



Quick Start Guide for the Catalyst 6500 Series and Cisco 7600 Series Network Analysis Module, Release 3.5

Revised: June 19, 2006, OL-8401-01

Overview

The Catalyst 6500 Series and Cisco 7600 Series Network Analysis Module (model numbers WS-SVC-NAM-1 and WS-SVC-NAM-2) is a hardware module, which can be installed in Catalyst 6000 and 6500 Series switches and Cisco 7600 Series routers, that monitors and analyzes network traffic. The NAM Traffic Analyzer is embedded software in the NAM that provides browser-based access to the monitoring features of the NAM. You can use the NAM 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 the NAM and Traffic Analyzer.
- 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.



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2006 Cisco Systems, Inc. All rights reserved.

Package Contents

- Catalyst 6500 Series and Cisco 7600 Series NAM
- *Installation and Configuration Note for the Catalyst 6500 Series and Cisco 7600 Series Network Analysis Module Release 3.5*
- *Documentation Guide for the Network Analysis Module Release 3.5*
- *Copyright Notices for the Network Analysis Module Release 3.5*

Software and Hardware System Requirements

This section provides NAM Traffic Analyzer software and hardware requirements. [Table 1](#) lists the minimum software versions required to use NAM-1 and NAM-2 modules with NAM 3.5.

Table 1 Software Requirements for Minimum OS Versions

Module	Software Release	Orderable Product Number	Minimum IOS Software Versions Supported	Minimum CatOS Software Versions Supported
WS-SVC-NAM-1 WS-SVC-NAM-2	3.5	SC-SVC-NAM-3.5	<ul style="list-style-type: none"> • Release 12.1(13)E¹ or later with a Supervisor Engine 2 with an MSFC2. • Release 12.1(19E)1 or later with a Supervisor Engine 1A with an MSFC2. • Release 12.2(14)SX1 or later with a WS-SUP720. • Release 12.2(18)SXF with SUP32 	<ul style="list-style-type: none"> • Release 7.3(1) or later with Supervisor Engine 1A or 2. • Release 8.2(1) or later with a WS-SUP720.

1. If you are running a 12.1(13)E-based release, Cisco recommends a later 13E release such as 12.1(13)E11 over 12.1(13)E3.

[Table 2](#) lists the Cisco IOS and CatOS versions used when testing and developing NAM 3.5.

Table 2 Latest Supported IOS and Cat OS Versions

Modules	Cisco IOS Versions	Catalyst OS Versions
WS-SVC-NAM-1	12.2(18)SXD4	CatOS 8.5
WS-SVC-NAM-2	12.2(18)SXD7	
	12.2(18)SXE4	
	12.2(18)SXF3	
	12.2(18)SXF4 (Modular IOS)	

Please note the following:

- Cisco IP Phone firmware 6.0 and above is required for SIP voice packet quality monitoring

- IOS 12.2(18)SXE4, at minimum, is required to support the ERSPAN feature. Dependencies and limitations for ERSPAN can be found in *Configuring Local SPAN, RSPAN, and ERSPAN, Guidelines and Restrictions*, at:

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

- IOS 12.2(18)SXD or CatOS 8.5, at minimum, are required to support the Virtual SPAN feature

Table 3 identifies the Catalyst 6500 Series and Cisco 7600 supervisors and platforms that are compatible with NAM-1 and NAM-2.

Table 3 *Catalyst 6500 Series and Cisco 7600 Series NAM Hardware Compatibility*

Module	Running Catalyst OS Software	Running Cisco IOS Software	Platform or Devices
WS-SVC-NAM-1 WS-SVC-NAM-2	<ul style="list-style-type: none"> • SUP2 with MSFC2 • SUP720 • SUP32 		<ul style="list-style-type: none"> • Catalyst 6000 Series • Catalyst 6500 Series • Cisco 7600 Series

Table 4 describes the browser requirements for all platforms.

Table 4 *Browser Requirements*

Browser	Version	Platform	Java Plug-In Support ¹
Internet Explorer (recommended)	6.0	Windows Windows XP Professional	JRE Version 5.0 Update 6
Mozilla	1.7	Windows Windows XP Professional Solaris	
Firefox	1.5	Windows Windows XP Professional Solaris Linux (Redhat, SuSe)	

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.

