Release Notes for Cisco Network Assistant 1.0 and Later

February 2005

These release notes include important information about Cisco Network Assistant 1.0(1), 1.0(1a), 1.0(2), and any limitations, restrictions, and caveats that apply to these releases.

Contents

This information is in the release notes:

- "System Requirements" section on page 2
- "Downloading Network Assistant" section on page 4
- "Updating Network Assistant" section on page 4
- "Upgrading a Switch by Using Network Assistant" section on page 4
- "Minimum Cisco IOS Release" section on page 4
- "Limitations and Restrictions" section on page 5
- "Important Notes" section on page 8
- "Open Caveats" section on page 9
- "Resolved Caveats" section on page 12
- "Related Documentation" section on page 13
- "Obtaining Documentation" section on page 13
- "Documentation Feedback" section on page 14
- "Cisco Product Security Overview" section on page 14
- "Obtaining Technical Assistance" section on page 15
- "Obtaining Additional Publications and Information" section on page 17

CISCO SYSTEMS

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

System Requirements

The system requirements are described in these sections:

- "Installation Requirements" section on page 2
- "Devices Supported" section on page 2
- "Devices Not Supported" section on page 3
- "Cluster Compatibility" section on page 3

Installation Requirements

The PC on which you install Network Assistant must meet these minimum hardware requirements:

- Processor speed: Pentium 233 MHz
- DRAM: 128 MB
- Disk space: 50 MB of hard disk space
- Number of colors: 65536
- Resolution: 1024 x 768
- Font size: small

These operating systems support Network Assistant:

- Windows 98, second edition
- Windows NT 4.0, Service Pack 6 or later
- Windows 2000, Service Pack 3 or later
- Windows XP, Service Pack 1 or later

Note Network Assistant on Windows 98 and Windows NT cannot manage Catalyst 4500 series switches.

Devices Supported

Network Assistant can manage these devices:

- Catalyst 4500 series
  - Switches:
    Catalyst 4503 (WS-C4503)
    Catalyst 4506 (WS-C4506)
  - Supervisors:
    Supervisor Engine II-Plus (WS-X4013+)
    Supervisor Engine IV (WS-X4515)
    Supervisor II-Plus-TS (WS-X4013+TS)

  - Switching modules:
    6-port 1000BASE-X Gigabit Ethernet (WS-X4306-GB)
    24-port 10/100/1000BASE-T Gigabit Ethernet (WS-X4424-GB-RJ45)
    24-port IEEE 802.3af-compliant Power over Ethernet (PoE) 10/100BASE-TX RJ-45 (WS-X4224-RJ45V)
    24-port 10/100-Mbps RJ-45 (WS-X4124-RJ45)
    48-port 10/100-Mbps Fast Ethernet (WS-X4148-RJ)
    48-port IEEE 802.3af-compliant PoE 10/100BASE-TX RJ-45 (WS-X4248-RJ45V)
    48-port 10/100/1000BASE-T Gigabit Ethernet (WS-X4548-GB-RJ45)
  - Power supplies:
    PWR-C45-1000AC
    PWR-C45-1300ACV

Note Network Assistant does not support Catalyst 4500 series switches that are not in the previous list.

- Catalyst 3750 switches
- Catalyst 3560 switches
- Catalyst 3550 switches
- Catalyst 3500 XL switches
- Catalyst 2970 switches
- Catalyst 2955 switches
- Catalyst 2950 switches
- Catalyst 2940 switches
- Catalyst 2900 XL switches

Devices Not Supported

Network Assistant does not support these devices:

- Catalyst 1900 and 2820 switches
- Catalyst 2900 4-MB XL switches
- Catalyst 3750 Metro switches

Cluster Compatibility

This section describes how to choose command and standby command devices when a cluster consists of a mixture of Catalyst switches. When creating a device cluster or adding a devices to a cluster, follow these guidelines:

- When you create a device cluster, we recommend configuring the highest-end device in your cluster as the command device.
- If you are managing the cluster through Network Assistant, the device that has the latest software release should be the command device.

- The standby command device must be the same type as the command device. For example, if the command device is a Catalyst 3750 switch, all standby command devices must be Catalyst 3750 switches.

Note Catalyst 4500 series switches cannot be configured as standby command devices.

Downloading Network Assistant

You can download Network Assistant from this site:

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

For information on installing, launching, and connecting to Network Assistant, see *Getting Started with Cisco Network Assistant* at this site:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cna/v1_0/gsg/index.htm

Updating Network Assistant

To update Network Assistant, follow these steps:

1. Launch Network Assistant.
2. Choose **Applications > Application Updates**.
3. In the Authentication window, enter your Cisco.com username and password.
4. In the Application Updates window, select **Latest** from the **Show** list.
5. Select all the listed packages.
6. Click **Install Packages**.

