If you are migrating from ISM V1R3.0, you can follow the procedures in the "Migrating from ISM V1R3.0" and "Uninstalling ISM V1R3.0" chapters of "CiscoWorks Blue ISM Installation Guide V2R1.0". These procedures will allow you to convert you existing ISM V1R3.0 router definitions and operator profiles to the format used by ISM version 2.

Benefits of Migrating

Benefits of migrating ISM V1R3.0 data to ISM V2 include:

- Use ISM V1R3.0 router definitions, and operator profiles from ISM V2.
- Execute ISM V1R3.0 by using a procedure from a previous NetView version. However, you must first back up the NetView **DSIPARM** data set, and the NetView procedure used in ISM V1R3.0.
- Use all router management functions within the enhanced ISM V2 environment.

Handling ISM Data

Migrating ISM V1R3.0 router definitions and configuration data converts a copy of your existing data files so they are compatible with ISM V2. The original ISM V1R3.0 data files remain intact.

When you migrate your ISM V1R3.0 installation, you convert a copy of your existing ISM V1R3.0 data files to the new VSAM key structures and new VSAM data sets that are supported in ISM V2.

Converting ISM V1R3.0 Files

After completing the ISM V2 installation, you must convert ISM V1R3.0 files. To convert the ISM V1R3.0 files:

Step 1 Copy member **NSPDSB** from the **NSPI200** samplib to the NetView **DSIPARM** data set used in the conversion. The NetView **CLIST**s automatically perform the conversion functions:

- NSPCONVR—Converts the router control files
- ISMCONVU—Copies the ISM V1R3.0 operator profiles to the ISM V2 control data set

Step 2 Run NetView with ISM V2.

Step 3 From a NetView command prompt, enter the following command:

ALLOCATE FI(NSPDSB) DS(xxxxx) SHR

Where *xxxxx* is the name of the **NSPDSA** data set used for ISM V1R3.0.

NetView responds as follows:

```
CNM272I NSPDSB IS NOW ALLOCATED
```

Step 4 From a NetView command prompt, enter the following command:

Start task=nspdsb

NetView responds as follows:

```
DSI166I NSPDSB IS ACTIVATED BY HAL2
DSI556I NSPDSB : VSAM DATASET 'OPEN' COMPLETED, DDNAME = 'ISMDSB'
RETURN CODE = X'00', ACB ERROR FIELD = X'00'
DSI530I 'NSPDSB  ' : 'DST' IS READY AND WAITING FOR WORK
```

Step 5 From a NetView command prompt, enter the following command:

nspconvu

NetView responds as follows:

```
NSPCONVU 105 User Records Copied.
```

Step 6 When the NSPCONVU command executes, type the **nspconvr** and press **Enter.**

Step 7 Verify that the output is similar to the following output and that you receive the "NSPR to IR Conversion complete" message:

```
* CNM01 NSPCONVR
C CNM01 NSPCONVR 170 Records Converted
>>This means that 85 routers were migrated.
```

```
Each router from ISM Release 2 will be converted to two records in
ISM Version 2.
C CNM01 NSPCONVR NSPR to IR Conversion Complete
```

Planning the Next Steps

Once you have migrated to ISM V2R2, you must configure the ISM setup options.

CHAPTER 5

Configuring ISM

This chapter describes how to start ISM and configure its setup options. If you are responsible for installing ISM on the mainframe, complete the following tasks before configuring ISM:

Step 1 Read Chapter 1, “Preparing to Install ISM,” to verify the system requirements.

Step 2 Perform the tasks described in Chapter 2, “Configuring the Mainframe-to-Router Link.”

Step 3 Perform the tasks described in Chapter 3, “Installing ISM.”

Step 4 Optional step for existing ISM sites: Perform the tasks described in Chapter 4, “Migrating from a Prior Release of ISM.”

Note If you want to convert your existing ISM router configurations and user profiles, you should convert your ISM V1R3.0 data before configuring ISM.

