Quick Start Guide

Cisco 2600, 2600XM, 2800, 3660, 3700, and 3800 Series Network Analysis Module

1 Network Analysis Module Overview

The Network Analysis Module (NM-NAM) is a network module installed in select models of Cisco 2600, 2600XM, 2800, 3660, 3700, and 3800 Series routers, that monitors and analyzes network traffic. (See Table 2 for a list of supported routers.)

The NAM Traffic Analyzer is software embedded in the NAM that gives you browser-based access to the monitoring features of the NAM. You use this software to troubleshoot and monitor network availability and health. In this document you will find:

- Package contents, including links for accessing online documentation.
- Hardware and software requirements.
- Installation and configuration procedures for getting the NAM and Traffic Analyzer running.
- Pointers to additional documentation that provides detailed procedures for installing and using the product.
- Information about ordering documentation and contacting Cisco Systems for additional assistance.

Package Contents

- NM-NAM module.
- *Cisco Network Modules Quick Start Guide.*

Note Only available for spare NM-NAM orders.

- *Cisco Network Modules and Interface Cards Regulatory Compliance and Safety Information.*
- *Copyright Notices for the Network Analysis Module Release 3.4.*

2 Software and Hardware System Requirements

This section provides NAM Traffic Analyzer software and hardware requirements:

- Table 1 describes the software requirements for installing and using the NAM Traffic Analyzer.
- Table 2 describes the hardware requirements for installing and using the NAM Traffic Analyzer.
- Table 3 describes the browser requirements for all platforms.

Table 1 Software Requirements

Module	Application Image	Cisco IOS Software
NM-NAM	3.4 or later (pre-installed)	Release 12.3(4)XD or later. Release 12.3(7)T or later.

Table 2 Hardware Requirements

Module	Cisco Hardware
NM-NAM	Network module slot in one of the following supported routers: • Cisco 262xXM • Cisco 265xXM • Cisco 2691 Multiservice Platform • Cisco 2811 Integrated Services Router • Cisco 2821 Integrated Services Router • Cisco 2851 Integrated Services Router • Cisco 3660 Multiservice Platform • Cisco 3725 Multiservice Access Router • Cisco 3745 Multiservice Access Router • Cisco 3825 Integrated Services Router • Cisco 3845 Integrated Services Router

Table 3 Browser Requirements

Browser	Version	Platform	Java Plug-In Support[1]
Internet Explorer (recommended)	6.0 and later.	Windows 2000.	1.3.1_03 1.4.1_02
Netscape Navigator	7.0 and 7.1.	Windows 2000 and Solaris.	1.4.1_02 (Windows 2000) 1.4.0_01 (Solaris)

1. Although Traffic Analyzer does not require a Java plug-in, one might be required to use the Java Virtual Machine (JVM). The Java plug-in versions listed have been tested for browsers that require a plug-in for the JVM.

3 Installing the NAM

For information on physically installing the NAM into the router, see the *Cisco Network Modules Quick Start Guide* and the "Connecting Cisco Network Analysis Modules" chapter of *Cisco Network Modules Hardware Installation Guide*.

http://cco/univercd/cc/td/doc/product/access/acs_mod/cis2600/hw_inst/nm_inst/nm-doc/index.htm

4 Setting Up the NAM

The NAM has three interfaces for communication (Figure 1):

- Analysis-Module Interface—Associated with the router.
- Internal NAM Interface—Associated with the NAM.
- External NAM Interface—Associated with the NAM.

This document shows you how to configure the Analysis-Module interface and internal NAM interface for managing and monitoring traffic. Alternatively, you can use the external NAM interface for managing and monitoring. However, this document does not cover that configuration. For more information on using the external NAM interface, see the *Network Analysis Module (NM-NAM)* feature module or the *User Guide for the Network Analysis Module Traffic Analyzer Release 3.4*.

