Catalyst 6500 Series Switch and Cisco 7600 Series Internet Router
Network Analysis Module Installation and Configuration Note
Release 3.1(1)
May 2003

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

Customer Order Number:
Text Part Number: 78-15354-01
THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco’s installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco’s written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

This document is to be used in conjunction with the documents listed in the “Related Documentation” section.

Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networks logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0501R)

Copyright © 2003 Cisco Systems, Inc. All rights reserved.
Preface vii

Audience vii
Organization viii
Conventions viii
Safety Overview ix
Related Documentation xi

Obtaining Documentation xi
Cisco.com xi
Documentation CD-ROM xii
Ordering Documentation xii
Documentation Feedback xii

Obtaining Technical Assistance xiii
Cisco.com xiii
Technical Assistance Center xiii
Cisco TAC Website xiv
Cisco TAC Escalation Center xiv

Obtaining Additional Publications and Information xiv

CHAPTER 1 1-1

Overview 1-1
Before You Begin 1-2
Understanding How the NAM Works 1-3
Understanding How the NAM Uses SPAN 1-3
Understanding How the NAM Uses VACLs 1-5
Understanding How the NAM Uses NDE 1-6
Managing the NAM 1-7
New NAM Features 1-8
Monitoring 6500/7600 WAN Interfaces Through VACL 1-8
WAN Monitoring Through NetFlow Data Export (NDE) from Remote Routers and Switches 1-8
Historical Reporting 1-9
VLAN Traffic Statistics 1-9
Multiple NAM Configuration Support 1-9
Online Documentation Enhancements 1-9
Front Panel Description 1-9
STATUS LED 1-10
Chapter 2  Installing the NAM  2-1

System Requirements  2-1
  Memory and Storage Requirements  2-1
Software Requirements  2-2
Hardware Requirements  2-3
Required Tools  2-3
Installing and Removing the NAM  2-3
  Slot Assignments  2-4
  Removing a Module  2-5
  Installing a Module  2-6
  Verifying the Installation  2-12
    Cisco IOS Software  2-12
    Catalyst Operating System Software  2-13

Chapter 3  Getting Started  3-1

Configuring the NAM  3-1
  Cisco IOS Software  3-2
    Initial Configuration  3-2
    Configuring VLANs  3-5
  Catalyst Operating System Software  3-5
    Initial Configuration  3-5
    Configuring VLANs  3-8
    Configuring the SNMP Agent  3-8
Configuring Traffic Sources for Capturing NAM Traffic  3-10
  Cisco IOS Software  3-11
    Using SPAN as a Traffic Source  3-11
    Using VACL as a Traffic Source  3-13
    Using NetFlow Data Export as a Traffic Source  3-14
  Catalyst Operating System Software  3-17
    Using SPAN as a Traffic Source  3-17
    Using LAN VACL as a Traffic Source  3-17
    Using NetFlow Data Export as a Traffic Source  3-18
Operating-System-Independent Configuration  3-20
  Configuring Automatic RMON Collections  3-20
  Configuring the HTTP or HTTP Secure Server  3-21
  Configuring the HTTP Server  3-21
Contents

CHAPTER 4
Administering the NAM 4-1
Cisco IOS Software 4-1
Logging In to the NAM 4-1
Changing the NAM CLI Passwords 4-3
Resetting the NAM 4-4
Upgrading the NAM Software 4-5
Upgrading the NAM Application Software 4-5
Upgrading the NAM Maintenance Software 4-8
Configuring Mini-RMON 4-11
Catalyst Operating System Software 4-11
Logging In to the NAM 4-12
Changing the NAM CLI Passwords 4-13
Resetting the NAM 4-15
Upgrading the NAM Software 4-17
Upgrading the NAM Application Software 4-17
Upgrading the NAM Maintenance Software 4-19
Configuring Mini-RMON 4-20
Operating-System-Independent NAM Administration 4-20
Adding NAM Patch Software 4-21
Additional NAM Software Administrative Commands 4-22
Cisco IOS Commands 4-28
EXEC Commands 4-29
Configuration Commands 4-30
Global Configuration Mode 4-30
Interface Configuration Mode 4-30
Unsupported Supervisor Engine CLI Commands 4-30

CHAPTER 5
Troubleshooting the NAM 5-1
Netflow Data Export 5-1
Web Application 5-1
NDE Flow Records Interfaces 5-4
Interface Special (0) 5-6
NDE Flow-mask and v8 Aggregation Cache 5-6
Error Messages 5-8
<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Username and Password Guidelines</td>
<td>5-13</td>
</tr>
<tr>
<td>Supported MIB Objects</td>
<td>5-15</td>
</tr>
<tr>
<td>Local Interfaces in the NAM ifTable</td>
<td>5-19</td>
</tr>
</tbody>
</table>
Preface

Product Numbers:
WS-SVC-NAM-1
WS-SVC-NAM-2
WS-X6380-NAM

This publication describes how to install the Catalyst 6500 series switch and Cisco 7600 series Internet Router Network Analysis Module (NAM) and how to configure the NAM using the command-line interface (CLI) for the operating system supporting your NAM (Cisco IOS or the Catalyst operating system).

You can also use the NAM Traffic Analyzer application to configure the NAM. The traffic analyzer online help and user guide describe its use.

See the “Related Documentation” section on page xi for more information about software configuration for the switch.

Although NAM software release 3.1 does support the WS-X6380-NAM, this publication does not describe the WS-X6380-NAM in detail. This publication does describe the configuration differences between the WS-SVC-NAM-1, WS-SVC-NAM-2, and the WS-X6380-NAM when necessary.

For additional information about the WS-X6380-NAM, refer to the Catalyst 6000 Network Analysis Module WS-X6380-NAM documentation.

Note
For translations of the warnings in this publication, see the “Safety Overview” section on page ix and refer to the Regulatory Compliance and Safety Information for the Catalyst 6500 series switch and Cisco 7600 series Internet Router.

Note
Third-party software used under license accompanies the Network Analysis Module software, Release 3.1. Notices that may apply to the license and to the use of such third-party software are listed in the Release Notes for Catalyst 6500 Series and Cisco 7600 Series Network Analysis Module, software release 3.1.

Audience

Only trained and qualified service personnel (as defined in IEC 60950 and AS/NZS3260) should install, replace, or service the equipment described in this publication.
Organization

This publication is organized as follows:

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1</td>
<td>Overview</td>
<td>Presents an overview of the Catalyst 6500 series and Cisco 7600 series Network Analysis Module (NAM).</td>
</tr>
<tr>
<td>Chapter 2</td>
<td>Installing the NAM</td>
<td>Describes how to install the NAM.</td>
</tr>
<tr>
<td>Chapter 3</td>
<td>Getting Started</td>
<td>Describes how to configure the NAM.</td>
</tr>
<tr>
<td>Chapter 4</td>
<td>Administering the NAM</td>
<td>Describes how to administer the NAM from the CLI for each switch operating system.</td>
</tr>
<tr>
<td>Chapter 5</td>
<td>Troubleshooting the NAM</td>
<td>Provides troubleshooting information for the NAM.</td>
</tr>
</tbody>
</table>

Conventions

This publication uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong> font</td>
<td>Commands, command options, and keywords are in <strong>boldface</strong>.</td>
</tr>
<tr>
<td><em>italic</em> font</td>
<td>Arguments for which you supply values are in <em>italics</em>.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>{ x</td>
<td>y</td>
</tr>
<tr>
<td>[ x</td>
<td>y</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td><strong>screen</strong> font</td>
<td>Terminal sessions and information the system displays are in <strong>screen</strong> font.</td>
</tr>
<tr>
<td><strong>boldface screen</strong> font</td>
<td>Information you must enter is in <strong>boldface screen</strong> font.</td>
</tr>
<tr>
<td><em>italic screen</em> font</td>
<td>Arguments for which you supply values are in <em>italic screen</em> font.</td>
</tr>
<tr>
<td>^</td>
<td>The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.</td>
</tr>
<tr>
<td>&lt; &gt;</td>
<td>Nonprinting characters, such as passwords are in angle brackets.</td>
</tr>
</tbody>
</table>
Notes use the following conventions:

**Note** Means reader take note. Notes contain helpful suggestions or references to material not covered in the publication.

Tips use the following conventions:

**Tip** Means the following information will help you solve a problem. The tips information might not be troubleshooting or even an action, but it could be useful information, similar to a Timesaver.

Cautions use the following conventions:

**Caution** Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

## Safety Overview

Safety warnings appear throughout this publication in procedures that, if performed incorrectly, may harm you. A warning symbol precedes each warning statement.

**Warning** This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. To see translations of the warnings that appear in this publication, refer to the Regulatory Compliance and Safety Information document that accompanied this device.

**Waarschuwing** Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico’s en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen. Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het document Regulatory Compliance and Safety Information (Informatie over naleving van veiligheids- en andere voorschriften) raadplegen dat bij dit toestel is ingesloten.

**Varoitus** Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytköntöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. Tässä julkaisussa esiintyvien varoitusten käänänkiset löydät laitteen mukana olevasta Regulatory Compliance and Safety Information -kirjapainesta (määräysten noudattaminen ja tietoa turvallisuudesta).
Attention  Ce symbole d’avertissement indique un danger. Vous vous trouvez dans une situation pouvant causer des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions d’avertissements figurant dans cette publication, consultez le document Regulatory Compliance and Safety Information (Conformité aux réglements et consignes de sécurité) qui accompagne cet appareil.


Avvertenza  Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nel documento Regulatory Compliance and Safety Information (Conformità alle norme e informazioni sulla sicurezza) che accompagna questo dispositivo.

Advarsel  Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du vare oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. Hvis du vil se oversettelser av deadvarslene som finnes i denne publikasjonen, kan du se i dokumentet Regulatory Compliance and Safety Information (Overholdelse av forskrifter og sikkerhetsinformasjon) som ble levert med denne enheten.

Aviso  Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos físicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. Para ver as traduções dos avisos que constam desta publicação, consulte o documento Regulatory Compliance and Safety Information (Informação de Segurança e Disposições Regulatórias) que acompanha este dispositivo.

¡Advertencia!  Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. Para ver una traducción de las advertencias que aparecen en esta publicación, consultar el documento titulado Regulatory Compliance and Safety Information (Información sobre seguridad y conformidad con las disposiciones reglamentarias) que se acompaña con este dispositivo.

Related Documentation

- For additional FCC class compliance information, refer to the Catalyst 6500 Series Switch Regulatory Compliance and Safety Information publication.
- For additional information about the WS-SVC-NAM1 and WS-SVC-NAM-2, refer to the following:
  - Catalyst 6500 Series Switch Network Analysis Module Documentation.
  - Catalyst 6500 Series Switch and Cisco 7600 Series Internet Router Network Analysis Module Installation and Configuration Note.
  - Catalyst 6500 Series Switch and Cisco 7600 Series Internet Router Network Analysis Module Command Reference.
  - User Guide for the Network Analysis Module Traffic Analyzer Release 3.1
- For additional information about the WS-X6380-NAM, refer to the following:
  - Catalyst 6500 Series Switch Network Analysis Module Documentation.
  - Catalyst 6500 Series Switch Network Analysis Module Installation and Configuration Note.
- For additional information about the NAM Traffic Analyzer application, refer to the online help and User Guide for the Network Analysis Module NAM Traffic Analyzer Release 3.1 (available in PDF format in the online help).
- For additional information about configuring the NAM for Real Time Monitor (RTM), refer to the Configuring the Catalyst 6000 Network Analysis Module with nGenius Real-Time Monitor.
- For additional information about Catalyst 6500 series switches and command-line interface (CLI) commands, refer to the following:
  - Release Notes for Catalyst 6500 Series Switch Software Release 6.x
  - Catalyst 6500 Series Switch Software Configuration Guide
  - Catalyst 6500 Series Switch Command Reference
  - Site Preparation and Safety Guide
- For detailed hardware configuration and maintenance procedures, refer to the Catalyst 6500 Series Switch Module Installation Guide.

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com
International Cisco websites can be accessed from this URL:

Documentation CD-ROM

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

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

All users can order monthly or quarterly subscriptions through the online Subscription Store:
http://www.cisco.com/go/subscription

Ordering Documentation

You can find instructions for ordering documentation at this URL:

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click Feedback at the top of the page.

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

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.
Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world. Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL: http://tools.cisco.com/RPF/register/register.do

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.
Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:


If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

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

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:


Before calling, please check with your network operations center to determine the Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Product Catalog describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide, and the Internetworking Design Guide. For current Cisco Press titles and other information, go to Cisco Press online at this URL:
  http://www.ciscopress.com
- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:  

- *iQ* Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access *iQ* Magazine at this URL:  

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:  

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:  
Overview

This chapter describes the Catalyst 6000 series switch NAM, how it operates, and how to manage it. This chapter includes these sections:

- Before You Begin, page 1-2
- Understanding How the NAM Works, page 1-3
- Managing the NAM, page 1-7
- New NAM Features, page 1-8
- Front Panel Description, page 1-9
- Specifications, page 1-11
Before You Begin

To help you get started using the NAM, refer to this roadmap:

Getting Started with the NAM

Is the Catalyst 6500 switch installed on your network?

Yes

Begin to install the NAM

Release Notes for Catalyst 6500 Family Network Analysis Module Software Release 2.2

Catalyst 6500 Family Network Analysis Module Installation and Configuration Note

Information about the NAM in this release

Software and hardware requirements for the NAM

Installing and Removing the NAM

Configuring the NAM

Sessioning into the NAM

Setting up the IP address, host, gateway, domain, name server and SNMP information

Starting the web server on the NAM (which starts the NAM Traffic Analyzer application) and pointing your web browser at the NAM you want to configure.

Administering the NAM

Troubleshooting the NAM

No

Install and configure the NAM

If you need information about installing the 6500 family switch, refer to the following documentation.

Catalyst 6500 Family Installation Guide

Configure and use the NAM Traffic Analyzer

This guide is part of the online help for the Traffic Analyzer. To access the online help, point your web browser at the NAM and click on the Help link in the upper right of the screen.

Getting the Latest Software Information

Catalyst 6500 Release Notes

Software Configuration Guide

ATM Configuration Guide and Command Reference

System Message Guide

Troubleshooting Tips

Quick Configuration Guide

Command Reference

User Guide for the Catalyst 6500 Network Analysis Module Traffic Analyzer

Getting the Latest Software Information

Catalyst 6500 Family Installation Guide
Understanding How the NAM Works

The NAM monitors and analyzes network traffic for the Catalyst 6500 series switches and Cisco 7600 series Internet Routers using remote monitoring (RMON), RMON extensions for switched networks (SMON), and other management information bases (MIBs). (See the “Supported MIB Objects” section on page 5-15.)

The NAM monitors, analyzes, and views NetFlow on remote devices and supports the following RMON groups:

- RMON groups defined in RFC 1757
- RMON2 groups defined in RFC 2021

The NAM also can monitor individual Ethernet VLANs, which allows it to serve as an extension to the basic RMON support provided by the Catalyst 6500 series, Cisco 7600 series, Catalyst 6000 family supervisor engine.

You can use any other IETF-compliant RMON application to access link, host, protocol, and response-time statistics for capacity planning, departmental accounting, and real-time application protocol monitoring. You also can use filters and capture buffers to troubleshoot the network.

The NAM can analyze Ethernet VLAN traffic from the following sources:

- Ethernet, Fast Ethernet, Gigabit Ethernet, trunk port, or Fast EtherChannel SPAN.
  
  For more information about SPAN and RSPAN, refer to the “Configuring SPAN and RSPAN” chapter in the Catalyst 6500 Series Switch Software Configuration Guide.

- RSPAN VLAN destination port for NAM.
- VLAN Access Control Lists (VACL).
- NetFlow Data Export (NDE).
  
  For more information about NDE, refer to the Catalyst 6500 Series Switch Software Configuration Guide.

Table 1-1 Summary of Traffic Sources for NAM Monitoring

<table>
<thead>
<tr>
<th>Traffic Source</th>
<th>LAN</th>
<th>WAN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Ports</td>
<td>VLANs</td>
</tr>
<tr>
<td>VLAN Access Control List (VACL)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>NetFlow Data Export NDE (local)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>NetFlow Data Export NDE (remote)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SPAN</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Understanding How the NAM Uses SPAN

The WS-SVC-NAM-1 platform provides a single destination port for SPAN sessions. The WS-SVC-NAM-2 platform provides two possible destination ports for SPAN and VACL sessions. Multiple SPAN sessions to the NAM are supported, but they must be destined for different ports. The NAM destination ports for use by the SPAN graphical user interface (GUI) are named DATA PORT 1 and DATA PORT 2 by default. In the CLI, SPAN ports are named as shown in Table 1-2.
Table 1-2 SPAN Port Names

<table>
<thead>
<tr>
<th>Cisco IOS</th>
<th>Catalyst Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>data-port 1, data-port 2</td>
<td>For NAM-1 module number:3</td>
</tr>
<tr>
<td></td>
<td>For NAM-2 module number:7 or module number:8</td>
</tr>
</tbody>
</table>

Each of these ports is independent. You may create collections that are populated by only the traffic from one of the ports, or collections can be populated by traffic from both ports. You can still create VLAN-based collections, with packets from either port that match the specified VLAN populating such collections.

SPAN Session

A SPAN session is an association of a destination interface with a set of source interfaces; you configure SPAN sessions using parameters that specify the type of network traffic to monitor. SPAN sessions allow you to monitor traffic on one or more interfaces, or one or more VLANs, and send either ingress traffic, egress traffic, or both to a destination interface.

You can configure up to six separate SPAN sessions (two ingress, four egress) with separate or overlapping sets of SPAN source interfaces or VLANs. A bi-directional SPAN session counts as both one ingress and one egress session. Both switched and routed interfaces can be configured as SPAN sources.

SPAN sessions do not interfere with the normal operation of the switch. When enabled, a SPAN session might become active or inactive based on various events or actions; a syslog message indicates this. The show monitor session command displays the operational status of a SPAN session.

A SPAN session will remain inactive after system boot-up until the destination interface is operational.

Destination Interface

A destination interface (also called a monitor interface) is a switched or routed interface where SPAN sends packets for analysis. Once an interface becomes an active destination interface, incoming traffic is disabled. You cannot configure a SPAN destination interface to receive ingress traffic. The interface does not forward any traffic except that required for the SPAN session.

An interface specified as a destination interface in one SPAN session cannot be a destination interface for another SPAN session. An interface configured as a destination interface cannot be configured as a source interface. EtherChannel interfaces cannot be SPAN destination interfaces.

Specifying a trunk interface as a SPAN destination interface stops trunking on the interface.

Source Interface

A source interface is an interface monitored for network traffic analysis. One or more source interfaces can be monitored in a single SPAN session with user-specified traffic types (ingress, egress, or both) applicable for all the source interfaces. All sources for a particular SPAN session are spanned in the same direction.

You can configure source interfaces for any VLAN. You can configure VLANs as source interfaces, which means that all interfaces in the specified VLANs are source interfaces for the SPAN session. Trunk interfaces can be configured as source interfaces and can be mixed with nontrunk source interfaces; however, the destination interface never encapsulates, so you do not see any encapsulation out of the SPAN destination interface.
Traffic Types

Ingress SPAN (Rx) copies network traffic received by the source interfaces for analysis at the destination interface. Egress SPAN (Tx) copies network traffic transmitted from the source interfaces. Specifying the configuration option “both” copies network traffic received and transmitted by the source interfaces to the destination interface.

VLAN-Based SPAN

VLAN-based SPAN analyzes the network traffic in one or more VLANs. You can configure VLAN based-SPAN as ingress SPAN, egress SPAN, or both. All of the interfaces in the source VLANs become source interfaces for the VLAN-based SPAN session.

Use the following guidelines for VLAN-based SPAN sessions:

- Trunk interfaces are included as source interfaces for VLAN-based SPAN sessions.
- For VLAN-based SPAN sessions with both ingress and egress SPAN configured, two packets are forwarded by the SPAN destination interface if the packets get switched on the same VLAN.
- When a VLAN is cleared, it is removed from the source list for VLAN-based SPAN sessions.
- Inactive VLANs are not allowed for VLAN-based SPAN configuration.
- If a VLAN is being ingress monitored and the switch routes traffic from another VLAN to the monitored VLAN, that traffic is not monitored—it is not seen on the SPAN destination interface. Additionally, traffic that gets routed from an egress-monitored VLAN to some other VLAN does not get monitored.

SPAN Traffic

All network traffic, including multicast and bridge protocol data unit (BPDU) packets, can be monitored using SPAN.

In some SPAN configurations, multiple copies of the same source packet are sent to the SPAN destination interface. For example, a bidirectional (both ingress and egress) SPAN session is configured for sources a1 and a2 to a destination interface d1. If a packet enters the switch through a1 and gets switched to a2, both incoming and outgoing packets are sent to destination interface d1; both packets would be the same (unless a Layer-3 rewrite had occurred, in which case the packets would be different).

Understanding How the NAM Uses VACLs

VACL is a way to forward traffic from either a WAN interface or VLANs to a data port on the NAM. This feature provides an alternative to using SPAN for similar purposes. The VACL data analysis capability is not supported for the WS-X6380-NAM.

There are two types of VACLs, one which captures all bridged or routed VLAN packets and another which captures a selected subset of all bridged or routed VLAN packets. Catalyst operating system VACLs can only be used to capture VLAN packets because they are initially routed or bridged into the VLAN on the switch.

VACLs can provide access control for all packets that are bridged within a VLAN or that are routed into or out of a VLAN or, with releases 12.1(13)E or later, a WAN interface. Unlike regular Cisco IOS standard or extended ACLs that are configured on router interfaces only and are applied on routed packets only, VACLs apply to all packets and can be applied to any VLAN or WAN interface. VACLs are processed in hardware.
VACLs use Cisco IOS ACLs. VACLs ignore any Cisco IOS ACL fields that are not supported in hardware. Standard and extended Cisco IOS ACLs are used to classify packets. Classified packets can be subject to a number of features such as access control (security), encryption, policy-based routing, and so on. Standard and extended Cisco IOS ACLs are only configured on router interfaces and applied on routed packets.

Once a VACL is configured on a VLAN, all packets (routed or bridged) entering the VLAN are checked against the VACL. Packets can either enter the VLAN through a switch port or through a router port after being routed. Unlike Cisco IOS ACLs, VACLs are not defined by direction (input or output).

A VACL contains an ordered list of access control entries (ACEs). Each ACE contains a number of fields that are matched against the contents of a packet. Each field can have an associated bit mask to indicate which bits are relevant. An action is associated with each ACE that describes what the system should do with the packet when a match occurs. The action is feature dependent. Catalyst 6500 family switches support three types of ACEs in the hardware: IP, IPX, and MAC-Layer traffic. VACLs applied to WAN interfaces support only IP traffic. VACLs can provide access control based on Layer 3 addresses for IP and IPX protocols. Unsupported protocols are access controlled through MAC addresses. MAC VACLs cannot be used to access control IP or IPX addresses.

When you configure a VACL and apply it to a VLAN, all packets entering the VLAN are checked against this VACL. If you apply a VACL to the VLAN and an ACL to a routed interface in the VLAN, a packet coming in to the VLAN is first checked against the VACL and, if permitted, is then checked against the input ACL before it is handled by the routed interface. When the packet is routed to another VLAN, it is first checked against the output ACL applied to the routed interface and, if permitted, the VACL configured for the destination VLAN is applied. If a VACL is configured for a packet type and a packet of that type does not match the VACL, the default action is deny.

When configuring VACLs the following apply:

- VACLs and CBAC cannot be configured on the same interface
- TCP Intercepts and Reflexive ACLs take precedence over a VACL action if these are configured on the same interface.
- IGMP packets are not checked against VACLs.

For details on how to configure VACL with Cisco IOS software, refer to the Network Analysis Module for Catalyst 6500 Series and Cisco 7600 Series Command Reference. For details on how to configure security ACLs with the Catalyst operating system, refer to the Catalyst 6500 Series Software Configuration Guide and the Catalyst 6500 Series Command Reference.

Understanding How the NAM Uses NDE

To use a remote device as an NDE data source for the NAM, you must configure the remote device itself to export NDE packets to UDP port 3000 on the NAM. You may need to configure the device itself on a per-interface basis. A screen has been added to the web application UI for specifying NDE devices. An NDE device is identified by its IP address. By default the switch’s local supervisor engine always is available as an NDE device.

You then can define additional NDE devices by specifying the IP addresses and (optionally) the community strings. Community strings are used to upload convenient textual strings for interfaces on the remote devices that are monitored in NetFlow records.

Distinguishing among different interfaces on the remote NDE devices is a feature in this release that allows you to arbitrarily bundle groups of interfaces on each remote NDE device into a conceptual data source rather than simply grouping all flows into the same collections.
If you tried to distinguish every single interface on every remote device (potentially in both directions separately) it is possible this action could result in a large, unmanageable number of data sources. By using conceptual data sources you are given complete flexibility to group all interfaces in all directions into one single conceptual data source.

