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

Release 3.4(1)
March 2005

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

Text Part Number: OL-7174-01

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.

CCSP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers 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)

Catalyst 6500 Series Switch and Cisco 7600 Series Router Network Analysis Module Installation and Configuration Note
Copyright © 2005 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

Product Numbers:

WS-SVC-NAM-1
WS-SVC-NAM-2

This publication describes how to install the Catalyst 6500 series switch, Catalyst 6000 series switch, or Cisco 7600 series router Network Analysis Module (NAM) running NAM software release 3.3(1) 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 xiv for more information about software configuration.

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, Catalyst 6000 series switch, or Cisco 7600 series router.

Note Third-party software used under license accompanies the Network Analysis Module software, Release 3.3. Notices that may apply to the license and to the use of such third-party software are listed in the *Copyright Notices for the Network Analysis Module Release 3.3.*

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:

Chapter	Title	Description
Chapter 1	Overview	Presents an overview of the Catalyst 6500 series switch, Catalyst 6000 series switch, or Cisco 7600 series router Network Analysis Module (NAM).
Chapter 2	Requirements for the Network Analysis Module	Describes the hardware and software requirements for the NAM.
Chapter 3	Getting Started	Describes how to configure the NAM.
Chapter 4	Administering the Network Analysis Module	Describes how to administer the NAM from the CLI for each switch operating system.
Chapter 5	Troubleshooting the Network Analysis Module	Provides troubleshooting information for the NAM.

Conventions

This publication uses the following conventions:

Convention	Description
boldface font	Commands, command options, and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
^	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.
< >	Nonprinting characters, such as passwords are in angle brackets.

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 **IMPORTANT SAFETY INSTRUCTIONS**

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. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Waarschuwing **BELANGRIJKE VEILIGHEIDSINSTRUCTIES**

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 de standaard praktijken om ongelukken te voorkomen. Gebruik het nummer van de verklaring onderaan de waarschuwing als u een vertaling van de waarschuwing die bij het apparaat wordt geleverd, wilt raadplegen.

BEWAAR DEZE INSTRUCTIES

Varoitus **TÄRKEITÄ TURVALLISUUSOHJEITA**

Tämä varoitusmerkki merkitsee vaaraa. Tilanne voi aiheuttaa ruumiillisia vammoja. Ennen kuin käsittelet laitteistoa, huomioi sähköpiirien käsittelemiseen liittyvät riskit ja tutustu onnettomuuksien yleisiin ehkäisytapoihin. Turvallisuusvaroitusten käännökset löytyvät laitteen mukana toimitettujen käännettyjen turvallisuusvaroitusten joukosta varoitusten lopussa näkyvien lausuntonumeroiden avulla.

SÄILYTÄ NÄMÄ OHJEET

Attention **IMPORTANTES INFORMATIONS DE SÉCURITÉ**

Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers liés aux circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions des avertissements figurant dans les consignes de sécurité traduites qui accompagnent cet appareil, référez-vous au numéro de l'instruction situé à la fin de chaque avertissement.

CONSERVEZ CES INFORMATIONS

Warnung **WICHTIGE SICHERHEITSHINWEISE**

Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu Verletzungen führen kann. Machen Sie sich vor der Arbeit mit Geräten mit den Gefahren elektrischer Schaltungen und den üblichen Verfahren zur Vorbeugung vor Unfällen vertraut. Suchen Sie mit der am Ende jeder Warnung angegebenen Anweisungsnummer nach der jeweiligen Übersetzung in den übersetzten Sicherheitshinweisen, die zusammen mit diesem Gerät ausgeliefert wurden.

BEWAHREN SIE DIESE HINWEISE GUT AUF.

Avvertenza **IMPORTANTI ISTRUZIONI SULLA SICUREZZA**

Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di intervenire su qualsiasi apparecchiatura, occorre essere al corrente dei pericoli relativi ai circuiti elettrici e conoscere le procedure standard per la prevenzione di incidenti. Utilizzare il numero di istruzione presente alla fine di ciascuna avvertenza per individuare le traduzioni delle avvertenze riportate in questo documento.

CONSERVARE QUESTE ISTRUZIONI

Advarsel **VIKTIGE SIKKERHETSINSTRUKSJONER**

Dette advarselssymbolet betyr fare. Du er i en situasjon som kan føre til skade på person. Før du begynner å arbeide med noe av utstyret, må du være oppmerksom på farene forbundet med elektriske kretser, og kjenne til standardprosedyrer for å forhindre ulykker. Bruk nummeret i slutten av hver advarsel for å finne oversettelsen i de oversatte sikkerhetsadvarslene som fulgte med denne enheten.

TA VARE PÅ DISSE INSTRUKSJONENE

Aviso **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

Este símbolo de aviso significa perigo. Você está em uma situação que poderá ser causadora de lesões corporais. Antes de iniciar a utilização de qualquer equipamento, tenha conhecimento dos perigos envolvidos no manuseio de circuitos elétricos e familiarize-se com as práticas habituais de prevenção de acidentes. Utilize o número da instrução fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham este dispositivo.

GUARDE ESTAS INSTRUÇÕES

¡Advertencia! **INSTRUCCIONES IMPORTANTES DE SEGURIDAD**

Este símbolo de aviso indica peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considere los riesgos de la corriente eléctrica y familiarícese con los procedimientos estándar de prevención de accidentes. Al final de cada advertencia encontrará el número que le ayudará a encontrar el texto traducido en el apartado de traducciones que acompaña a este dispositivo.

GUARDE ESTAS INSTRUCCIONES

Varning! **VIKTIGA SÄKERHETSANVISNINGAR**

Denna varningssignal signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanliga förfaranden för att förebygga olyckor. Använd det nummer som finns i slutet av varje varning för att hitta dess översättning i de översatta säkerhetsvarningar som medföljer denna anordning.

SPARA DESSA ANVISNINGAR

Figyelem FONTOS BIZTONSÁGI ELOÍRÁSOK

Ez a figyelmezeto jel veszélyre utal. Sérülésveszélyt rejto helyzetben van. Mielott bármely berendezésen munkát végezte, legyen figyelemmel az elektromos áramkörök okozta kockázatokra, és ismerkedjen meg a szokásos balesetvédelmi eljárásokkal. A kiadványban szereplo figyelmeztetések fordítása a készülékhez mellékelt biztonsági figyelmeztetések között található; a fordítás az egyes figyelmeztetések végén látható szám alapján keresheto meg.

ORIZZE MEG EZEKET AZ UTASÍTÁSOKAT!

Предупреждение ВАЖНЫЕ ИНСТРУКЦИИ ПО СОБЛЮДЕНИЮ ТЕХНИКИ БЕЗОПАСНОСТИ

Этот символ предупреждения обозначает опасность. То есть имеет место ситуация, в которой следует опасаться телесных повреждений. Перед эксплуатацией оборудования выясните, каким опасностям может подвергаться пользователь при использовании электрических цепей, и ознакомьтесь с правилами техники безопасности для предотвращения возможных несчастных случаев. Воспользуйтесь номером заявления, приведенным в конце каждого предупреждения, чтобы найти его переведенный вариант в переводе предупреждений по безопасности, прилагаемом к данному устройству.

СОХРАНИТЕ ЭТИ ИНСТРУКЦИИ

Aviso **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

Este símbolo de aviso significa perigo. Você se encontra em uma situação em que há risco de lesões corporais. Antes de trabalhar com qualquer equipamento, esteja ciente dos riscos que envolvem os circuitos elétricos e familiarize-se com as práticas padrão de prevenção de acidentes. Use o número da declaração fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham o dispositivo.

GUARDE ESTAS INSTRUÇÕES

Advarsel **VIGTIGE SIKKERHEDSANVISNINGER**

Dette advarselssymbol betyder fare. Du befinder dig i en situation med risiko for legemesbeskadigelse. Før du begynder arbejde på udstyr, skal du være opmærksom på de involverede risici, der er ved elektriske kredsløb, og du skal sætte dig ind i standardprocedurer til undgåelse af ulykker. Brug erklæringsnummeret efter hver advarsel for at finde oversættelsen i de oversatte advarsler, der fulgte med denne enhed.

GEM DISSE ANVISNINGER

تحذير **إرشادات الأمان الهامة**

يوضح رمز التحذير هذا وجود خطر. وهذا يعني أنك متواجد في مكان قد ينتج عنه التعرض لإصابات. قبل بدء العمل، احذر مخاطر التعرض للصدمات الكهربائية وكن على علم بالإجراءات القياسية للحيلولة دون وقوع أي حوادث. استخدم رقم البيان الموجود في أخر كل تحذير لتحديد مكان ترجمته داخل تحذيرات الأمان المترجمة التي تأتي مع الجهاز.