This chapter describes how to enable an ISM management environment and administrator profile.

If you are a new ISM site, you must configure the following ISM setup options and user profiles:

- ISM applications, or features to use
- Types of router interfaces to monitor
- Monitoring interval for ISM to check routers and interfaces

- CPU and memory performance thresholds that you want to define
- User profiles for those operating ISM

After you have installed and verified the ISM installation, you must enable the ISM management environment. Then you can start ISM to configure its administrator and user profiles and add its router definitions.

Configuring ISM for the first time includes the following tasks:

- Enabling the ISM Management Environment, page 5-2
- Starting ISM, page 5-7
- Running ISM, page 5-8
- Defining ISM User Profiles, page 5-9
- Creating, Changing, or Deleting User Profiles, page 5-11
- Adding Router Definitions, page 5-13

Enabling the ISM Management Environment

The ISM resource management setup options comprise four panels. To move back and forth among the panels when specifying options, use the **F7** and **F8** keys. When you have finished selecting the options, specify how you want the options to be implemented by selecting **Change Type** and **Action Type** on the first ISM Resource Management Setup panel (Figure 5-1) and then press **F4** to build the setup records.

Tip If you need more information about using an ISM panel, access online Help by pressing **F1**.

To start the ISM setup for the first time, complete the following steps:

Step 1 From a NetView command prompt, type the **ismsetup** command and press **Enter**. The “ISM Resource Management Setup—First Panel” (Figure 5-1) is displayed.

Note The first user to run the **ismsetup** command is automatically defined as an ISM administrator.

Figure 5-1 ISM Resource Management Setup—First Panel

Step 2 In the Applications section, type **Y** under the **Update** column to enable the ISM features you want to use.

Note If you are going to use the SNA Session Monitoring application, the ISM VTAM exit must be installed to support this function. For more information about installing this exit, see "Installing the VTAM XID Exit Routine" section in Chapter 3, “Installing ISM.”

Step 3 To display the “ISM Resource Management Setup—Second Panel (ISM Rules)” (Figure 5-2), press **F8**.

Note For more information on enabling SNMP and TN3270, see the *CiscoWorks Blue Internetwork Status Monitor User Guide.*

Figure 5-2 ISM Resource Management Setup—Second Panel (ISM Rules)

- Use the second ISM Resource Management Setup panel to enable the rules and change the ISM defaults.
- Press **Enter** to set the default values.

Step 4 To display the "ISM Resource Management Setup—Third Panel" (Figure 5-3), press **F8**.

Figure 5-3 ISM Resource Management Setup—Third Panel

Use the "ISM Resource Management Setup—Third Panel" (Figure 5-3) to enable the monitoring intervals and specify the router and CMCC thresholds to be monitored:

- To specify a monitoring threshold, type a 2-digit numeric value for the percentage of the CPU and memory that ISM monitors. If a threshold is exceeded, ISM flags the router with an alert status on the router Status panel.
- To stop measuring the threshold, type **00** for the CPU Utilization or Free Memory option.

Step 5 Press **F8** to display the "ISM Interface Management Setup—Fourth Panel" (Figure 5-4).

Figure 5-4 ISM Interface Management Setup—Fourth Panel

- The ISM Interface Management Setup—Fourth Panel enables interface monitoring. You can select the specific types of interfaces ISM monitors.
- To enable interface monitoring, type **Y** for the Application: Interface Monitoring option. For the Interfaces to be monitored option, type **Y** for each interface you want ISM to monitor.
- By default, ISM also monitors subinterfaces if the interface type is monitored. Place an "N" in the "Sub" column to suppress monitoring of that type of subinterface.
- To enable interface reliability threshold monitoring, enter the threshold value in the "Thresh" column. If the interface reliabilty as reported by the IOS "show interface" command it less than or equal to the threshold value, ISM will write an NSP1580I message to the NetView log. A threshold value of 0 suppresses reliability threshold monitoring.