You may also choose to create a separate conceptual data source for each interface on the device. In general, you can combine any number of “simple flow paths” together to form a conceptual data source. Each simple flow path may consist of a single interface in the input direction, the output direction, or both directions.

The following restrictions apply when creating conceptual data sources and assigning flow paths to them:

- Any interface that is specified as an input interface for a flow path cannot be specified as an input interface in another conceptual data source for the same device. It also cannot be specified as an input interface in another flow path for the same conceptual data source.
- Any interface that is specified as an output interface for a flow path cannot be specified as an output interface in another conceptual data source for the same device. It also cannot be specified as an output interface in another flow path for the same conceptual data source.
- Any interface that has been specified as a bidirectional interface for a flow path cannot be specified as a bidirectional interface in another conceptual data source for the same device. It also cannot be specified as a bidirectional interface in another flow path for the same conceptual data source.

Managing the NAM

The NAM is managed and controlled from the embedded web-based NAM Traffic Analyzer application (directing a web browser to the NAM) or a Simple Network Management Protocol (SNMP) management application, such as those bundled with CiscoWorks, or both.

The NAM Traffic Analyzer application provides access to the management features and monitoring features for NAM data and voice traffic through a web browser. To use the NAM Traffic Analyzer application, you first need to do some basic configuration tasks on the NAM using the CLI. You then can start the NAM Traffic Analyzer application with a single command.

With NAM Traffic Analyzer, you can do the following tasks:

- Configure and view historical reports about various traffic statistics.
- Configure SPAN resources
- Configure collections
- Monitor statistics
- Capture and decode packets
- Set and view alarms

For added security, you can use the NAM Traffic Analyzer application to configure the NAM to use a remote TACACS+ server. A TACACS+ server can be used for authentication and authorization for your web-based users. You also can use a local database on the NAM for security.

You also can manage the NAM using an SNMP management application such as the Cisco NetScout nGenius Real-Time Monitor (RTM). For more information about using RTM, refer to the CiscoWorks documentation or refer to this URL:


To use RMON and SNMP agent support, you configure the NAM using the CLI.
If you have a NAM that is already configured and running in the switch, and you are familiar with the NAM, you can begin using the NAM Traffic Analyzer application by entering the `ip http server enable` CLI command and then starting NAM Traffic Analyzer in your browser.

Refer to the User Guide for the Network Analysis Module Traffic Analyzer Release 3.1 for more information about using the NAM Traffic Analyzer application.

**New NAM Features**

These are the new features for the NAM platforms in software release 3.1:

**Monitoring 6500/7600 WAN Interfaces Through VACL**

VACL is used as a means of sourcing packets to the NAM for monitoring. VACL (VLAN Access Control Lists) capture support is now available for WAN cards on the NAM-1 and NAM-2. NetFlow also provides some information on the WAN traffic. The NAM utilizes these data sources to provide application level visibility into WAN traffic as follows:

- The NAM accepts traffic directed to it through VACL captures from WAN and LAN interfaces on Catalyst 6500 series switches and Cisco 7600 Internet routers. A PFC or PFC2 card must be present on the switch. VACL capture is possible only on NAM 1 and NAM 2. (WS-X6380-NAM is not supported.) VACLs are supported on the NAM with Cisco IOS Release 12.1(13)E or later or Catalyst 6500 series operating system release 7.5 and later.
- Statistics on the WAN traffic directed through VACL or NetFlow up to the application layer are provided. This information is organized allowing filtering by physical WAN ports (for example, a particular T1 or OC3 connection on a port adapter) or logical WAN interfaces (for example, separate channels on a channelized T3).
- Previous NAM hardware supports only WAN Monitoring enhancements that are possible with NetFlow.

**WAN Monitoring Through NetFlow Data Export (NDE) from Remote Routers and Switches**

The NAM can now accept NDE packets, specially formatted packets generated by routers and switches that summarize traffic levels for flows that have passed through the device, from external devices in addition to the local supervisor engine and has the ability to distinguish traffic on different interfaces of the NDE sources and monitor them as separate data sources.

- The NAM accepts NetFlow information from external switches and routers and uses it to provide application level visibility into the traffic traversing through these remote devices.
- The NAM receives and analyzes NetFlow data from routers providing L3-L7 information.
- The NAM supports NDE version 1, version 5, version 6, version 7, version 8, version 8-source-prefix, version 8-destination-prefix, version 8-protocol-port, and version 8-prefix-aggregation in this release.
- Each of the remote NetFlow sessions is identifiable separately with filtering to isolate information on a particular router or switch.
- In addition to the statistics provided currently with RMON2, the NAM displays additional information available from the NDE records related to the source and destination ports (physical interface, sub-interface).
In previous releases, the NAM software allows RMN2hos, RMON2 matrix and RMON2 protocol distribution collection creation on the NetFlow data source. In this release you may also create DSMON host, DSMON matrix, and DSMON protocol distribution collections on any or all of the conceptual data sources.

**Historical Reporting**

This feature provides three types of reports:

- Historical views of real time data on Monitor screens. These reports cover major areas where historical information and performance analysis are required. These reports provide instant historical views on the monitor screens that can be compared to the real time data to detect anomalies.
- Pre-defined reports: Allows you to define the reports before you review the data. You can specify the collections, granularity, etc. before any historical data can be made available. These reports are used for producing monthly analysis of utilization, detection of anomalies, etc.
- Real Time trends: These reports provide real time data in a graphical format. The display allows you to observe how data changed.

**VLAN Traffic Statistics**

- SMON support:
- Uses the SMON MIB in the Catalyst switch or router to provide utilization statistics for all VLANs in the switch or router.
- Dual SPAN ports on NAM-2:
- Enables dual SPAN ports on NAM-2 to allow the user to mix data sources and provides further differentiation for NAM-2.

**Multiple NAM Configuration Support**

- The addition of an expanded set of new CLI commands for configuration.
- The ability to export a configuration as a configuration file to an FTP server.
- The ability to import a configuration from a configuration file located on an FTP server.

**Online Documentation Enhancements**

- User friendly print capabilities are provided, allowing you to print desired screens, tabular information, or graphs.
- Percentage and total statistics are added to the monitoring screens to provide the total utilization of and the percentage for each entry displayed for the spanned traffic.

**Front Panel Description**

The NAM front panel (see Figure 1-1) includes a STATUS LED and SHUTDOWN button.
**Figure 1-1  Network Analysis Module**

![Network Analysis Module Diagram]

**STATUS LED**

The STATUS LED indicates the operating states of the NAM. Table 1-3 describes the LED operation.

<table>
<thead>
<tr>
<th>Color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>All diagnostic tests pass. The NAM is operational.</td>
</tr>
<tr>
<td>Red</td>
<td>A diagnostic other than an individual port test failed.</td>
</tr>
<tr>
<td>Orange</td>
<td>Indicates one of three conditions:</td>
</tr>
<tr>
<td></td>
<td>• The NAM is running through its boot and self-test diagnostic sequence.</td>
</tr>
<tr>
<td></td>
<td>• The NAM is disabled.</td>
</tr>
<tr>
<td></td>
<td>• The NAM is in the shutdown state.</td>
</tr>
<tr>
<td>Off</td>
<td>The NAM power is off.</td>
</tr>
</tbody>
</table>

**SHUTDOWN Button**

Caution: Do not remove the NAM from the switch until the NAM has shut down completely and the STATUS LED is orange. You can damage the NAM if you remove it from the switch before it completely shuts down.

To avoid corrupting the NAM hard disk, you must correctly shut down the NAM before you remove it from the chassis or disconnect the power. This shutdown procedure is normally initiated by commands entered at the supervisor engine CLI prompt or the NAM CLI prompt.

If the NAM fails to respond to these commands properly, press the SHUTDOWN button on the front panel to initiate the shutdown procedure.

The shutdown procedure may require several minutes. The STATUS LED turns off when the NAM shuts down.
Specifications

Table 1-4 describes the specifications for the NAM.

Table 1-4  **WS-SVC-NAM-1 and WS-SVC-NAM-2 Specifications**

<table>
<thead>
<tr>
<th>Specification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dimensions (H x W x D)</td>
<td>1.2 x 14.4 x 16 in. (3.0 x 35.6 x 40.6 cm)</td>
</tr>
<tr>
<td>Weight</td>
<td>Minimum: 3 lb (1.36 kg)</td>
</tr>
<tr>
<td></td>
<td>Maximum: 5 lb (2.27 kg)</td>
</tr>
<tr>
<td>Environmental conditions:</td>
<td></td>
</tr>
<tr>
<td>Operating temperature</td>
<td>32 to 104°F (0 to 40°C)</td>
</tr>
<tr>
<td>Nonoperating temperature</td>
<td>–40 to 158°F (–40 to 70°C)</td>
</tr>
<tr>
<td>Humidity</td>
<td>10 to 90%, noncondensing</td>
</tr>
<tr>
<td>Humidity - Ambient (Noncondensing)</td>
<td>5 to 95%</td>
</tr>
<tr>
<td>Nonoperating and Storage</td>
<td></td>
</tr>
<tr>
<td>Altitude</td>
<td>Sea level to 10,000 ft (3050 m)</td>
</tr>
</tbody>
</table>
Installing the NAM

This chapter describes the requirements to support the Catalyst 6500 series and Cisco 7600 series and Catalyst 6000 family NAM, and how to install and remove the NAM, and includes these sections:

- System Requirements, page 2-1
- Software Requirements, page 2-2
- Hardware Requirements, page 2-3
- Required Tools, page 2-3
- Installing and Removing the NAM, page 2-3

System Requirements

This section describes the software and hardware requirements for the module.

Memory and Storage Requirements

There are no additional memory or storage requirements for this module. The WS-SVC-NAM-1 and WS-SVC-NAM-2 modules contain a 64 MB compact flash.
# Software Requirements

Table 1 lists the NAM software versions supported by Catalyst operating system and Cisco IOS software.

## Table 1  NAM Software Compatibility

<table>
<thead>
<tr>
<th>Module</th>
<th>Application Image</th>
<th>Maintenance Image</th>
<th>Catalyst Operating System Software</th>
<th>Cisco IOS Software</th>
<th>Supported Browsers</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS-SVC-NAM-1</td>
<td>3.1(1)</td>
<td>1.1(1)m</td>
<td>Release 7.3(1) or later with Supervisor Engine 1A or 2</td>
<td>Release 12.1(13)E1 or later with a Supervisor Engine 2 with an MSFC2</td>
<td>Netscape 4.7 or later on Windows 2000 and Solaris Internet Explorer 5.0 and later on Windows 2000 Japanese Netscape 4.7 or later on Japanese Windows 2000 and Japanese Solaris 8 Japanese Internet Explorer 5.5 SP2 and later on Japanese Windows 2000</td>
</tr>
<tr>
<td>WS-SVC-NAM-2</td>
<td></td>
<td></td>
<td>Release 8.2(1) or later with a WS-SUP720</td>
<td>Release 12.1(19E)1 with a Supervisor Engine 1A with an MSFC2</td>
<td></td>
</tr>
<tr>
<td>WS-X6380-NAM</td>
<td>3.1(1)</td>
<td>1.2(1a)m²</td>
<td>Release 7.3(1) or later with Supervisor Engine 1A or 2</td>
<td>Release 12.1(13)E1 or later with a Supervisor Engine 1A and an MSFC2 or a Supervisor Engine 2 with an MSFC2</td>
<td>Netscape 4.7 or later on Windows 2000 and Solaris Internet Explorer 5.0 and later on Windows 2000 Japanese Netscape 4.7 or later on Japanese Windows 2000 and Japanese Solaris 8 Japanese Internet Explorer 5.5 SP2 and later on Japanese Windows 2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.2(1b)m</td>
<td></td>
<td>Release 12.1(20)E with a Supervisor Engine 1A with an MSFC2</td>
<td></td>
</tr>
</tbody>
</table>

1. If you are running a 12.1(13)E-based release, we recommend a later 13E release, for example 12.1(13)E11 over 12.1(13)E3.
2. When you upgrade to software release 3.1(1), the 1.2(1a)m maintenance image is automatically upgraded to the 1.2(1b)m image.
Hardware Requirements

Table 2 lists the NAM hardware versions supported by Catalyst operating system and Cisco IOS software.

### Table 2   NAM Hardware Compatibility

<table>
<thead>
<tr>
<th>Module</th>
<th>Catalyst Operating System Software</th>
<th>Cisco IOS Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS-SVC-NAM-1</td>
<td>Supervisor Engine 1A or 2</td>
<td>Supervisor Engine 2 with an MSFC2</td>
</tr>
<tr>
<td>WS-SVC-NAM-2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WS-SUP720</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WS-X6380-NAM</td>
<td>Supervisor Engine 1A or 2</td>
<td>Supervisor Engine 1A with an MSFC2 or a Supervisor 2 with an MSFC2</td>
</tr>
</tbody>
</table>

Required Tools

**Note**

Before installing the NAM, you must install the Catalyst 6500 series switch chassis, the Cisco 7600 series Internet Router chassis, or the Catalyst 6000 family switch chassis, and at least one supervisor engine. For information on installing the switch chassis, refer to the chassis installation guide.

These tools are required to install the NAM in the Catalyst 6500 series switch, the Cisco 7600 series Internet Router, or the Catalyst 6000 family switch:

- Flat-blade screwdriver
- Phillips-head screwdriver
- Wrist strap or other grounding device
- Antistatic mat or antistatic foam

Whenever you handle the NAM, always use a wrist strap or other grounding device to prevent electrostatic discharge (ESD).

Installing and Removing the NAM

**Warning**

During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.

All the Catalyst 6500 series and Cisco 7600 series and Catalyst 6000 family switches support hot swapping, which allows you to install, remove, replace, and rearrange modules without turning off the system power. For more information on removing the NAM from a switch, see the “Removing a Module” section on page 2-5.

**Caution**

We recommend that you shut down the NAM before you remove the module.
When the system detects that a module has been installed or removed, the system automatically runs diagnostic and discovery routines, acknowledges the presence or absence of the module, and resumes system operation.

To install and use the NAM, you need to complete the following actions:

- Perform the initial installation by placing the NAM in a switch.
- At the switch CLI, session to the NAM CLI and provide a basic configuration.
- Send a data source to the NAM (NetFlow data, switch port analyzer [SPAN] ports, VLANs, or EtherChannels).
- Configure collection types that you want to monitor (RMON, voice, application response time, and other collection monitoring as required for your network).
- Configure alarms.
- View monitored statistics, alarms, and use packet capture or decode functionality.

This section describes how to install and verify the operation of the NAM in the Catalyst 6000 family switches and contains the following sections:

- Slot Assignments, page 2-4
- Removing a Module, page 2-5
- Installing a Module, page 2-6
- Verifying the Installation, page 2-12

**Slot Assignments**

The Catalyst 6006 and 6506 switch chassis have six slots, the Catalyst 6009 and 6509 switch chassis have nine slots, and the Catalyst 6513 switch chassis has thirteen slots. The module can occupy any slot in the Catalyst 6500 series and Cisco 7600 series or 6000 family chassis.

**Note**

The Catalyst 6509-NEB switch has vertical slots numbered 1 to 9 from right to left. Install the modules with the component side facing to the right.

- Slot 1 is reserved for the supervisor engine.
- Slot 2 can contain an additional redundant supervisor engine in case the supervisor engine in slot 1 fails.
- If a redundant supervisor engine is not required, slots 2 through 6 on the 6-slot chassis, (slots 2 through 9 on the 9-slot chassis and slots 2 through 13 on the 13-slot chassis) are available for switching modules, such as the NAM.
- Install switching-module filler plates, which are blank switching-module carriers, in the empty slots to maintain consistent airflow through the switch chassis.
Removing a Module

This section describes how to remove an existing module from a chassis slot.

**Warning**
During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.

**Warning**
Before you install, operate, or service the system, read the *Site Preparation and Safety Guide*. This guide contains important safety information you should know before working with the system.

**Warning**
Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.

To remove a supervisor engine or module from the chassis, perform these steps:

**Step 1**
Disconnect any network interface cables attached to the supervisor engine or module.

*Note*
The NAM does not have any interface cable connections.

**Step 2**
Verify that the captive installation screws on all of the modules in the chassis are tight.

This action ensures that the space created by the removed module is maintained.

*Note*
If the captive installation screws are loose, the electromagnetic interference (EMI) gaskets on the installed modules will push the modules toward the open slot, reducing the opening size and making it difficult to install the replacement module.

**Step 3**
Loosen the two captive installation screws on the supervisor engine or module.

**Step 4**
Depending on the orientation of the slots in the chassis (horizontal or vertical), perform one of the following sets of steps:

**Horizontal slots**
- a. Place your thumbs on the left and right ejector levers, and simultaneously rotate the levers outward to unseat the module from the backplane connector.
- b. Grasp the front edge of the module and slide the module part of the way out of the slot. Place your other hand under the module to support the weight of the module. Do not touch the module circuitry.

**Vertical slots**
- a. Place your thumbs on the ejector levers located at the top and bottom of the module, and simultaneously rotate the levers outward to unseat the module from the backplane connector.
- b. Grasp the edges of the module, and slide the module straight out of the slot. Do not touch the module circuitry.
**Installing and Removing the NAM**

**Step 5**
Place the module on an antistatic mat or antistatic foam, or immediately reinstall it in another slot.

**Step 6**
If the slot is to remain empty, install a module filler plate to keep dust out of the chassis and to maintain proper airflow through the chassis.

---

**Warning**
Blank faceplates (filler panels) serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards and faceplates are in place.

---

**Installing a Module**

This section describes how to install modules in the Catalyst 6500 series and Cisco 7600 series and Catalyst 6000 family switches.

---

**Caution**
To prevent ESD damage, handle modules by the carrier edges only.

---

**Warning**
During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.

---

**Warning**
Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.

---

**Warning**
Before you install, operate, or service the system, read the Site Preparation and Safety Guide. This guide contains important safety information you should know before working with the system.

---

To install a supervisor engine or module in the chassis, perform these steps:

**Step 1**
Choose a slot for the supervisor engine or module.

**Step 2**
Verify that there is enough clearance to accommodate any interface equipment that you will connect directly to the supervisor engine or module ports. If possible, place modules between empty slots that contain only module filler plates.

**Step 3**
Verify that the captive installation screws are tightened on all modules installed in the chassis. This action ensures that the EMI gaskets on all modules are fully compressed in order to maximize the opening space for the new module or the replacement module.
Note: If the captive installation screws are loose, the EMI gaskets on the installed modules will push adjacent modules toward the open slot, reducing the opening size and making it difficult to install the replacement module.

Step 4: Remove the module filler plate by removing the two Phillips pan-head screws from the filler plate. To remove a module, refer to “Removing a Module” section on page 2-5.

Step 5: Fully open both ejector levers on the new or replacement module. (See Figure 2-1.)

Figure 2-1  Positioning the Module in a Horizontal Slot Chassis

Step 6: Depending on the orientation of the slots in the chassis (horizontal or vertical), perform one of these sets of steps:
Horizontal slots

a. Position the supervisor engine or module in the slot. (See Figure 2-1.) Make sure that you align the sides of the module carrier with the slot guides on each side of the slot.

b. Carefully slide the supervisor engine or module into the slot until the EMI gasket along the top edge of the module makes contact with the module in the slot above it and both ejector levers have closed to approximately 45 degrees in relation to the module faceplate. (See Figure 2-2.)

Figure 2-2 Clearing the EMI Gasket in a Horizontal Slot Chassis

Catalyst 6500 Series Switch and Cisco 7600 Series Internet Router Network Analysis Module Installation and Configuration Note

Caution
Do not press down too hard on the levers because they can bend and be damaged.

d. While pressing down, simultaneously close the left and right ejector levers to fully seat the supervisor engine or module in the backplane connector. The ejector levers are fully closed when they are flush with the module faceplate. (See Figure 2-3.)
Figure 2-3  Ejector Lever Closure in a Horizontal Slot Chassis

Note Failure to fully seat the module in the backplane connector can result in error messages.

e. Tighten the two captive installation screws on the supervisor engine or module.

Note Make sure that the ejector levers are fully closed before tightening the captive installation screws.

Vertical slots

a. Position the supervisor engine or switching module in the slot. (See Figure 2-4.) Make sure that you align the sides of the switching module carrier with the slot guides on the top and bottom of the slot.
b. Carefully slide the supervisor engine or module into the slot until the EMI gasket along the right edge of the module makes contact with the module in the slot adjacent to it and both ejector levers have closed to approximately 45 degrees with respect to the module faceplate. (See Figure 2-5.)

c. Using the thumb and forefinger of each hand, grasp the two ejector levers and exert a slight pressure to the left, moving the module approximately 0.040 inches (1 mm) to create a small gap between the module’s EMI gasket and the module adjacent to it. (See Figure 2-5.)
Do not exert too much pressure on the ejector levers. They will bend and be damaged.

d. While pressing on the ejector levers, simultaneously close them to fully seat the supervisor engine or module in the backplane connector. The ejector levers are fully closed when they are flush with the module faceplate. (See Figure 2-6.)
Installing and Removing the NAM

Figure 2-6  Ejector Lever Closure in a Vertical Slot Chassis

---

Chapter 2  Installing the NAM

Installing and Removing the NAM

e. Tighten the two captive installation screws on the module.

Note  Make sure that the ejector levers are fully closed before tightening the captive installation screws.

Verifying the Installation

This section describes how to verify the NAM installation.

Cisco IOS Software

To verify that the system acknowledges the new module and has brought it online, enter the `show module [mod-num | all]` command.

This example shows the output of the `show module` command:

```
Router# show module
Mod Slot Ports Module-Type               Model               Sub Status
--- ---- ----- ------------------------- ------------------- --- --------
1  1    2     1000BaseX Supervisor      WS-X6K-S2U-MSFC2    yes ok
15  1    1     Multilayer Switch Feature WS-F6K-MSFC2        no  ok
2   3    3     Network Analysis Module   WS-SVC-NAM-1        no  ok
Router#
```

All ejector levers flush with module faceplate
When the NAM initially boots, by default it runs a partial memory test. To perform a full memory test, enter the `hw-module module slot_number reset device:partition mem-test-full` command. This command is specific to Cisco IOS software and is not available in Catalyst operating system software.

A full memory test takes more time to complete than a partial memory test depending on the memory size.

**Note**

The `mem-test-full` option is applicable only for WS-SVC-NAM-1 and WS-SVC-NAM-2. For the WS-X6380-NAM there is only one boot time - 2 to 3 minutes (from shutdown state to okay).

Table 2-3 lists the memory test time and approximate boot time for a long memory test.

<table>
<thead>
<tr>
<th>Module</th>
<th>Memory Test</th>
<th>Catalyst Operating System Software</th>
<th>Cisco IOS Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS-SVC-NAM-1</td>
<td>Partial</td>
<td>~2-3 minutes.</td>
<td>~3 minutes</td>
</tr>
<tr>
<td></td>
<td>Full</td>
<td>~3 minutes</td>
<td>~6 minutes</td>
</tr>
<tr>
<td>WS-SVC-NAM-2</td>
<td>Partial</td>
<td>~3 minutes</td>
<td>~3 minutes</td>
</tr>
<tr>
<td></td>
<td>Full</td>
<td>~3 minutes</td>
<td>~7 minutes</td>
</tr>
</tbody>
</table>

You also can use the `hw-module module slot_number mem-test-full` command in a Cisco IOS system. This example shows how to do a full memory test for module 5:

```bash
Router(config)# hw-module module 5 mem-test-full
```

### Catalyst Operating System Software

To verify that the switch acknowledges the new NAM and has brought it online, enter the `show module` or `show port [mod/port]` command.

This example shows the output of the `show module` command:

```
Console> (enable) show module
Mod Slot Ports Module-Type               Model               Sub Status
--- ---- ----- ------------------------- ------------------- --- --------
1   1    2     1000BaseX Supervisor      WS-X6K-SUP1A-2GE    yes ok
15  1    1     Multilayer Switch Feature WS-F6K-MSFC         no  ok
3   3    2     Network Analysis Module   WS-SVC-NAM-1        no  ok
5   5    48    10/100BaseTX Ethernet     WS-X6248-RJ-45      no  ok
.
.
.
```

When the NAM initially boots, by default it runs a partial memory test. For Catalyst operating system software, you can perform a full memory test when you enter the `set boot device bootseq mod# mem-test-full` command. This command is specific to Catalyst operating system software and is not available in Cisco IOS software. This example shows how to do a full memory test:

```
Console (enable) set boot device cf:1 # mem-test-full
Device BOOT variable = cf:1
Memory-test set to FULL
Warning:Device list is not verified but still set in the boot string.
```
When specifying the boot device for the WS-X3860-NAM, you must use hdd:1 for the application image or hdd:2 for the maintenance image. When specifying the boot device for the WS-SVC-NAM-1 and the WS-SVC-NAM-2, you must use hdd:1 for the application image and cf:1 for the maintenance image.

```
Console> (enable) show boot device 4
Device BOOT variable = cf:1
Memory-test set to FULL

When you next reset the NAM, the full memory test runs. A full memory test takes more time to complete than a partial memory test. Table 2-3 shows the time for memory tests.

This example shows how to reset the partial memory test:

Console> (enable) set boot device cf:1 4
Device BOOT variable = cf:1
Memory-test set to PARTIAL
Warning:Device list is not verified but still set in the boot string.
Console> (enable)
Console> (enable)
show boot device 4
Device BOOT variable = cf:1
Memory-test set to PARTIAL
```
Getting Started

This chapter describes how to configure the Catalyst 6500 series and Cisco 7600 series and Catalyst 6000 family NAM, and includes these sections:

- Configuring the NAM, page 3-1
- Configuring Traffic Sources for Capturing NAM Traffic, page 3-10
- Operating-System-Independent Configuration, page 3-20

Configuring the NAM

How you configure the NAM on your switch depends on whether you are using Cisco IOS software or the Catalyst operating system software. Several NAM configuration tasks are common to both switch operating systems.