Figure 1 NAM Network Interfaces

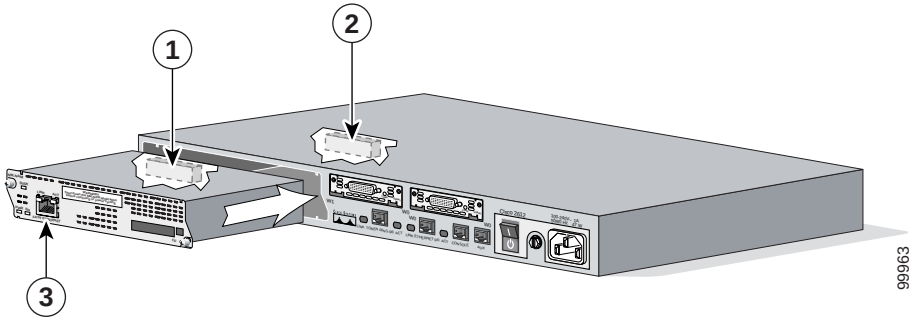

Table 4 NAM Network Interfaces

Figure 1 Callout	Interface	Interface type	Location	Configure and manage from
1	Internal NAM interface	FastEthernet	NM-NAM internal	NAM CLI
2	Analysis-Module interface	FastEthernet	Router internal	Cisco IOS CLI
3	External NAM interface	FastEthernet	NM-NAM faceplate	NAM CLI

Note The NM-NAM does not have an external console port. To access the NAM console, open a NAM console session from the router or use Telnet or SSH over the network. The lack of an external console port on the NM-NAM means that the initial boot configuration is possible only through the router.

After you install the NAM, you must do the following to begin using the Traffic Analyzer application:

- Configuring the Analysis-Module Interface on the Router, page 6
- Enabling Packet Monitoring, page 7
- Accessing the NAM CLI, page 8
- Configuring the NAM Management Network Parameters, page 9

Configuring the Analysis-Module Interface on the Router

To configure the Analysis-Module interface on the router CLI:

Step 1 Enter the interface configuration mode for the NAM.

```
Router(config)# interface analysis-module slot/port
```

Step 2 Assign an IP address by using the ip unnumbered command or by configuring a routable IP address and subnet mask on the internal interface.

a. If you use the ip unnumbered command:

```
Router (config-if)# ip unnumbered FastEthernet slot/port
```

b. If you use a routable IP address and subnet mask:

```
Router (config-if)# ip address 172.18.12.2 255.255.255.0
```

Note For the ip unnumbered command, make sure that a static route is configured on the router CLI for the NAM IP address that you configure through the NAM CLI in Step 2 of the "Configuring the NAM Management Network Parameters" section on page 9.

Note The following is a sample configuration: ip route <nam-ip-address> 255.255.255.255 Analysis-Module slot/0

Note On the NAM, the IP address must belong to the subnet of the parent interface for the Analysis-Module slot/0 (such as fa0/0). The NAM default gateway should be the parent interface IP.

Note For a detailed explanation, see: *Configuring a Static Route to the NAM Through the Analysis-Module Interface* at: http://www.cisco.com/en/US/products/sw/iosswrel/ps5413/products_feature_guide09186a00801d6096.html#wp1046001

Step 3 Activate the NAM interface.

```
Router (config-if)# no shutdown
```

Enabling Packet Monitoring

When you use the internal NAM interface for monitoring traffic, you must enable NAM packet monitoring on each router interface that you want to monitor. NAM packet monitoring uses Cisco Express Forwarding (CEF) to send a copy of each packet that is received in or sent out of the router interface to the NAM.

Step 1 Enable the CEF switching path.

```
Router(config)# ip cef
```

Step 2 Select an interface to configure.

```
Router (config)# interface type slot|wic-slot|port
```

Step 3 Enable NAM packet monitoring on the router interface.

```
Router (config-if)# analysis-module monitoring
```

Step 4 Repeat Step 2 and Step 3 for each interface the NAM should monitor.

Accessing the NAM CLI

The NM-NAM does not have an external console port. Console access to the NAM is established when you enter service-module analysis-Module *slot*/0 session in privileged EXEC mode on the router. The lack of an external console port on the NM-NAM means that the initial boot configuration can only be made through the router.