Note Shorter monitoring intervals will result in greater resource consumption.

Step 6 Press **F8** to display the “ISM Resource Management Constants Setup—Fifth Panel” (Figure 5-5). Here you can view the ISM defaults for database constants, variables, and wrap counts.

Figure 5-5 ISM Resource Management Constants Setup—Fifth Panel

Caution The database IDs on this panel can be modified only prior to initializing ISM for the first time.

Step 7 Press **F4** to save the management record and exit the ISM Resource Management Setup panel.

Starting ISM

Once you have installed and configured ISM V2 (and converted the ISM V1R3.0 data files, if applicable), you can start ISM and enable the user profiles and router definitions. If **ISMMGR** is already active, enter the following:

Stop Tasks=ismmgr

If the ISM autotask is not started by NetView, you can perform one of the following tasks to start ISM:

- To start the autotask, type the following command from a NetView command prompt:

  autotask opid=ismmgr

- Restart NetView to automatically start the autotask that you specified in the production NetView **CLIST**.

Running ISM

To run ISM complete the following steps:

Step 1 Log in to NetView.

Step 2 At the command line on the NetView main menu panel, type **ism** and press **Enter**. The ISM main menu panel (Figure 5-6) is displayed.

Figure 5-6 Internetwork Status Monitor (ISM) Main Menu Panel

Note The contents of the ISM main menu panel depend on which applications you select when performing **ISMSETUP**.

Defining ISM User Profiles

ISM user profiles provide the following functions:

- Administration—Specifies the operator ID and authority to perform ISM and router functions.
- Enabled User—Permits modification to the rules used to monitor routers.
- Disabled User—Permits operation of ISM in a "read-only"mode.

For existing ISM V1R3.0 sites that have converted the ISM configuration data by running the **CLIST NSPCONVU**, the existing ISM V1R3.0 user profile records are available from ISM V2. You must define the user profiles if you want to add new operators.

For new ISM V2 sites, the ISM user profiles must be defined by an ISM administrator. By default, the first user to run **ismsetup** is automatically defined as an administrator by ISM.

In order to use ISM, the operator must have an ISM profile.

Overview of Operator Types

The ISM user profile management function provides four operator types. Each type dictates the actions an operator can perform using ISM.

When using the WEB interface, all operators are disabled users.

ISM operator types are:

- Enabled ISM Administrator
- Disabled ISM Administrator
- ISM Enabled User
- ISM Disabled User

ISM administrators maintain the ISM management environment. They assign the "authority levels" to ISM users. An ISM administrator can be an ISM Enabled User as well.

An ISM Enabled User may issue Cisco IOS software enable commands—an ISM Disabled User may not.

A disabled ISM administrator may perform the following operations:

- Create operator profiles and assign user authority
- Configure and change the ISM management environment
- Set group filters

An enabled ISM administrator can perform the following operations:

- Issue the Cisco IOS software enable command and issue commands that control and configure Cisco routers
- Add, modify, or delete router and DSPU router definitions
- Modify interface settings

An ISM Enabled User is defined by an **E** in the router Enable Authority option on the ISM User Administration panel (Figure 5-8). An ISM Disabled User is defined by a **D** in the router Enable Authority option on the ISM User Administration panel.

Note You must know the password to a router to issue the **enable** command. If the router supports TACACS, you must know the userid and password as well.

An ISM Disabled User may do the following:

- Collect and display data with which to monitor the status of the Cisco routers, interfaces, and other routers in their network
- Set status filters

An ISM Enabled User may do the following (in addition to the above tasks):

- Issue the Cisco IOS software enable command and issue commands that control and configure Cisco routers
- Add, modify, or delete router and DSPU router definitions
- Modify interface settings

Creating, Changing, or Deleting User Profiles

All ISM users should have an operator profile for identification and status filtering purposes. Only an ISM administrator can create or change an authority level of another operator's profile.