The following sections describe how to configure the NAM from the CLI for each switch operating system:

- Cisco IOS Software, page 3-2
- Catalyst Operating System Software, page 3-5

After you have set up the NAM initial configuration, you can configure VACLs, NetFlow Data Export (NDE) either local or remote, and SPAN to monitor network traffic in this section.

- Configuring Traffic Sources for Capturing NAM Traffic, page 3-10

When you have completed configuring the software-dependent attributes for the NAM, you can configure the software-independent attributes in this section:

- Operating-System-Independent Configuration, page 3-20
Cisco IOS Software

These sections describe how to configure the NAM from the Catalyst 6500 series and Cisco 7600 series and Catalyst 6000 family switch when using Cisco IOS:

- Initial Configuration, page 3-2
- Configuring VLANs, page 3-5

Initial Configuration

Before you can use the NAM for network analysis, you must log into the NAM root account and configure the following:

- IP address
- Subnet mask
- IP broadcast address
- IP host name
- Default gateway
- Domain name
- If applicable, the DNS name server
- If you are using an external SNMP manager to communicate with the NAM, configure the following:
  - SNMP MIB variables
  - Access control for the SNMP agent
  - System group settings on the NAM

To start the web server, use the `ip http server enable` command.

To configure these parameters for the NAM, follow these steps:

---

**Step 1** Enter this command to verify that the NAM is installed and that the power is on:

```
Router# show module module_number
```

**Step 2** Establish a console session with the NAM by entering:

```
Router# session slot module_number processor processor-id
```

**Step 3** At the login prompt, type `root` to log in to the root account.

**Step 4** At the password prompt, type `root` as the root password.

---

**Note** If you have not changed the password from the factory-set default, a warning message displays. If you decide to change the password from the default, see the “Changing the NAM CLI Passwords” section on page 4-3 for more information.

**Step 5** Configure the IP address and subnet mask by entering:

```
root@localhost# ip address ip-address subnet-mask
```

**Step 6** Configure the IP broadcast address by entering:

```
root@localhost# ip broadcast broadcast-address
```
Configure the IP host name used in the CLI prompt, `show` commands, and log messages by entering:
```
root@localhost.localdomain# ip host [host-name]
```

**Step 7** Configure the default gateway by entering:
```
root@nam1.localdomain# ip gateway default-gateway
```

**Step 8** Configure the domain name for the NAM by entering:
```
root@localhost# ip domain domain-name
```

**Step 9** Configure one or more IP addresses as DNS name servers by entering:
```
root@localhost.localdomain# ip nameserver ip-address [name-server1] [name-server2]
```

**Note** The `ip nameserver` command can accept up to a maximum of three name server addresses (two addresses are optional).

**Step 10** Verify the NAM configuration by entering:
```
root@localhost.localdomain# show ip
```

**Step 11** Configure the SNMP `syslocation` MIB variable by entering:
```
root@localhost.localdomain# snmp location location-string
```

**Note** The MIB variables in **Step 12** and **Step 13** must be valid DisplayString texts, each with a maximum length of 64 characters.

**Step 12** Set the SNMP `sysContact` MIB variable by entering:
```
root@localhost.localdomain# snmp contact contact-string
```

**Step 13** Set the SNMP `sysName` MIB variable by entering:
```
root@nam1.cisco.com# snmp name name-string
```

**Note** You can delete the SNMP location, SNMP contact, or SNMP name by entering the respective command without any parameters.

**Step 14** Set the SNMP agent community string parameter password for read-write access by entering:
```
root@localhost.localdomain# snmp community community-string rw
```

**Step 15** Set the SNMP agent community string parameter password for read-only access by entering:
```
root@localhost.localdomain# snmp community community-string ro
```

**Note** Clear the SNMP community string with the `snmp delete community community-string` command.

**Step 16** Verify the SNMP access controls and settings by entering:
```
root@localhost.localdomain# show snmp
```
After completing this configuration, the NAM is ready to use with any other IETF-compliant RMON application.

**Note**

If you are using the Real Time Monitor (RTM), you need to input the community strings in RTM exactly as you enter them in the NAM.

This example shows how to configure the NAM:

```
Router# session slot 8 processor 1
The default escape character is Ctrl-^, then x.
You can also type ‘exit’ at the remote prompt to end the session
Trying 127.0.0.81 ... Open

Cisco Network Analysis Module (WS-SVC-NAM-1)

login: root
Password:

Network Analysis Module (WS-SVC-NAM-1) Console, 2.1(1)
Copyright (C) 1999, 2000, 2001 Cisco Systems, Inc.

WARNING! Default password has not been changed!

root@localhost# ip address 172.18.52.29 255.255.255.224
root@localhost# ip broadcast 172.18.52.31
root@localhost/localhost# ip host nam1
root@nam1/localhost# ip gateway 172.69.2.132
root@localhost# ip domain cisco.com
root@nam1.cisco.com# ip nameserver 171.62.2.132
root@nam1.cisco.com# show ip
IP address:        172.20.98.182
Subnet mask:       255.255.255.192
IP Broadcast:      172.20.255.255
DNS Name:          nam.cisco.com
Default Gateway:   172.20.98.129
Nameserver(s):     171.69.2.133
HTTP server:       Enabled
HTTP secure server:Disabled
HTTP port:         80
HTTP secure port:  443
TACACS+ configured:No
Telnet:            Enabled
SSH:               Disabled
root@nam1.cisco.com# snmp location "Cisco Lab, Building X, Floor 1"
root@nam1.cisco.com# snmp contact "Jane Doe, Cisco Systems, (408) 111-1111"
root@nam1.cisco.com# snmp name "6k-NAM - Slot 2"
root@nam1.cisco.com# snmp community public ro
root@nam1.cisco.com# snmp community private rw

root@nam1.cisco.com# show snmp
SNMP Agent:        nam1.cisco.com 172.18.52.29
SNMPv1:            Enabled
SNMPv2C:           Enabled
SNMPv3:            Disabled

community public read
community private write
```
sysDescr         "Catalyst 6500 Network Management Module (WS-SVC-NAM-1)"
sysObjectID      enterprises.9.5.1.3.1.1.2.914
sysContact       "Jane Doe, Cisco Systems, (408) 111-1111"
syssize          "6k-NAM - Slot 2"
sysLocation      "Cisco Lab, Building X, Floor 1"
root@localhost#

Configuring VLANs

To configure a VLAN for the NAM management port, you must use the **analysis module mod_num management-port access-vlan vlan_id** command.

Catalyst Operating System Software

These sections describe how to configure the NAM from the CLI:

- Initial Configuration, page 3-5
- Configuring VLANs, page 3-8
- Configuring the SNMP Agent, page 3-8

Initial Configuration

Before you can use the NAM for network analysis, you must log into the NAM root account and configure the following:

- IP address
- Subnet mask
- IP broadcast address
- IP host name
- Default gateway
- Domain name
- If applicable, the DNS name server
- If you are using an external SNMP manager to communicate with the NAM, you must configure the following:
  - SNMP MIB variables
  - Access control for the SNMP agent
  - System group settings on the NAM

To start the web server, use the **ip http server enable** command.

To configure these parameters for the NAM, follow these steps in privileged mode:

**Step 1**  Verify that the NAM is installed and that the power is on by entering:

```
Console> show module module_number
```

**Step 2**  Establish a console session with the NAM by entering:

```
Console> (enable) session module_number
```
Configuring the NAM

Note The NAM must be running the application image (rather than the maintenance image) for the next steps. If you see a maintenance image message when sessioning into the NAM, use the `reset module_number` command from the switch CLI and then session into the NAM again.

Step 3 At the password prompt, type `root` as the root password.

Note If you have not changed the password from the factory-set default, a warning message is displayed. To change the password from the default, see the “Changing the NAM CLI Passwords” section on page 4-13 for more information.

Step 4 Configure the IP address and subnet mask by entering:

```
root@localhost# ip address ip-address subnet-mask
```

Step 5 Configure the IP broadcast address by entering:

```
root@localhost# ip broadcast broadcast-address
```

Step 6 Configure the IP host name used in the CLI prompt, `show` commands, and log messages by entering:

```
root@localhost.localdomain# ip host name
```

Step 7 Configure the default gateway by entering:

```
root@nam1.localdomain# ip gateway default-gateway
```

Step 8 Configure the domain name for the NAM by entering:

```
root@localhost# ip domain domain-name
```

Step 9 Configure one or more IP addresses as DNS name servers by entering:

```
root@nam1.localdomain# ip nameserver ip-address [ip-address]
```

Step 10 Verify the NAM configuration by entering:

```
root@nam1.localdomain# show ip
```

Step 11 Configure the SNMP syslocation MIB variable by entering:

```
root@nam1.localdomain# snmp location location-string
```

Note The MIB variables in Step 12 and Step 13 must be valid DisplayString texts, each with a maximum length of 64 characters.

Step 12 Set the SNMP sysContact MIB variable by entering:

```
root@nam1.localdomain# snmp contact contact-string
```

Step 13 Set the SNMP sysName MIB variable by entering:

```
root@nam1.localdomain# snmp name name-string
```
Chapter 3  Getting Started

Configuring the NAM

Note  You can delete the SNMP location, SNMP contact, or SNMP name by entering the respective command without any parameters.

Step 14  Set the SNMP agent community string parameter password for read-write access by entering:

   root@localhost# snmp community community-string rw

Step 15  Set the SNMP agent community string parameter password for read-only access by entering:

   root@nam1.localdomain# snmp community community-string rw

Note  Clear the SNMP community string with the snmp delete community community-string command.

Step 16  Verify the SNMP access controls and settings by entering:

   root@nam1.localdomain# show snmp

After completing this configuration, you can use the NAM with any other IETF-compliant RMON application.

This example shows how to configure the NAM:

Console> (enable) session 2
Trying NAM-2...
Connected to NAM-2.
Escape character is ^]'.

Network Analysis Module (WS-SVC-NAM-1)

login: root
Password:

Network Analysis Module (WS-SVC-NAM-1) Console, 3.1(0.1)
Copyright (c) 1999-2002 by Cisco Systems, Inc.

WARNING! Default password has not been changed!

root@localhost# ip address 172.18.52.29 255.255.255.224
root@localhost# ip broadcast 172.18.52.31
root@localhost.localdomain# ip host nam1
root@nam1.localdomain# ip gateway 172.69.2.132
root@nam1.localdomain# ip domain cisco.com
root@nam1.cisco.com# ip nameserver 171.62.2.132
root@nam1.cisco.com# show ip
IP address: 172.20.98.182
Subnet mask: 255.255.255.192
IP Broadcast: 172.20.255.255
DNS Name: namlab-kom6.cisco.com
Default Gateway: 172.20.98.129
Nameserver(s): 171.69.2.133
HTTP server: Enabled
HTTP secure server: Disabled
HTTP port: 80
HTTP secure port: 443
TACACS+ configured: No
Telnet: Enabled
### Configuring the NAM

SSH: Disabled

```
root@nam1.cisco.com#
root@nam1.cisco.com# snmp location "Cisco Lab, Building X, Floor 1"
```

```
root@nam1.cisco.com# snmp contact "Jane Doe, Cisco Systems, (408) 111-1111"
root@nam1.cisco.com# snmp name "6k-NAM - Slot 2"
root@nam1.cisco.com# snmp community public ro
root@nam1.cisco.com# snmp community private rw
```

```
root@nam1.cisco.com# show snmp
```

SNMP Agent: nam1.Cisco.com 172.18.52.29

- SNMPv1: Enabled
- SNMPv2C: Enabled
- SNMPv3: Disabled

```
community public read
community private write
```

**sysDescr** "Catalyst 6500 Network Management Module (WS-SVC-NAM-1)"

**sysObjectID** enterprises.9.5.1.3.1.1.2.914

**sysContact** "Jane Doe, Cisco Systems, (408) 111-1111"

**sysName** "6k-NAM - Slot 2"

**sysLocation** "Cisco Lab, Building X, Floor 1"

### Configuring VLANs

You do not need to configure a VLAN as the NAM management port because that port automatically synchronizes to the VLAN assigned to interface sc0 on the supervisor engine.

---

**Note**

You cannot set the NAM management port VLAN with the `set vlan mod/port` command.

### Configuring the SNMP Agent

---

**Note**

If you are using the NAM Traffic Analyzer application, the information in this section is optional.

You can configure the SNMP agent through the CLI or the NAM Traffic Analyzer application. Before you can use the NAM for SNMP support or in hybrid mode using an external SNMP source or a web server, you must log into the NAM root account and configure the following:

- SNMP MIB variables
- Access control for the SNMP agent
- System group settings on the NAM

To configure these parameters for NAM, follow these steps:

---

**Step 1**
Configure the SNMP sysLocation MIB variable by entering:

```
root@localhost# snmp location location-string
```

**Note** The MIB variables you enter in Step 2 and Step 3 must be valid DisplayString texts, each with a maximum length of 64 characters.

**Step 2** Set the SNMP sysContact MIB variable by entering:

```
root@localhost# snmp contact contact-string
```

**Step 3** Set the SNMP sysName MIB variable by entering:

```
root@localhost# snmp name name-string
```

**Note** You can delete the SNMP location, SNMP contact, or SNMP name by entering the appropriate command without any parameters.

**Step 4** Set the SNMP agent community string parameter password for read-write access by entering:

```
root@localhost# snmp community community-string rw
```

**Step 5** Set the SNMP agent community string parameter password for read-only access by entering:

```
root@localhost# snmp community community-string ro
```

**Note** To clear the SNMP community string, enter the `snmp delete community community-string` command.

**Step 6** Verify the SNMP access controls and settings by entering:

```
root@localhost# show snmp
```

After completing this configuration, you can use the NAM with NetScout nGenius Real-Time Monitor, or any other IETF-compliant RMON application.

This example shows how to configure the NAM:

```
Console> (enable) session 2
Trying NAM-2...
Connected to NAM-2.
Escape character is '^]'.

Network Analysis Module (WS-SVC-NAM-1)

login: root
Password:

Network Analysis Module (WS-SVC-NAM-1) Console, 3.1(0.1)
Copyright (c) 1999-2002 by Cisco Systems, Inc.

WARNING! Default password has not been changed!

root@localhost# ip address 172.18.52.29 255.255.255.224
root@localhost# ip broadcast 172.18.52.31
root@localhost# ip host nam1
root@localhost# ip gateway 172.69.2.132
root@localhost# ip domain Cisco.com
root@localhost# ip nameserver 171.62.2.132
```
Configuring Traffic Sources for Capturing NAM Traffic

The WS-SVC-NAM-1 platform provides a single destination port for SPAN sessions.

**Note**

The WS-X6380-NAM provides a single destination port for SPAN sessions, but does not support VACL.

The WS-SVC-NAM-2 platform provides two possible destination ports for VACL and SPAN sessions. The destination ports for use by the SPAN GUI are named DATA PORT 1 and DATA PORT 2 by default. For the CLI SPAN port names, refer to SPAN Port Names, page 1-4.

VACL and SPAN cannot be applied to the same port simultaneously. Table shows the SPAN and VACL port configurations supported on the NAM

<table>
<thead>
<tr>
<th>Table 3-1 NAM SPAN and VACL Port Configurations</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAM-1</td>
</tr>
<tr>
<td>One SPAN session only.</td>
</tr>
<tr>
<td>One VACL session only.</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

After you have set up the NAM initial configuration, use these sections to configure VACLs, NetFlow Data Export (NDE) either local or remote, and SPAN to monitor network traffic with the NAM.
Cisco IOS Software

You can capture traffic for NAM monitoring from a single VLAN or from multiple VLANs. If you want to monitor traffic from specific VLANs only, you will need to clear the VLANs you do not want to monitor from the capture feature.

Using SPAN as a Traffic Source

You can configure SPAN as a traffic source using both the CLI and the NAM Traffic Analyzer application.

The NAM can analyze Ethernet traffic from Ethernet, Fast Ethernet, Gigabit Ethernet, trunk port, or Fast EtherChannel SPAN source ports. You can also specify an Ethernet VLAN as the SPAN source.

For more information on SPAN, refer to the Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide at the following website:


You cannot use ports on the NAM module as SPAN source ports.

To enable SPAN on the NAM, perform one of these tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router (config)# monitor session {session_number} {source {interface type slot/port}</td>
<td>{vlan vlan_ID}) [,.</td>
</tr>
<tr>
<td>Router (config)# monitor session {session_number} {destination analysis module NAM module number data-port port}</td>
<td>Enables port 1 of the NAM as a SPAN destination.</td>
</tr>
<tr>
<td>Router (config)# no monitor session session_number</td>
<td>Disables the monitor session.</td>
</tr>
<tr>
<td>Router (config)# monitor session {session_number} {filter {vlan_ID} [,</td>
<td>- ]}</td>
</tr>
<tr>
<td>Router # show monitor session {session_number}</td>
<td>Shows current monitor sessions.</td>
</tr>
</tbody>
</table>

This example shows how to enable SPAN on the NAM:

Router# show monitor
Session 1
----------
Source Ports:  RX Only: None
               TX Only: None
               Both: None
Source VLANs:  RX Only: None
               TX Only: None
               Both: None
Destination Ports: None
Filter VLANs: None

Session 2
Configuring Traffic Sources for Capturing NAM Traffic

---

Source Ports:
- RX Only: None
- TX Only: None
- Both: None

Source VLANs:
- RX Only: None
- TX Only: None
- Both: None

Source RSPAN VLAN: None

Destination Ports: None

Filter VLANs: None

Router# conf t
Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# monitor session 1 source vlan 1 both

Note
If you are using the switch CLI to configure SPAN as a traffic source to NAM-1, the SPAN destination port for NAM-1 is data-port 1. The SPAN destination ports for NAM-2 is data-port 1 and data-port 2.

Router# 00:21:10:%SYS-5-CONFIG_I:Configured from console by console
Router# conf t
Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# monitor session 1 destination analysis-module 8 data-port 1
Router# show monitor
Session 1
---
Type : Local Session
Source Ports:
- RX Only: None
- TX Only: None
- Both: None
Source VLANs:
- RX Only: None
- TX Only: None
- Both: None
Source RSPAN VLAN: None

Destination Ports: analysis-module 8 data-port 1

Filter VLANs: None
Dest RSPAN VLAN: None

Session 2
---
Type : Local Session
Source Ports:
- RX Only: None
- TX Only: None
- Both: None
Source VLANs:
- RX Only: None
- TX Only: None
- Both: None
Source RSPAN VLAN: None

Destination Ports: None
Filter VLANs: None
Dest RSPAN VLAN: None
Using VACL as a Traffic Source

This section contains the configuration steps required to configure a VACL for a switch running native IOS version 12.1(13)E1 or higher. To configure LAN VACL on the Catalyst operating system, the security ACL feature can be used to achieve the same result. Refer to Operating-System-Independent Configuration, page 3-20.

Configuring VACL on a WAN Interface

Because WAN interfaces do not support the SPAN function, to monitor traffic on a WAN interface using a Network Analysis Module, a VACL has to be manually configured on the switch using the switch CLI. This feature only works for IP traffic over the WAN interface. Additional filtering rules can also be applied to target specific data flows.

---

Note

The VACL data analysis capability is not supported for WS-X6380-NAM.

VACL can also be used if there are no available SPAN sessions to direct traffic to the NAM. In this scenario, a VACL can be set up instead of SPAN for monitoring VLAN traffic.

The following examples illustrate the configuration steps required to configure a VACL for a switch running Cisco IOS Release 12.1(13)E1 or higher. To configure LAN VACL on a switch running the Catalyst operating system, the security use the ACL feature to achieve the same result.

This example shows how to configure VACL on an ATM WAN interface and forward both ingress and egress traffic to the NAM.

Cat6500# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Cat6509(config)# access-list 100 permit ip any any
Cat6509(config)# vlan access-map wan 100
Cat6509(config-access-map)# match ip address 100
Cat6509(config-access-map)# action forward capture
Cat6509(config-access-map)# exit
Cat6509(config)# vlan filter wan interface ATM6/0/0.1
Cat6509(config)# analysis module 3 data-port 1 capture allowed-vlan 1-4094
Cat6509(config)# analysis module 3 data-port 1 capture
Cat6509(config)# exit

When monitoring only egress traffic, the VLAN ID that is associated with the WAN interface can be obtained by using the following command:

Cat6509# show cwan vlan
Hidden VLAN swldb->if_number Interface
-----------------------------------------------
1017 94                          ATM6/0/0.1

After the VLAN ID is obtained, configure the NAM data port capture as follows:

Cat6509(config)# analysis module 3 data-port 1 capture allowed-vlan 1017

For monitoring ingress traffic, VLAN 1017 in the previous capture configuration should be replaced with the VLAN ID that carries the ingress traffic. For example, the following configuration allows NAM to monitor only ingress traffic on a WAN interface:

Cat6509(config)# analysis module 3 data-port 1 capture allowed-vlan 1
Configuring VACL on a LAN VLAN Interface

For VLAN traffic monitoring on the LAN, the traffic can be forwarded to the NAM by using the SPAN feature of the switch or router. However, in some rare circumstances, if the traffic spanned exceeds the NAM's monitoring capability, it may be desirable to pre-filter the LAN traffic before it is forward to the NAM. This result can be achieved by using the VACL as described below.

This example shows how to configure a VACL for the LAN VLAN interfaces. In this example, all traffic directed to the server 172.20.122.226 on VLAN 1 is captured and forwarded to the NAM located in slot 3.

Cat6500# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Cat6509(config)# access-list 100 permit ip any any
Cat6509(config)# access-list 110 permit ip any host 172.20.122.226
Cat6509(config)# vlan access-map lan 100
Cat6509(config-access-map)# match ip address 110
Cat6509(config-access-map)# action forward capture
Cat6509(config-access-map)# exit
Cat6509(config)# vlan access-map lan 200
Cat6509(config-access-map)# match ip address 100
Cat6509(config-access-map)# action forward
Cat6509(config-access-map)# exit
Cat6509(config)# vlan filter lan vlan-list 1
Cat6509(config)# analysis module 3 data-port 1 capture allowed-vlan 1
Cat6509(config)# analysis module 3 data-port 1 capture
Cat6509(config)# exit

Using NetFlow Data Export as a Traffic Source

NetFlow Data Export (NDE) makes traffic statistics available for analysis by an external data collector. You can use NDE to monitor all Layer 3-switched and all routed IP unicast traffic. To use NDE as a traffic source for the NAM, enable the NetFlow Monitor option to allow the NAM to receive the NDE stream. The statistics are presented on reserved ifIndex.3000.

Configuring NDE for a NetFlow device so that it exports NDE packets to the NAM is platform specific and version specific to the sending device. Refer to the device NDE configuration guidelines for necessary configuration steps as well as the usage guidelines for the NDE device. In general, NetFlow devices running Cisco IOS or the Catalyst operating system follow these configuration steps:

NDE Configuration

To configure NDE for the Cisco IOS software for both local and remote NDE devices, follow these steps:

---

**Step 1** Configure NDE as follows:

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface type slot/port

**Step 2** Enable NetFlow for the interface.

Router(config)# ip route-cache flow

**Step 3** Export the routed flow cache entries to the NAM UDP port 3000.

Router(config)# ip flow-export destination NAM-address 3000
The UDP port number must be set at 3000.

When you configure a NAM module as an NDE collector, you should use the IP address of the NAM (set up by sessioning into the NAM module).

This example shows how to set up a basic NDE configuration:

```bash
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface vlan 2
Router(config)# ip route-cache flow
Router(config)# ip flow-export destination 172.20.104.74 3000
Router(config)# exit
```

NDE Configuration from MLS Cache

To configure NDE from the PFC (Multi-layer switching cache), follow these steps:

**Step 1** Enter configuration mode.

```bash
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

**Step 2** Select the version of NDE.

```bash
Router(config)# mls nde sender version version-number
```

**Note** NAM supports NDE version 1, 5, 6, 7, 8, and version 8 aggregation caches. Refer to the Cisco IOS documentation for NDE versions supported by the switch software to determine which NDE versions are available to the NAM.

**Step 3** Select the NDE flow mask.