Upgrading a Switch by Using Network Assistant

You can upgrade switch software by using Network Assistant, except for the software on Catalyst 4500 series switches. From the feature bar, select **Administration > Software Upgrade**. For detailed instructions, click **Help**.

Minimum Cisco IOS Release

Table 1 lists the minimum software releases required for the Catalyst switches that support Network Assistant.

Table 1 Minimum Cisco IOS Release Supported

Switch	Minimum Cisco IOS Release
Catalyst 4500 series	12.2(20)EWA
Catalyst 3750	12.1(11)AX

Table 1 Minimum Cisco IOS Release Supported (continued)

Switch	Minimum Cisco IOS Release
Catalyst 3560	12.1(19)EA1b
Catalyst 3550	12.1(4)EA1
Catalyst 2970	12.1(11)AX
Catalyst 2955	12.1(12c)EA1
Catalyst 2950	12.0(5.2)WC(1)
Catalyst 2950 LRE[1]	12.1(11)JY
Catalyst 2940	12.1(13)AY
Catalyst 3500 XL	12.0(5.1)XU
Catalyst 2900 XL (8-MB switches)	12.0(5.1)XU

1. LRE = Long-Reach Ethernet

Limitations and Restrictions

You should review this section before you begin working with the device. These are known limitations that will not be fixed, and there is not always a workaround. Some features might not work as documented, and some features could be affected by recent changes to the device hardware or software.

These sections describe the limitations and restrictions:

- "Cluster Limitations and Restrictions" section on page 5
- "Network Assistant Limitations and Restrictions" section on page 6

Cluster Limitations and Restrictions

These limitations apply only to the Catalyst 4500 series switches:

- By default, clustering is disabled on the Catalyst 4500 series switches.
- You must assign an IP address to the Catalyst 4500 series switch if it is a cluster command switch candidate. If the switch is a cluster member candidate, you might not need to assign an IP address.
- By default, the HTTP server is disabled on the Catalyst 4500 series switch. To connect the switch to Network Assistant, you must enable the HTTP server on all cluster members.
- The HTTP port number on Network Assistant and the Catalyst 4500 series switch must match.
- A Catalyst 4500 switch can be a cluster member only if another Catalyst 4500 switch is the command device.
- By default, the Catalyst 4500 series switch is configured with five vty lines. If the switch (such as a cluster command device with multiple cluster members) is connected to Network Assistant, you must configure at least eight + *x* vty lines, where *x* is the number of vty lines used by other applications. A maximum of 16 vty lines can be configured.
- Create a switch virtual interface (SVI) to use for intracluster communication. The SVI must be in the **no shut** state.

This limitation applies only to the Catalyst 4500 series and Catalyst 3750, 3560, 3550, and 2970 switches:

- If a Catalyst 2900 XL or 3500 XL cluster command device is connected to a Catalyst 3550 or a 3750 switch, the command device does not find any cluster candidates beyond the 3550 or the 3750 switch candidates. You must add the 3550 or the 3750 switch to the cluster to see other cluster candidates. (CSCdt09918)

These limitations apply only to the Catalyst 3750, 3560, 3550, and 2970 switches:

- If both the active command device and the standby command device fail at the same time, the cluster is not automatically recreated. Even if there is a third passive command device, it might not recreate all cluster members because it might not have all the latest cluster configuration information. You must manually recreate the cluster if both the active and standby command devices simultaneously fail. (CSCdt43501)
- When the active device fails in a device cluster that uses Hot Standby Routing Protocol (HSRP) redundancy, the new active device might not contain a full cluster member list.

  The workaround is to ensure that the ports on the standby cluster members are not in the Spanning Tree Protocol (STP) blocking state. See the "Configuring STP" chapter in the software configuration guide for more information about verifying port status. (CSCec31495)

These limitations apply only to the Catalyst 2955, 2950, and 2940 switches:

- When a cluster of devices have Network Time Protocol (NTP) configured, the command device is not synchronized with the rest of the devices. (CSCdz88305)
- When the active device fails in a device cluster that uses HSRP redundancy, the new active device might not contain a full cluster member list.

  The workaround is to ensure that the ports on the standby cluster members are not in the STP blocking state. See the "Configuring STP" chapter in the software configuration guide for information about verifying port status. (CSCec31495)

Network Assistant Limitations and Restrictions

The Network Assistant limitations and restrictions are described in these sections.