قم بحفظ هذه الإرشادات

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*.
  - *Release Notes for Catalyst 6500 Series Switch and Cisco 7600 Series Router Network Analysis Module Software Release 3.3*.
  - *Quick Start Guide for the Catalyst 6500 Series and Cisco 7600 Series Network Analysis Module*
  - *Catalyst 6500 Series Switch and Cisco 7600 series Router Network Analysis Module Command Reference*
  - *User Guide for the Network Analysis Module Traffic Analyzer Release 3.3*
- 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 3.3* (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 8.x*
  - *Catalyst 6500 Series Switch Software Configuration Guide*

  - *Catalyst 6500 Series Switch Command Reference*
- For detailed hardware configuration and maintenance procedures, refer to the *Catalyst 6500 Series Switch Module Installation Guide*.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain 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 at this URL:

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

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation 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.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your 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.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

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

- *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:

  http://www.cisco.com/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

CHAPTER 1

Overview

This chapter describes the Catalyst 6500 series switch, Catalyst 6000 series switch, or Cisco 7600 series router Network Analysis Module (NAM), how it operates, and how to manage it.

Note This installation and configuration note applies to users who have Catalyst operating system and Cisco_IOS software. The procedures in this note that pertain to each operating system are specified in separate sections for each operating system.

This chapter contains these sections:

Before You Begin

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

Understanding How the NAM Works

This section describes how the Catalyst 6500 series switch, Catalyst 6000 series switch, or Cisco 7600 series router Network Analysis Module (NAM) operates. This section contains these subsections:

The NAM monitors and analyzes network traffic using remote monitoring (RMON), RMON extensions for switched networks (SMON), and other management information bases (MIBs). For more information, see the "Supported MIB Objects" section on page 5-15.

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

- RMON groups defined in RFC 2819
- RMON2 groups defined in RFC 2021
- DSMON groups defined in RFC 3287
- High-capacity RMON groups defined in RFC 3273 (except the media Independent Group)
- SMON groups defined in RFC 2613
- All groups defined in the Application Response Time MIB
- NetFlow Version 9 records; the NetFlow listening mode now shows data sources using NetFlow Version 9

The NAM can also monitor individual Ethernet VLANs, which allows it to serve as an extension to the basic RMON support provided by the Catalyst 6500 series 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 or RSPAN source port.

  For more information about SPAN and RSPAN, refer to the "Configuring SPAN and RSPAN" chapter in the *Catalyst 6500 Series Switch Software Configuration Guide*.

- NetFlow Data Export (NDE).

  For more information about NDE, refer to the *Catalyst 6500 Series Switch Software Configuration Guide.*

Table 1-1 summarizes the traffic sources that are used for NAM monitoring.

Table 1-1 Summary of Traffic Sources for NAM Monitoring

Traffic Source	LAN		WAN	
	Ports	**VLANs**	**Ports**	**VLANs**
VACL capture	Yes	Yes	Yes	N/A
NetFlow Data Export NDE (local)	Yes	Yes	Yes	Yes
NetFlow Data Export NDE (remote)	Yes	Yes	Yes	Yes

Table 1-1 Summary of Traffic Sources for NAM Monitoring (continued)

Traffic Source	LAN		WAN	
	Ports	VLANs	Ports	VLANs
SPAN	Yes	Yes	No	No
ERSPAN	Yes	Yes	No	No

Understanding How the NAM Uses SPAN

A switched port analyzer (SPAN) session is an association of a destination port with a set of source ports, configured with parameters that specify the monitored network traffic. You can configure multiple SPAN sessions in a switched network.

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

Module	Cisco IOS Software	Catalyst Operating System Software
NAM-1	data-port 1	*module number*:3
NAM-2	data-port 1 and data-port 2	*module number*:7 or *module number*:8

Each of these ports is independent. You may create data-port collections that are populated by only the traffic from one of the ports 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.

For more information about SPAN and how to configure it on the Catalyst 6000 and 6500 series switches, use this URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sy/swcg/span.htm#1032978

For more information about SPAN and how to configure it on the Cisco 7600 series router, use this URL:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/software/122sx/swcg/span.htm

The NAM supports Encapsulated Remote SPAN (ERSPAN) traffic on the management port and uses that traffic as a data source. All collection types are supported on the ERSPAN traffic.

ERSPAN is an extension of SPAN where packets are encapsulated in a generic routing encapsulation (GRE) packet and sent to an ERSPAN destination. The ERSPAN sources and destinations are usually Supervisor Engine 720 with a PFC5 or later releases. Because the ERSPAN traffic uses IP or GRE to encapsulate the packets sent across the routers, the deencapsulated traffic can then be sent to the NAM data ports.

Understanding How the NAM Uses VACLs

A VLAN access control list (VACL) can forward traffic from either a WAN interface or VLANs to a data port on the NAM. A VACL provides an alternative to using SPAN; a VACL can provide access control based on Layer 3 addresses for IP and IPX protocols. The unsupported protocols are access controlled through the MAC addresses. A MAC VACL cannot be used to access control IP or IPX addresses.

There are two types of VACLs: one that captures all bridged or routed VLAN packets and another that 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.

A VACL 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 Release 12.1(13)E or later releases, 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, the VACLs apply to all packets and can be applied to any VLAN or WAN interface. The VACLs are processed in the hardware.

A VACL uses Cisco IOS access control lists (ACLs). A VACL ignores any Cisco IOS ACL fields that are not supported in the 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, and policy-based routing. 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, the 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. Each ACE is associated with an action that describes what the system should do with the packet when a match occurs. The action is feature dependent. Catalyst 6000 and 6500 series switches and Cisco 7600 series routers support three types of ACEs in the hardware: IP, IPX, and MAC-Layer traffic. The VACLs that are applied to WAN interfaces support only IP traffic.

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, note the following:

- VACLs and context-based access control (CBAC) cannot be configured on the same interface.
- TCP Intercepts and Reflexive ACLs take precedence over a VACL action on the same interface.
- IGMP packets are not checked against VACLs.

For details on how to configure a 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

NetFlow Data Export (NDE) is a remote device that allows you to monitor port traffic on the NAM. To use an NDE data source for the NAM, you must configure the remote device to export the NDE packets to UDP port 3000 on the NAM. You may need to configure the device on a per-interface basis. A screen has been added to the web application user interface for specifying NDE devices (an NDE device is identified by its IP address). By default, the switch's local supervisor engine is always available as an NDE device.

You 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.

For more information about the NDE data sources of the NAM, go to the NAM Traffic Analyzer online help menu and choose the **Contents > Setting Up the Application > Setting Up Data Sources > Understanding NetFlow Interfaces**.

Managing the NAM

You can manage the NAM 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 CiscoWorks2000.

NAM Traffic Analyzer provides access to the management and monitoring features for NAM data and voice traffic through a web browser. To use NAM Traffic Analyzer, you need to do some basic configuration tasks on the NAM using the CLI. You then can start NAM Traffic Analyzer 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 NAM Traffic Analyzer to configure the NAM to use a remote TACACS+ server. A TACACS+ server provides 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), which is a component of CiscoWorks2000 LAN management solutions (NMS). For more information about using RTM, refer to the CiscoWorks documentation or this URL:

http://www.Cisco.com/univercd/cc/td/doc/product/lan/cat6000/fam_mod/rel2_1_2/ol_2428.htm

To use RMON and SNMP agent support, you configure the NAM using the CLI.

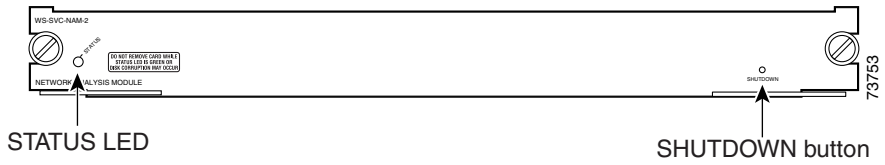
If you have a NAM that is already configured and running in the switch, and you are familiar with the NAM, you can begin using NAM Traffic Analyzer by entering the **ip http server enable** CLI command and then starting NAM Traffic Analyzer in your browser.

Refer to the *User Guide for the Network Analysis Module Traffic Analyzer Release 3.3* for more information about using NAM Traffic Analyzer.

Front Panel Description

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

Figure 1-1 Network Analysis Module



STATUS LED

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

Table 1-3 STATUS LED Description

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

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 risk disk corruption if you remove the NAM from the switch before the NAM 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.

Note If disk corruption occurs, you can recover the disk by reupgrading the application image with the **--install** option. See the "Upgrading the NAM Application Software with Catalyst Operating System Software" section on page 17.

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

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

CHAPTER 2

Requirements for the Network Analysis Module

This chapter describes the software and hardware requirements to support the Catalyst 6500 series switch, Catalyst 6000 series switch, or Cisco 7600 series router NAM. This chapter contains these sections:

Software Requirements

Note Starting with maintenance image release 2.1(1), there is a single maintenance image for services modules. Refer to this URL: http://www.cisco.com/cgi-bin/tablebuild.pl/cat6000-serv-maint

Table 2-1 lists the NAM software releases that are supported by Catalyst operating system software and Cisco IOS software.

Table 2-1 NAM Software Compatibility

Module	Application Image	Maintenance Image	Catalyst Operating System Software	Cisco IOS Software	Supported Browsers	Java Plug-in Support[1]
WS-SVC-NAM-1 WS-SVC-NAM-2	3.4(1)	1.1(1)m 2.1(1)	Release 7.3(1) or later with Supervisor Engine 1A or 2[2]	Release 12.1(13)E[3] or later with a Supervisor Engine 2 with an MSFC2	Recommended — Internet Explorer 6.0 and later on Windows 2000	1.3.1_03 or 1.4.1_02
				Release 12.1(19)E1 or later with a Supervisor Engine 1A with an MSFC2	Netscape 7.0 or 7.1 on Windows 2000 and Solaris	1.4.1_02 (Windows 2000) and 1.4.0_01 (Solaris)
			Release 8.2(1) or later with a WS-SUP720	Release 12.2(14)SX1 with a WS-SUP720		
			Release 8.5(1) or later.			