```bash
Router(config)# mls flow ip [interface-full | full]
```

**Note** Flow mask “full” is required to include additional details of collection data.

**Step 4** Enable NetFlow export.

```bash
Router(config)# mls nde sender
```

**Step 5** Export NetFlow packets to the NAM UDP port 3000.

```bash
Router(config)# ip flow-export destination NAM-Address 3000
```

This example shows how to set up an NDE configuration from the MSFC:

```bash
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# mls nde sender version 5
```
Chapter 3      Getting Started
Configuring Traffic Sources for Capturing NAM Traffic

Router(config)# mls flow ip full
Router(config)# mls nde sender
Router(config)# ip route-cache flow
Router(config)# ip flow-export destination 172.20.104.74 3000
Router# show ip cache flow
Router# show ip flow export

Note
For more information on configuring NDE on the PFC, refer this URL:
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/nde.htm - xtocid14

NDE Configuration for Version 8 Aggregation

Note
Although the NAM supports NDE aggregation, the information you receive for a specified aggregation type is limited to that aggregation, and other NDE details are not available. To receive more information about your NDE configuration, use the full flow mode.

If the NetFlow device supports NDE version 8 aggregations, flows from one or more of the version 8 aggregation caches may be exported to the NAM as follows:

Step 1  Select an NDE version 8 aggregation.
Router(config)# ip flow-aggregation cache aggregation-type

The supported aggregation types are:
- Destination-prefix
- Source-prefix
- Protocol-port
- Prefix

Step 2  Enable the aggregation cache.
Router(config-flow-cache)# enable

Step 3  Export the flows entries in the aggregation cache to NAM UDP port 3000.
Router(config-flow-cache)# export destination NAM-Address 3000

Step 4  Verify NDE.
Router# show ip cache flow-aggregation aggregation-type

This example shows how to set up an NDE version 8 aggregation configuration:

Router(config)# ip flow-aggregation cache prefix
Router(config-flow-cache)# enable
Router(config-flow-cache)# export destination 172.20.104.74 3000
Router(config-flow-cache)# exit
Router(config)# show ip cache flow-aggregation prefix
Catalyst Operating System Software

You can capture traffic for NAM monitoring from a single VLAN or from multiple VLANs. If you want to monitor traffic from specific VLANs only, you will need to clear the VLANs you do not want to monitor from the capture feature.

Using SPAN as a Traffic Source

You can configure SPAN as a traffic source using both the NAM Traffic Analyzer application and the switch CLI. We recommend that you use the NAM Traffic Analyzer.

You can use RSPAN traffic as a SPAN source for the NAM. Verify that the SPAN source is set to the same VLAN ID that is used for RSPAN. The SPAN destination should be set to nam_module/port.

Note

If you are using the switch CLI to configure SPAN as a traffic source to NAM-1, set the destination port to 3. If you are configuring SPAN as a traffic source to NAM-2, set the SPAN Port to destination port 7. Destination port 8 is not available in this NAM release although switch and hardware support is available.

Note

You cannot use NAM ports as SPAN source ports.

The NAM can analyze Ethernet traffic from Ethernet, Fast Ethernet, Gigabit Ethernet, trunk ports, or Fast EtherChannel SPAN source ports. You also can specify an Ethernet VLAN as the SPAN source.

For more information on configuring SPAN and RSPAN, refer to the switch software configuration guide.

To set the NAM as a SPAN destination port, perform this task in privileged mode:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the NAM as a SPAN destination port.</td>
<td>set span { src_mod/src_ports</td>
</tr>
</tbody>
</table>

This example shows how to SPAN VLAN 1 to a NAM-2 located in slot 5:

Console> (enable) set span 1 5/7

Using LAN VACL as a Traffic Source

Unlike WAN VACLs, which can be used to capture inbound or outbound VLAN packets, Catalyst operating system VACLs can only be used to capture VLAN packets as they are initially routed or bridged into the VLAN on the switch (this is not the same as saying that only inbound packets can be captured).

These examples show the Catalyst operating system command used to configure VACLs:

To create a VACL that captures all IP packets bridged or routed into VLAN 1 on the switch to the NAM-1 data port 6/3 use these commands:

Console> (enable) set security acl ip LANCAPTURE permit ip any any capture
Configuring Traffic Sources for Capturing NAM Traffic

Console> (enable)  commit
Console> (enable)  set security acl map LANCAPTURE 1
Console> (enable)  set sec acl cap 6/3

To create a VACL that captures a specific VLAN 1 conversation use these commands:

Console> (enable)  set sec acl ip LANCAPTURE permit ip host 172.20.122.70 host 172.20.122.226 capture
Console> (enable)  set security acl ip LANCAPTURE permit ip any any
Console> (enable)  commit
Console> (enable)  set security acl map LANCAPTURE 1
Console> (enable)  set sec acl cap 6/3

Using NetFlow Data Export as a Traffic Source

To use NetFlow Data Export (NDE) as a traffic source for the NAM, you must enable the NetFlow Monitor option to allow the NAM to receive the NDE stream. For a local switch, the statistics are presented on reserved ifIndex.3000 as in previous NAM releases. The remote switch uses ifIndex.50000 and greater.

Note: You need to configure the Multilayer Switch Function Card (MSFC) to use the NetFlow feature. For information on configuring NDE, refer to the Catalyst 6500 Series Switch Software Configuration Guide.

Note: There are no CLI commands for creating NetFlow custom data sources. To create a NetFlow custom data source, you must use the NAM Traffic Analyzer GUI.

NDE Configuration

To enable the NetFlow Monitor option for the Catalyst operating system, perform this task:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Select the NDE version.</td>
</tr>
<tr>
<td></td>
<td>set mls nde version nde-version-number</td>
</tr>
<tr>
<td>Note</td>
<td>The NAM supports NDE versions 1, 5, 6, 7, 8, and version 8 aggregation caches. Refer to the Cisco IOS documentation for NDE versions supported by the switch software to determine which NDE versions are available to the NAM.</td>
</tr>
</tbody>
</table>

| Step 2 | Select NDE flow mask to full. |
| | set mls flow full |
| Note | Although the NAM supports NDE aggregation, the information you receive for a specified aggregation type is limited to that aggregation and other NDE details are not available. To receive more information about your NDE configuration, use the full flow mode. |
Configuring Traffic Sources for Capturing NAM Traffic

This example shows how to enable the NetFlow Monitor option and verify that it is enabled:

```
Console> (enable) set snmp extendedrmon netflow enable
Snmp extended RMON netflow enabled
Console> (enable) show snmp
RMON: Enabled
Extended RMON NetFlow Enabled : Module 2
Traps Enabled:
None
Port Traps Enabled: None
Community-Access     Community-String
----------------     --------------------
read-only            public
read-write           private
read-write-all       secret

Trap-Rec-Address                           Trap-Rec-Community
----------------------------------------   --------------------
<...output truncated...>
```

Note
If a NAM is installed, you do not need to specify an external data collector with a `set mls nde collector_ip [udp_port_number]` command as described in the *Catalyst 6500 Series Software Configuration Guide*. Ignore any messages that indicate that the host and port are not set.

Exporting NDE From Bridged Flows Statistics

If the switch supports exporting NDE from bridged-flow statistics, you can use bridged-flow statistics to export NDE to the NAM.

To configure bridged-flow statistics export for NDE, perform this task:

```
Task | Command
--- | ---
Step 1 | Enable bridged-flow statistics on VLANs
       | set mls bridged-flow-statistics enable vlan-list
Step 2 | Export NDE packets to UDP port 3000 of the NAM.
       | set mls nde NAM-address 3000
```
Operating-System-Independent Configuration

The following sections describe the NAM configurations that are not dependent on the switch operating system.

Configuring Automatic RMON Collections

RMON collections can be configured explicitly through SNMP by a management station on some data sources. Collections that are explicitly configured through SNMP take precedence over autostart collections, so if both collections are configured, only the explicitly configured collections are started on each data source when the NAM initializes.

You can specify that some collections be automatically configured on every available data source (including all known VLANs) whenever the NAM is initialized by using the `autostart` command.

**Note**

We recommend that you explicitly configure those collections you require instead of using autostart to reduce the possibility of performance degradation due to many collections being started for each data source.

**Note**

When you enter the `autostart` command, you must reboot the NAM for that command to take effect.

The following collection types can be started automatically:

- addressMap—addressMapTable from RMON2-MIB (RFC 2021)
  
  If the NMS never sets the addressMapMaxDesiredEntries scalar, then the NAM uses the value -1 (for no limit).

- art—artControlTable from draft-warth-rmon2-artmib-01.txt

- etherStat—etherStatsTable from RMON-MIB (RFC 1757)

- prioStats—smonPrioStatsControlTable from SMON-MIB (RFC 2613)

- vlanStats—smonVlanStatsControlTable from SMON-MIB (RFC 2613)

For example, each dataSource (interface or VLAN) is configured with an etherStatsEntry (from RMON-1) after you enter the `autostart etherstats enable` command and reboot the NAM. The etherStatsOwner field is set to the `monitor` value.

The automatic start process occurs after you set up any collections that were explicitly created through SNMP by a management station and stored in the NVRAM in the NAM. Automatic start collections are not configured on data sources that already have a collection of that type configured through SNMP.

To enable collections for the automatic start process, do the following:

- Enable the etherStat collection type by entering this command from the root account of the NAM:

  ```
  root@localhost# autostart etherstat enable
  ```

- Enable the addressMap collection type by entering this command from the root account of the NAM:

  ```
  root@localhost# autostart addressmap enable
  ```

- Enable the prioStats collection type by entering this command from the root account of the NAM:

  ```
  root@localhost# autostart priostats enable
  ```
- Enable the vlanStats collection type by entering this command from the root account of the NAM:
  
  ```
  root@localhost# autostart vlanstats enable
  ```

- Disable the vlanStats collection type by entering this command from the root account of the NAM:
  
  ```
  root@localhost# autostart vlanstats disable
  ```

After enabling or disabling one or more collection types, you must reboot the NAM before the configuration takes effect.

### Configuring the HTTP or HTTP Secure Server

Before you can access the NAM through a web browser (HTTP or HTTPS), you must enable the NAM Traffic Analyzer application from the NAM CLI. For HTTP, use the `ip http server enable` command. For HTTPS, use the `ip http secure server enable` command. You also can optionally configure the HTTP (or HTTPS) servers to run on a different TCP port from the default.

---

**Note**

You can use the HTTP server or the HTTP secure server, but not both.

---

**Note**

The `ip http secure` commands are all disabled by default, and you must first download and install the NAM strong crypto patch from http://www.Cisco.com before you can enable them.

### Configuring the HTTP Server

To configure the HTTP server parameters for the NAM, follow these steps:

**Step 1**

(Optional) Configure the HTTP port by entering:

```
root@localhost# ip http port 8080
```

The HTTP server is enabled now. You must restart the server to change HTTP port. Continue [y/n]? y

The port number range is from 1 to 65535.

---

**Note**

Web users are different from the CLI users. Usernames and passwords for web users and CLI users are administered separately. For changing the user names and passwords on the NAM CLI, refer to the “Cisco IOS Software” section on page 4-1 and the “Catalyst Operating System Software” section on page 4-11. To change user names and passwords through the web interface, refer to the NAM Traffic Analyzer application online help and the User Guide for the Network Analysis Module NAM Traffic Analyzer Release 3.1.

**Step 2**

Enable the HTTP server by entering:

```
root@localhost# ip http server enable
```

Enabling HTTP server... 
No web users configured!
Please enter a web administrator username [admin]:admin
New password: 
Confirm password
User admin added.
Successfully enabled HTTP server.

Configuring the HTTP Secure Server

The `ip http secure` commands are all disabled by default, and you must enable the HTTP secure server by installing a strong crypto patch. If you prefer to use SSH instead of Telnet, you also must install a strong crypto patch.

To install a strong crypto patch, follow these steps:

**Step 1** Download the patch from http://www.Cisco.com and publish the patch in an FTP server.

**Step 2** Install the patch by entering:

```
root@localhost# patch ftp-url
```

`ftp-url` is the FTP location and the name of the strong crypto patch.

This example shows how to install a patch:

```
Console># # patch ftp://host/path/c6nam-3.1-strong-cryptoK9-patch-1-0.bin
Proceeding with installation. Please do not interrupt.
If installation is interrupted, please try again.

Downloading c6nam-3.1-strong-cryptoK9-patch-1-0.bin. Please wait...
ftp://host/path/c6nam-3.1-strong-cryptoK9-patch-1-0.bin (1K)
- [########################] 1K | 228.92K/s

1891 bytes transferred in 0.01 sec (225.40k/sec)
Verifying c6nam-3.1-strong-cryptoK9-patch-1-0.bin. Please wait...
Patch c6nam-3.1-strong-cryptoK9-patch-1-0.bin verified.

Applying /usr/local/nam/patch/workdir/c6nam-3.1-strong-cryptoK9-patch-1-0.bin.
Please wait...

Patch applied successfully.
```

**Step 3** (Optional) Configure the HTTPS server by entering:

```
root@localhost# ip http secure port 8080
```

The HTTP server is enabled now. You must restart the server to change HTTP port. Continue [y/n]? y

The port number range is from 1 to 65535.

**Note** Web users are different from the CLI users.

**Step 4** Enable the HTTPS server by entering:

```
root@localhost# ip http secure server enable
```

Enabling HTTP server...
No web users configured!
Please enter a web administrator username [admin]: admin
New password:
Confirm password
Generating Certificates

Certificates are used to validate the secure server connection. You can generate a self-signed certificate or obtain and install a certificate from a certification authority.

To generate a self-signed certificate, enter this command:

```
Console> (enable)# ip http secure generate self-signed-certificate
```

A certificate-signing request already exists. Generating a new self signed certificate will invalidate the existing signing request and any certificates already generated from the existing request. Enter y to reuse the existing certificate-signing request or n to generate a new one.

Reuse existing certificate-signing request? [y/n] y

The HTTP server is enabled now. You must restart to generate the certificate. Continue [y/n]? y

```
-----BEGIN CERTIFICATE-----
MIIDAzCCAmygAwIBAgIBADANBgkqhkiG9w0BAQQFADBlMQswCQYDVQQGEwJBVTETMBEGA1UECBMKU29t
ZSIrTGFZTEhMB8GA1UEChMYSXu2XQgV21kZ2l0cyBQdHkgTHRkMR4wHAYDVQQDExVuYW1sYWItcGl
rMy5jaXNjby5jb20wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAQN1k0wZwo1A8IQ89Gh6WP05SO
nFmJ+Bf0Nw2vKk/SjS5/3cH7cjsCZve4eU9lCiw6OxwNgtxsVy/3c21o+O87YDvK6s/imJGdXh
-----END CERTIFICATE-----
```

Disabling HTTP server...
Successfully disabled HTTP server.
Enabling HTTP server...
Successfully enabled HTTP server.

To obtain a certificate from a certification authority, you need to first generate a certificate-signing request and then submit the certificate-signing request manually to the certification authority. After obtaining the certificate from the certification authority, install the certificate.

Installing Certificates

To install a certificate from a certification authority, follow these steps:

**Step 1** Generate a certificate signing request by entering:

```
root@localhost# ip http secure generate certificate-request
```

A certificate-signing request already exists. Generating a new one will invalidate the existing one and any certificates already generated from the existing request. Do you still want to generate a new one? [y/n] y

524 semi-random bytes loaded
Generating RSA private key, 1024 bit long modulus

+-----+
| e is 65537 (0x10001)
| Using configuration from /usr/local/nam/defaults/openssl.cnf

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

Country Name (2 letter code) [AU]: IN
State or Province Name (full name) [Some-State]: Tamil Nadu
Locality Name (eg, city) []: Chennai
Organization Name (eg, company) [Internet Widgits Pty Ltd]: Cisco Systems
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [hostname.Cisco.com]: xxx@Cisco.com

-----BEGIN CERTIFICATE REQUEST-----
MIIBzzCCATgCAQAwgY4xCzAjBgNVAYTAKTAlOMRMwEQYDVQQIEw1ew1DhL3BQVQgMB4GA1UdDwEB/wQEAwIBBgcQEAwDQYJKoZIhvcNAQELBQAD

-----END CERTIFICATE REQUEST-----

Step 2 Install a certificate obtained from a certification authority by entering:

root@localhost# ip http secure install certificate

The HTTP server is enabled now. You must restart the server to install certificate. Continue [y/n]? y

Cut and paste the certificate you received from Certificate Authority. Enter a period (.), then press enter to indicate the end of the certificate.

-----BEGIN CERTIFICATE-----
MIIDAzCCAmygAwIBAgIBADANBgkqhkiG9w0BAQQAQFADB1MQswCQYDVQQGEwJBTETMBEGAIUECKHYSW50tZJ01twVl2k220cyQy

-----END CERTIFICATE-----

Chapter 3 Getting Started

Operating-System-Independent Configuration

A certificate-signing request already exists. Generating a new one will invalidate the existing one and any certificates already generated from the existing request. Do you still want to generate a new one? [y/n] y

524 semi-random bytes loaded
Generating RSA private key, 1024 bit long modulus

+-----+
| e is 65537 (0x10001)
| Using configuration from /usr/local/nam/defaults/openssl.cnf

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

Country Name (2 letter code) [AU]: IN
State or Province Name (full name) [Some-State]: Tamil Nadu
Locality Name (eg, city) []: Chennai
Organization Name (eg, company) [Internet Widgits Pty Ltd]: Cisco Systems
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [hostname.Cisco.com]: xxx@Cisco.com

-----BEGIN CERTIFICATE REQUEST-----
MIIBzzCCATgCAQAwgY4xCzAjBgNVAYTAKTAlOMRMwEQYDVQQIEw1ew1DhL3BQVQgMB4GA1UdDwEB/wQEAwIBBgcQEAwDQYJKoZIhvcNAQELBQAD

-----END CERTIFICATE REQUEST-----

Step 2 Install a certificate obtained from a certification authority by entering:

root@localhost# ip http secure install certificate

The HTTP server is enabled now. You must restart the server to install certificate. Continue [y/n]? y

Cut and paste the certificate you received from Certificate Authority. Enter a period (.), then press enter to indicate the end of the certificate.

-----BEGIN CERTIFICATE-----
MIIDAzCCAmygAwIBAgIBADANBgkqhkiG9w0BAQQAQFADB1MQswCQYDVQQGEwJBTETMBEGAIUECKHYSW50tZJ01twVl2k220cyQy

-----END CERTIFICATE-----
Using a TACACS+ Server

TACACS+ is a Cisco Systems authentication protocol that provides remote access authentication and related services. With TACACS+, user passwords are administered in a central database instead of individual routers.

When a user logs into NAM Traffic Analyzer, TACACS+ determines if the user name and password is valid and what access privileges the user has.

Before you can use the NAM with TACACS+, you must configure both the NAM and the TACACS+ server.

To configure the NAM for TACACS+, follow these steps:

---

Step 1  Start the NAM Traffic Analyzer application.

Step 2  Click the Admin tab.

Step 3  Choose Users.

Step 4  Choose TACACS+.

Step 5  Click the Enable TACACS+ Administration and Authentication box.

Step 6  Follow the instructions in the online help.

---
Administering the NAM

How you administer the NAM on your switch or router depends on whether you are using the Cisco IOS software or the Catalyst operating system software. Several NAM administration tasks are common to either operating system.

The following sections describe how to administrate the NAM from the CLI for each operating system:

- Cisco IOS Software, page 4-1
- Catalyst Operating System Software, page 4-11

When you have completed administrating the software-dependent attributes for the NAM, you can configure the software-independent NAM attributes in this section:

- Operating-System-Independent NAM Administration, page 4-20

These sections describe how to administer the NAM:

Cisco IOS Software

This section contains the various administrative tasks you can perform on the NAM with Cisco IOS:

- Logging In to the NAM, page 4-1
- Changing the NAM CLI Passwords, page 4-3
- Resetting the NAM, page 4-4
- Upgrading the NAM Software, page 4-5
- Configuring Mini-RMON, page 4-11

Logging In to the NAM

The NAM has two user levels with different access privileges:

- guest—Read-only access
  The default password is “guest.”
- root—All read and write access
  The default password is “root.”
Cisco IOS Software

Chapter 4  Administering the NAM

Note The root account uses the # prompt; the guest account uses the > prompt. The default root and guest passwords for the maintenance image is cisco if the NAM is the WS-SVC-NAM-1 or WS-SVC-NAM-2 module. The default root and guest passwords for the WS-X6380-NAM module is root.

Table 4-1 shows the user levels and passwords for the NAM.

Table 4-1  NAM Users and Passwords

<table>
<thead>
<tr>
<th>Module</th>
<th>Application Image (located on the hard disk)</th>
<th>Maintenance Image (located on the compact flash)</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS-SVC-NAM-1</td>
<td>User Password</td>
<td>User Password</td>
</tr>
<tr>
<td>WS-SVC-NAM-2</td>
<td>root root</td>
<td>root cisco</td>
</tr>
<tr>
<td></td>
<td>guest guest</td>
<td>guest cisco</td>
</tr>
<tr>
<td>WS-X6380-NAM</td>
<td>User Password</td>
<td>User Password</td>
</tr>
<tr>
<td></td>
<td>root root</td>
<td>root root</td>
</tr>
<tr>
<td></td>
<td>guest guest</td>
<td>guest guest</td>
</tr>
</tbody>
</table>

Note The guest account in the NAM maintenance image has All Read and All Write privileges.

When you boot into either the application image or the maintenance image and set up IP information, that information is synchronized between the images. However, if you change passwords, that information is not synchronized between the images and is not reflected on the unchanged image.

To allow remote Telnet sessions, use the exsession on command. SSH also can be used to log into the NAM. You must install the crypto patch to use this feature. To enable SSH on the NAM, use the exsession on ssh command.

To log in to the NAM, follow these steps:

Step 1 Log in to the switch or router using the Telnet connection or the console port connection.

Step 2 At the CLI prompt, establish a console session with the NAM using the session slot slot_number processor 1 command, as follows:

Router# session slot 8 processor 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.81 ... Open

Cisco Network Analysis Module (WS-SVC-NAM-1)

Step 3 At the NAM login prompt, type root to log in as the root user or guest to log in as a guest user.

login: root

Step 4 At the password prompt, enter the password for the account. The default password for the root account is “root” and the default password for the guest account is “guest.”

Password:
After a successful login, the command line prompt appears as follows:

```
Network Analysis Module (WS-SVC-NAM-1) Console, 2.1(1)
Copyright (c) 1999, 2000, 2001 by cisco Systems, Inc.
WARNING! Default password has not been changed!
root@localhost#
```

---

**Changing the NAM CLI Passwords**

If you have not changed the password from the factory-set default, a warning message displays when you log in to the NAM.

You can use the web application on the local database. If the administrator is unknown, you can use the CLI to remove the local web users from the web user database with the `rmwebusers` command.

---

**Note**

New passwords must be at least six characters in length, and may include uppercase and lowercase letters, numbers, and punctuation marks.

---

**Note**

For the WS-SVC-NAM-1 and WS-SVC-NAM-2 module, if the NAM maintenance image passwords are lost for the root or guest account, the maintenance image must be upgraded. After the upgrade, the passwords are set to the default. See Table 4-1 on page 4-2 or Table 4-5 on page 4-12.

To change the password, follow these steps while you are logged in to the root account on the NAM:

---

**Step 1**

Enter this command:

```
root@localhost# password username
```

**Note**

In NAM release 2.2, the `username` argument is required.

To change the root password, make a Telnet connection to the NAM and then use the `password root` command.

To change the guest password, make a Telnet connection to the NAM and then use the `password guest` command.

---

**Step 2**

Enter the new password:

```
Changing password for user root
New UNIX password:
```

**Step 3**

Enter the new password again:

```
Retype new UNIX password:
passwd: all authentication tokens updated successfully
```
This example shows how to set the password for the root account:

```
root@localhost# password root
Changing password for user root
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully
```

If you forget or lose the password, you can enter the `clear module pc-module module-number password` command from the switch CLI to restore the password for the root account to root and the guest account to guest on the application image.

## Resetting the NAM

If you cannot reach the NAM through the CLI or an external Telnet session, enter the `hw-module module module_number reset` command to reset and reboot the NAM. The reset process requires several minutes.

When the NAM initially boots, by default it runs a partial memory test. To perform a full memory test, use the `mem-test-full` keyword in the `hw-module module module_number reset device:partition mem-test-full` command. This command is specific to Cisco IOS and is not available in Catalyst operating system software.

The `mem-test-full` option is applicable only for WS-SVC-NAM-1 and WS-SVC-NAM-2.

For information on Catalyst operating system software, refer to “Resetting the NAM” section on page 4-15.

When you next reset the NAM, the full memory test runs. A full memory test takes more time to complete than a partial memory test. See Table 2-3 for memory test times.

You can also use the `hw-module module module_number mem-test-full` command to run a memory test. This example shows a full memory test for module 5:

```
Router(config)# hw-module module 5 boot-device mem-test-full
```

To reset the module from the CLI, perform this task in privileged mode:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset the module.</td>
<td><code>hw-module module mod_num reset device:partition mem-test-full</code></td>
</tr>
<tr>
<td></td>
<td>The device:partition value is the string for PC boot device, for example:</td>
</tr>
<tr>
<td></td>
<td><code>hdd:x</code> designates the hard disk, <code>cf:x</code> designates the compact Flash where</td>
</tr>
<tr>
<td></td>
<td><code>x</code> is the number for the partition on each device.</td>
</tr>
<tr>
<td></td>
<td>When specifying boot devices, for the NAM, refer to Table 4-2.</td>
</tr>
</tbody>
</table>

### Table 4-2 NAM Boot Devices

<table>
<thead>
<tr>
<th>WS-X6380-NAM</th>
<th>WS-SVC-NAM-1 and WS-SVC-NAM-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>When specifying the boot device, you must use hdd:1 for the application image and hdd:2 for the maintenance image.</td>
<td>When specifying the boot device for the WS-SVC-NAM-1 and the WS-SVC-NAM-2, you must use hdd:1 for the application image and cf:1 for the maintenance image.</td>
</tr>
</tbody>
</table>
This example shows how to reset the NAM that is installed in slot 9 from the CLI:

```sh
Router# hw-module mod 9 reset cf:1 memtest-full
Proceed with reload of module? [confirm] y
% reset issued for module 9
```

Note

When specifying the boot device for the WS-X3860-NAM, you must use hdd:1 for the application image or hdd:2 for the maintenance image. When specifying the boot device for the WS-SVC-NAM-1 and the WS-SVC-NAM-2, you must use hdd:1 for the application image and cf:1 for the maintenance image.

### Upgrading the NAM Software

You can upgrade both the application software and the maintenance software. To upgrade the application software, see the “Upgrading the NAM Application Software” section on page 4-17. To upgrade the maintenance software, see the “Upgrading the NAM Maintenance Software” section on page 4-19.

The NAM application and maintenance images are not inter-changeable.

- The images for the WS-X6380-NAM should not be used to upgrade the WS-SVC-NAM-1 and WS-SVC-NAM-2.
- The images for the WS-SVC-NAM-1 and WS-SVC-NAM-2 should not be used to upgrade the WS-X6380-NAM.

Table 4-3 lists the NAM image prefixes.

<table>
<thead>
<tr>
<th>Module</th>
<th>Application Image</th>
<th>Maintenance Image</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS-SVC-NAM-1</td>
<td>c6svc-nam</td>
<td>c6svc-nam-maint</td>
</tr>
<tr>
<td>WS-SVC-NAM-2</td>
<td>c6svc-nam</td>
<td>c6svc-nam-maint</td>
</tr>
<tr>
<td>WS-X6380-NAM</td>
<td>c6nam</td>
<td>c6nam-maint</td>
</tr>
</tbody>
</table>

### Upgrading the NAM Application Software

To upgrade the NAM application software, follow these steps:

**Step 1**

Copy the NAM application software image to a directory accessible to FTP.

**Step 2**

Log in to the switch through the console port or through a Telnet session.

**Step 3**

If the NAM is running in the maintenance image, go to **Step 4**. If the NAM is not running in the maintenance image, enter this command in privileged mode:

```sh
Router# hw-module module 9 reset cf:1
```

```
Device BOOT variable for reset = cf:1
Warning:Device list is not verified.
Proceed with reload of module? [confirm] y
% reset issued for module 9
```

```
00:03:31:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:03:31:SP:The PC in slot 9 is shutting down. Please wait ...
00:03:41:%SNMP-5-COLDSTART:SNMP agent on host R1 is undergoing a cold
```
Step 4 After the NAM is back online, establish a console session with the NAM and log in to the root account.

Router# session slot 9 proc 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.91 ... Open
Cisco Network Analysis Module (WS-SVC-NAM-1)
Maintenance Partition
login: root
Password:
Network Analysis Module (WS-SVC-NAM-1) Console, 1.2(1a)m
Copyright (c) 1999, 2000, 2001 by cisco Systems, Inc.

Step 5 Upgrade the NAM application software by entering either:

root@localhost# upgrade ftp-url

ftp-url is the FTP location and name of the NAM software image file.

or

root@localhost# upgrade ftp-url --install

Note The --install option wipes and recreates all of the NAM partitions; similar to the factory default state. The --install option is only applicable to the WS-SVC-NAM-1 and WS-SVC-NAM-2 modules. If you use the --install option, the previously stored reports data (if any), will be lost.

Note If the FTP server does not allow anonymous users, use this syntax for the ftp-url value:
ftp://user@host/absolute-path/filename. Enter your password when prompted.

Step 6 Follow the screen prompts during the upgrade.

Step 7 After completing the upgrade, log out of the NAM.

Step 8 Reset the NAM by entering:

Router# hw-module mod 9 reset
Device BOOT variable for reset =
Warning:Device list is not verified.
Proceed with reload of module? [confirm]
% reset issued for module 9
Router#
For optimal performance on the NAM, you must use an additional one-time reboot immediately after booting to the application partition after you upgrade the NAM software.

**Step 9**
(Optional) Verify the initial configuration after the NAM comes back online by logging into the NAM root account and then entering:

```
root@localhost# show ip
root@localhost# show snmp
root@localhost# show version
```

This example shows how to upgrade the NAM application software:

```
Router# hw-module module 9 reset cf:1
Device BOOT variable for reset = cf:1
Warning:Device list is not verified.

Proceed with reload of module? [confirm]
% reset issued for module 9

Router# 00:16:06:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:16:06:SP:The PC in slot 9 is shutting down. Please wait ...
00:16:21:SP:PC shutdown completed for module 9
00:16:21:%C6KPWR-SP-4-DISABLED:power to module in slot 9 set off (admin request)
00:16:24:SP:Resetting module 9 ...
00:16:24:%C6KPWR-SP-4-ENABLED:power to module in slot 9 set on
00:18:21:%SNMP-5-MODULETRAP:Module 9 [Up] Trap
00:18:21:%DIAG-SP-6-BYPASS:Module 9:Online Diagnostics is Bypassed
00:18:21:%OIR-SP-6-INSCARD:Card inserted in slot 9, interfaces are now online

Router# session slot 9 proc 1
The default escape character is Ctrl-~, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.91 ... Open

Cisco Network Analysis Module (WS-SVC-NAM-1)

Maintenance image

login:root
Password:

Maintenance image version:1.1(0.1)

root@localhost.cisco.com# upgrade ftp://mylab-pc1/pub/rmon/c6nam3.1-2-0-8.bin.gz
```

Upgrading will wipe out the contents on the hard disk.
Do you want to proceed installing it [y|N]:
```
Proceeding with upgrade. Please do not interrupt. 
If the upgrade is interrupted or fails, boot into 
Maintenance image again and restart upgrade.

Creating NAM application image file...

Initializing the application image partition...
Applying the image, this may take several minutes...
Performing post install, please wait...
Upgrade complete. You can boot from the Application image.

00:21:50:%NAM-3-NO_RESP:Module 9 is not responding
Upgrade complete. You can boot the new application partition.
root@hostname.cisco.com# exit

[Connection to 127.0.0.91 closed by foreign host]
Router#

Router# hw-module module 9 reset
Device BOOT variable for reset =
Warning:Device list is not verified.

Proceed with reload of module? [confirm] y
% reset issued for module 9

Router#
00:24:04:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:24:04:SP:The PC in slot 9 is shutting down. Please wait ... 
00:24:18:SP:PC shutdown completed for module 9
00:24:18:%C6KPWR-SP-4-DISABLED:power to module in slot 9 set off (admin request)
00:24:21:SP:Resetting module 9 ...
00:24:21:%C6KPWR-SP-4-ENABLED:power to module in slot 9 set on
00:26:19:%SNMP-5-MODULETRAP:Module 9 [Up] Trap
00:26:19:%OIR-SP-6-INSCARD:Card inserted in slot 9, interfaces are now online

Upgrading the NAM Maintenance Software

To upgrade the NAM maintenance software, follow these steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Copy the NAM maintenance software image to a directory accessible to FTP.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Log in to the switch through the console port or through a Telnet session.</td>
</tr>
<tr>
<td>Step 3</td>
<td>If the NAM is running in the application image go to Step 5. If the NAM is not running in the application image, enter this command in the privileged mode:</td>
</tr>
</tbody>
</table>

Router# hw-module module 9 reset hdd:1
Device BOOT variable for reset = hdd:1
Warning:Device list is not verified.

Proceed with reload of module? [confirm] y
% reset issued for module 9

Router#
00:31:11:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:31:11:SP:The PC in slot 9 is shutting down. Please wait ... 
00:31:25:SP:PC shutdown completed for module 9
00:31:25:%C6KPWR-SP-4-DISABLED:power to module in slot 9 set off (admin request)
Step 4  After the NAM is back online, establish a console session with the NAM and log in to the root account.

Step 5  Upgrade the NAM maintenance software by entering:

```
root@localhost# upgrade ftp-url
```

*ftp-url* is the FTP location and name of the NAM software image file.

**Note**  If the FTP server does not allow anonymous users, use the following syntax for the *ftp-url* value: `ftp://user@host/absolute-path/filename`. Enter your password when prompted.

Step 6  Follow the screen prompts during the upgrade.

Step 7  After completing the upgrade, log out of the NAM.

Step 8  Boot into the maintenance image with this command to reset the NAM maintenance software:

```
Router# hw-module module 9 reset cf:1
Device BOOT variable for reset = cf:1
Warning:Device list is not verified.
```

Proceed with reload of module? [confirm]
% reset issued for module 9

```
Router#
```

Step 9  *(Optional)* Verify the initial configuration after the NAM comes back online by logging into the NAM root account and enter the following command:

```
root@localhost# show ip
```

Step 10  *(Optional)* Reboot into the application image by entering:

```
Router# hw-module module 9 reset
```

This example shows how to upgrade the NAM maintenance software:

```
Router# hw-module module 9 reset hdd:1
Device BOOT variable for reset = hdd:1
Warning:Device list is not verified.
```
Proceed with reload of module? [confirm]
% reset issued for module 9
Router#
00:31:11:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:31:11:SP:The PC in slot 9 is shutting down. Please wait ...
00:31:25:SP:PC shutdown completed for module 9
00:31:25:%C6KPWR-SP-4-DISABLED:power to module in slot 9 set off (admin request)
00:31:28:SP:Resetting module 9 ...
00:31:28:%C6KPWR-SP-4-ENABLED:power to module in slot 9 set on
00:33:26:%SNMP-5-MODULETRAP:Module 9 [Up] Trap
00:33:26:%DIAUG-SP-6-BYPASS:Module 9:Online Diagnostics is Bypassed
00:33:26:%OIR-SP-6-INSocard:Card inserted in slot 9, interfaces are now online
Router#

Router# session slot 9 proc 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.91 ... Open

Cisco Network Analysis Module (WS-SVC-NAM-2)

login:root
Password:

Cisco Network Analysis Module (WS-SVC-NAM-2) Console, 3.1(0.1)
Copyright (c) 1999-2002 by cisco Systems, Inc.

WARNING! Default password has not been changed!
root@localhost.cisco.com#

root@localhost.cisco.com# upgrade ftp://host/pub/rmon/mp.1-1-0-1.bin.gz

Downloading image...
ftp://host/pub/rmon/mp.1-1-0-1.bin.gz (11065K)
- [####################] 11065K | 837.65K/s
11331153 bytes transferred in 13.21 sec (837.64k/sec)

Uncompressing the image...

Verifying the image...

Applying the Maintenance image.
This may take several minutes...

Upgrade of Maintenance image completed successfully.
root@hostname.cisco.com# exit

Router# hw-module module 9 reset cf:1
Device BOOT variable for reset = cf:1
Warning:Device list is not verified.

Proceed with reload of module? [confirm]
% reset issued for module 9
Router#
02:27:19:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
02:27:19:SP:The PC in slot 9 is shutting down. Please wait ...
02:27:36:SP:PC shutdown completed for module 9
02:27:36:%C6KPWR-SP-4-DISABLED:power to module in slot 9 set off (admin request)
Configuring Mini-RMON

In Cisco IOS, you must explicitly enable mini-RMON per interface. To configure mini-RMON for each interface enter the `rmon collection stats collection-control-index owner owner-string`. You must enter the `collection-control-index` and `owner-string` command values.

Note
The NAM only displays mini-RMON collections configured with an owner string of `monitor`.

This example shows how to configure mini-RMON on Fast Ethernet module 4 port 1 using control index 3000 and an owner string of `monitor`:

```
Router# config term
Router(config)# interface fast4/1
router(config-if)# rmon collection stats 3000 owner "monitor"
router(config-if)# end
```

Catalyst Operating System Software

This section contains the various administrative tasks you can perform on the NAM using the Catalyst operating system software:

- Logging In to the NAM, page 4-12
- Changing the NAM CLI Passwords, page 4-13
- Resetting the NAM, page 4-15
- Upgrading the NAM Software, page 4-17
- Configuring Mini-RMON, page 4-20

You can administer the NAM by using the NAM Traffic Analyzer application. Refer to the User Guide for the Network Analysis Module NAM Traffic Analyzer Release 3.1 for more information about Traffic Analyzer.

You can perform these administrative tasks on the NAM:

- Add and remove NAM users and change passwords using either the CLI or the NAM Traffic Analyzer application.
- Recover passwords as superuser (but not change passwords).
- Change local and remote (TACACS+ server) users and passwords by using the NAM Traffic Analyzer application. Refer to the NAM Traffic Analyzer application online help topic “User and System Administration” for information about user and password administration.
Table 4-4 describes the user administration tasks you can perform using the CLI and NAM Traffic Analyzer application.

Table 4-4  NAM User Administration

<table>
<thead>
<tr>
<th>User Interface</th>
<th>Add Users</th>
<th>Remove Users</th>
<th>Set Password</th>
<th>Recover Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLI</td>
<td>No</td>
<td>No</td>
<td>Use the password command.</td>
<td>No</td>
</tr>
<tr>
<td>Traffic Analyzer</td>
<td>Add the first user with the CLI when starting the web server. Add all subsequent users through the web GUI for the local database or through TACACS+ if the TACACS+ server is used. Additionally, you can create web users with the CLI web-user command.</td>
<td>Use the no web-user command.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traffic Analyzer</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>local database</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traffic Analyzer</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>TACACS+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Logging In to the NAM

There are two levels of access on the NAM, each with different privileges:

- **Guest**—Read-only CLI access (default password is guest)
- **Root**—Full read-write access (default password is cisco)

Note: The root account uses the # prompt; the guest account uses the > prompt. The default root and guest passwords for the maintenance image is **cisco**.

Table 4-5 shows the user levels and passwords for the NAM.

Table 4-5  NAM Users and Passwords

<table>
<thead>
<tr>
<th>Application Image (located on the hard disk)</th>
<th>Maintenance Image (located on the compact flash)</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Password</td>
</tr>
<tr>
<td>root</td>
<td>root</td>
</tr>
<tr>
<td>guest</td>
<td>guest</td>
</tr>
</tbody>
</table>

Note: The guest account in the NAM maintenance image has All Read and All Write privileges.
When you boot into either the application image or the maintenance image and setup IP information, that information is synchronized between the images. If you change passwords, that information is not synchronized between the images and is not reflected on the unchanged image.

To log into the NAM, follow these steps:

**Step 1** Log into the Catalyst 6500 series switch using the Telnet connection or the console port connection.

*Note* To make remote Telnet sessions, use the `exsession on` command. SSH also can be used to log into the NAM. You must install the crypto patch to use this feature. To enable SSH on the NAM, use the `exsession on ssh` command.

**Step 2** Establish a console session with the NAM at the CLI prompt, using the `session mod` command:

```
Console> (enable) session 4
Trying NAM-4...
Connected to NAM-4.
Escape character is '^]'.
Cisco Network Analysis Module (WS-SVC-NAM-1)
login: root
Password:
```

**Step 3** To log into the NAM, type `root` to log in as the root user or `guest` to log in as a guest user at the login prompt.

```
login: root
```

**Step 4** At the password prompt, enter the password for the account. The default password for the root account is “root,” and the default password for the guest account is “guest.”

```
Password:
```

After a successful login, the command-line prompt appears as follows:

```
Network Analysis Module (WS-SVC-NAM-1) Console, 3.1(0.1)
Copyright (c) 1999-2002 by Cisco Systems, Inc.
WARNING! Default password has not been changed!
root@localhost#
```

### Changing the NAM CLI Passwords

You can use these methods to change and recover passwords:

- Use a Telnet connection to the NAM and CLI.
  
  You can configure, change, and recover root and guest passwords:
  
  - To change the password, use a Telnet connection to the NAM, and then use the `password` command to change the password.
  
  - To recover the password, use the Telnet connection to the supervisor engine, and then use the `clear module password module` command.
If you forget or lose the password, you can enter the `clear module password` command from the switch CLI to restore the password for the root account to root and the guest account to guest.

To restore the NAM password to the factory-set defaults, enter this command in privileged mode:

```
Console> (enable) clear module password module
```

- Use the NAM Traffic Analyzer on the local database.

You create the initial NAM Traffic Analyzer application user with the CLI. After starting NAM Traffic Analyzer, you can establish and edit additional user passwords. You use NAM Traffic Analyzer or the TACACS+ server to change passwords as follows:

- As the NAM Traffic Analyzer application administrator, you can reset passwords.
- If the administrator is unknown, you can use the CLI to remove the local web user database from the web database with the `rmwebusers` command.

- Use the instructions in the TACACS+ server documentation.

If the NAM maintenance image passwords are lost for the root or guest account, the maintenance image must be upgraded. After the upgrade, the passwords are set to the default. See Table 4-1 on page 4-2 or Table 4-5 on page 4-12.

If you have not changed the password from the factory-set default password, a warning message appears when you log into the NAM.

New passwords must be at least six characters in length, and may include uppercase and lowercase letters, numbers, and punctuation marks.

To change a password, follow these steps while logged into the NAM as root:

**Step 1**

Enter this command:

```
root@localhost# password username
```

**Note**

In NAM software release 2.2, the `username` argument is required.

To change the root password, make a Telnet connection to the NAM and then use the `password root` command.

To change the guest password, make a Telnet connection to the NAM and then use the `password guest` command.

**Step 2**

Enter the new password:

```
Changing password for user root
New UNIX password:
```

**Step 3**

Enter the new password again:

```
Retyp new UNIX password: passwd: all authentication tokens updated successfully
```
This example shows how to set the password for the root account:

```
root@localhost# password root
Changing password for user root
New UNIX password:
Retype new UNIX password:
pwd: all authentication tokens updated successfully
```

If you forget or lose the password, you can enter the `clear module password` command from the CLI to restore the password for the root account to root and the guest account to guest.

**Resetting the NAM**

If you cannot reach the NAM through the CLI or an external Telnet session, enter the `reset mod_num boot_string` command to reset and reboot the NAM. The reset process requires several minutes.

When the NAM initially boots, by default it runs a partial memory test. To perform a full memory test, enter the `set boot device bootseq mod# mem-test-full` command. This command is specific to Catalyst operating system software and is not available in Cisco IOS software.

The `mem-test-full` option is applicable only for WS-SVC-NAM-1 and WS-SVC-NAM-2.

For Cisco IOS, refer to the “Resetting the NAM” section on page 4-4.

To enable a full memory test use the `set boot device bootseq mod# mem-test-full` command. This example shows how to do a full memory test:

```
Console (enable) set boot device cf:1 4 mem-test-full
Device BOOT variable = cf:1
Memory-test set to FULL
Warning:Device list is not verified but still set in the boot string.

Console> (enable)
Device BOOT variable = cf:1
Memory-test set to FULL

When you next reset the NAM, the full memory test runs.

This example shows how to reset the partial memory test:

```
Console> (enable) set boot device cf:1 4
Device BOOT variable = cf:1
Memory-test set to PARTIAL
Warning:Device list is not verified but still set in the boot string.
Console> (enable)
Console> (enable) show boot device 4
Device BOOT variable = cf:1
Memory-test set to PARTIAL
```
To reset the NAM from the CLI, perform this task in privileged mode:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset the NAM</td>
<td><code>reset mod_num boot_string</code></td>
</tr>
</tbody>
</table>

The `mod_num boot_string` variable is the string for PC boot device, for example: `hdd:x` designates the hard disk, `cf:x` designates the compact flash where `x` is the number for the partition on each device.

When specifying boot devices, refer to Table 4-6 for boot device specifications for the NAM.

### Table 4-6 NAM Boot Devices

<table>
<thead>
<tr>
<th>WS-X6380-NAM</th>
<th>WS-SVC-NAM-1 and WS-SVC-NAM-2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>When specifying the boot device, you must use hdd:1 for the application image and hdd:2 for the maintenance image.</td>
</tr>
</tbody>
</table>

This example shows how to reset the NAM, installed in slot 9:

```
Router# reset 9 hdd:1
Proceed with reload of module? [confirm] y
% reset issued for module 9
```

**Note**

For the boot device, you can specify hdd:1 for the application image or cf:1 for the maintenance image.

```
Router#
00:26:55:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:26:55:SP:The PC in slot 8 is shutting down. Please wait ...
```

To reset the module to the maintenance image, from the enable mode enter the following command:

```
Console> (enable) reset <module #> cf:1
```

To reset the module to the NAM application image, from the enable mode enter the following command:

```
Console> (enable) reset <module #> |
```

This example shows how to reset the NAM that is installed in slot 4 from the CLI:

```
Console> (enable) reset 4
This command will reset module 4.
Unsaved configuration on module 4 will be lost
Do you want to continue (y/n) [n]? y
ResetPcBlade:start shutdown module 4
SendShutDownMsg - proc_id (1): shut down PC success.
```
Module 4 shut down in progress, please don’t remove module until shutdown completed.
Module 4 is online.

You can enable a full memory test when you use the `set boot device bootseq mod# mem-test-full` command. This option is disabled by default. This example shows how to do a full memory test:

```plaintext
Console (enable) set boot device cf:1 4 mem-test-full
Device BOOT variable = cf:1
Memory-test set to FULL
Warning:Device list is not verified but still set in the boot string.

Console> (enable) show boot device 4
Device BOOT variable = cf:1
Memory-test set to FULL

When you next reset the NAM, the full memory test will run. A full memory test takes more time to complete than a partial memory test. See Table 2-3 for memory test times.

This example shows how to reset the partial memory test:

```plaintext
Console> (enable) set boot device cf:1 4
Device BOOT variable = cf:1
Memory-test set to PARTIAL
Warning:Device list is not verified but still set in the boot string.

Console> (enable)
Console> (enable) show boot device 4
Device BOOT variable = cf:1
Memory-test set to PARTIAL
```

**Upgrading the NAM Software**

You can upgrade both the application software and the maintenance software. To upgrade the application software, see the “Upgrading the NAM Application Software” section on page 4-17. To upgrade the maintenance software, see the “Upgrading the NAM Maintenance Software” section on page 4-19.

**Upgrading the NAM Application Software**

To upgrade the NAM application software, follow these steps:

1. **Step 1** Copy the NAM application software image to a directory accessible to FTP.
2. **Step 2** Log into the switch through the console port or through a Telnet session.
3. **Step 3** If the NAM is already running in the maintenance image, go to **Step 4**. If the NAM is not running in the maintenance image, enter this command in privileged mode:
   ```plaintext
   Console> (enable) reset mod cf:1
   ```
4. **Step 4** After the NAM is back online, establish a console session with the NAM and log into the root account.
5. **Step 5** Upgrade the NAM application software by entering:
   ```plaintext
   root@localhost# upgrade ftp-url
   
   ftp-url is the FTP location and name of the NAM software image file.
   ```
   or
   ```plaintext
   root@localhost# upgrade ftp-url --install
   ```
The `--install` option wipes and recreates all of the NAM partitions; similar to the factory default state.

If the FTP server does not allow anonymous users, use the following syntax for the `ftp-url` value: `ftp://user@host/absolute-path/filename`. Enter your password when prompted.

**Step 6** Follow the screen prompts during the upgrade.

**Step 7** After completing the upgrade, log out of the maintenance image.

**Step 8** Reset to the NAM application image by entering:

```
Console> (enable) reset mod
```

**Step 9** (Optional) Verify the initial configuration after the NAM comes back online by logging into the NAM root account and entering the following commands:

```
root@localhost# show ip
root@localhost# show snmp
```

This example shows how to upgrade the NAM application software:

```
Console> (enable) reset 4 cf:1
This command will reset module 4.
Unsaved configuration on module 4 will be lost
Do you want to continue (y/n) [n]? y
2002 May 07 22:21:20 %SYS-5-MOD_RESET:Module 4 reset from Software
Console> (enable) 2002 May 07 22:24:41 %SYS-3-SUP_OSBOOTSTATUS:MP OS Boot Status :finished booting

Console> (enable) session 4
Trying NAM-4...
Connected to NAM-4.
Escape character is '^]'.

Maintenance image

login: root
Password:

Maintenance image version:1.1(0.1)

root@localhost# upgrade ftp://mylab-pc1/pub/rmon/c6nam3.1-2-0-8.bin.gz
Downloading the image. This may take several minutes... 
/tmp/upgrade.gz [###############################] 59198K | 821.24K/s 60619473 bytes transferred in 72.08 sec (821.23k/sec)

Upgrading will wipe out the contents on the hard disk.
Do you want to proceed installing it [y|N]: y
Proceeding with upgrade. Please do not interrupt.
If the upgrade is interrupted or fails, boot into Maintenance image again and restart upgrade.

Creating NAM application image file...
```
Initializing the application image partition...
Applying the image, this may take several minutes...
Performing post install, please wait...
Upgrade complete. You can boot from the Application image.