All Devices

These limitations apply to all the devices described in the “Devices Supported” section on page 2:

- A red border appears around the text-entering area of some Network Assistant windows. The color of the border changes to green when text is entered. The colored border does not prevent you from entering text. (CSCdv82352)
- You cannot switch modes (for example, from guide mode to expert mode) for an open Network Assistant window. The workaround is to close the open window, select the mode that you want, and then reopen the Network Assistant window. For the mode change to take effect on any other Network Assistant window that is open, you need to close that window and then reopen it after you select the new mode. (CSCdw87550)
- If you open a window in which you can enter text, open another window, and return to the first window, right-clicking in the text field might make the cursor in this field disappear. You can still enter text in the field. (CSCdy44189)

Catalyst 4500 Series Switches

Network Assistant supports only these features on the Catalyst 4500 series switch:

- Administration menu—IP Address, SNMP, System Time, HTTP Port, Users and Passwords, Console Baud Rate, MAC Addresses, ARP, Save Configuration, Restore Configuration, and System Reload
- Cluster menu—Create Cluster, Delete Cluster, Add to Cluster, Remove From Cluster, and Hop Count
- Device menu—Host Name
- VLAN menu—VLAN
- View menu—Front Panel, Topology Options, Automatic Topology Layout, and Save Topology Layout

Catalyst 3750, 3560, 3550, 2970, 2955, 2950, and 2940 Switches

These limitations apply only to the Catalyst 3750, 3560, 3550, 2970, 2955, 2950, and 2940 switches:

- Network Assistant fails when a device is running the cryptographic software image and the vty lines have been configured by using the **transport input ssh** and **line vty 0 15** global configuration commands to use only SSH. The workaround is to allow SSH and Telnet access through the vty lines by using the **transport input ssh telnet** and **line vty 0 15** global configuration commands. (CSCdz01037)
- When you add a new member with a username and password that is different from the existing cluster member usernames and passwords, Network Assistant produces an exception error because of an authentication failure. The workaround is to add the new member without a username and password. When the new member is added to the cluster, remove the existing username and password from the Username and Password fields, enter a new username and password, and then apply it to all cluster members. (CSCdz07957)
- When the Link Graphs application has run for hours displaying packet drop and error information, sometimes the X-axis crosses the Y-axis at a negative Y value instead of at Y= 0. This condition occurs with all supported operating systems, browsers, and Java plug-ins. There is no workaround. (CSCdz32584)
- After you click **Apply** or **Refresh** in the Simple Network Management Protocol (SNMP) window, the window size changes. (CSCdz75666, CSCdz84255)
- When you enable log scaling for Link Graphs, the Y-axis scale becomes illegible. There is no workaround. (CSCdz81086)
- Changing the password or current authentication while Network Assistant is running causes HTTP requests to fail. The workaround is to close all Network Assistant sessions and then to relaunch it. (CSCeb33995)
- When TACACS authentication is enabled only on a command device, member devices cannot be configured. The workaround is to enable TACACS authentication on the member devices. (CSCed27723)
- When there are Catalyst 2950 and 2955 devices in a cluster, and you launch the QoS Queue window to configure the devices, and then try to view the settings for other devices by using the device selection menu, Network Assistant halts after 20 to 30 selections.

  The workaround is to close and then to restart Network Assistant. (CSCed39693)

- If an access control list (ACL) is deleted from a device, all QoS classes on Catalyst 2970 and 3750 switches that use this ACL for traffic classification become unusable. The modification of these classes to use any other traffic classification (match statement) fails. The workaround is to delete the QoS class that uses the undefined ACL and then to recreate it with the intended traffic classification (match statement). (CSCed40866)
- When an Open Shortest Path First (OSPF) summary address is added for a 10.x.x.x network, a Windows exception error sometimes occurs.

  The workaround is to add the address by using the **router ospf** <*process-id*>, **area** <*area-id*>, and **range** <*address*> <*mask*> configuration commands. (CSCed87031)
- When you select a remote device from the VLAN menu, the displayed table might not show all the connected links between the devices selected in the Host Name and the Remote Device lists. This can also occur when you add a new device to a cluster and open VLAN menu.

  To work around the problem, follow these steps:

  1. Click **Refresh** on the Network Assistant toolbar two or three times, or select **View** > **Refresh** two or three times.
  2. Click **Refresh** in the VLAN window.

  (CSCee06244)
- A Java exception error occurs when Network Assistant is in read-only mode and you launch the Port Settings window. This only occurs on Catalyst 3500 XL, 2950 LRE, and 2900 XL switches.