1. Traffic Analyzer does not require a Java plug-in although a plug-in might be required to use Java Virtual Machine (JVM). The Java plug-in versions listed have been tested for browsers that require a plug-in for JVM.
2. Supervisor 1A with MSFC1 or MSFC2, Supervisor 2 with MSFC2 only.
3. If you are using a 12.1(13)E-based release, we recommend that you use a later 13E release, for example, Release 12.1(13)E11 over 12.1(13)E3.

Hardware Requirements

Table 2-2 lists the NAM hardware releases that are supported by Catalyst operating system software and Cisco IOS software.

Table 2-2 NAM Hardware Compatibility

Module	Catalyst Operating System Software	Cisco IOS Software	Platform
WS-SVC-NAM-1 WS-SVC-NAM-2	Supervisor Engine 1A or 2 or WS-SUP720	Supervisor Engine 1 with MSFC2, Supervisor Engine 2 with an MSFC2 or WS-SUP720	Catalyst 6000 series switches, Catalyst 6500 series switches, Cisco 7600 series routers

CHAPTER 3

Getting Started

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

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.

For initial configuration of the NAM. refer to the *Quick Start Guide for the Catalyst 6500 Series and Cisco 7600 Series Network Analysis Module*.

After you set up the NAM initial configuration, you can configure VLAN access control lists (VACLs), either local or remote NetFlow Data Export (NDE), and the switched port analyzer (SPAN) to monitor network traffic. For more information, see the "Configuring Traffic Sources for Capturing NAM Traffic" section on page 3-1.

When you complete configuring the software-dependent attributes for the NAM, you can configure the software-independent attributes. For more information, see the "Operating-System-Independent Configuration" section on page 3-12.

Configuring Traffic Sources for Capturing NAM Traffic

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 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 Table 1-2 on page 1-4.

VACL and SPAN cannot be applied to the same port simultaneously. Table 3-1 shows the SPAN and VACL port configurations that are supported on the NAM.

For more information about SPAN, see these URLs:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/span.htm
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_8_2/confg_gd/span.htm

For more information about VACLs, see these URLs:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/vacl.htm
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_82/confg_gd/acc_list.htm#1053650

For more information about NDE, see these URLs:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/nde.htm#1035105
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_8_2/confg_gd/nde.htm

These sections describe how to configure VACLs, either local or remote NDE, and SPAN to monitor network traffic with the NAM:

- Cisco IOS Software, page 3-2
- Catalyst Operating System Software, page 3-8

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 need to clear the VLANs that 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 this URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/index.htm

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

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

Command	Purpose
Router (config)# **monitor session** *{session_number}* {**source** {**interface type** *slot/port*} | {**vlan** *vlan_ID*}} [, | - | **rx** | **tx** | **both**]	Sets the source interfaces and VLANs for the monitor session.
Router (config)# **monitor session** {*session_number*} {**destination analysis module** *NAM module number* **data-port** *port*}	Enables port 1 of the NAM as a SPAN destination.
Router (config)# **no monitor session** *session_number*	Disables the monitor session.
Router (config)# **monitor session** *{session_number}* {**filter** *{vlan_ID}* [, | -]}	Filters the SPAN session so that only certain VLANs are seen from switch port trunks.
Router # **show monitor session** {*session_number*}	Shows current monitor sessions.

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
---------
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

Router# configure terminal
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 are 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:          1
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 a VACL as a Traffic Source

This section describes how to configure a VACL for a switch running Cisco IOS Release 12.1(13)E1 or later releases. To configure a LAN VACL on the Catalyst operating system, you can use the security ACL feature to achieve the same result. For more information, see the "Operating-System-Independent Configuration" procedure on page 3-12.

Configuring a VACL on a WAN Interface

Because WAN interfaces do not support SPAN if you want to monitor traffic on a WAN interface using a NAM, you need to manually configure a VACL on the switch using the switch CLI. This feature only works for IP traffic over the WAN interface. You can apply additional filtering rules to target specific data flows.

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

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

This example shows how to configure a 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, you can obtain the VLAN ID that is associated with the WAN interface command as follows:

```
Cat6509# show cwan vlan
Hidden VLAN  swidb->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, you should replace VLAN 1017 in the previous capture configuration with the VLAN ID that carries the ingress traffic. For example, this configuration allows the NAM to monitor only ingress traffic on a WAN interface:

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

Configuring a VACL on a LAN VLAN Interface

To monitor VLAN traffic on the LAN, you can forward the traffic to the NAM by using SPAN. However, in some rare circumstances, if the spanned traffic exceeds the NAM's monitoring capability, you can prefilter the LAN traffic before it is forwarded to the NAM.

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

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

Using NetFlow Data Export as a Traffic Source

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 more information.

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
```

Note 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:

```
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 (multilayer switching cache), follow these steps:

Step 1 Enter configuration mode.

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

Step 2 Select the version of NDE.

```
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 that are supported by the switch software to determine which NDE versions are available to the NAM.

Step 3 Select the NDE flow mask.

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

Note Use the full keyword to include additional details of the collection data in the flow mask.

Step 4 Enable NetFlow export.

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

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

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

This example shows how to set up an NDE configuration from the Multilayer Switch Feature Card (MSFC):

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mls nde sender version 5
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 Policy Feature Card (PFC), see 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 that 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. To export flows from the aggregation caches, perform these steps:

Step 1 Select an NDE version 8 aggregation.

```
Router(config)# ip flow-aggregation cache aggregation-type
```

The supported aggregation types are as follows:

- Destination-prefix
- Source-prefix
- Protocol-port
- Prefix

Step 2 Enable the aggregation cache.

```
Router(config-flow-cache)# enable
```

Step 3 Export the flow 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 need to clear the VLANs that you do not want to monitor from the capture feature.

Using SPAN as a Traffic Source

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

For more information about SPAN and RSPAN, refer to the "Configuring SPAN and RSPAN" chapter in the *Catalyst 6500 Series Switch Software Configuration Guide*.

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:

Task	Command
Set the NAM as a SPAN destination port.	**set span** {*src_mod/src_ports* | *src_vlans* | **sc0**} {*dest_mod* | *dest_port*} [**rx** | **tx** | **both**] [**inpkts** {**enable** | **disable**}] [**learning** {**enable** | **disable**}] [**multicast** {**enable** | **disable**}] [**filter** *vlans...*] [**create**]

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

```
Console> (enable) set span 1 5/7
```

Using a 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 example shows how to create a VACL that captures all the IP packets that are bridged or routed into VLAN 1 on the switch to the NAM-1 data port 6/3:

```
Console> (enable) set security acl ip LANCAPTURE permit ip any any capture
Console> (enable) commit
Console> (enable) set security acl map LANCAPTURE 1
Console> (enable) set security acl capture 6/3
```

This example shows how to create a VACL that captures a specific VLAN 1 conversation:

```
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 security acl capture 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 NetFlow. For more information, 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 for the Catalyst operating system, perform this task:

	Task	Command
Step 1	Select the NDE version. **Note** 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.	**set mls nde version** *nde-version-number*
Step 2	Set the NDE flow mask to 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.	**set mls flow full**
Step 3	Direct NDE packets to the NAM.	**set snmp extendedrmon netflow** [**enable** | **disable**] *mod* **set mls nde** *NAM-address* **3000**
Step 4	Enable NDE export.	**set mls nde enable**

	Task	Command
Step 5	(Optional) Make sure that the device exports if-index. **Note** Use this step if you want to break out NetFlow data by interface and direction at the NAM.	**set mls nde destination-ifindex enable** **set mls nde source-ifindex enable**
Step 6	Verify NDE export. On the local device: On the remote device:	 **show snmp and show mls nde** **show mls nde**

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

```
Console> (enable) set snmp extendedrmon netflow enable 2
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 the **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 Flow 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 the 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

These 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 are 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 that 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 as follows:

```
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 usernames and passwords on the NAM CLI, see the "Cisco IOS Software" section on page 4-1 and the "Catalyst Operating System Software" section on page 4-11. To change usernames 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 3.3.*

Step 2 Enable the HTTP server as follows:

```
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 as follows:

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

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

This example shows how to install a patch:

```
root@localhost# patch ftp://host/path/c6nam- 3.3-strong-cryptoK9-patch-1-0.bin

Proceeding with installation. Please do not interrupt.
If installation is interrupted, please try again.

Downloading c6nam- 3.3-strong-cryptoK9-patch-1-0.bin. Please wait...
ftp://host/path/c6nam- 3.3-strong-cryptoK9-patch-1-0.bin (1K)
-                         [########################]       1K |  228.92K/s
1891 bytes transferred in 0.01 sec (225.40k/sec)

Verifying c6nam- 3.3-strong-cryptoK9-patch-1-0.bin. Please wait...
Patch c6nam- 3.3-strong-cryptoK9-patch-1-0.bin verified.

Applying /usr/local/nam/patch/workdir/c6nam- 3.3-strong-cryptoK9-patch-1-0.bin.
Please wait...
########################################### [100%]
########################################### [100%]

Patch applied successfully.
```