To create or change an operator profile, complete the following steps:

Step 1 To access the Cisco router User Administration panel, use one of the following methods:

- Type **ism** and press **PF 8**.
- Position the cursor on the USER line and press **Enter**.
- If you are an ISM administrator and are creating or changing an operator's profile, position the cursor in the ID field on the ISM Administration menu panel, enter the operator's name, and press **Enter**.

The ISM User Administration panel (Figure 5-7) is displayed.

Figure 5-7 ISM User Administration Panel

Step 2 To use the ISM User Administration panel to enable the operator authority (if you are an ISM administrator), complete one of the following tasks:

- To define a Disabled ISM Administrator, type **Y** for ISM Administrator Authority and **D** for Router Disable Authority.
- To define an Enabled ISM Administrator, type **Y** for ISM Administrator Authority and **E** for Router Enable Authority.
- To define an ISM Disabled User, type **N** for ISM Administrator Authority and **D** for Router Enable Authority.
- To define an ISM Enabled User, type **N** for ISM Administrator Authority and **E** for Router Enable Authority.

Step 3 To use the ISM User Administration panel to enable group filters, type **Y**. To view a set of routers assigned to a group name, type the name of the router group (up to two) that you want to view.

The routers defined to the specified group name will be the only routers to appear on the ISM Router Status and Status Summary panels.

Step 4 To use the ISM User Administration panel to enable status filters, type **Y** and perform the following tasks:

- To view routers with a certain status, type **I** in the Exclude/Include option and specify the status type (up to three) to view.

  The routers with the specified status will be the only routers to appear on the ISM Router Status Panel.

- To disable viewing of routers with a certain status, type **X** in the Exclude/Include option and specify the type of status (up to three) that you want to exclude.

  The routers with the specified status will not appear on the ISM Router Status Panel.

Step 5 To save the user profile, perform the following tasks:

a. Specify a value for the record Change Type (**1** for new or **2** for update).

b. Type **3** for the record Action Type to permanently update the record.

c. Press **F4** to update the record.

Adding Router Definitions

Now that you have installed and configured ISM on your mainframe, the next step is to add your router definitions and begin monitoring them using ISM. For detailed information about adding router definitions and using ISM to manage your Cisco routers, see the CiscoWorks Blue Internetwork Status Monitor User Guide.

If you have ISM V1R3.0 installed at your site and have converted your router definitions using the CLIST NSPCONVR, you can access these definitions and update them from ISM V2.

Troubleshooting

This chapter describes the procedures for troubleshooting problems you may encounter when installing ISM:

Mainframe-to-Router Link Configuration Problems

This section describes procedures to determine the following router configuration problems:

Router Is Not Defined to VTAM

Problem

If the router is not defined to VTAM, then you may see the following conditions when you execute a **runcmd** command for the router or try to display it from VTAM:

- Executing **runcmd sp=***router_name***,appl=console,show ?** produces the following message:

- CNM01 DSI358I RUNCMD FAILED. ID'*router_name*' IS INVALID, SENSE CODES = X'08060000'

- Executing **d net,id=***router_name* produces the following message:

```
CNM01 IST453I ID PARAMETER VALUE INVALID
```

These messages indicate that an SSCP-to-PU session has not been established between VTAM and the router. Another possible cause for the error is that the **uservarname** command has been specified on the ID operand of the **display ncpstor** command.

Action

To define the router in VTAM, see the "Configuring a VTAM Connection" section on page 2-3.