Console> (enable) reset 4
This command will reset module 4.
Unsaved configuration on module 4 will be lost
Do you want to continue (y/n) [n]? y
ResetPcBlade:start shutdown module 4
SendShutDownMsg - proc_id (1):shut down PC success.
Module 4 shut down in progress, please don't remove module until shutdown completed.
Console> (enable) 2002 May 07 23:19:03 %SYS-5-MOD_OK:Module 4 is online

Upgrading the NAM Maintenance Software

To upgrade the NAM maintenance software, follow these steps:

---

**Step 1**  
Copy the NAM maintenance software image to a directory that is accessible to FTP.

**Step 2**  
Log into the switch through the console port or through a Telnet session.

**Step 3**  
If the NAM is running in the application image, go to **Step 4**. If the NAM is not running in the application image, enter this command in privileged mode:

```
Console> (enable) reset mod
```

**Step 4**  
After the NAM is back online, establish a console session with the NAM and log into the root account.

**Step 5**  
Upgrade the NAM maintenance software by entering:

```
root@localhost# upgrade ftp-url
```

*ftp-url* is the FTP location and the name of the NAM software image file.

**Note**  
If the FTP server does not allow anonymous users, use the following syntax for the *ftp-url* value: *ftp://user@host/absolute-path/filename*. Enter your password when prompted.

**Step 6**  
Follow the screen prompts during the upgrade.

**Step 7**  
After completing the upgrade, log out of the NAM.

**Step 8**  
Boot into the maintenance image with this command to reset the NAM maintenance software:

```
Console> (enable) reset mod cf:1
```

**Step 9**  
(Optional) Verify the initial configuration after the NAM comes back online by logging into the NAM root account, and enter the following commands:

```
root@localhost# show ip
root@localhost# show snmp
```

**Step 10**  
(Optional) Reboot into the application image by entering:

```
Console> (enable) reset mod
```
This example shows how to upgrade the NAM maintenance software:

Console> (enable) reset 4
This command will reset module 4.
Unsaved configuration on module 4 will be lost
Do you want to continue (y/n) [n]? y
ResetPcBlade:start shutdown module 4
SendShutDownMsg - proc_id (1): shut down PC success.
Module 4 shut down in progress, please don’t remove module until shutdown completed.
Console> (enable) 2002 May 07 23:19:03 %SYS-5-MOD_OK: Module 4 is online

Console> (enable) session 4
Trying NAM-4...
Connected to NAM-4.
Escape character is '^]'.

Cisco Network Analysis Module (WS-SVC-NAM-2)

login: root
Password:

Cisco Network Analysis Module (WS-SVC-NAM-2) Console, 3.1(0.1)
Copyright (c) 1999-2002 by cisco Systems, Inc.

WARNING! Default password has not been changed!
root@localhost.cisco.com# upgrade ftp://host/pub/rmon/mp.1-1-0-1.bin.gz

downloading image...
ftp://host/pub/rmon/mp.1-1-0-1.bin.gz (11065K)
[-] 11331153 bytes transferred in 13.21 sec (837.64k/sec)

Uncompressing the image...

Verifying the image...

Applying the Maintenance image.
This may take several minutes...

Upgrade of Maintenance image completed successfully.

Configuring Mini-RMON

In Catalyst operating system software, you can enable mini-RMON for the switch.

This example shows how to configure mini-RMON:

Console (enable)# set snmp rmon enable

Operating-System-Independent NAM Administration

The following section describes NAM administration that is not dependent of the switch operating system.
Adding NAM Patch Software

To install a patch on the NAM, follow these steps:

**Step 1** Log into the switch through the console port or through a Telnet session.

**Step 2** If the NAM is running in the application image, go to Step 4. If the NAM is in the maintenance image, enter this command in privileged mode:

For Cisco IOS software, enter:

```
Console> (enable) hw-module module module_number reset
```

For Catalyst operating system software, enter:

```
Console> (enable) reset mod hdd:1
```

**Step 3** After the NAM is back online, establish a console session with the NAM, and then log into the root account.

**Step 4** Install the patch software to the NAM software by entering:

```
root@localhost# patch ftp-url
```

`ftp-url` is the FTP location and the name of the NAM patch software image file.

**Note** If the FTP server does not allow anonymous users, use the following syntax for the `ftp-url` value: `ftp://user@host/absolute-path/filename`. Enter your password when prompted.

**Step 5** Follow the screen prompts during the patch application process.

**Step 6** (Optional) Verify the initial configuration after the NAM comes back online by logging into the NAM root account and then entering these commands:

```
root@localhost# show ip
root@localhost# show patches
```

**Note** If HTTP or the HTTP server are running, and you are running the NAM Traffic Analyzer web application, click on the About link in the GUI to display a list of installed patches. If nothing appears, no patches were installed.

This Catalyst operating system software example shows how to apply patch software:

```
Console> (enable) reset 4
This command will reset module 4.
Unsaved configuration on module 4 will be lost
Do you want to continue (y/n) [n]? y
ResetPcBlade: start shutdown module 4
SendShutDownMsg - proc_id (1): shut down PC success.
Module 4 shut down in progress, please don't remove module until shutdown completed.
Console> (enable) 2002 May 07 23:19:03 %SYS-5-MOD_OK: Module 4 is online
Console> (enable) session 4
Trying NAM-4...
Connected to NAM-4.
```
Additional NAM Software Administrative Commands

Refer to the Catalyst 6500 Series and Cisco 7600 Series Network Analysis Module Command Reference for information on NAM commands available through the NAM CLI.

The NAM supports these additional administrative commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip</td>
<td>Clears the network configuration for the interface. This command is not available in the application partition. The corresponding command for the application partition is: <code>config clear ip</code>. This command is used only for the WS-SVC-NAM-1 and the WS-SVC-NAM-2 module maintenance image.</td>
</tr>
<tr>
<td>clear log upgrade</td>
<td>Clears the application image upgrade log file. This command is available only in the maintenance image and the guest account in the maintenance image. This command is used only for the WS-SVC-NAM-1 and the WS-SVC-NAM-2 module maintenance image.</td>
</tr>
</tbody>
</table>
### Command Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| `config clear`           | Restores the NAM to the factory default state but does not `config clear ip` parameters. **Note** All the `config clear` commands require a reboot, which is done after you are prompted. The `config clear` and `config clear all` commands wipe historic report data. Default settings cleared include the following:  
  - Deleting all RMON control tables.  
  - Deleting all RMON1 and RMON2 filters.  
  - Returning the RMON configuration file to the default configuration.  
  - Restores the protocol directory to default.  
  - The web server is stopped (if a web server was running).  
  - These configurations are cleared:  
    - Remote device configuration.  
    - Local web users.  
    - All custom capture and custom decode filters.  
    - Report configurations.  
    - Web access logs.  
    - DSMON aggregate configurations.  
  - Syslog configurations are reset.  
  - NAM web preferences are reset.  
  - Autostart configurations are reset.  
  - External Telnet sessions are switched off.  
  - No IP host configuration data is deleted.  
  - The NAM is rebooted automatically after entering the `config clear` command to allow these changes to take effect.  
  - This command can be used by the root account only. |
| `config clear ip`        | Restores only the NAM IP parameters to the factory default state.            |
| `config clear all`       | Restores all NAM configuration to factory default state. This command also clears the IP parameters. |
| `coredump ftp://host/absolute-path` | Sends a core file to an anonymous FTP server after the RMON agent crashes. This command can upload multiple core files. The command uploads all of the core files for the form “core” located under the `/ust/local/nam/bin` directory. You should always copy and save this information to a file before calling the Cisco Technical Assistance Center (TAC). Cisco TAC needs this information to analyze and troubleshoot the NAM. Only one core dump file is maintained. A newly created core dump file overwrites an existing core dump file. This command can be used only by the root account. **Note** If the FTP server does not allow anonymous users, use the following syntax: `coredump ftp://user:password@host/absolute-path`. |
### Command Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>disable-guest</strong></td>
<td>Disables the guest account from the maintenance image. This command is used only for the WS-SVC-NAM-1 and the WS-SVC-NAM-2 module maintenance image.</td>
</tr>
<tr>
<td><strong>enable-guest</strong></td>
<td>Enables the guest account from the maintenance image. This command is used only for the WS-SVC-NAM-1 and the WS-SVC-NAM-2 module maintenance image.</td>
</tr>
<tr>
<td>**exsession [on</td>
<td>off] [ssh]**</td>
</tr>
<tr>
<td></td>
<td><strong>exsession on</strong> — Enables Telnet.</td>
</tr>
<tr>
<td></td>
<td><strong>exsession on ssh</strong> — Enables SSH.</td>
</tr>
<tr>
<td></td>
<td><strong>exsession off</strong> — Disables Telnet.</td>
</tr>
<tr>
<td></td>
<td><strong>exsession off ssh</strong> — Disables SSH.</td>
</tr>
<tr>
<td><code>[command] help</code></td>
<td>Displays a list of top-level commands or additional information for an individual command.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: The maintenance image does not have this command. You must type a ? for help instead.</td>
</tr>
<tr>
<td><strong>ip</strong></td>
<td>Sets the IP parameters. This command is available from the application and maintenance image and the guest account in the maintenance image.</td>
</tr>
<tr>
<td><strong>ip address</strong></td>
<td>Specifies the IP address and subnet for a node on the network.</td>
</tr>
<tr>
<td><strong>ip broadcast</strong></td>
<td>Specifies the IP broadcast address for a node on the network.</td>
</tr>
<tr>
<td><strong>ip domain</strong></td>
<td>Specifies the domain name.</td>
</tr>
<tr>
<td><strong>ip gateway</strong></td>
<td>Specifies the default IP gateway.</td>
</tr>
<tr>
<td><strong>ip host</strong></td>
<td>Specifies an IP host name.</td>
</tr>
<tr>
<td><strong>ip hosts add</strong></td>
<td>Adds a host entry to the hosts file.</td>
</tr>
<tr>
<td><code>ftp://user:passwd@host/full-path/filename</code></td>
<td>Adds the host entries from the remote file to the hosts file.</td>
</tr>
<tr>
<td><strong>ip hosts delete</strong></td>
<td>Deletes a host entry from the hosts file.</td>
</tr>
<tr>
<td><code>ftp://user:passwd@host/full-path/filename</code></td>
<td>Deletes the host entries from the remote file in the hosts file.</td>
</tr>
<tr>
<td><strong>ip nameserver</strong></td>
<td>Specifies the IP name server used to resolve network names into network addresses.</td>
</tr>
<tr>
<td></td>
<td>Disables the configured name servers.</td>
</tr>
</tbody>
</table>
### Command Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>logout</strong></td>
<td>Logs you out of the shell from the maintenance image and the guest account from the maintenance image.</td>
</tr>
<tr>
<td></td>
<td>This command is used only for the WS-SVC-NAM-1 and the WS-SVC-NAM-2 module maintenance image.</td>
</tr>
<tr>
<td><strong>nslookup hostname [server]</strong></td>
<td>Allows name server queries for information about a host. If the optional server is not specified, the NAM DNS servers are used.</td>
</tr>
<tr>
<td><strong>passwd</strong></td>
<td>Sets the password for the current user. In the application software, this command requires that the user name is specified as an argument. For example: passwd root passwd guest</td>
</tr>
<tr>
<td><strong>passwd-guest</strong></td>
<td>Sets the password for the guest account from the maintenance image.</td>
</tr>
<tr>
<td></td>
<td>This command is used only for the WS-SVC-NAM-1 and the WS-SVC-NAM-2 module maintenance image.</td>
</tr>
<tr>
<td><strong>patch</strong></td>
<td>Applies a patch to the application software from the specified location.</td>
</tr>
<tr>
<td>ftp://user:passwd@host/full-path/filename</td>
<td></td>
</tr>
<tr>
<td>**ping [-nv] [-c count] [-i wait] [-p pattern] [-s packetsize] hostname</td>
<td>Sends ICMP echo-request packets to another node on the network. To configure ping, you can also use the command without arguments.</td>
</tr>
<tr>
<td></td>
<td>The following options are supported:</td>
</tr>
<tr>
<td></td>
<td>-n—Shows network addresses as numbers.</td>
</tr>
<tr>
<td></td>
<td>-v—Provides verbose output.</td>
</tr>
<tr>
<td></td>
<td>-c count—Stops after sending count ECHO_REQUEST packets.</td>
</tr>
<tr>
<td></td>
<td>-i wait—Waits seconds between sending each packet.</td>
</tr>
<tr>
<td></td>
<td>-p pattern—Up to 16 pad bytes can be used to fill out packets you send.</td>
</tr>
<tr>
<td></td>
<td>-s packetsize—The 8 bytes of ICMP header data.</td>
</tr>
<tr>
<td><strong>reboot</strong></td>
<td>Reboots the NAM from the application image.</td>
</tr>
<tr>
<td>**rmon artmib {enable</td>
<td>disable}**</td>
</tr>
<tr>
<td><strong>show</strong></td>
<td>Displays the system parameters from the maintenance and guest account from the maintenance image.</td>
</tr>
<tr>
<td><strong>show autostart</strong></td>
<td>Enables reporting for statistics, address mappings, VLANs, and MIBs.</td>
</tr>
<tr>
<td><strong>show bios</strong></td>
<td>Displays system information about the BIOS and module (including NAM serial number) that the Cisco TAC might need for troubleshooting. Copy and save the information to a file before calling TAC. This command can be used by both root and guest accounts.</td>
</tr>
<tr>
<td><strong>show certificate</strong></td>
<td>Displays certificates you have installed for secure servers.</td>
</tr>
<tr>
<td><strong>show certificate-request</strong></td>
<td></td>
</tr>
<tr>
<td><strong>show cpu</strong></td>
<td>Displays current processor load on the NAM CPU for all combined functions. This command can be used by both root and guest accounts.</td>
</tr>
<tr>
<td><strong>show date</strong></td>
<td>Displays current time-of-day information maintained by the NAM. This command can be used by both root and guest accounts.</td>
</tr>
</tbody>
</table>
### Command Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show diaglog</code></td>
<td>Displays the diagnostics log file from the guest account in the maintenance image. This command is used only for the WS-SVC-NAM-1 and the WS-SVC-NAM-2 module maintenance image.</td>
</tr>
<tr>
<td><code>show ethif</code></td>
<td>Displays the Ethernet interface information from the guest account in the maintenance image. This command is used only for the WS-SVC-NAM-1 and the WS-SVC-NAM-2 module maintenance image.</td>
</tr>
<tr>
<td><code>show hosts</code></td>
<td>Displays the hosts file.</td>
</tr>
<tr>
<td><code>show images</code></td>
<td>Lists the image that is installed in the NAM application image. This command is available only from the maintenance image. This command is used only for the WS-SVC-NAM-1 and the WS-SVC-NAM-2 module maintenance image.</td>
</tr>
<tr>
<td><code>show ip</code></td>
<td>Displays current IP configuration including the HTTP server, secure server, port, secure port, and TACACS+ information.</td>
</tr>
<tr>
<td><code>show log</code></td>
<td>Displays the application image log. This command is used only for the WS-SVC-NAM-1 and the WS-SVC-NAM-2 module maintenance image.</td>
</tr>
<tr>
<td><code>show log config</code></td>
<td>Displays the output of the previous configuration import. For example, the <code>config network</code> command.</td>
</tr>
<tr>
<td><code>show log upgrade</code></td>
<td>Displays the maintenance image upgrade log when you are booted into application image. Displays the application image upgrade log when you are booted into the maintenance image.</td>
</tr>
<tr>
<td><code>show memory</code></td>
<td>Displays system memory statistics. Memory sizes are rounded to the nearest Megabyte. This command can be used by both root and guest accounts.</td>
</tr>
<tr>
<td><code>show options</code></td>
<td>Displays ART MIB and voice monitoring configuration status.</td>
</tr>
<tr>
<td><code>show patches</code></td>
<td>Displays installed software patches.</td>
</tr>
<tr>
<td><code>show rxcounters</code></td>
<td>Displays RX data counters.</td>
</tr>
<tr>
<td><code>show snmp</code></td>
<td>Displays the SNMP configuration.</td>
</tr>
</tbody>
</table>
### Additional NAM Software Administrative Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show tech-support</strong></td>
<td>Displays system information without page-breaks that the Cisco TAC might need for troubleshooting. Copy and save the information to a file before calling TAC. This command can be used by the root account only.</td>
</tr>
<tr>
<td></td>
<td>From a UNIX system, do the following:</td>
</tr>
<tr>
<td></td>
<td>a. Telnet to the switch supervisor.</td>
</tr>
<tr>
<td></td>
<td>b. Session to the NAM module.</td>
</tr>
<tr>
<td></td>
<td>c. Log in to the NAM as root user.</td>
</tr>
<tr>
<td></td>
<td>d. In the NAM CLI type,</td>
</tr>
<tr>
<td></td>
<td># show tech-support</td>
</tr>
<tr>
<td></td>
<td># exit</td>
</tr>
<tr>
<td></td>
<td>$ exit</td>
</tr>
<tr>
<td></td>
<td>e. A file tech.txt is created in the UNIX system.</td>
</tr>
<tr>
<td></td>
<td>From a Windows system, do the following:</td>
</tr>
<tr>
<td></td>
<td>a. Launch Windows HyperTerminal and connect to switch supervisor.</td>
</tr>
<tr>
<td></td>
<td>b. Session to the NAM module.</td>
</tr>
<tr>
<td></td>
<td>c. Log in to the NAM as the root user.</td>
</tr>
<tr>
<td></td>
<td>d. In the HyperTerminal menu, select <strong>Transfer &gt; Capture Text</strong>.</td>
</tr>
<tr>
<td></td>
<td>e. Enter a file name in a dialog that pops up and click <strong>Start</strong>.</td>
</tr>
<tr>
<td></td>
<td>f. In the NAM CLI type,</td>
</tr>
<tr>
<td></td>
<td># show tech-support</td>
</tr>
<tr>
<td></td>
<td># exit</td>
</tr>
<tr>
<td></td>
<td>g. In the Hyper Terminal menu, select <strong>Transfer &gt; Capture Text &gt; Stop</strong>.</td>
</tr>
<tr>
<td><strong>show version</strong></td>
<td>Displays the NAM maintenance image version, daughter card information, and NAM application image version.</td>
</tr>
<tr>
<td></td>
<td>• The NAM application image version is not displayed as part of the <strong>show version</strong> command output if you are running this command from the maintenance image.</td>
</tr>
<tr>
<td></td>
<td>• The NAM maintenance image version is not displayed as part of the <strong>show version</strong> command output if you are running this command from the application image.</td>
</tr>
<tr>
<td><strong>snmp community</strong></td>
<td>Sets the SNMP community string value.</td>
</tr>
<tr>
<td><em>community-string</em> {ro</td>
<td>rw}</td>
</tr>
</tbody>
</table>
### Cisco IOS Commands

The NAM also supports these CLI commands, which are described in more detail in the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication. These commands are grouped according to mode. These sections describe the Cisco IOS commands that interact with the NAM:

- EXEC Commands, page 4-29
- Configuration Commands, page 4-30

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>traceroute</strong> [ -I ] [ -f first_ttl ] [ -m max_ttl ] [ -p port ] [ -s src_addr ] [ -t tos ] [ -w waittime ] destination host name</td>
<td>The following options are supported:</td>
</tr>
<tr>
<td></td>
<td>-I—Uses ICMP ECHO instead of UDP datagrams.</td>
</tr>
<tr>
<td></td>
<td>-n—Prints hop addresses numerically.</td>
</tr>
<tr>
<td></td>
<td>-v—Provides verbose output.</td>
</tr>
<tr>
<td></td>
<td>-f first_ttl—Sets the initial time-to-live used in the first outgoing packet.</td>
</tr>
<tr>
<td></td>
<td>-m max_ttl—Sets the maximum time-to-live (max number of hops) used.</td>
</tr>
<tr>
<td></td>
<td>-p port—Sets the base UDP port number used in probes.</td>
</tr>
<tr>
<td></td>
<td>-s src_addr—Forces the source address to something different than the IP address of the interface the packet is sent on.</td>
</tr>
<tr>
<td></td>
<td>-t tos—Sets the type-of-service in packets to the following value.</td>
</tr>
<tr>
<td></td>
<td>-w waittime—Sets the time (in seconds) to wait for a response to a probe.</td>
</tr>
<tr>
<td><strong>upgrade</strong> [ftp-url] [device:partition-num]</td>
<td>Upgrades the maintenance image from the specified location when the NAM is booted into the application image. This command is also available from the guest account in the maintenance image.</td>
</tr>
<tr>
<td></td>
<td>Upgrades the NAM application image from the specified location when the NAM is booted into the maintenance image.</td>
</tr>
<tr>
<td><strong>upgrade bios</strong></td>
<td>Installs a new BIOS image. This command is available in the guest account from the maintenance image.</td>
</tr>
</tbody>
</table>

**Caution**

If used improperly, this command can cause the NAM to become inoperable.

| **voice monitoring**                  | Enables voice monitoring from the application image.                                                 |
## EXEC Commands

The following commands are all performed in EXEC mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>analysis module slot_number management-port access-vlan vlan_number</strong></td>
<td>Sets the NAM management port and the capture mode characteristics of the interface. Sets the VLANs that are allowed when the interface is in capture mode.</td>
</tr>
<tr>
<td><strong>analysis module slot_number data-port port_number capture [allowed-vlan vlan-list]</strong></td>
<td>Sets the NAM data port and the capture mode characteristics of the interface. Sets the VLANs that are allowed when the interface is in capture mode.</td>
</tr>
<tr>
<td><strong>set boot device partition_number module_number [fast]</strong></td>
<td>Allows enabling a fast boot when setting the boot device partition using the <code>set boot device partition_number module_number [fast]</code> command. This option is disabled by default. This option operates similarly to the Cisco IOS [fast] command option, by skipping the BIOS memory test and allowing the NAM to boot faster.</td>
</tr>
<tr>
<td>**show analysis module slot_number management-port state</td>
<td>traffic**</td>
</tr>
<tr>
<td>**show analysis module slot_number data-port port_number state</td>
<td>traffic**</td>
</tr>
<tr>
<td><strong>show module</strong></td>
<td>Displays installed modules, versions, and states. <strong>Note</strong> This command does not show the signature level.</td>
</tr>
<tr>
<td><strong>reload</strong></td>
<td>Reloads the entire switch.</td>
</tr>
<tr>
<td><strong>show running-config</strong></td>
<td>Displays the configuration that is currently running.</td>
</tr>
<tr>
<td><strong>show startup-config</strong></td>
<td>Displays the saved configuration.</td>
</tr>
<tr>
<td><strong>hw-module module module_number reset word [fast]</strong></td>
<td>Resets the module into the application image by default. The fast option allows you to skip the BIOS memory test for a faster boot. <strong>Note</strong> If you do not specify a boot device for this command, the <code>&lt;empty&gt;</code> message is displayed. For example:</td>
</tr>
<tr>
<td><strong>hw-module module slot_number reset cf:1</strong></td>
<td>Resets the module into the maintenance image.</td>
</tr>
<tr>
<td><strong>hw-module module slot_number shutdown</strong></td>
<td>Resets the module into the maintenance image and shuts down the module.</td>
</tr>
<tr>
<td><strong>show interfaces Gigabit slot_number/port_number</strong></td>
<td>Displays status of the interface.</td>
</tr>
<tr>
<td><strong>show interfaces switchport module slot_number</strong></td>
<td>Displays current switch settings for the interfaces.</td>
</tr>
<tr>
<td><strong>show interface trunk module slot_number</strong></td>
<td>Displays current trunk settings for the interfaces.</td>
</tr>
<tr>
<td><strong>clock set time date module slot_number</strong></td>
<td>Sets the current time and date.</td>
</tr>
<tr>
<td><strong>clock update-calendar</strong></td>
<td>Updates the calendar time to the clock time.</td>
</tr>
<tr>
<td><strong>clock read-calendar</strong></td>
<td>Updates clock time to the calendar time.</td>
</tr>
</tbody>
</table>
Configuration Commands

The following commands are all performed in either global configuration mode or the interface configuration mode:

- Global Configuration Mode, page 4-30
- Interface Configuration Mode, page 4-30

Global Configuration Mode

The following commands are all performed in global configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>power enable module slot_number</code></td>
<td>Turns on the power for the NAM if it is not already on.</td>
</tr>
<tr>
<td><code>no power enable module slot_number</code></td>
<td>Shuts down the NAM and removes power.</td>
</tr>
<tr>
<td><code>clock timezone zone offset</code></td>
<td>Sets the timezone for the switch or NAM.</td>
</tr>
<tr>
<td><code>clock summer-time zone recurring</code></td>
<td>Sets the switch to use summertime settings.</td>
</tr>
<tr>
<td><code>clock calendar valid</code></td>
<td>Sets the current calendar time as the switch time on startup.</td>
</tr>
<tr>
<td><code>interface GigabitEthernet slot_number/port_number</code></td>
<td>Begins configuration for each NAM port.</td>
</tr>
<tr>
<td>`monitor session session {source {interface interface interface-number</td>
<td>{vlan vlan-id}</td>
</tr>
<tr>
<td><code>monitor session {session_number} {destination analysis module NAM module number data-port port}</code></td>
<td>Sets the destination for a SPAN session.</td>
</tr>
</tbody>
</table>

Interface Configuration Mode

The following commands are configuration commands performed in interface configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>switchport</code></td>
<td>Sets interface as a switchport.</td>
</tr>
<tr>
<td><code>switchport trunk encapsulation dot1q</code></td>
<td>Sets dot1q as the encapsulation type.</td>
</tr>
<tr>
<td><code>switchport trunk native vlan vlan</code></td>
<td>Sets native VLAN for the trunk port.</td>
</tr>
<tr>
<td><code>switchport trunk allowed vlan vlans</code></td>
<td>Sets allowed VLANs for a trunk.</td>
</tr>
<tr>
<td><code>switchport mode trunk</code></td>
<td>Sets the interface as a trunk port.</td>
</tr>
<tr>
<td><code>switchport capture</code></td>
<td>Sets the interface as a capture port.</td>
</tr>
<tr>
<td><code>switchport access vlan vlan</code></td>
<td>Sets the access VLAN for the interface.</td>
</tr>
<tr>
<td><code>switchport mode access</code></td>
<td>Sets the interface as an access port.</td>
</tr>
</tbody>
</table>

Unsupported Supervisor Engine CLI Commands

These CLI commands are not supported by the NAM:

- `set port broadcast`
- `set port channel`
- set port cops
- set port disable
- set port enable
- set port flowcontrol
- set port gmrp
- set port gvrp
- set port host
- set port inlinepower
- set port jumbo
- set port membership
- set port negotiation
- set port protocol
- set port qos
- set port rsvp
- set port security
- set port speed
- set port trap
- set protocolfilter
- set rgmp
- set rspan
- set snmp
- set spantree
- set trunk
- set uddi
- set vlan
- set vtp
Troubleshooting the NAM

This chapter provides troubleshooting information for the NAM, and includes these sections:

- Netflow Data Export, page 5-1
- Error Messages, page 5-8
- Web Username and Password Guidelines, page 5-13
- Supported MIB Objects, page 5-15
- Local Interfaces in the NAM ifTable, page 5-19

Note

Additional troubleshooting help is available to the NAM Traffic Analyzer application users in the online help “Troubleshooting” section.