Step 3 (Optional) Configure the HTTPS server as follows:

Note If you specify a port other than the default (443), add :*port_number.*

```
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 as follows:

```
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
User admin added.
Successfully enabled HTTP server.
```

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.

This example shows how to generate a self-signed certificate:

```
root@localhost# ip http secure generate self-signed-certificate

The HTTP secure server is enabled now. You must restart
to generate the certificate. Continue [y/n]? y
5243 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.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:CA
Locality Name (eg, city) []:San Jose
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco Systems, Inc.
Organizational Unit Name (eg, section) []:NAM
Common Name (eg, your name or your server's hostname) [r2d2-186.cisco.com]:
Email Address []:kjchen@cisco.com
Using configuration from /usr/local/nam/defaults/openssl.cnf
-----BEGIN CERTIFICATE-----
MIIDlTCCAv6gAwIBAgIBADANBgkqhkiG9w0BAQQFADCBlDELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAkNBMREwDwYDVQQHEwhTYW4gSm9zZTEcMBoGA1UEChMTQ2lzY28g
U3lzdGVtcywgSW5jLjEMMAoGA1UECxMDTkFNMRswGQYDVQQDExJyMmQyLTE4Ni5j
aXNjby5jb20xHDAaBgkqhkiG9w0BCQEWDW5hbUBjaXNjby5jb20wHhcNMDQwMjI0
MDAwNDAxWhcNMDUwMjIzMDAwNDAxWjCBlDELMAkGA1UEBhMCVVMxCzAJBgNVBAgT
AkNBMREwDwYDVQQHEwhTYW4gSm9zZTEcMBoGA1UEChMTQ2lzY28gU3lzdGVtcywg
SW5jLjEMMAoGA1UECxMDTkFNMRswGQYDVQQDExJyMmQyLTE4Ni5jaXNjby5jb20x
HDAaBgkqhkiG9w0BCQEWDW5hbUBjaXNjby5jb20wgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBAMDrGqhw2Kt8fimI+b11bk6+z9nTEQago1Qfoo8DehBLZ10eoJ/0
YAWlCqx3fnW3csSmGiHj6aEjJhm0WO5GvJRbzzbxeSPadDv7IdbIhXTLtPklW11g
```

```
byhUzvi5R8UFGSmerbbnc7qkTDXQdrQ2vETAfxK4oysq+HF55qVjY2KpAgMBAAGj
gfQwgfEwHQYDVR0OBBYEFEjcj4+vFJmLAo1NjnO9MYE/Hn9eMIHBBgNVHSMEgbkw
gbaAFEjcj4+vFJmLAo1NjnO9MYE/Hn9eoYGapIGXMIGUMQswCQYDVQQGEwJVUzEL
MAkGA1UECBMCQ0ExETAPBgNVBAcTCFNhbiBKb3NlMRwwGgYDVQQKExNDaXNjbyBT
eXN0ZW1zLCBJbmMuMQwwCgYDVQQLEwNOQU0xGzAZBgNVBAMTEnIyZDItMTg2LmNp
c2NvLmNvbTEcMBoGCSqGSIb3DQEJARYNbmFtQGNpc2NvLmNvbYIBADAMBgNVHRME
BTADAQH/MA0GCSqGSIb3DQEBBAUAA4GBAHwBnz9OALHWkyK4qYTTbBno2MFbmI49
gU4IIpFSgWjoqdiXXGJs7c1q0dMPzdmDIG1TjmkLx2HC1+dVuq/2X4RrOFaoog/s
K9GmULi8OtgRkDhXJHT/gDfv+L7gQpQCCpq1TUFMVlzxzAHSsBGnlQ8oTysXScEJ
nSr0tR/OKB0t
-----END CERTIFICATE-----
Disabling HTTP secure server...
Successfully disabled HTTP secure server.
Enabling HTTP secure server...
Successfully enabled HTTP secure server.
root@localhost#
```

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 as follows:

```
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
5244 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.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
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]:
Email Address []:xxx@Cisco.com
-----BEGIN CERTIFICATE REQUEST-----
MIIBzzCCATgCAQAwgY4xCzAJBgNVBAYTAklOMRMwEQYDVQQIEwpUYW1pbCBOYWR1
MRAwDgYDVQQHEwdDaGVubmFpMRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMR4wHAYD
VQQDExVuYW1sYWItcGlrMy5jaXNjby5jb20xIDAeBgkqhkiG9w0BCQEWEXNla2Fy
YmNAY2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8+SR503gS
ygkf6pnHuh0LelNf6LqJjzwFfjqjS8vpkFq/QVbwqTNDIggUfbvRAIRWEKVWhpRf
rr+II2o/Xzb0RLpV2J2p3HGgoRrKC3nArIFFiSqXniEU+g2mPqsFNcOyxHNXIxEj
iBQf80DxbmvWFOpunmOQ/pGuEysNfU/46wIDAQABoAAwDQYJKoZIhvcNAQEEBQAD
```

```
gYEAVAX89pCAcRDOqPgaBEMQCmWD+wqZPnALovr7C81OLBYTgLLqdwPqoSjSYosE
w/pFnIxWN1sJ7MC8+hjnJJLjoCwbyrEyvoiAvzpsGsnAZgWUVaUpR7jlNbf8x2A1
hAOH9KchS0TpSNy13OyhuAkv0pUcM2AJqB/93u4YvuHfNOA=
-----END CERTIFICATE REQUEST-----
```

Step 2 Install a certificate obtained from a certification authority as follows:

```
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-----
MIIDAzCCAmygAwIBAgIBADANBgkqhkiG9w0BAQQFADBlMQswCQYDVQQGEwJBVTET
MBEGA1UECBMKU29tZS1TdGF0ZTEhMB8GA1UEChMYSW50ZXJuZXQgV2lkZ2l0cyBQ
dHkgTHRkMR4wHAYDVQQDExVuYW1sYWItcGlrMy5jaXNjby5jb20wHhcNMDExMDMw
MTAxMDI4WhcNMDIxMDMwMTAxMDI4WjBlMQswCQYDVQQGEwJBVTETMBEGA1UECBMK
U29tZS1TdGF0ZTEhMB8GA1UEChMYSW50ZXJuZXQgV2lkZ2l0cyBQdHkgTHRkMR4w
HAYDVQQDExVuYW1sYWItcGlrMy5jaXNjby5jb20wgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBANsO1T5ayA6pvkJad413V+N/ibvND0XRyXfFycTQRzeA8F4A+etV
s0Iq0muFfiL9mDr/es9TkyfIM+T2F6+NE13DxJ53ZBbh7ndb6WOnzeHLKh9EDfSI
cy2s7751CPCjfLcMsWQLWSU7XUbi/ExDpb9e2wQQgi6QBED/YRkr73KNAgMBAAGj
gcIwgb8wHQYDVR0OBBYEFIHsyecd8AW4cvt7voCFeZMarXIqMIGPBgNVHSMEgYcw
gYSAFIHsyecd8AW4cvt7voCFeZMarXIqoWmkZzBlMQswCQYDVQQGEwJBVTETMBEG
A1UECBMKU29tZS1TdGF0ZTEhMB8GA1UEChMYSW50ZXJuZXQgV2lkZ2l0cyBQdHkg
THRkMR4wHAYDVQQDExVuYW1sYWItcGlrMy5jaXNjby5jb22CAQAwDAYDVR0TBAUw
AwEB/zANBgkqhkiG9w0BAQQFAAOBgQACDyWhULAUeSIXyt9tuUrdPfF97hrpFkKy
nj1yEU4piuc9qQtxG9yCGsofAm+CiGFg6P4qJZtBF47mq81qF+48JTYwi68CGCye
suZgw0iCPQVv4KDirHBKFc0Vr/2SMrXcJImczoV2WGcxWxsVaXwpkBKF8pcMFFYd
iOULMcvFxg==
-----END CERTIFICATE-----
.
Disabling HTTP server...
Successfully disabled HTTP server.
Enabling HTTP server...
Successfully enabled HTTP server.
```

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 username 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.

CHAPTER 4

Administering the Network Analysis Module

How you administer the NAM on your Catalyst 6500 series switch, Catalyst 6000 series switch, or Cisco 7600 series 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.

These sections describe how to administer the NAM from the CLI for each operating system:

When you complete administering the software-dependent attributes for the NAM, you can configure the software-independent NAM attributes. For more information, see the .

-

Cisco IOS Software

You can perform these various administrative tasks on the NAM with Cisco IOS software:

Logging In to the NAM with Cisco IOS Software

The NAM has two user levels with different access 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** if the NAM is the WS-SVC-NAM-1 or WS-SVC-NAM-2 module.

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

Table 4-1 NAM Users and Passwords

Module	Application Image (located on the hard disk)		Maintenance Image (located on the compact flash)	
WS-SVC-NAM-1 WS-SVC-NAM-2	**User**	**Password**	**User**	**Password**
	root	root	root	cisco
	guest	guest	guest	cisco

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. 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 can also 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 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 with Cisco IOS Software

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 4-4 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 as follows:

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

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 as follows:

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

Step 3 Enter the new password again as follows:

```
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 with Cisco IOS Software

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 software and is not available in Catalyst operating system software.