Step 1 Establish a console session with the NAM.

```
Router# service-module analysis-module slot/0 session
```

Note If the Connection refused by remote host message is displayed, you must clear the existing session.

```
Router# service-module analysis-module slot/0 session clear
```

Step 2 At the login prompt, enter root to log in to the root account.

Step 3 If you have not changed the password from the factory-set default, enter root as the root password.

Step 4 Perform the required tasks in the NAM CLI. For information on NAM CLI tasks, see the "Configuring the NAM Management Network Parameters" section on page 9. When you want to end the NAM console session and return to the Cisco IOS CLI, enter exit.

Note If you are in a subcommand mode, continue to enter the exit command until you see the NAM login prompt.

Step 5 Hold CTRL-Shift and press 6. Release all keys, then press x to suspend and close the Telnet session.

Step 6 Enter disconnect to disconnect the line.

Note For 12.3(11)T or later, use the command disconnect <*session_id*> to disconnect the line.

Configuring the NAM Management Network Parameters

When you configure the internal NAM interface as the management interface, the IP address must be in the same subnet as the IP address of the Analysis-Module interface configured on the router CLI.

Step 1 Specify the internal NAM interface for handling management traffic.

```
root@localhost# ip interface internal
```

Step 2 Configure the NAM system IP address and subnet mask.

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

Step 3 Configure the NAM system broadcast address.

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

Note This step is optional.

Step 4 Configure the NAM system default gateway address.

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

Step 5 Set the NAM system domain name.

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

Step 6 Set the NAM system host name.

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

Step 7 Set one or more NAM system name servers.

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

Note This step is optional but highly recommended. Unexpected delays can occur if a name server is not set.

Step 8 Optionally check the connectivity to the device by pinging an external host or address.

```
root@localhost# ping host
or
root@localhost# ping ip-address
```

Step 9 Verify that the device is properly configured.

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

Step 10 Enable the NAM Traffic Analyzer application.

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

Step 11 Enter a web username and password.

Step 12 To access Traffic Analyzer, open a web browser and enter the NAM system IP address as the URL.

5 Where to Go Next

After you install the module and perform the necessary post-installation tasks, you are ready to use Traffic Analyzer. For more information, see the following documentation:

- *User Guide for the Network Analysis Module Traffic Analyzer Release 3.4*

  You can access this document:

- In HTML and PDF on Cisco.com:
  a. Log into Cisco.com.
  b. Select Products & Services > Network Management CiscoWorks > Cisco Network Analysis Module Software > Technical Documentation.
  c. Select the appropriate document type from the list, then the document written for this release.
- From the Traffic Analyzer online help.
- *Network Analysis Module Command Reference Release 3.4*

You can access this document in HTML and PDF on Cisco.com:

1. Log into Cisco.com.
2. Select Products & Services >Network Management CiscoWorks > Cisco Network Analysis Module Software > Technical Documentation.
3. Select the appropriate document type from the list, then the document written for this release.

6 Related Documentation

Note Although every effort has been made to validate the accuracy of the information in the printed and electronic documentation, you should also review the documentation on Cisco.com for any updates.

For information about installing, troubleshooting, and using the product, see the sources of information in Table 5:

Table 5 Related Documentation

To learn more about...	See this document	In the product package?	On Cisco.com?	In the online help?
The known product bugs (DDTSs)	*Release Notes for the Network Analysis Module Analyzer 3.4*	No	Yes	No
Installing the NM-NAM	*Cisco Network Modules Quick Start Guide*	Yes	Yes	No
Features, tasks, and troubleshooting	• *Network Analysis Module (NM-NAM)*	No	Yes	No
	• *User Guide for the Network Analysis Module Traffic Analyzer Release 3.4*	No	Yes	Yes
	• *Network Analysis Module Command Reference Release 3.4*	No	Yes	No

7 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).

8 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.

9 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

10 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.

11 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

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

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the

Cisco Website at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE
Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico
The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore
Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA on recycled paper containing 10% postconsumer waste.
78-16947-01
DOC-7816947=