Netflow Data Export

This section contains troubleshooting information for NDE.

Web Application

Explanation When you are on the Monitor>Hosts, Monitor>Apps, or Monitor>Conversations page, the data shows only every other or more auto-refresh cycles. This problem is caused by the implementation operation of the NDE source device. Entries in the NetFlow cache are expired after being inactive for a time, or when the end of a connection is detected, or the expiration time has reached. The expired flow is exported to the destination. If the aging time is longer than the NAM refresh interval, there will be no expired flows and NetFlow packets flow in one refresh interval of the NAM.

Recommended Action To solve the problem, either increase the auto refresh interval on the Setup>Preferences menu, or change the aging time of the NetFlow entries. However, before you make any change to the aging time at the NDE source device, refer to the NDE usage guidelines for performance issues.

Cisco IOS:

For the MSFC or routers, use the following command to specify the aging time.

```
Router(config)# ip flow-cache timeout "active"|"inactive" seconds
Router(config)# mls aging "fast time" | "long" | "normal" seconds
```
Catalyst Operating System:

For the PFC, use the following commands to specify the aging time.

```
Router(enable) set mls agingtime [long-duration | fast | ip]
```

To set the aging time for flows that are long active, use the **long-duration** keyword.
To set the aging time for flows that does not exceed packets threshold, use the **fast** keyword.
To set aging time for IP flows, use the **ip** keyword.

**Explanation**  The Monitor>Hosts and Monitor>Conversations page does not contain data of an active flow. This problem could be caused if the active flow is not expired yet, if the device has an NDE filter, or if a full cache is preventing insertion of new entries. The active flow is not in the NetFlow packets that are exporting to the NAM.

**Recommended Action**  Check for filter, for long duration aging time, or for dropped flow packets as follows:

Verify for long duration aging time with these commands:

```
Router>(enable) show ip cache flow
```

or

```
Router>(enable) show mls netflow aging
```

or

```
Router>(enable) show mls
```

Active flows that have active time below the long duration aging time are not expired yet, and they have not been exported to the NAM. The aging time could be set to lower value. Refer to the NDE usage guidelines for the device.

Verify for flow packets dropped with these commands:

```
Router>(enable) show ip cache flow
```

or

```
Router>(enable) show mls netflow aging
```

or

```
Router>(enable) show mls
```

Flows could be dropped because they are not entered into the caches allowing their export to the NAM when they are expired. This condition may be that the NetFlow cache is full because of busy networks. To correct the problem, you could increase the cache sized. An alternative is to adjust NDE export with NDE flow mask or version 8 aggregation cache. Refer to the NDE usage guidelines for the device.

**Explanation**  There is no data for the default NetFlow data source of the device.

**Recommended Action**  In the GUI, go to the Setup>Data Sources>NetFlow>Listening Mode page and click on the Start button. Wait for a few auto refresh cycles. If the device is not displayed in the table, the NAM is not receiving any NetFlow packets from the device. This condition could be a network problem, or the device may not be configured correctly.
To verify that a NetFlow device is configured to send NetFlow packets to UDP port 3000 of the NAM, use the following commands:

Router# show ip flow export

or

Router# show mls nde

Displayed information should show whether or not NetFlow export is enabled or disabled and show the IP address and port to which the NetFlow packets are being exported. If the information is not correct, refer to the configuration section in the User Guide for the Network Analysis Module Traffic Analyzer Release 3.1 to correct it.

Explanation  There is no data for NetFlow data sources that are configured for specific interfaces, but the default NetFlow data source for the device has data.

Recommended Action  This problem could occur because there a NetFlow record does not exist that has the specified interfaces information. To find out what interfaces that NetFlow records have, do the following:

Step 1  Go to the Setup>Data Sources>NetFlow>Listening Mode screen.
Step 2  Click Start to initiate the listening process.
Step 3  Wait until the row for the device has more than three NDE packets counted.
Step 4  Select the device.
Step 5  Click Details. A window appears displaying a list of interfaces that the NAM has seen in the NDE packets.
Step 6  Make sure that the interfaces selected for the NetFlow devices are included in the list. If the interfaces are not included in the list, configure the NetFlow source devices using the following commands:

For the IP routed cache use these commands:

Router(config)# interface type slot/port
Router(config-if)# ip route cache flow

For MLS cache:
Cisco IOS:

Router(config)# mls nde interface

Catalyst operating system:

Console>(enable) set mls nde destination-ifindex enable

or,

Catalyst operating system:

Console>(enable) set mls nde source-ifindex enable

Make sure that the flow mask is set to “full,” “interface-destination-source,” or “interface-full.”

If the information is not correct, refer to the configuration section in the User guide for Network Analysis Module Traffic Analyzer Release 3.1 to correct it.
**Explanation** When creating a NetFlow data source from the Setup>Data Sources>NetFlow>Custom Data Sources screen, only the local device’s address appears in the drop down box.

**Recommended Action** A device is created in the Setup>Data Sources>NetFlow>Devices screen. After adding a device from this screen, a default NetFlow data source for the device appears in the Setup>Data Sources>NetFlow>Custom Data Sources screen. Now, the drop down box displays the device address included in the list.

**Explanation** When creating a NetFlow data source, no available interfaces list is displayed.

Make sure the provided community string is correct by doing the following:

---

**Step 1**
Go to the Setup>Data Sources>NetFlow>Devices menu.

**Step 2**
Click on the radio button of the device to display interfaces information.

**Step 3**
Click Test.

A pop up window appears displaying the status of the device. If there is error in this window, the community string may not be correct. Correct the community string by selecting the device, click Edit, and provide the correct community string. Also, ensure that the remote device accepts SNMP connections.

**Explanation** Monitor>Conversations page has the source column being 0.0.0.0 for all entries. This problem occurs due to the NDE device flow mask being set to “destination.”

To set the flow mask to “full,” “interface-destination-source,” or “interface-full,” do the following:

For Cisco IOS:

```
Prompt(config)# mls flow ip "full" || "interface-destination-source" || "interface-full"
```

For the Catalyst operating system:

```
Router(enable) set mls flow "destination-source" || "full"
```

---

**Note** The NAM supports NDE versions 1, 5, 6, 7, 8, source-prefix, destination-prefix, prefix, and protocol-port aggregations.

---

**NDE Flow Records Interfaces**

**Explanation** An NDE packet has multiple NDE flow records. Each flow record has fields of flow input SNMP if-index and flow output SNMP if-index. The information may not be available due to unsupported NDE feature of the Cisco IOS or Catalyst operating system version, or NDE flow masks configuration.

**Figure 5-1** and **Figure 5-2** show the network configuration for this situation, and **Table 5-1** and **Table 5-2** show the reporting flow records.
The configuration is as follows:

```
Router# configuration terminal
Router(config)# interface a
Router(config-if)# ip route cache flow
Router(config-if)# exit
Router(config)# ip flow export destination NAM-Address 3000
Router(config)# exit
Router#
```

### Table 5-1  Reporting Flow Records

<table>
<thead>
<tr>
<th>Input Interface</th>
<th>Output Interface</th>
<th>Are Flows Reported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>b</td>
<td>Yes</td>
</tr>
<tr>
<td>a</td>
<td>c</td>
<td>Yes</td>
</tr>
<tr>
<td>b</td>
<td>c</td>
<td>No</td>
</tr>
<tr>
<td>b</td>
<td>a</td>
<td>No</td>
</tr>
<tr>
<td>c</td>
<td>a</td>
<td>No</td>
</tr>
<tr>
<td>c</td>
<td>b</td>
<td>No</td>
</tr>
</tbody>
</table>

```
Router# configuration terminal
Router(config)# interface a
Router(config-if)# ip route cache flow
Router(config-if)# exit
```

---

**Figure 5-1  NDE Configuration**

```
Host A

Host B

Router

Host C
```

**Figure 5-2  NDE Configuration**

```
Host A

Host B

Router

Host C
```
Router(config)# interface b
Router(config-if)# ip route cache flow
Router(config-if)# exit
Router(config)# ip flow export destination NAM-Address 3000
Router(config)# exit
Router#

**Table 5-2  Reporting Flow Records**

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Are Flows Reported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>b</td>
<td>Yes</td>
</tr>
<tr>
<td>a</td>
<td>c</td>
<td>Yes</td>
</tr>
<tr>
<td>b</td>
<td>c</td>
<td>Yes</td>
</tr>
<tr>
<td>b</td>
<td>a</td>
<td>Yes</td>
</tr>
<tr>
<td>c</td>
<td>a</td>
<td>No</td>
</tr>
<tr>
<td>c</td>
<td>b</td>
<td>No</td>
</tr>
</tbody>
</table>

**Recommended Action** In most cases, turning on NetFlow on an interface will populate the NetFlow cache in a switch or router with flows that are in the input direction of the interface. As a result, the input SNMP if-index field in the flow record will have the if-index of the interface that has NetFlow turned on.

**Interface Special (0)**

**Explanation** NDE packets sometimes have NetFlow records reporting either or both input if-index and output if-index fields being 0. This may be due to one or more of the following reasons:

- Flows that are terminated at the device.
- Configurations of the device.
- Unsupported NetFlow feature of the platform at the device.

**Recommended Action** Remove flows terminated at the device, check the device configuration, make sure there are no unsupported features on this platform at the device.

**NDE Flow-mask and v8 Aggregation Cache**

This section describes how some of the flow-masks and NDE version 8 aggregation flows affect the data collection screens in the NAM. Table 5-3 lists these affects. Due to lack of information, some collections may have “Others” only in the Monitor>Apps, 0.0.0.0 in Monitor>Hosts and Monitor>Conversation pages.
### Table 5-3 Affects on Data Collection Screens

<table>
<thead>
<tr>
<th>Flow</th>
<th>Affect</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full flow-mask is supported</td>
<td>Highly recommended. Refer to the NDE usage guidelines for the device to apply full flow-masks.</td>
<td>Although the NAM supports NDE aggregation, the information you receive for a specified aggregation type is limited to that aggregation and other NDE details are not available. To receive more information about your NDE configuration, use the full flow mode.</td>
</tr>
<tr>
<td>Destination only flow-mask.</td>
<td>• Monitor&gt;Apps displays “Others” only.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Monitor&gt;Apps detail popup screen has no data.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Monitor&gt;Hosts has 0.0.0.0. Detail popup screen has no data.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Monitor&gt;Conversations has 0.0.0.0 to some hosts. Detail popup screen has no data.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Support NetFlow custom data sources that are set up for specific interfaces.</td>
<td></td>
</tr>
<tr>
<td>Destination-Source flow-mask.</td>
<td>• Monitor&gt;Apps displays “Others” only.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Monitor&gt;Apps detail popup screen has no data.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Monitor&gt;Hosts has data. Detail popup screen has no data.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Monitor&gt;Conversations has data. Detail popup screen has no data.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Support NetFlow custom data sources that are set up for specific interfaces.</td>
<td></td>
</tr>
<tr>
<td>NDE version 8-Protocol-Port-Aggregation</td>
<td>• Monitor&gt;Apps displays data.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Monitor&gt;Apps detail pop up displays no data. only 0.0.0.0.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Monitor&gt;Host displays only 0.0.0.0.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Monitor&gt;Conversation displays only 0.0.0.0 to 0.0.0.0.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• No data for custom NetFlow data sources that are setup for some specific interfaces.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• No DiffServ other than TOS 0 and DSCP 0.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Setup&gt;Data Sources&gt;NetFlow Listening Mode detail popup screen does not display interfaces information.</td>
<td></td>
</tr>
<tr>
<td>NDE version 8-Destination-Prefix-Aggregation</td>
<td>• Monitor&gt;Apps displays only “Others.”</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Monitor&gt;Host displays data with subnets as well as 0.0.0.0. The detail pop up screen displays no data.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Monitor&gt;Conversation displays data with 0.0.0.0 to subnets (as well as 0.0.0.0 to 0.0.0.0). Detail pop up screen displays no data.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Support NetFlow custom data sources that are set up for specific interfaces.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• No DiffServ other than TOS 0 and DSCP 0.</td>
<td></td>
</tr>
</tbody>
</table>
### Error Messages

**Symptom**  When a `reset` command is entered from the supervisor CLI, the system always boots into the maintenance image.

**Possible Cause**  If the boot device is configured in the supervisor as `cf:1`, typing a `reset module` command always boots to the maintenance image.

**Recommended Action**  Override the configured boot device in the supervisor by entering the boot string during reset.

- In Cisco IOS software, to boot to the application image, use the `hw-module mod 9 reset hdd:1` command.
- In Catalyst operating system software, to boot to the application image, use the `reset 9 hdd:1` command.

---

### Table 5-3  Affects on Data Collection Screens (continued)

<table>
<thead>
<tr>
<th>Flow</th>
<th>Affect</th>
</tr>
</thead>
<tbody>
<tr>
<td>NDE version 8-Prefix-Aggregation</td>
<td>- Monitor&gt;Apps displays “Others” only.</td>
</tr>
<tr>
<td></td>
<td>- Monitor&gt;Host displays data as subnets (as well as 0.0.0.0). The</td>
</tr>
<tr>
<td></td>
<td>detail pop up screen displays no data.</td>
</tr>
<tr>
<td></td>
<td>- Monitor&gt;Conversation displays data (as well as 0.0.0.0 to 0.0.0.0).</td>
</tr>
<tr>
<td></td>
<td>Detail pop up screen displays no data.</td>
</tr>
<tr>
<td></td>
<td>- Support NetFlow custom data sources that are setup for specific</td>
</tr>
<tr>
<td></td>
<td>interfaces.</td>
</tr>
<tr>
<td></td>
<td>- No DiffServ other than TOS 0 and DSCP 0.</td>
</tr>
</tbody>
</table>

| NDE version 8-Source-Prefix-Aggregation | - Monitor>Apps displays “Others” only.                                |
|                                       | - Monitor>Host displays data with subnets (as well as 0.0.0.0). The  |
|                                       |   detail pop up screen displays no data.                             |
|                                       | - Monitor>Conversation displays data with subnets to 0.0.0.0 (as     |
|                                       |   well as 0.0.0.0 to 0.0.0.0). Detail popup screen displays no data. |
|                                       | - Support NetFlow custom data sources that are set up for specific   |
|                                       |   interfaces.                                                        |
|                                       | - No DiffServ other than TOS 0 and DSCP 0.                            |

| NDE version 8-AS-Aggregation        | Not supported.                                                        |
Symptom  You receive a verification failed message when installing a patch on the NAM.

Possible Cause  The time and date on the NAM are not correct; the patch is not the same as an official Cisco patch; the patch might be of the previous release of NAM; the FTP process may have failed; or the FTP image being pointed to is not a patch (it may be a full application image).

Recommended Action  Be sure that the signature verification is used to ensure that the patch is an authentic Cisco patch. Be sure that the patch is for the correct NAM release. For example, a patch for the NAM 2.2 release cannot be applied to a NAM running the NAM 3.1 software. Be sure the date and time on the NAM either is set to synchronize with the switch or with the Network Time Protocol (NTP). Make sure the URL location is valid for the patch (username in particular).

Symptom  You are unable to log into the maintenance image with the same password for the NAM application image.

Note  This message is applicable only for the WS-SVC-NAM-1 and the WS-SVC-NAM-2 modules.

Possible Cause  The NAM application image and the maintenance image have different password databases for the root and guest accounts. The default passwords for root and guest differ between the maintenance image and the NAM application image. Any password change performed in the NAM application image does not change the maintenance image password and vice versa.

Recommended Action  Use the maintenance image password.

Symptom  You lost your password for the maintenance image and want to recover it.

Possible Cause  The maintenance image does not support resetting passwords from the switch. Upgrading the maintenance image sets the password for root and guest to default in the maintenance image.

Recommended Action  Use the default maintenance image passwords. Refer to Table 4-1 on page 4-2 or Table 4-5 on page 4-12.

Symptom  When attempting to load the new NAM 3.1 image on the NAM the following message is received:

Incompatible image! Upgrade aborted.

Possible Cause  This image is not supported on the specified NAM. There are three NAM 3.1 images available: One each for the WS-SVC-NAM-1, WS-SVC-NAM-2 and one for the WS-X6380-NAM. This symptom occurs only if an incompatible image is used.

Recommended Action  Do not use the NAM software release 2.2 image on the WS-X6380-NAM. The application and maintenance file image formats are different between the WS-X6380-NAM and the newer WS-SVC-NAM-1 and WS-SVC-NAM-2. The newer NAM shares a common format and the same image filename for upgrades can be used.
Symptom  When attempting to load the WS-X6380-NAM image on a WS-SVC-NAM-1 or WS-SVC-NAM-2 the following message is received:

ERROR: /tmp/upgrade: No space left on device

**Possible Cause**  This image is not supported on the specified NAM. There are three NAM 3.1 images available: One each for the WS-SVC-NAM-1, WS-SVC-NAM-2 and one for the WS-X6380-NAM. This symptom occurs only if an incompatible image is used.

**Recommended Action**  Do not use the WS-X6380-NAM image on a WS-SVC-NAM-1 or WS-SVC-NAM-2. The application and maintenance file image formats are different between the WS-X6380-NAM and the newer WS-SVC-NAM-1 and WS-SVC-NAM-2. The newer NAM shares a common format, and the same image filename for upgrades can be used between these newer modules.

Symptom  A SPAN session does not show up in the Traffic Analyzer *Active SPAN* window.

**Possible Cause**  In Catalyst operating system software, a SPAN session becomes inactive if the module containing the destination port is removed from the switch chassis. The NAM is not seen by the SPAN session because the SPAN configuration is removed from the SNMP agent by the supervisor engine.

**Recommended Action**  Replace the module.

Symptom  In Cisco IOS software, a SPAN create request failed for a partially configured SPAN session.

**Possible Cause**  The NAM does not see this partial SPAN session, or the SPAN create request can fail if there is a conflict in either the source type or destination port.

**Recommended Action**  Because SPAN session can be partially defined with either source or destination only, reconfigure the SPAN session with both a source and destination.

Symptom  When the NAM initially boots, by default it runs a partial memory test and you want to run a complete memory test.

**Possible Cause**  The partial memory test is the default configuration.

**Recommended Action**  To perform a full memory test, enter the `hw-module module module_number reset device:partition mem-test-full` command.

**Note**  A full memory test takes significantly more time to complete.

This command is specific to Cisco IOS and is not available in Catalyst operating system software. (See the “Resetting the NAM” section on page 4-15.)

You can also use the `hw-module module module_number mem-test-full` command. For example:

```
Router(config)# hw-module module 5 mem-test-full
```
For the Catalyst operating system software, you can enable a full memory test when you use the `set boot device bootseq mod# mem-test-full` command. This option is disabled by default. For example:

```
Console (enable) set boot device cf:1 4 mem-test-full
Device BOOT variable = cf:1
Memory-test set to FULL
Warning: Device list is not verified but still set in the boot string.
```

```
Console> (enable) show boot device 4
Device BOOT variable = cf:1
Memory-test set to FULL
```

This example shows how to reset the partial memory test:

```
Console> (enable) set boot device cf:1 4
Device BOOT variable = cf:1
Memory-test set to PARTIAL
Warning: Device list is not verified but still set in the boot string.
Console> (enable)
Console> (enable) show boot device 4
Device BOOT variable = cf:1
Memory-test set to PARTIAL
```

**Symptom** When you click the **Test** button in the **Set up>Switch Parameters** menu window, the popup window indicates that both the SNMP read and write to the switch failed.

**Possible Cause** Verify that the SNMP read-write community string entered is the same as the SNMP read-write community string defined for the switch.

**Note** The password is case sensitive.

**Recommended Action** If the community string is correct and the test still fails, check that the switch has enabled the IP permit list as follows:

**Step 1** Log in to the switch in enable mode.

**Step 2** Enter the **show IP permit** command.

If the IP permit list is enabled, make sure that the NAM internal address is added to the IP permit list. The NAM address is 127.0.0.X, where X is the NAM module number times 10+1. For example, if the NAM is at module 4, then its address should be 127.0.0.41.

After you determine the NAM internal IP address, go to **Step 3**.

**Step 3** Enter the **set IP permit NAM-address SNMP** command.

**Symptom** When a NAM is running in a switch with Catalyst operating system software, the NAM may be shown as unreachable when you use the **ping** command or the NAM Traffic Analyzer application.

**Possible Cause** The NAM IP address and the IP address of the switch (interface sc0) are not in the same subnet. This problem can occur if you change the switch IP address and the NAM VLAN assignment. The NAM automatically synchronizes its VLAN assignment to the same VLAN in which the switch (interface sc0) resides. When this occurs, the NAM IP address resides on a
different subnet from the VLAN assigned to the NAM. The router then drops any packet destined to the NAM IP address. You cannot add a static route to the router because of route overlap caused by improper VLAN assignments and subnetting.

**Recommended Action** Make sure that the NAM IP address and the switch are in the same subnet and in the same VLAN.

**Symptom** You cannot connect to the NAM.

**Possible Cause** The initial configuration is incorrect or not configured.

**Recommended Action** Reconfigure the NAM as described in the “Configuring the NAM” section on page 3-1.

**Symptom** You cannot connect to the NAM Traffic Analyzer application.

**Possible Cause** The configuration for the HTTP server is not correct.

**Recommended Action** Check the NAM configuration for the HTTP server as described in the “Configuring the HTTP or HTTP Secure Server” section on page 3-21.

**Symptom** The NAM fails to upgrade.

**Possible Cause** The URL to the server or the image name is incorrect.

**Recommended Action** Make sure the URL you specified is valid. Make sure the image name you specified in the URL is an official Cisco image name.

**Symptom** You cannot enable the HTTP server.

**Possible Cause** No web users are configured, or a secure server is already enabled.

**Recommended Action** Configure web users as described in the “Configuring the HTTP or HTTP Secure Server” section on page 3-21.