Note 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, see the "Resetting the NAM with Catalyst Operating System Software" section on page 4-14.

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.

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:

Software Image	Task	Command
Maintenance Image	Reset the module.	**hw-module module** *mod_num* **reset device:***partition* [**mem-test-full**] The device:*partition* value is the string for the PC boot device; for example, **hdd:1** designates the hard disk and **cf:1** designates the compact Flash where **x** is the number for the partition on each device. .
Application Image	Reset the module.	**hw-module module** *mod_num* **reset device:***partition* [**mem-test-full**] The device:*partition* value is the string for the PC boot device; for example, **hdd:1** designates the hard disk and **cf:1** designates the compact Flash where **x** is the number for the partition on each device.

This example shows how to reset the NAM that is installed in slot 9 from the CLI:

```
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 with Cisco IOS Software

You can upgrade both the application software and the maintenance software. To upgrade the application software, see the "Upgrading the NAM Application Software with Cisco IOS Software" section on page 4-5. To upgrade the maintenance software, see the "Upgrading the NAM Maintenance Software with Cisco IOS Software" section on page 4-8.

The NAM application and maintenance images are not interchangeable.

Table 4-2 lists the NAM image prefixes.

Table 4-2 NAM Image Prefixes

Module	Application Image	Maintenance Image
WS-SVC-NAM-1	nam-app	c6svc-nam-maint
WS-SVC-NAM-2	nam-app	c6svc-nam-maint

Upgrading the NAM Application Software with Cisco IOS 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:

```
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#
00:03:31:%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
start
00:03:46:SP:PC shutdown completed for module 9
00:03:46:%C6KPWR-SP-4-DISABLED:power to module in slot 9 set off (admin
request)
00:03:49:SP:Resetting module 9 ...
00:03:49:%C6KPWR-SP-4-ENABLED:power to module in slot 9 set on
00:05:53:%SNMP-5-MODULETRAP:Module 9 [Up] Trap
00:05:53:%DIAG-SP-6-BYPASS:Module 9:Online Diagnostics is Bypassed
00:05:53:%OIR-SP-6-INSCARD:Card inserted in slot 9, interfaces are now
online
Router#
```

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 as follows:

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

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

or

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

Note The **--install** keyword clears and recreates all of the NAM partitions; this action is similar to restoring the factory-default state. The **--install** keyword is only applicable to the WS-SVC-NAM-1 and WS-SVC-NAM-2 modules. If you use the **--install** keyword, the previously stored reports and 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 as follows:

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

Note 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 as follows:

```
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

namlab-sup3#sess slot 3 processor 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.31 ... Open

Cisco Maintenance image

login: root
Password:

Maintenance image version: 2.1(0.7)

root@namlab-kom3.cisco.com# upgrade ftp://namlab-pc1/pub/rmon/nam-app.3-3-0-15.bin.gz
Downloading the image. This may take several minutes...
ftp://namlab-pc1/pub/rmon/nam-app.3-3-0-15.bin.gz (58699K)
/tmp/upgrade.gz           [##########################]   58699K | 6499.18K/ss
60108348 bytes transferred in 9.03 sec (6499.05k/sec)

Upgrade file ftp://namlab-pc1/pub/rmon/nam-app.3-3-0-15.bin.gz is downloaded.
Upgrading will wipe out the contents on the storage media.
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.
This process may take several minutes...

Applying the image, this process may take several minutes...

Performing post install, please wait...
Application image upgrade complete. You can boot the image now.
root@namlab-kom3.cisco.com#

Console> (enable) reset 3
This command will reset module 3.
Unsaved configuration on module 3 will be lost
Do you want to continue (y/n) [n]? y
ResetPcBlade:start shutdown module 3
```

```
SendShutDownMsg - proc_id (1):shut down PC success.
Module 4 shut down in progress, please don't remove module until shutdown completed.
Console> (enable) 2004 May 07 23:19:03 %SYS-5-MOD_OK:Module 4 is online
```

Upgrading the NAM Maintenance Software with Cisco IOS Software

To upgrade the NAM maintenance software, follow these steps:

Step 1 Copy the NAM maintenance 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 application image, go to Step 5. If the NAM is not running in the application image, enter this command in the privileged mode:

```
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:%DIAG-SP-6-BYPASS:Module 9:Online Diagnostics is Bypassed
00:33:26:%OIR-SP-6-INSCARD:Card inserted in slot 9, interfaces are now
online
```

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 as follows:

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

where *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#
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#
```

Step 9 (Optional) Verify the initial configuration after the NAM comes back online by logging into the NAM root account as follows:

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

Step 10 (Optional) Reboot into the application image as follows:

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

This example shows how to upgrade the NAM maintenance software:

```
Router#
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:%DIAG-SP-6-BYPASS:Module 9:Online Diagnostics is Bypassed
00:33:26:%OIR-SP-6-INSCARD: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,  3.3(0.1)
Copyright (c) 2004 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)
02:27:39:SP:Resetting module 9 ...
02:27:39:%C6KPWR-SP-4-ENABLED:power to module in slot 9 set on
02:29:37:%SNMP-5-MODULETRAP:Module 9 [Up] Trap
02:29:37:%DIAG-SP-6-BYPASS:Module 9:Online Diagnostics is Bypassed
02:29:37:%OIR-SP-6-INSCARD:Card inserted in slot 9, interfaces are now
online
Router#
```

Configuring Mini-RMON with Cisco IOS Software

With Cisco IOS software, you must explicitly enable mini-RMON for each 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. You can also enable mini-RMON with the NAM Traffic Analyzer application using the **Setup** tab.

Note The NAM only displays mini-RMON collections that are 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

You can perform these administrative tasks on the NAM using the Catalyst operating system software:

- Logging in to the NAM with Catalyst Operating System Software, page 4-12
- Changing the NAM CLI Passwords with Catalyst Operating System Software, page 4-13
- Resetting the NAM with Catalyst Operating System Software, page 4-14
- Upgrading the NAM Software with Catalyst Operating System Software, page 4-16
- Configuring a Mini-RMON with Catalyst Operating System Software, page 4-20

You can administer the NAM by using NAM Traffic Analyzer. Refer to the *User Guide for the Network Analysis Module NAM Traffic Analyzer Release 3.3* for more information.

You can perform these administrative tasks on the NAM:

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

Table 4-3 describes the user administration tasks that you can perform using the CLI and NAM Traffic Analyzer.

Table 4-3 NAM User Administration

User Interface	Add Users	Remove Users	Set Password	Recover Password
CLI	No	No	Use the **password** command.	No
Traffic Analyzer	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.	Use the **no web-user** command or NAM Traffic Analyzer to remove users.		
Traffic Analyzer local database	Yes	Yes	Yes	Contact the NAM administrator to reset through the GUI. From the NAM CLI, use the **rmwebusers** command.
Traffic Analyzer TACACS+	Yes	Yes	Yes	Use a TACACS+ server, or use the **ip http tacacs+ disable** command.

Logging in to the NAM with Catalyst Operating System Software

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

Table 4-4 NAM Users and Passwords

Application Image (located on the hard disk)		Maintenance Image (located on the compact flash)	
User	**Password**	**User**	**Password**
root	root	root	cisco
guest	guest	guest	cisco

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. 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 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** 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,  3.3(0.1)
Copyright (c) 2004 by Cisco Systems, Inc.
WARNING! Default password has not been changed!

root@localhost#
```

Changing the NAM CLI Passwords with Catalyst Operating System Software

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 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.

Note 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 4-4 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.

Note 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 as follows:

```
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 as follows:

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

Step 3 Enter the new password again as follows:

```
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 password** command from the CLI to restore the password for the root account to root and the guest account to guest.

Resetting the NAM with Catalyst Operating System Software

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.

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

For Cisco IOS software, see the "Resetting the NAM with Cisco IOS Software" 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) 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.

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

Software Image	Task	Command
Maintenance Image	Reset the module.	**hw-module module** *mod_num* **reset device:***partition* [**mem-test-full**] The device:*partition* value is the string for the PC boot device; for example, **hdd:1** designates the hard disk and **cf:1** designates the compact Flash where **x** is the number for the partition on each device.
Application Image	Reset the module.	**hw-module module** *mod_num* **reset device:***partition* [**mem-test-full**] The device:*partition* value is the string for the PC boot device; for example, **hdd:1** designates the hard disk and **cf:1** designates the compact Flash where **x** is the number for the partition on each device.

This example shows how to reset the NAM that is 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 ...
```

This example shows how to reset the module to the maintenance image from the enable mode:

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

This example shows how to reset the module to the NAM application image from the enable mode:

```
Console> (enable) reset mod_num
```

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 comple
ted.
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:

```
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 runs. A full memory test takes more time to complete than a partial memory test.

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
```

Upgrading the NAM Software with Catalyst Operating System Software

You can upgrade both the application software and the maintenance software. To upgrade the application software, see the "Upgrading the NAM Application Software with Catalyst Operating System Software" section on page 4-17. To upgrade the maintenance software, see the "Upgrading the NAM Maintenance Software with Catalyst Operating System Software" section on page 4-18.

Upgrading the NAM Application Software with Catalyst Operating System 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 into the switch through the console port or through a Telnet session.