Router Is Not Active

Problem

If the router is defined to VTAM, but a connection has never been established, you may see the following conditions when you execute a **runcmd** command for the router or try to display the router from VTAM:

- Executing **runcmd sp=***router_name***,appl=console,show ?** produces the following message:

  - CNM01 DSI264I RUNCMD FAILED FOR *router_name* -
  RTNCD=X'04',FDBK2=X'04',
  SYSTEM SENSE=X'0807',USER SENSE=X'0000'

- Executing **d net,id=***router_name* produces the following message:

```
  CNM01  IST097I DISPLAY ACCEPTED
` CNM01
IST075I NAME=router_name    , TYPE=PU_T2
IST486I STATUS=CONCT   , DESIRED STATE=CONCT
IST1043I CP NAME=***NA***,CP NETID=NETA  ,DYNAMIC LU=YES
IST136I SWITCHED SNA MAJOR NODE=SWDRTRS
IST654I I/0 TRACE=OFF,BUFFER TRACE=OFF
IST1500I STATE TRACE=OFF
IST314I END
```

Action

Verify that the configuration arguments for the router's VTAM definition correspond to the SNA service point configuration by completing the following steps:

Step 1 Telnet to the router and run the **show sna** command.

- If the PU STATUS=ACTIVE, then the router probably has a session to VTAM but is using the wrong XID.
- If the PU STATUS=XID, then the router is attempting to contact VTAM but has not had a response. This can indicate any of the following problems:
  - No path to VTAM
  - XID mismatch
  - *rmac* argument in the router's SNA host configuration does not match the *mac_address* argument on the MVS system

Step 2 From VTAM, execute the **debug sna packet** command to verify that the router is sending an XID request every 30 seconds.

If the XID does not exist on the MVS system, the MVS log shows a VTAM message indicating a mismatch. VTAM writes a message to the log whenever it receives an XID that it does not recognize.

For more information on verifying your configuration, see the "Correlating the Router and VTAM Configuration Information" section on page 2-9.

Router Service Point Is Disabled

Problem

If the router is active, but the service point is disabled, you may see the following conditions when you execute a **runcmd** command for the router or try to display the router from VTAM:

- Executing **runcmd sp=***router_name***,appl=console,show ?** produces the following message:

  - CNM01 DW0614E RUNCMD REQUEST NOT PERFORMED BY ID *router_name* FOR APPL='CONSOLE',SENSE CODE=X'080C005' FUNCTION INACTIVE

- Executing **d net,id=***router_name* produces the following message:

```
  CNM01 IST097I DISPLAY ACCEPTED
` CNM01
IST075I NAME=router_name   , TYPE=PU_T2.1
IST486I STATUS=ACTIV   , DESIRED STATE=ACTIV
IST1043I CP NAME=router_name, CP NETID=NETA  ,DYNAMIC LU=YES
IST136I SWITCHED SNA MAJOR NODE=SWDLURSJ
IST654I I/O TRACE=OFF,BUFFER TRACE=OFF
IST1500I STATE TRACE=OFF
IST314I END
```

Action

If the service point has not been enabled, see the "Configuring the Router" section on page 2-4.

If you need further information on configuring the router service point, see the Cisco IOS software *Bridging and IBM Networking Configuration Guide* and *Bridging and IBM Networking Command Reference*.

ISM Installation Problems

This section describes the procedures for diagnosing problems which may be found during verification of the ISM installation:

ISM Task Not Known to NetView

Problem

If you receive the error message "DSI077A 'NSPDSR' STATION NAME UNKNOWN" after issuing the **list** *taskname* command from NetView, then the ISM task has not been included in the DSIDMN member of the NetView DSIPARM data set.

Action

You can start the task manually for the current system, and then update the DSIPARM data set to fix the problem permanently.

Step 1 To manually start the unknown task, enter the following command from a NetView console (where *taskname* is the name of the unknown task, and *membername* is the DD name in the DSIDMN member of NetView's DSIPARM data set):

START TASK=*taskname***,MOD=DSIZDST,MEM=***membername***,PRI=6**

Step 2 Verify that the corresponding display is similar to the following for your taskname:

```
DSI166I NSPDSR IS ACTIVATED BY HAL2
DSI556I NSPDSR : VSAM DATASET 'OPEN' COMPLETED, DDNAME =
'NSPHISTR'
RETURN CODE = X'00', ACB ERROR FIELD = X'00'
DSI530I 'NSPDSR ' ; 'DST' IS READY AND WAITING FOR WORK
```

Step 3 To update NetView permanently, complete the tasks described in the "Updating the DSIPARM Members" section in Chapter 3, "Installing ISM."