Installing the NAM

For information on physically installing the NAM into the switch, see the *Installation and Configuration Note for the Catalyst 6500 Series and Cisco 7600 Series Network Analysis Module Release 3.5*.

http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_book09186a00805e081e.html

Setting Up the NAM

To set up the NAM, perform the actions described in the following sections:

- [Selecting a VLAN for Management \(For Cisco IOS Only\)](#), page 4

- [Configuring the NAM Management Network Parameters, page 4](#)

Selecting a VLAN for Management (For Cisco IOS Only)



Note

Devices running Catalyst OS do not need to configure a VLAN as the NAM management port. The port is automatically synchronized to the VLAN assigned to interface sc0 on the Supervisor engine.

To select a VLAN for management, enter the configuration mode for the NAM and enter the following:

```
analysis module slot_number management-port access-vlan vlan_number
```

This example shows how to select VLAN 5 for management.
 Switch# configure terminal
 Enter configuration commands, one per line. End with CNTL/Z.
 Switch(config)#

```
analysis module 4 management-port access-vlan 5
```

```
exit
```

Configuring the NAM Management Network Parameters

-
- Step 1** Access the NAM CLI by establishing a console session with the NAM.
- For devices running Cisco IOS enter:


```
session slot module_number processor 1
```
 - For devices running Catalyst OS enter:


```
session module_number
```
- Step 2** At the login prompt, enter **root** to log in to the root account.
- If you have not changed the password from the factory-set default, enter **root** as the root password.
 - If you are still at the factory set default, enter **password root** to change the root password.
- Step 3** Configure the NAM IP address and subnet mask.
- ```
ip address ip-address subnet-mask
```
- Step 4** Configure the NAM system default gateway address.
- ```
ip gateway default-gateway
```
- Step 5** Set the NAM system domain name.
- ```
ip domain domain-name
```
- Step 6** Set the NAM system hostname.
- ```
ip host name
```



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

Step 7 Set one or more NAM system name servers.

ip nameserver *ip-address*

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

ping *hostname*

or

ping *ip-address*

Step 9 Verify that the device is properly configured.

show ip

Step 10 If you want to use an external SNMP management application to access the NAM, configure the SNMP MIB system variables. These steps are optional.

- a. Configure the SNMP **syslocation** MIB variable.

snmp location *location-string*

- b. Set the SNMP **sysContact** MIB variable.

snmp contact *contact-string*

- c. Set the SNMP **sysName** MIB variable.

snmp name *name-string*

- d. Set the SNMP agent community string parameter password for read-write access.

snmp community *community-string rw*

- e. Set the SNMP agent community string parameter password for read-only access.

snmp community *community-string ro*



Note You can clear the SNMP community string using the **snmp delete community *community-string*** command.

- f. Verify the SNMP access controls and settings.

show snmp

Step 11 Enable the NAM Traffic Analyzer application.

ip http server enable

Step 12 Enter a web username and password.

- Step 13** To access Traffic Analyzer, open a web browser and enter the NAM IP address as the URL.
- Step 14** Log in with the NAM username and password that you entered in Step 13.
- Step 15** To end the NAM console session and return to the Cisco IOS CLI, enter the following:

exit

The following example shows how to configure a NAM running Catalyst OS.

```

namlab-6k#
namlab-6k#session 9
Trying NAM-9
Connected to NAM-9
Escape character is '^]'.

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

login: root
Password:
Last login: wed Feb 18 17:04:40 from joe
Terminal type: vt100

Cisco Network Analysis Module (WS-SVC-NAM-2) Console, 3.5(0.9)
Copyright (c) 1999-2006 by cisco Systems, Inc.

WARNING! Default password has not been changed!
root@localhost.cisco.com# password root
Changing password for user root
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully
root@localhost.cisco.com# ip address 172.20.104.103 255.255.255.192
root@localhost.cisco.com# ip gateway 172.20.104.65
root@localhost.cisco.com# ip domain cisco.com
root@localhost.cisco.com# ip host lab-nam
root@lab-nam.cisco.com# ip nameserver 171.69.2.133
root@lab-nam.cisco.com# ping 171.69.2.133
PING 171.69.2.133 (171.69.2.133) from 172.20.104.103 : 56(84) bytes of data.
64 bytes from 171.69.2.133: icmp_seq=0 ttl=247 time=515 usec
64 bytes from 171.69.2.133: icmp_seq=1 ttl=247 time=609 usec
root@lab-nam.cisco.com# show ip
IP address:                172.20.104.103
Subnet mask:                255.255.255.192
IP Broadcast:              172.20.104.127
DNS Name:                   lab-nam.cisco.com
Default Gateway:           172.20.104.65
Nameserver(s):              171.69.2.133
HTTP server:                Disabled
HTTP secure server:         Disabled
HTTP port:                  80
HTTP secure port:           443
TACACS+ configured:        No
Telnet:                     Enabled
SSH:                        Disabled
root@lab-nam.cisco.com# ip http server enable
Enabling HTTP server...

No web users are configured.
Please enter a web administrator user name [admin]:
New password:
Confirm password:

```

```

User admin added.
Successfully enabled HTTP server.
root@lab-nam.cisco.com# snmp location bldn NAM lab
root@lab-nam.cisco.com# snmp contact sysadmin
root@lab-nam.cisco.com# snmp community public ro
root@lab-nam.cisco.com# snmp community private rw
root@lab-nam.cisco.com# show snmp

SNMP Agent:   lab-nam.cisco.com   172.20.104.103

SNMPv1:   Enabled
SNMPv2C:  Enabled
SNMPv3:   Disabled

community   private   write
community   public    read

sysDescr          Cisco Network Analysis Module (WS-SVC-NAM-2), Version 3.5(0.9)
Copyright (c) 1999-2006 by cisco Systems, Inc.

sysObjectID       enterprises.9.5.1.3.1.1.2.914
sysContact        sysadmin
sysName           NAM
sysLocation       bldn NAM lab
root@lab-nam.cisco.com#

```

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:

- *Release Notes for the Cisco Network Analysis Module, Release 3.5*
http://www.cisco.com/en/US/products/sw/cscowork/ps5401/prod_release_note09186a00806adcc5.html
- *User Guide for the Network Analysis Module Traffic Analyzer, Release 3.5*
http://www.cisco.com/en/US/products/sw/cscowork/ps5401/products_user_guide_book09186a00806ad84a.html
- *Network Analysis Module Command Reference Release 3.5*
http://www.cisco.com/en/US/products/hw/switches/ps708/products_command_reference_book09186a00805e081d.html
- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Network Analysis Module Release 3.5 Installation and Configuration Note*
http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_book09186a00805e081e.html

You can find documentation for all releases of the Cisco Network Analysis Module at the following:

http://www.cisco.com/en/US/products/sw/cscowork/ps5401/tsd_products_support_series_home.html

You can find documentation about Cisco Catalyst 6500 Series Switches at the following:

http://www.cisco.com/en/US/customer/products/hw/switches/ps708/tsd_products_support_series_home.html

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)	<i>Release Notes for the Network Analysis Module Analyzer 3.5</i>	No	Yes	No
Installing the NM-NAM	<i>Catalyst 6500 Series Switch and Cisco 7600 Series Router Network Analysis Module Installation Note</i>	Yes	Yes	No
	<i>Cisco Network Modules Quick Start Guide</i>	No	Yes	No
Features, tasks, and troubleshooting	<i>Network Analysis Module (NM-NAM)</i>	No	Yes	No
	<i>User Guide for the Network Analysis Module Traffic Analyzer Release 3.5</i>	No	Yes	Yes
	<i>Network Analysis Module Command Reference Release 3.5</i>	No	Yes	No

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/techsupport>

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

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

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

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation 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 will find information about how to:

- 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, security notices, and security responses for Cisco products is available at this URL:

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at 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 have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only — security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies — psirt@cisco.com

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

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



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

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

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation 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, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation 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 & Documentation 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 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 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)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations 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 the network is impaired, while 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.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

<http://www.cisco.com/go/guide>

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, 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>

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- *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>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- 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>

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.

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0705R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© <2006> Cisco Systems, Inc. All rights reserved.