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:

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

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 application software by entering as follows:

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

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

or

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

Note The **--install** keyword clears and recreates all of the NAM partitions. This action is similar to restoring the factory-default state.

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 maintenance image.

Step 8 Reset to the NAM application image as follows:

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

Step 9 (Optional) Verify the initial configuration after the NAM comes back online by logging into the NAM root account as follows:

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

This example shows how to upgrade the NAM application software:

```
Console> (enable) reset 3 cf:1
This command will reset module 3.
Unsaved configuration on module 3 will be lost
Do you want to continue (y/n) [n]? y
ResetPcBlade:start shutdown module 3
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

namlab-sup2# session 3
The default escape character is Ctrl-^, then x.
```

```
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.31 ... Open

Cisco Maintenance image

login: root
Password:

Maintenance image version: 2.1(0.7)

root@namlab-kom2.cisco.com# upgrade ftp://namlab-pc1/pub/rmon/nam-app.3-3-0-15.bin.gz
Downloading the image. This may take several minutes...
ftp://namlab-pc1/pub/rmon/nam-app.3-3-0-15.bin.gz (58699K)
/tmp/upgrade.gz           [########################]   58699K | 6499.18K/ss
60108348 bytes transferred in 9.03 sec (6499.05k/sec)

Upgrade file ftp://namlab-pc1/pub/rmon/nam-app.3-3-0-15.bin.gz is downloaded.
Upgrading will wipe out the contents on the storage media.
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.
This process may take several minutes...

Applying the image, this process may take several minutes...

Performing post install, please wait...
Application image upgrade complete. You can boot the image now.
root@namlab-kom3.cisco.com#

Console> (enable) reset 3
This command will reset module 3.
Unsaved configuration on module 3 will be lost
Do you want to continue (y/n) [n]? y
ResetPcBlade:start shutdown module 3
SendShutDownMsg - proc_id (1):shut down PC success.
Module 4 shut down in progress, please don't remove module until shutdown completed.
Console> (enable) 2004 May 07 23:19:03 %SYS-5-MOD_OK:Module 4 is online
```

Upgrading the NAM Maintenance Software with Catalyst Operating System 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 as follows:

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

where *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 to reset the NAM maintenance software as follows:

```
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 as follows:

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

Step 10 (Optional) Reboot into the application image as follows:

```
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,  3.3(0.1)
Copyright (c) 2004 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.
```

Configuring a Mini-RMON with Catalyst Operating System Software

With Catalyst operating system software, you can enable mini-RMON.

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 on 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 as follows:

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

For Catalyst operating system software, enter as follows:

```
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 as follows:

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

where *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 as follows:

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

Note If the 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 3
This command will reset module 3.
Unsaved configuration on module 3 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 3 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 3 is online

namlab-sup2# session slot 3 processor 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.31 ... Open

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

login: root
Password:
Terminal type: vt100

Cisco Network Analysis Module (WS-SVC-NAM-1) Console, 3.3(0.15)
Copyright (c) 1999-2004 by cisco Systems, Inc.

WARNING! Default password has not been changed!
root@namlab-kom3.cisco.com# patch
ftp://guest@namlab-pc1/home/guest/patch_rpms/nam-app.3-3.cryptoK9.patch.1-0.bin

Proceeding with installation. Please do not interrupt.
If installation is interrupted, please try again.

Downloading nam-app.3-3.cryptoK9.patch.1-0.bin. Please wait...
Password for guest@namlab-pc1:
ftp://guest@namlab-pc1/home/guest/patch_rpms/nam-app.3-3.cryptoK9.patch.1-0.bin (1K)
-                          [##########################]       1K |  114.28K/s
1891 bytes transferred in 0.02 sec (112.09k/sec)

Verifying nam-app.3-3.cryptoK9.patch.1-0.bin. Please wait...
Patch nam-app.3-3.cryptoK9.patch.1-0.bin verified.

Applying /usr/local/nam/patch/workdir/nam-app.3-3.cryptoK9.patch.1-0.bin. Please wait...
########################################### [100%]
########################################### [100%]
```

Additional NAM Software Administrative Commands

Refer to the following document for information about NAM commands available through the NAM CLI.

- *Catalyst 6500 Series and Cisco 7600 Series Network Analysis Module Command Reference*

Using the NAM Graphical User Interface

The Cisco NAM Traffic Analyzer supports browser-based access to the NAM graphical user interface (GUI). To access the NAM GUI, enter a machine and domain name or an IP address in your browser address fieldas in the following:

http://your_machine.cisco.com

The NAM GUI prompts you for your user name and password. After you enter your user name and password, click **Login** to access the NAM GUI.

CHAPTER 5

Troubleshooting the Network Analysis Module

This chapter describes how to troubleshoot the NAM and includes these sections:

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, when the end of a connection is detected, or when the expiration time has been 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. 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 Software

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 Software

For the PFC, use the following commands to specify the aging time:

```
Console(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 do not exceed the packet threshold, use the **fast** keyword.

To set the aging time for IP flows, use the **ip** keyword.

Explanation The Monitor > Hosts and Monitor > Conversations page does not contain the 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 the filter long duration aging time or dropped flow packets as follows:

Verify the long duration aging time with these commands:

```
Console(enable) show ip cache flow
```

or

```
Console(enable) show mls netflow aging
```

or

```
Console(enable) show mls
```

Active flows that have their active time below the long duration aging time are not expired yet, and they have not been exported to the NAM. You can set the aging time to a lower value. Refer to the NDE usage guidelines for the device.

Verify the dropped flow packets with these commands:

```
Console(enable) show ip cache flow
```

or

```
Console(enable) show mls netflow aging
```

or

```
Console(enable) show mls
```

Flows could drop because they are not entered into the caches allowing their export to the NAM when they are expired. The NetFlow cache might be full because of busy networks. To correct the problem, you could increase the cache size, or adjust NDE export with the 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 **Start**. 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:

```
Console> show ip flow export
```

or

```
Console> 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 3.3*.

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 a NetFlow record that contains contains nformation about the specified interfaces does not exist. To find out which interfaces the NetFlow records have, follow these steps:

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:

```
Console(config) interface type slot/port
Console(config-if) ip route cache flow
```

For the MLS cache, use these commands for Cisco IOS software:

```
Console(config)# mls nde interface
```

For the MLS cache, use these commands for the Catalyst operating system software:

```
Console>(enable) set mls nde destination-ifindex enable
```

or

```
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 the *Network Analysis Module Traffic Analyzer Release 3.3*.

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.

To make sure that the community string is correct, follow these steps:

Step 1 Go to the Setup > Data Sources > NetFlow > Devices menu.

Step 2 Click on the radio button of the device to display information about the interfaces.

Step 3 Click **Test**.

A popup window appears displaying the status of the device. If there is an 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 The Monitor > Conversations page has the source column as 0.0.0.0 for all entries. This problem occurs when the NDE device flow mask is set to destination.

Cisco IOS Software

If using Cisco IOS software to set the flow mask to full, interface-destination-source, or interface-full, enter this command:

```
Router(config)# mls flow ip "full"|"interface-destination-source"|"interface-full"
```

Catalyst Operating System Software

If using Catalyst operating system software to set the flow mask to full, interface-destination-source, or interface-full, enter this command:

```
Console(enable)# set mls flow "destination-source" | "full"
```

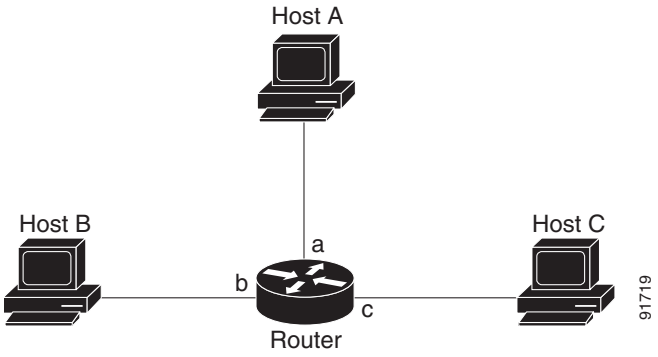
Note The NAM supports NDE versions 1, 5, 6, 7, 8, source-prefix, destination-prefix, prefix, and protocol-port aggregations.

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 an unsupported NDE feature of the Cisco IOS or Catalyst operating system version or misconfiguration of the NDE flow masks.

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.

Figure 5-1 NDE Configuration



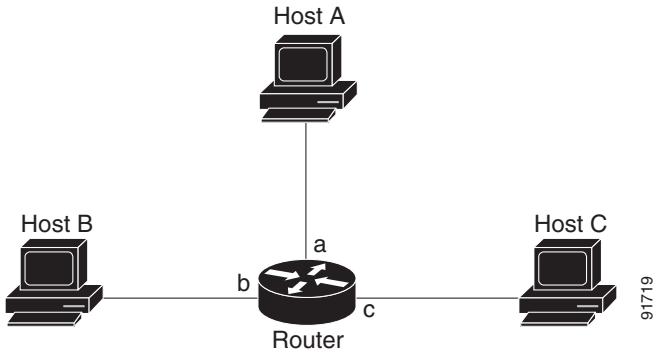
The configuration is as follows:

```
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

Input Interface	Output Interface	Are Flows Reported?
a	b	Yes
a	c	Yes
b	c	No
b	a	No
c	a	No
c	b	No

Figure 5-2 NDE Configuration




```
Router# configuration terminal
Router(config)# interface a
Router(config-if)# ip route cache flow
Router(config-if)# exit
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

From	To	Are Flows Reported?
a	b	Yes
a	c	Yes
b	c	Yes
b	a	Yes
c	a	No
c	b	No

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 as 0. This problem 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 that terminate at the device, check the device configuration, and make sure that there are no unsupported features on this platform at the device.