**Symptom** After configuration, the TACACS+ authentication and authorization fails.

**Possible Cause** There are three possible causes: the name and password do not match the login configuration in the TACACS+ server; the TACACS+ secret key configured in the NAM does not match the secret key configured in the server; and the wrong TACACS+ server IP address is configured in the NAM.

**Recommended Action** To determine the cause to take the appropriate course of action follow these steps:

**Step 1** Log in as a local user.
**Step 2** Choose Admin > Diagnostics > Tech Support.  
**Step 3** Scroll down to view the /var/log/messages area.
Step 4  Look for the following messages near the end of the log and take the recommended actions:

...PAM-tacplus[612]:auth failed:Login incorrect
   Possible Cause  The name and password do not match the login configuration in the TACACS+ server.
   Recommended Action  Log in to the TACACS+ server and configure the authenticate and authorize NAM user. (See the TACACS+ documentation for information on login configuration.)

...httpd:tac_authen_pap_read:invalid reply content, incorrect key?
   ...PAM-tacplus[616]:auth failed:Authentication error, please contact administrator.
   Possible Cause  The TACACS+ secret key configured in the NAM does not match the key in the TACACS+ server.
   Recommended Action  Choose Admin > User > TACACS+ and enter the correct secret key.

...httpd:tac_connect:connection to 172.18.122.183 failed:Connection timed out
   ...httpd:tac_connect:all possible TACACS+ servers failed
   ...PAM-tacplus[613]:connection failed srv 0:Connection timed out
   ...PAM-tacplus[613]:no more servers to connect
   Possible Cause  The wrong TACACS+ server IP address is configured on the NAM.
   Recommended Action  Choose Admin > User > TACACS+ and enter the correct TACACS+ server address.

Symptom  The TACACS+ user can log in successfully but receives the “Not authorized...” error messages when accessing NAM Traffic Analyzer application.

   Possible Cause  You do not have the necessary access rights.
   Recommended Action  Log in to the TACACS+ server and grant access rights to the affected users. (See the TACACS+ documentation for information on login configuration.)

---

Web Username and Password Guidelines

Observe the following web username and password guidelines:

- You cannot use the CLI username (root or guest) and password to log into the NAM Traffic Analyzer application because they are administered separately. You also cannot use your NAM Traffic Analyzer application username and password to log into the NAM CLI.

You can create web users with a local database or using TACACS+. You can create a web user with the same username and password as used on the CLI. However, you must still make password changes in both places.
You can use TACACS+ in addition to a local database or instead of a local database. (The local database is always checked first.) To use only TACACS+, eliminate the local database users by either of these methods:

- Use the NAM CLI `rmwebusers` command to remove only local users, not TACACS+ users, because they are administered separately on the TACACS+ server.
- From the Admin tab, click Users, and then delete all local database users individually.

**Caution**
Do not delete all local database web users until you have verified that you can log into the NAM Traffic Analyzer application as a TACACS+ user.

You can recover the password in situations where you have forgotten the local web admin user password, or when another user with account permission logged in and changed the local web admin user password.

To recover the password if no TACACS+ server is configured on the NAM, follow these steps:

**Step 1** Access the NAM CLI.

**Step 2** Remove all web users by entering:

```
rmwebusers
```

WARNING: Doing this will stop the web server and remove all locally defined web users from web user database.

Are you sure you want to continue (y/n) [n]? y

Disabling HTTP server...
Successfully disabled HTTP server.

All locally defined web users have been removed from web user database.
root@namlab-kom2.cisco.com#

**Step 3** Start the HTTP (or HTTPs, if applicable) server by entering:

```
ip http server enable
ip http secure server enable
```

**Step 4** At the prompt, enter the web admin username and password.

You can now log in using the new admin account and create other web accounts by clicking the Admin tab, then clicking Users.

To recover the password if the TACACS+ server is configured on the NAM, follow these steps:

**Step 1** Log into the NAM Traffic Analyzer application as a TACACS+ user.

You must be configured on the TACACS+ server with Account Management permission.

**Step 2** Change the password of the local web admin user.
Note

If a TACACS+ server has been configured and the local web user account is deleted, you can still create the web admin user on the TACACS+ server. In this case, the admin user created on the TACACS+ server can log into the NAM Traffic Analyzer application and change the password of the local web admin user, you do not need to create another admin user.

When the TACACS+ configuration may become confused between the NAM and the TACACS+ server, and a local database user account is not available to fix the TACACS+ configuration on the NAM, you may not be able to fix this problem from the TACACS+ server. To recover the passwords, follow these steps:

Step 1 Access the NAM CLI.
Step 2 Enter these commands:

```
rmwebusers
ip http tacacs+ disable
ip http server enable
```

(or `ip http secure server enable` if using HTTPs)

Step 3 When prompted, enter the new local database admin username and password.
Step 4 Log into the NAM Traffic Analyzer application.
Step 5 Click the Admin tab.
Step 6 Click Users.
Step 7 In the contents, click TACACS+.
Step 8 Enter the correct information.
Step 9 Click Apply.

There are restrictions on using passwords when performing upgrades or applying patches. Do not include the password as an argument in upgrade and patch commands. Use the following command syntax:

```
patch ftp://username@host/full-patch/hostname
```

Enter the password when prompted for it.

**Supported MIB Objects**

Table 4 lists the RMON and RMON2 MIB objects supported by the supervisor engine and the NAM. The supervisor engine implements some objects from the RMON MIBs as specified in Table 4. The supervisor engine RMON implementation is completely independent of the NAM implementation, and no MIB objects are shared.

To collect etherStats from a physical interface on the switch, configure the etherStatTable on the supervisor engine instead of on the NAM. The etherStats are collected accurately on multiple physical interfaces simultaneously.

If you are interested in the etherStats for a specific VLAN, configure the etherStatsTable on the NAM. For the data source, use the ifIndex corresponding to that VLAN.
Any alarmVariable configured on the supervisor engine must reference a MIB object on the supervisor engine. An alarmVariable configured on the NAM must reference a MIB object on the NAM.

**Note**
You cannot configure an alarmVariable on the NAM that references a MIB object on the supervisor engine or configure an alarmVariable on the supervisor engine that references a MIB object on the NAM.

---

**Table 4  Supervisor Engine Module and NAM RMON Support**

<table>
<thead>
<tr>
<th>Module</th>
<th>Object Identifier (OID) and Description</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supervisor Engine</td>
<td>...mib-2(1).rmon(16).statistics(1).etherStatsTable(1)...mib-2(1).rmon(16).statistics(1).tokenRingMLStatsTable(2) ...mib-2(1).rmon(16).statistics(1).tokenRingPStatsTable(3)</td>
<td>RFC 2819 (RMON-MIB) RFC 1513 (TOKEN-RING-RMON MIB) RFC 1513 (TOKEN-RING-RMON MIB)</td>
</tr>
<tr>
<td></td>
<td>Counters for packets, octets, broadcasts, errors, etc.</td>
<td></td>
</tr>
<tr>
<td>Supervisor Engine</td>
<td>...mib-2(1).rmon(16).history(2).historyControlTable(1) ...mib-2(1).rmon(16).history(2).etherHistoryTable(2) ...mib-2(1).rmon(16).history(2).tokenRingMLHistoryTable(3) ...mib-2(1).rmon(16).history(2).tokenRingPHistoryTable(4)</td>
<td>RFC 2819 (RMON-MIB) RFC 2819 (RMON-MIB) RFC 1513 (TOKEN-RING-RMON MIB) RFC 1513 (TOKEN-RING-RMON MIB)</td>
</tr>
<tr>
<td></td>
<td>Periodically samples and saves statistics group counters for later retrieval.</td>
<td></td>
</tr>
<tr>
<td>Supervisor Engine</td>
<td>...mib-2(1).rmon(16).alarm(3)</td>
<td>RFC 2819 (RMON-MIB)</td>
</tr>
<tr>
<td></td>
<td>A threshold that can be set on critical RMON variables for network management.</td>
<td></td>
</tr>
<tr>
<td>Network Analysis</td>
<td>...mib-2(1).rmon(16).alarm(3)</td>
<td>RFC 2819 (RMON-MIB)</td>
</tr>
<tr>
<td></td>
<td>A threshold that can be set on critical RMON variables for network management.</td>
<td></td>
</tr>
<tr>
<td>Network Analysis</td>
<td>...mib-2(1).rmon(16).hosts(4)</td>
<td>RFC 2819 (RMON-MIB)</td>
</tr>
<tr>
<td></td>
<td>Maintains statistics on each host device on the segment or port.</td>
<td></td>
</tr>
<tr>
<td>Network Analysis</td>
<td>...mib-2(1).rmon(16).hostTopN(5)</td>
<td>RFC 2819 (RMON-MIB)</td>
</tr>
<tr>
<td></td>
<td>A user-defined subset report of the Hosts group, sorted by a statistical counter.</td>
<td></td>
</tr>
<tr>
<td>Network Analysis</td>
<td>...mib-2(1).rmon(16).statistics(1).etherStatsTable(1)</td>
<td>RFC 2819 (RMON-MIB)</td>
</tr>
<tr>
<td>Network Analysis</td>
<td>...mib-2(1).rmon(16).matrix(6)</td>
<td>RFC 2819 (RMON-MIB)</td>
</tr>
<tr>
<td></td>
<td>Maintains conversation statistics between hosts on a network.</td>
<td></td>
</tr>
<tr>
<td>Network Analysis</td>
<td>...mib-2(1).rmon(16).filter(7)</td>
<td>RFC 2819 (RMON-MIB)</td>
</tr>
<tr>
<td></td>
<td>A filter engine that generates a packet stream from frames that match a specified pattern.</td>
<td></td>
</tr>
<tr>
<td>Module</td>
<td>Object Identifier (OID) and Description</td>
<td>Source</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------------------------------------------------------------------------------------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>Network Analysis</td>
<td>...mib-2(1).rmon(16).capture(8)</td>
<td>RFC 2819 (RMON-MIB)</td>
</tr>
<tr>
<td></td>
<td>Manages buffers for packets captured by the Filter group for uploading to the management console.</td>
<td></td>
</tr>
<tr>
<td>Supervisor Engine</td>
<td>...mib-2(1).rmon(16).event(9)</td>
<td>RFC 2819 (RMON-MIB)</td>
</tr>
<tr>
<td></td>
<td>Generates SNMP traps when an Alarms group threshold is exceeded and logs the events.</td>
<td></td>
</tr>
<tr>
<td>Network Analysis</td>
<td>...mib-2(1).rmon(16).event(9)</td>
<td>RFC 2819 (RMON-MIB)</td>
</tr>
<tr>
<td></td>
<td>Generates SNMP traps when an Alarms group threshold is exceeded and logs the events.</td>
<td></td>
</tr>
<tr>
<td>Supervisor Engine</td>
<td>...mib-2(1).rmon(16).event(9)</td>
<td>RFC 2819 (RMON-MIB)</td>
</tr>
<tr>
<td></td>
<td>Generates SNMP traps when an Alarms group threshold is exceeded and logs the events.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>...mib-2(1).rmon(16).tokenRing(10).ringStationControlTable(1)</td>
<td>RFC 1513 (TOKEN-RING-RMON MIB)</td>
</tr>
<tr>
<td></td>
<td>...mib-2(1).rmon(16).tokenRing(10).ringStationTable(2)</td>
<td>RFC 1513 (TOKEN-RING-RMON MIB)</td>
</tr>
<tr>
<td></td>
<td>...mib-2(1).rmon(16).tokenRing(10).ringStationOrderTable(3)</td>
<td>RFC 1513 (TOKEN-RING-RMON MIB)</td>
</tr>
<tr>
<td></td>
<td>...mib-2(1).rmon(16).tokenRing(10).ringStationConfigControlTable(4)</td>
<td>RFC 1513 (TOKEN-RING-RMON MIB)</td>
</tr>
<tr>
<td></td>
<td>...mib-2(1).rmon(16).tokenRing(10).ringStationConfigTable(5)</td>
<td>RFC 1513 (TOKEN-RING-RMON MIB)</td>
</tr>
<tr>
<td></td>
<td>...mib-2(1).rmon(16).tokenRing(10).sourceRoutingStatsTable(6)</td>
<td>RFC 1513 (TOKEN-RING-RMON MIB)</td>
</tr>
<tr>
<td></td>
<td>Aggregates detailed Token Ring statistics.</td>
<td></td>
</tr>
<tr>
<td>Network Analysis</td>
<td>...mib-2(1).rmon(16).protocolDir(11)</td>
<td>RFC 2021 (RMON2-MIB)</td>
</tr>
<tr>
<td></td>
<td>A table of protocols for which the Network Analysis Module monitors and maintains statistics.</td>
<td></td>
</tr>
<tr>
<td>Network Analysis</td>
<td>...mib-2(1).rmon(16).protocolDist(12)</td>
<td>RFC 2021 (RMON2-MIB)</td>
</tr>
<tr>
<td></td>
<td>A table of statistics for each protocol in protocolDir(11).</td>
<td></td>
</tr>
<tr>
<td>Network Analysis</td>
<td>...mib-2(1).rmon(16).addressMap(13)</td>
<td>RFC 2021 (RMON2-MIB)</td>
</tr>
<tr>
<td></td>
<td>List of MAC-to-network-layer address bindings.</td>
<td></td>
</tr>
<tr>
<td>Network Analysis</td>
<td>...mib-2(1).rmon(16).nlHost(14)</td>
<td>RFC 2021 (RMON2-MIB)</td>
</tr>
<tr>
<td></td>
<td>Statistics for each network layer address.</td>
<td></td>
</tr>
<tr>
<td>Network Analysis</td>
<td>...mib-2(1).rmon(16).nlMatrix(15)</td>
<td>RFC 2021 (RMON2-MIB)</td>
</tr>
<tr>
<td></td>
<td>Traffic statistics for pairs of network layer addresses.</td>
<td></td>
</tr>
<tr>
<td>Network Analysis</td>
<td>...mib-2(1).rmon(16).alHost(16)</td>
<td>RFC 2021 (RMON2-MIB)</td>
</tr>
<tr>
<td></td>
<td>Statistics by application layer protocol for each network address.</td>
<td></td>
</tr>
<tr>
<td>Network Analysis</td>
<td>...mib-2(1).rmon(16).alMatrix(17)</td>
<td>RFC 2021 (RMON2-MIB)</td>
</tr>
<tr>
<td></td>
<td>Traffic statistics by application layer protocol for pairs of network layer addresses.</td>
<td></td>
</tr>
<tr>
<td>Network Analysis</td>
<td>...mib-2(1).rmon(16).usrHistory(18)</td>
<td>RFC 2021 (RMON2-MIB)</td>
</tr>
<tr>
<td></td>
<td>Extends history beyond RMON1 link-layer statistics to include any RMON, RMON2, MIB-I, or MIB-II statistic.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 4  Supervisor Engine Module and NAM RMON Support (continued)

<table>
<thead>
<tr>
<th>Module</th>
<th>Object Identifier (OID) and Description</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supervisor Engine</td>
<td>\texttt{...mib-2(1).rmon(16).probeConfig(19)}. Displays a list of agent capabilities and configurations.</td>
<td>RFC 2021 (RMON2-MIB)</td>
</tr>
<tr>
<td>Network Analysis</td>
<td>\texttt{...mib-2(1).rmon(16).switchRMON(22).smonMIBObjects(1). dataSourceCaps(1).dataSourceCapsTable(1)}. Maps physical entities and VLANs to ifEntries.</td>
<td>RFC 2613 (SMON-MIB)</td>
</tr>
<tr>
<td>Network Analysis</td>
<td>\texttt{...mib-2(1).rmon(16).switchRMON(22).smonMIBObjects(1). smonStats(2).smonVlanStatsControlTable(1)}. Traffic statistics by VLAN ID number.</td>
<td>RFC 2613 (SMON-MIB)</td>
</tr>
<tr>
<td>Network Analysis</td>
<td>\texttt{...mib-2(1).rmon(16).switchRMON(22).smonMIBObjects(1). smonStats(2).smonPrioStatsControlTable(3)}. Traffic statistics by 802.1p user priority value.</td>
<td>RFC 2613 (SMON-MIB)</td>
</tr>
<tr>
<td>Network Analysis</td>
<td>\texttt{...frontier(141).mibdoc2(2).netscout2(1).art(5).artControlTable(2)}. Application response time statistics.</td>
<td>draft-warth-rmon2-artmib-01.txt (ART-MIB)</td>
</tr>
<tr>
<td>Network Analysis</td>
<td>\texttt{...mib-2(1).rmon(16).mediaIndependentStats(21)}. Counters for packets, octets, broadcasts, errors, etc.</td>
<td>RFC 3273 (HC-RMON-MIB)</td>
</tr>
<tr>
<td></td>
<td>\texttt{rmon.dsonmMib(26).dsmonObjects(1).dsmonStatsObjects(2). dsmonStatsControlTable(1). rmon.dsonmMib(26).dsmonObjects(1).dsmonStatsObjects(2). dsmonStatsTable(2). Per-datasource statistics collection tables}</td>
<td>RFC 3287 (DSMON-MIB)</td>
</tr>
</tbody>
</table>
### Local Interfaces in the NAM ifTable

There are three versions of the Network Analysis Module (NAM) for the Catalyst 6500 Series switch. These are:
- WS-X6380-NAM
- WS-SVC-NAM-1
- WS-SVC-NAM-2

<table>
<thead>
<tr>
<th>Module</th>
<th>Object Identifier (OID) and Description</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>rmon.dsmonMib(26).dsmonObjects(1).dsmonPdistObjects(3).dsmonPdistCtlTable(1)</td>
<td>RFC 3287 (DSMON-MIB)</td>
<td></td>
</tr>
<tr>
<td>rmon.dsmonMib(26).dsmonObjects(1).dsmonPdistObjects(3).dsmonPdistStatsTable(2)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rmon.dsmonMib(26).dsmonObjects(1).dsmonPdistObjects(3).dsmonPdistTopNCTtTable(3)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rmon.dsmonMib(26).dsmonObjects(1).dsmonPdistObjects(3).dsmonPdistTopNTable(4)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Per-protocol statistics collection tables**

<table>
<thead>
<tr>
<th>Module</th>
<th>Object Identifier (OID) and Description</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>rmon.dsmonMib(26).dsmonObjects(1).dsmonHostObjects(4).dsmonHostCtlTable(1)</td>
<td>RFC 3287 (DSMON-MIB)</td>
<td></td>
</tr>
<tr>
<td>rmon.dsmonMib(26).dsmonObjects(1).dsmonHostObjects(4).dsmonHostTable(2)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rmon.dsmonMib(26).dsmonObjects(1).dsmonHostObjects(4).dsmonHostTopNCTtTable(3)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rmon.dsmonMib(26).dsmonObjects(1).dsmonHostObjects(4).dsmonHostTopNTable(4)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Per-host statistics collection tables**

<table>
<thead>
<tr>
<th>Module</th>
<th>Object Identifier (OID) and Description</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>rmon.dsmonMib(26).dsmonObjects(1).dsmonCapsObjects(5).dsmonCapabilities(1)</td>
<td>RFC 3287 (DSMON-MIB)</td>
<td></td>
</tr>
</tbody>
</table>

**DSMON capabilities variable**

<table>
<thead>
<tr>
<th>Module</th>
<th>Object Identifier (OID) and Description</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>rmon.dsmonMib(26).dsmonObjects(1).dsmonMatrixObjects(6).dsmonMatrixCtlTable(1)</td>
<td>RFC 3287 (DSMON-MIB)</td>
<td></td>
</tr>
<tr>
<td>rmon.dsmonMib(26).dsmonObjects(1).dsmonMatrixObjects(6).dsmonMatrixSDTTable(2)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rmon.dsmonMib(26).dsmonObjects(1).dsmonMatrixObjects(6).dsmonMatrixDSTable(3)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rmon.dsmonMib(26).dsmonObjects(1).dsmonMatrixObjects(6).dsmonMatrixTopNCTtTable(4)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rmon.dsmonMib(26).dsmonObjects(1).dsmonMatrixObjects(6).dsmonMatrixTopNTable(5)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Matrix statistics collection tables**

### Table 4  Supervisor Engine Module and NAM RMON Support (continued)

<table>
<thead>
<tr>
<th>Module</th>
<th>Object Identifier (OID) and Description</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>rmon.dsmonMib(26).dsmonObjects(1).dsmonPdistObjects(3).dsmonPdistCtlTable(1)</td>
<td>RFC 3287 (DSMON-MIB)</td>
<td></td>
</tr>
<tr>
<td>rmon.dsmonMib(26).dsmonObjects(1).dsmonPdistObjects(3).dsmonPdistStatsTable(2)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rmon.dsmonMib(26).dsmonObjects(1).dsmonPdistObjects(3).dsmonPdistTopNCTtTable(3)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rmon.dsmonMib(26).dsmonObjects(1).dsmonPdistObjects(3).dsmonPdistTopNTable(4)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Per-protocol statistics collection tables
This section explains the differences between the newer NAM-1 and NAM-2 and the previous version the WS-X6380-NAM and how to configure and manage the NAM-1 and NAM-2 in respect to their management and data ports for SNMP and CLI as seen both from the NAM and the Supervisor module.

The WS-X6380-NAM shows up in the Supervisor CLI and ifTable as two ports. The first port is the data port, used for receiving SPAN traffic. The second port is the management port. On the NAM these two ports show up in the ifTable as the first two ports (with ifIndex.1 for data and ifIndex.2 for management).

The WS-SVC-NAM-1 shows up in the Supervisor CLI (in the Catalyst operating system) and ifTable as three ports. The first port is unused. The second port is the management port. The third port is the data port (for receiving SPAN traffic). The Supervisor CLI (in Cisco IOS) abstracts the ports (“analysis module . . .”). On the NAM’s ifTable the management port shows up as the first port (ifIndex.1) and the data port shows up as the second (ifIndex.2).

The WS-SVC-NAM-2 shows up in the Supervisor CLI (in the Catalyst operating system) and ifTable as eight ports. Ports 1, 3, 4, 5, and 6 are unused. Port 2 is the management port (the same as on WS-SVC-NAM-1). Ports 7 and 8 are both data ports and can be SPAN targets. The Supervisor CLI (in Cisco IOS) abstracts the ports (“analysis module . . .”). On the NAM’s ifTable the interfaces are as follows:

- ifIndex.1: Is designated the management port.
- ifIndex.2: Represents the traffic from both data ports (also known as “All SPAN”).
- ifIndex.3: Represents the traffic from the first data port (named “data port 1”)
- ifIndex.4: Represents the traffic from the second data port (named “data port 2”)

For WS-SVC-NAM-1 and WS-SVC-NAM-2 the data ports are 802.1q trunk ports. Packets are received with an 802.1q header (except for packets with the ports native VLAN Id), affecting offsets (for example filters on IP headers) in packets.

### Table 5-5   NAM Local Interface Designations

<table>
<thead>
<tr>
<th>SNMP OID</th>
<th>WS-X6380-NAM</th>
<th>WS-SVC-NAM-1</th>
<th>WS-SVC-NAM-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supervisor engine number of ports</td>
<td>cisco.5.1.3.1.1.2.223</td>
<td>cisco.5.1.3.1.1.2.914</td>
<td>cisco.5.1.3.1.1.2.291</td>
</tr>
<tr>
<td>Supervisor engine management port</td>
<td>2</td>
<td>3</td>
<td>8</td>
</tr>
<tr>
<td>Supervisor engine data ports</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>NAM management port</td>
<td>ifIndex.2</td>
<td>ifIndex.1</td>
<td>ifIndex.1</td>
</tr>
<tr>
<td>NAM data port</td>
<td>ifIndex.1</td>
<td>ifIndex.2</td>
<td>ifIndex.2, ifIndex.3, ifIndex.4</td>
</tr>
</tbody>
</table>

**Explanation**  
When I import a configuration using “config network”, the download of configuration file goes through fine, but import operation failed giving an error.

**Recommended Action**  
Use the `show log config` command to determine where exactly the configuration failed. Depending on the seriousness of failure you could either ignore or correct the configuration file and try the `config network` command again.
**Explanation** From NAM-1 or NAM-2 application image tried to upgrade Maintenance image, I got this error: Image verification failed.

The image you are trying to upgrade is not a valid Maintenance image or is not compatible with this release.

**Recommended Action** You need to use the correct maintenance image for NAM-1 or NAM-2 and WS-X6380-NAM maintenance image should not be used.

**Explanation** From WS-X6380-NAM application image, when I try to upgrade the maintenance image I get this error.

Incompatible image! Upgrade aborted.

**Recommended Action** You need to use the correct maintenance image for WS-X6380-NAM and the NAM-1, NAM-2 maintenance image should not be used.

**Explanation** When I try to upgrade the WS-X6380-NAM Maintenance image, I get the following error:

restore operation failed.

**Explanation** You are trying to load an application image the NAM-1 or NAM-2, which causes this error. Try loading WS-X6380-NAM application image to correct this problem.