  The workaround is to open the Port Settings window with Network Assistant in read-write mode. (CSCee25870)
- Host names and Domain Name System (DNS) server names with commas for a cluster command device, member device, or candidate device can cause Network Assistant to behave unexpectedly. You can avoid this instability in the interface by not using commas in host names or DNS names. Do not enter commas when also entering multiple DNS names in the IP Configuration tab of the IP Management window in Network Assistant.
- Access control entries (ACEs) that contain the **host** keyword precede all other ACEs in standard ACLs. You can reposition the ACEs in a standard ACL with one restriction: No ACE with the **any** keyword or a wildcard mask can precede an ACE with the **host** keyword.

Important Notes

These sections describe the important notes related to Network Assistant and clustering:

- "Cluster Notes" section on page 8
- "Network Assistant Notes" section on page 9

Cluster Notes

This note applies to cluster configuration only on the Catalyst 3550 switches:

The **cluster setup** privileged EXEC command and the **standby mac-address** interface configuration command have been removed from the command-line interface (CLI) and the documentation because they did not function correctly.

Network Assistant Notes

These notes apply to Network Assistant configuration on all the devices described in the "Devices Supported" section on page 2:

- If you use Network Assistant on Windows 2000, it might not apply configuration changes if the enable password is changed from the CLI during your Network Assistant session. You have to restart Network Assistant and enter the new password when prompted. Platforms other than Windows 2000 prompt you for the new enable password when it is changed.
- Network Assistant does not display QoS classes that are created through the CLI if these classes have multiple match statements. When using Network Assistant, you cannot create classes that match more than one match statement. Network Assistant does not display policies that have such classes.
- Within an ACL, you can change the sequence of ACEs that have the **host** keyword. However, because such ACEs are independent of each other, the change has no effect on the way the ACL filters traffic.
- In the Front Panel view or Topology view, Network Assistant does not display error messages in read-only mode for these devices:
  - Catalyst 3550 member switches running Cisco IOS Release 12.1(6)EA1 or earlier
  - Catalyst 2950 member switches running Cisco IOS Release 12.0(5)WC2 or earlier
  - Catalyst 2900 XL or 3500 XL member switches running Cisco IOS Release 12.0(5)WC2 or earlier

  In the Front Panel view, if the device is running one of the software releases listed previously, the device LEDs do not appear. In Topology view, if the member is an LRE switch, the CPE devices that are connected to the switch do not appear. The Bandwidth and Link graphs also do not appear in these views.

Open Caveats

These sections describe the open caveats with possible unexpected activity in this software release:

- "Open Network Assistant Caveats" section on page 9
- "Open Cluster Caveats" section on page 12

Open Network Assistant Caveats

These Network Assistant caveats apply to the all the devices described in the "Devices Supported" section on page 2:

- CSCee06244

  When you select a remote device from the VLAN menu, the displayed table might not show all the connected links between the devices selected in the Host Name and the Remote Device lists. This can also occur when you add a new device to a cluster and open the VLAN menu.

This is the workaround. Follow these steps:

1. Click **Refresh** on the Network Assistant toolbar two or three times, or select **View > Refresh** two or three times.
2. Click **Refresh** in VLAN window.

- CSCee91784

  If Network Assistant loses IP connectivity to the switch and an action is performed in the IP Address window, a Java exception error occurs.

  The workaround is to close and to reopen the IP Address window when connectivity is restored.

- CSCee93695

  After the switch loses connectivity, the connect icon in the status bar incorrectly displays a connect status instead of a disconnect status.

  There is no workaround.

- CSCee96650

  If you select multiple ports and launch the Port Settings window from the popup menu of the Front Panel view, it might take approximately 7 seconds to launch.

  The workaround is to launch the Port Settings window from the feature bar.

- CSCef02719

  The Network Assistant window flickers if you click **Cancel** in the **Application > Print** window.

  There is no workaround.

- CSCef20111

  If you try to add or delete a cluster from the CLI and from Network Assistant simultaneously, you might get Java exception errors.

  The workaround is to not to add or delete clusters simultaneously from the CLI and Network Assistant.

- CSCef24188

  A Java exception error occurs if Cisco Discovery Protocol (CDP) is disabled on a cluster member.

  There is no workaround.

- CSCef44654

  If you click **Install Packages** in the Application Updates window and enter a wrong username or password in the network authentication window, or if you click **Cancel**, an error window appears, and you cannot install any packages.

  The workaround is to restart Network Assistant.