NDE Flow Mask and Version 8 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 the effects on the data collection screens. Due to a lack of information, some collections may display "Others" only in the Monitor > Apps, 0.0.0.0 in Monitor > Hosts and Monitor > Conversation pages.

Table 5-3 Effects on Data Collection Screens

Flow	Effect
Full flow-mask is supported	Highly recommended. Refer to the NDE usage guidelines for the device to apply full flow masks. **Note** Although the NAM supports NDE aggregation, the information that you received 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.
Destination only flow-mask	• Monitor > Apps displays "Others" only. • Monitor > Apps detail popup window has no data. • Monitor > Hosts has 0.0.0.0. Detail popup window has no data. • Monitor > Conversations has 0.0.0.0 to some hosts. Detail popup window has no data. • Support NetFlow custom data sources that are set up for specific interfaces.
Destination-Source flow-mask	• Monitor > Apps displays "Others" only. • Monitor > Apps detail popup window has no data. • Monitor > Hosts has data. Detail popup window has no data. • Monitor > Conversations has data. Detail popup window has no data. • Support NetFlow custom data sources that are set up for specific interfaces.

Table 5-3 Effects on Data Collection Screens (continued)

Flow	Effect
NDE version 8-Protocol-Port-Aggregation	• Monitor > Apps displays data. • Monitor > Apps detail popup window displays only 0.0.0.0. • Monitor > Host displays only 0.0.0.0. • Monitor > Conversation displays only 0.0.0.0 to 0.0.0.0. • No data for custom NetFlow data sources that are set up for some specific interfaces. • No DiffServ other than ToS 0 and DSCP 0. • Setup > Data Sources > NetFlow Listening Mode detail popup window does not display interfaces information.
NDE version 8-Destination-Prefix-Aggregation	• Monitor > Apps displays only “Others.” • Monitor > Host displays data with subnets as well as 0.0.0.0. The detail popup window displays no data. • Monitor > Conversation displays data with 0.0.0.0 to subnets (as well as 0.0.0.0 to 0.0.0.0). Detail popup window 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-Prefix-Aggregation	• Monitor > Apps displays “Others” only. • Monitor > Host displays data as subnets (as well as 0.0.0.0). The detail popup window displays no data. • Monitor > Conversation displays data (as well as 0.0.0.0 to 0.0.0.0). Detail popup window 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-Source-Prefix-Aggregation	• Monitor > Apps displays “Others” only. • Monitor > Host displays data with subnets (as well as 0.0.0.0). The detail popup window 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 window 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.

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 engine as cf:1, typing a **reset** *module* command always boots to the maintenance image.

Recommended Action Override the configured boot device in the supervisor engine 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**.**

Symptom You receive a verification failed message when installing a patch on the NAM.

Possible Cause The cause could be that 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 from a previous release of the 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 Make sure that the signature verification is used to ensure that the patch is an authentic Cisco patch and 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 3.3 software. Make sure that the date and time on the NAM is set to synchronize with the switch or with the Network Time Protocol (NTP). Make sure that the URL location is valid for the patch (verify the username)

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 4-4 on page 4-12.

Symptom When attempting to load the new NAM 3.3 image on the NAM, the following message displays:

```
Incompatible image! Upgrade aborted.
```

Possible Cause This image is not supported on the specified NAM. Two NAM 3.3 images are available: One each for the WS-SVC-NAM-1 and WS-SVC-NAM-2. This symptom occurs only if an incompatible image is used.

Recommended Action The newer NAM shares a common format and the same image filename for upgrades can be used.

Symptom When attempting to load the wrong image on a WS-SVC-NAM-1 or WS-SVC-NAM-2, the following message displays:

```
ERROR: /tmp/upgrade:No space left on device
```

Possible Cause This image is not supported on the specified NAM. Two NAM 3.3 images are available: One each for the WS-SVC-NAM-1 and WS-SVC-NAM-2. This symptom occurs only if an incompatible image is used.

Recommended Action The application and maintenance file image formats are different between the previous NAM releases 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 the 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 software and is not available in Catalyst operating system software. (See the "Resetting the NAM with Catalyst Operating System Software" section on page 4-14.)

You can also use the **hw-module module** *module_number* **mem-test-full** command as follows:

```
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. This example shows how to enable 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) 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 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 multiplied by 10 plus 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 3-13.

Symptom The NAM fails to upgrade.

Possible Cause The URL to the server or the image name is incorrect.

Recommended Action Make sure that the URL you specified is valid. Make sure that 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 3-13.

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, or the wrong TACACS+ server IP address is configured in the NAM.

Recommended Action To determine the cause of the problem, 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 authentication and authorization for the 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 the 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.)

Symptom When importing a configuration using the **configure network** command, the configuration file download succeeds, but the import operation fails and displays an error.

Possible Cause The configuration file is not correct.

Recommended Action Use the **show log config** command to determine where the configuration failed. You could either ignore or correct the configuration file and enter the **config network** command again.

Symptom When upgrading an application image from a NAM-1 or a NAM-2 to a maintenance image, this message displays:

```
Image verification failed.
```

Possible Cause The image that 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 the NAM-1 or the NAM-2. Do not use the WS-X6380-NAM maintenance image.

Symptom When upgrading from a WS-X6380-NAM application image, this message displays:

```
Incompatible image! Upgrade aborted.
```

Possible Cause The WS-X6380-NAM image cannot be used on the NAM-1 or NAM-2.

Recommended Action You need to use the correct maintenance image for the WS-X6380-NAM. Do not use the NAM-1 or NAM-2 maintenance image.

Symptom When upgrading the WS-X6380-NAM maintenance image, this message displays:

```
restore operation failed.
```

Possible Cause There was a problem with the upgrade process.

Recommended Action Load the WS-X6380-NAM application image to correct this problem.

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 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 NAM Traffic Analyzer 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 passwords, follow these steps:

Step 1 Access the NAM CLI.

Step 2 Enter these commands:

```
web-user
user name name
exit
```

Step 3 At the prompt, enter the new password.

Step 4 Enter **Y** to confirm the new password.

When the NAM TACACS+ setting is misconfigured and a local database user account is not available to fix this problem from the web interface, you may be able to fix the TACACS+ configuration by using the CLI interface.

To recover the passwords, follow these steps:

Step 1 Access the NAM CLI.

Step 2 Enter this command:

```
ip http tacacs+ enable tacacs+ server
```

Step 3 Follow the commands to enter the TACACS+ secret key.

Supported MIB Objects

Table 5-4 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 5-4. 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 5-4 Supervisor Engine Module and NAM RMON Support

Module	Object Identifier (OID) and Description	Source
Supervisor Engine	...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)	RFC 2819 (RMON-MIB) RFC 1513 (TOKEN-RING-RMON MIB) RFC 1513 (TOKEN-RING-RMON MIB)
	Counters for packets, octets, broadcasts, errors, etc.	
Supervisor Engine	...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)	RFC 2819 (RMON-MIB) RFC 2819 (RMON-MIB) RFC 1513 (TOKEN-RING-RMON MIB) RFC 1513 (TOKEN-RING-RMON MIB)
	Periodically samples and saves statistics group counters for later retrieval.	
Supervisor Engine	...mib-2(1).rmon(16).alarm(3)	RFC 2819 (RMON-MIB)
	A threshold that can be set on critical RMON variables for network management.	
Network Analysis	...mib-2(1).rmon(16).alarm(3)	RFC 2819 (RMON-MIB)
	A threshold that can be set on critical RMON variables for network management.	
Network Analysis	...mib-2(1).rmon(16).hosts(4)	RFC 2819 (RMON-MIB)
	Maintains statistics on each host device on the segment or port.	
Network Analysis	...mib-2(1).rmon(16).hostTopN(5)	RFC 2819 (RMON-MIB)
	A user-defined subset report of the Hosts group, sorted by a statistical counter.	
Network Analysis	...mib-2(1).rmon(16).statistics(1).etherStatsTable(1)	RFC 2819 (RMON-MIB)
Network Analysis	...mib-2(1).rmon(16).matrix(6)	RFC 2819 (RMON-MIB)
	Maintains conversation statistics between hosts on a network.	
Network Analysis	...mib-2(1).rmon(16).filter(7)	RFC 2819 (RMON-MIB)
	A filter engine that generates a packet stream from frames that match a specified pattern.	
Network Analysis	...mib-2(1).rmon(16).capture(8)	RFC 2819 (RMON-MIB)
	Manages buffers for packets captured by the Filter group for uploading to the management console.	

Table 5-4 Supervisor Engine Module and NAM RMON Support (continued)

Module	Object Identifier (OID) and Description	Source
Supervisor Engine	...mib-2(1).rmon(16).event(9)	RFC 2819 (RMON-MIB)
	Generates SNMP traps when an Alarms group threshold is exceeded and logs the events.	
Network Analysis	...mib-2(1).rmon(16).event(9)	RFC 2819 (RMON-MIB)
	Generates SNMP traps when an Alarms group threshold is exceeded and logs the events.	
Supervisor Engine	...mib-2(1).rmon(16).tokenRing(10).ringStationControlTable(1) ...mib-2(1).rmon(16).tokenRing(10).ringStationTable(2) ...mib-2(1).rmon(16).tokenRing(10).ringStationOrderTable(3) ...mib-2(1).rmon(16).tokenRing(10).ringStationConfigControlTable(4) ...mib-2(1).rmon(16).tokenRing(10).ringStationConfigTable(5) ...mib-2(1).rmon(16).tokenRing(10).sourceRoutingStatsTable(6)	RFC 1513 (TOKEN-RING-RMON MIB) RFC 1513 (TOKEN-RING-RMON MIB) RFC 1513 (TOKEN-RING-RMON MIB) RFC 1513 (TOKEN-RING-RMON MIB) RFC 1513 (TOKEN-RING-RMON MIB) RFC 1513 (TOKEN-RING-RMON MIB)
	Aggregates detailed Token Ring statistics.	
Network Analysis	...mib-2(1).rmon(16).protocolDir(11)	RFC 2021 (RMON2-MIB)
	A table of protocols for which the Network Analysis Module monitors and maintains statistics.	
Network Analysis	...mib-2(1).rmon(16).protocolDist(12)	RFC 2021 (RMON2-MIB)
	A table of statistics for each protocol in protocolDir(11).	
Network Analysis	...mib-2(1).rmon(16).addressMap(13)	RFC 2021 (RMON2-MIB)
	List of MAC-to-network-layer address bindings.	
Network Analysis	...mib-2(1).rmon(16).nlHost(14)	RFC 2021 (RMON2-MIB)
	Statistics for each network layer address.	
Network Analysis	...mib-2(1).rmon(16).nlMatrix(15)	RFC 2021 (RMON2-MIB)
	Traffic statistics for pairs of network layer addresses.	
Network Analysis	...mib-2(1).rmon(16).alHost(16)	RFC 2021 (RMON2-MIB)
	Statistics by application layer protocol for each network address.	
Network Analysis	...mib-2(1).rmon(16).alMatrix(17)	RFC 2021 (RMON2-MIB)
	Traffic statistics by application layer protocol for pairs of network layer addresses.	
Network Analysis	...mib-2(1).rmon(16).usrHistory(18)	RFC 2021 (RMON2-MIB)
	Extends history beyond RMON1 link-layer statistics to include any RMON, RMON2, MIB-I, or MIB-II statistic.	
Supervisor Engine	...mib-2(1).rmon(16).probeConfig(19).	RFC 2021 (RMON2-MIB)
	Displays a list of agent capabilities and configurations.	

Table 5-4 Supervisor Engine Module and NAM RMON Support (continued)

Module	Object Identifier (OID) and Description	Source
Network Analysis	...mib-2(1).rmon(16).switchRMON(22).smonMIBObjects(1). dataSourceCaps(1).dataSourceCapsTable(1).	RFC 2613 (SMON-MIB)
	Maps physical entities and VLANs to ifEntries.	
Network Analysis	...mib-2(1).rmon(16).switchRMON(22).smonMIBObjects(1). smonStats(2).smonVlanStatsControlTable(1).	RFC 2613 (SMON-MIB)
	Traffic statistics by VLAN ID number.	
Network Analysis	...mib-2(1).rmon(16).switchRMON(22).smonMIBObjects(1). smonStats(2).smonPrioStatsControlTable(3).	RFC 2613 (SMON-MIB)
	Traffic statistics by 802.1p user priority value.	
Network Analysis	...frontier(141).mibdoc2(2).netscout2(1).art(5).artControlTable(2).	draft-warth-rmon2-artmib-01.txt (ART-MIB)
	Application response time statistics.	
Network Analysis	...mib-2(1).rmon(16).mediaIndependentStats(21).	RFC 3273 (HC-RMON-MIB)
	Counters for packets, octets, broadcasts, errors, etc.	
	rmon.dsmonMib(26).dsmonObjects(1).dsmonAggObjects(1). dsmonMaxAggGroups(1) rmon.dsmonMib(26).dsmonObjects(1).dsmonAggObjects(1). dsmonAggControlLocked(2) rmon.dsmonMib(26).dsmonObjects(1).dsmonAggObjects(1). dsmonAggControlChanges(3) rmon.dsmonMib(26).dsmonObjects(1).dsmonAggObjects(1). .dsmonAggControlLastChangeTime(4) rmon.dsmonMib(26).dsmonObjects(1).dsmonAggObjects(1). dsmonAggControlTable(5) rmon.dsmonMib(26).dsmonObjects(1).dsmonAggObjects(1). dsmonAggProfileTable(6) rmon.dsmonMib(26).dsmonObjects(1).dsmonAggObjects(1). .dsmonAggGroupTable(7)	RFC 3287 (DSMON-MIB)
	Aggregation or profile control variables and tables	
	rmon.dsmonMib(26).dsmonObjects(1).dsmonStatsObjects(2). dsmonStatsControlTable(1) rmon.dsmonMib(26).dsmonObjects(1).dsmonStatsObjects(2). dsmonStatsTable(2)	RFC 3287 (DSMON-MIB)
	Per-datasource statistics collection tables	

Table 5-4 Supervisor Engine Module and NAM RMON Support (continued)

Module	Object Identifier (OID) and Description	Source
	rmon.dsmonMib(26).dsmonObjects(1).dsmonPdistObjects(3). dsmonPdistCtlTable(1) rmon.dsmonMib(26).dsmonObjects(1).dsmonPdistObjects(3). dsmonPdistStatsTable(2) rmon.dsmonMib(26).dsmonObjects(1).dsmonPdistObjects(3). dsmonPdistTopNCtlTable(3) rmon.dsmonMib(26).dsmonObjects(1).dsmonPdistObjects(3). dsmonPdistTopNTable(4)	RFC 3287 (DSMON-MIB)
	Per-protocol statistics collection tables	
	rmon.dsmonMib(26).dsmonObjects(1).dsmonHostObjects(4). dsmonHostCtlTable(1) rmon.dsmonMib(26).dsmonObjects(1).dsmonHostObjects(4). dsmonHostTable(2) rmon.dsmonMib(26).dsmonObjects(1).dsmonHostObjects(4). dsmonHostTopNCtlTable(3) rmon.dsmonMib(26).dsmonObjects(1).dsmonHostObjects(4). dsmonHostTopNTable(4)	RFC 3287 (DSMON-MIB)
	Per-host statistics collection tables	
	rmon.dsmonMib(26).dsmonObjects(1).dsmonCapsObjects(5). dsmonCapabilities(1)	RFC 3287 (DSMON-MIB)
	DSMON capabilities variable	
	rmon.dsmonMib(26).dsmonObjects(1).dsmonMatrixObjects(6). dsmonMatrixCtlTable(1) rmon.dsmonMib(26).dsmonObjects(1).dsmonMatrixObjects(6). dsmonMatrixSDTable(2) rmon.dsmonMib(26).dsmonObjects(1).dsmonMatrixObjects(6). dsmonMatrixDSTable(3) rmon.dsmonMib(26).dsmonObjects(1).dsmonMatrixObjects(6). dsmonMatrixTopNCtlTable(4) rmon.dsmonMib(26).dsmonObjects(1).dsmonMatrixObjects(6). dsmonMatrixTopNTable(5)	RFC 3287 (DSMON-MIB)
	Matrix statistics collection tables	

Local Interfaces in the NAM ifTable

This section explains the differences between the newer NAM-1 and NAM-2 and the previous version of the WS-X6380-NAM. The three versions of the Network Analysis Module (NAM) are as follows:

- WS-X6380-NAM
- WS-SVC-NAM-1
- WS-SVC-NAM-2

The WS-X6380-NAM appears in the supervisor engine CLI and ifTable as two ports. The first port, the data port, is 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 appears in the supervisor engine 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 engine CLI (in Cisco IOS software) parses the ports to ("analysis module . . ."). On the NAM's ifTable, the management port appears as the first port (ifIndex.1) and the data port appears as the second (ifIndex.2).

The WS-SVC-NAM-2 appears in the supervisor engine 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 engine CLI (in the Cisco IOS software) parses the ports to ("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")
- fIndex.4: Represents the traffic from the second data port (named "data port 2")

Note For the WS-SVC-NAM-1 and WS-SVC-NAM-2, the data ports are IEEE 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, the filters on the IP headers) in the packets.

Table 5-5 lists the local interface designations for the NAM.

Table 5-5 NAM Local Interface Designations

	WS-X6380-NAM	WS-SVC-NAM-1	WS-SVC-NAM-2
SNMP OID	cisco.5.1. 3. 3.3.2.223	cisco.5.1. 3. 3.3.2.914	cisco.5.1. 3. 3.3.2.291
Supervisor engine number of ports	2	3	8
Supervisor engine management port	2	2	2
Supervisor engine data ports	1	3	7,8
NAM management port	ifIndex.2	ifIndex.1	ifIndex.1
NAM data port	ifIndex.1	ifIndex.2	ifIndex.2, ifIndex.3, ifIndex.4

INDEX

O

P

R

S

T

U

V

W