ISM Task Not Started

Problem

If you receive the message "STATUS: NOT ACTIVE" after issuing the **list** *taskname* command from NetView, then the ISM task has not been started by NetView.

Action

You can start the task manually for the current system, and then update the DSIPARM data set to fix the problem permanently.

Step 1 To manually start the task, enter the following command from a NetView console:

START TASK=*taskname*

Step 2 Verify that the corresponding display is similar to the following for your taskname:

```
DSI166I NSPDSR IS ACTIVATED BY HAL2
DSI556I NSPDSR : VSAM DATASET 'OPEN' COMPLETED, DDNAME =
'NSPHISTR'
RETURN CODE = X'00', ACB ERROR FIELD = X'00'
DSI530I 'NSPDSR ' ; 'DST' IS READY AND WAITING FOR WORK
```

Step 3 To update NetView permanently, complete the tasks described in the "Updating the DSIPARM Members" section in Chapter 3, "Installing ISM."

VSAM Data Set Not Available to NetView

Problem

If you receive the messages "DSI553I *taskname*: ERROR OCCURRED DURING VSAM 'OPEN' PROCESSING IN 'PRIMARY'" and "DSI554I *taskname*: DST VSAM SERVICES INITIALIZATION HAS FAILED" after issuing the **list** *taskname* command from NetView, then the corresponding VSAM data set for the task is not available to NetView.

Action

You can dynamically allocate the data set to NetView for the current system, and then update the DSIPARM data set to fix the problem permanently by completing the following tasks:

Step 1 To dynamically allocate the VSAM data set, enter the following command from a NetView console:

ALLOCATE DS(vsam.dataset) F1(ddname) SHR

Where *vsam.dataset* is the name of the unavailable VSAM data set, and *ddname* is the DD name in the DSIDMN member of NetView's DSIPARM data set.

Step 2 Verify that the corresponding display is similar to the following for your VSAM DD name:

```
CNM272I NSPHISTR IS NOW ALLOCATED
```

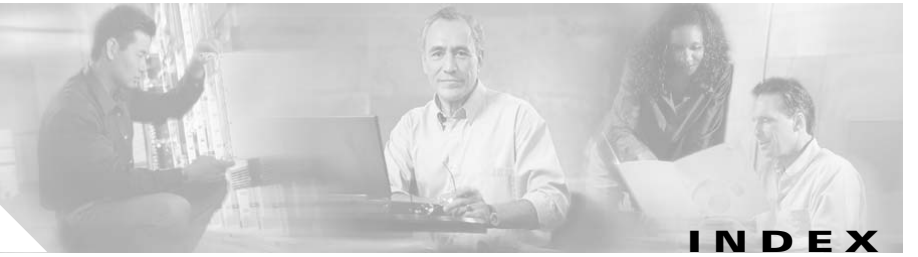
Step 3 To start the task associated with the VSAM data set manually, enter the following command from a NetView console:

START TASK=*taskname*

Step 4 Verify that the corresponding display is similar to the following for your taskname:

```
DSI166I NSPDSR IS ACTIVATED BY HAL2
DSI556I NSPDSR : VSAM DATASET 'OPEN' COMPLETED, DDNAME =
'NSPHISTR'
RETURN CODE = X'00', ACB ERROR FIELD = X'00'
DSI530I 'NSPDSR ' ; 'DST' IS READY AND WAITING FOR WORK
```

Step 5 To update NetView permanently, complete the tasks described in the "Updating NetView" section in Chapter 3, "Installing ISM." Be sure that the corresponding DD statement for this data set has been added to your NetView procedure.



A

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

V

X