- CSCef47554

  A Java exception error occurs in the IGMP Report window when Network Assistant is in read-only mode and is connected through a secure HTTP (HTTPS) connection to a command switch running a Cisco IOS cryptographic image.

  There is no workaround.

- CSCef49951

  If you launch the Application Updates window and enter the wrong username or password in the network authentication window, or if you click **Cancel**, an error window appears, and no packages appear in the Application Updates window.

The workaround is to click **Refresh** in the Application Updates window three times or to restart Network Assistant.

- CSCef67553

  In Network Assistant, some windows such as VLAN, Host Name, and so on might not launch from the Front Panel view popup menu for Catalyst 4500 series switches.

  The workaround is to close Network Assistant and relaunch it.

- CSCeg38631

  After you upgrade Network Assistant packages to 1.0(2), the About window still shows the version as 1.0(1a).

  You can verify the upgrade by opening the About window and clicking **Package Info**, which opens the Installed Packages window. You see a table that lists the installed packages. The first column lists the device package names and their versions. The versions should be 1.0(2). Ignore the information in the Version column.

- CSCeg60113

  On Catalyst 3750 switches, when you add a trap manager with all the traps enabled, the trap manager is not applied to the switch.

  There is no workaround in Network Assistant. Use the command-line interface to configure trap managers with all the traps enabled.

- CSCeg75813

  The Application Updates window and the Installed Packages window show two version numbers for each package.

  The Name column in the Application Updates window shows the names of packages and the correct version numbers. Ignore the values in the Version column and Installed Version column.

  The Name column in the Installed Packages window shows the names of packages and the correct version numbers. Ignore the values in the Version column.

- CSCeg78814

  A feature might show an unusual error after a Network Assistant package is installed.

  All the available package updates were not installed. Choose **Application > Application Updates** from the feature bar, select **Latest** from the **Show** list, and install all the packages.

- CSCeh12708

  If you upgrade a Catalyst switch to Cisco IOS 12.1(22)EA3 or later or to Cisco IOS 12.2(25)SEA or later, Network Assistant no longer recognizes the switch.

  Network Assistant connects to Cisco.com to get an application update when this happens. When it displays an authentication window, enter your Cisco.com username and password. When the Application Updates window appears, choose **Latest** in the drop-down list, select all the packages that are shown in the window, and click **Install**.

  After the application update is installed, you are forced to close Network Assistant. When you restart it, it can recognize and manage the upgraded Catalyst switch.

Open Cluster Caveats

This cluster caveat applies to the all the devices described in the "Devices Supported" section on page 2:

- CSCef48257

  After the cluster command device is reloaded, it might not be able to re-establish communication with the cluster members connected through its routed ports.

  This is the workaround. Follow these steps:

  1. Use the **no cluster run** global configuration command on the cluster command device and the cluster members that have lost connectivity to the command device.
  2. Use the **cluster member** global configuration command to add the cluster members back to the cluster.

- CSCeg60365

  If a Catalyst 2970 switch is a cluster command device and a Catalyst 3750 or 3550 switch is a cluster member, enabling IGRP on a network on the Catalyst 3750 or 3550 switch creates a *Premature EOF* error.

  There is no workaround. Make the Catalyst 3750 or 3550 switch the command device.

Resolved Caveats

This section describes the resolved caveats.

Caveats Resolved in Network Assistant 1.0(2)

These caveats were resolved in this release:

- CSCee06206

  When a Catalyst 3750 stack member leaves or joins the device stack, the entire stack no longer disappears from the Topology view.

- CSCee26671

  When you click **Refresh** in the Stack Settings window, the latest information about the device cluster now appears.

- CSCee82854

  An error no longer occurs when you modify the port settings of multiple ports by using the Modify Port Settings window launched from the popup menu of the Front Panel view.

- CSCef31685

  In the Topology view, the EtherChannel links between two Catalyst 4500 series switches now correctly appear in red (blocked) instead of green (forwarding).

Caveats Resolved in Network Assistant 1.0(1a)

This caveat was resolved in this release:

- CSCef89938

  When Network Assistant 1.0(1) is launched, and when the locale settings in the **Control Panel** > **Regional Options** window in Microsoft Windows are not set to English (United States), the error message `None of the version files parsed correctly` no longer appears, and the application works correctly.

Related Documentation

This online document provides complete information about Network Assistant:

Getting Started with Cisco Network Assistant

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cna/v1_0/gsg/index.htm

You can order printed copies of documents with a DOC-xxxxxx= number from the Cisco.com sites and from the telephone numbers listed in the "Obtaining Documentation" section on page 13.

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 ripostes 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

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