Release Notes for Cisco Network Assistant 5.0

August 31, 2006

These release notes include important information about Cisco Network Assistant 4.0 and 4.1 and any limitations, restrictions, and caveats that apply to these releases.

Contents

This information is in the release notes:

CISCO SYSTEMS

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

New Features

When you install and launch Cisco Network Assistant 4.0, you can

- Use the IP Addresses feature to assign an IP address to the integrated wireless LAN controller on the Catalyst 3750G-24WS-S25 and 3750G-24WS-S50 switches.

- Access the command-line interface (CLI) through the Telnet feature. It is available on the feature bar and on device popup windows in the Topology view and Front Panel view.

- Create communities with an unlimited number of access points.

- Use colors to highlight VLAN links in the Topology view. This option is available only if you are managing a community. To access it, you open Topology Options window and use the Highlighting tab.

- Print windows in a report format. In this format, none of the window information is truncated, as can happen if you use the **PrtSc** key to print the screen. The report format is also time-stamped, and pages are numbered.

- Print the Topology view or the Front Panel view in a fit-to-page format.

- Launch the device manager for devices in your network from device popup windows in the Topology view or Front Panel view.

- Stop the process of discovering neighbors at any point when you create or modify a community.

Cisco Network Assistant 4.1 adds these features:

- A graphical user interface and online help in additional languages: French, Spanish, Italian, German, Japanese, and simplified Chinese

- Limited support for the Cisco Catalyst 4006 Chassis, WS-C4006

- Support for Cisco 850 Series Integrated Services Routers and Cisco 870 Series Integrated Services Routers

System Requirements

The system requirements are described in these sections:

Installation Requirements

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

- Processor speed: Pentium 3, 1 GHz

- DRAM: 256 MB minimum, 512 MB recommended for better performance

- Hard-disk space: 70 MB for the application alone, 200 MB recommended

- Number of colors: 65536

- Resolution: 1024 x 768

- Font size: Small

These operating systems support Network Assistant:

- Windows XP, Service Pack 1 or later

- Windows 2000, Service Pack 3 or later

Devices Supported

Network Assistant manages these routers, switches, access points, and firewalls. It manages Catalyst Express 500 switches, routers, access points, and firewalls only as community members; these devices cannot be cluster members.

Routers

- Cisco 3800 series, models 3825 and 3845

- Cisco 3700 series, models 3725 and 3745

- Cisco 2800 series, models 2801, 2811, 2821, and 2851

- Cisco 2600 series, models 2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651, 2651XM, and 2691

- Cisco 1800 series, models 1801, 1801W, 1802, 1802W, 1803, 1803W, 1811, 1811W, 1812, 1812W, and 1841

- Cisco 1700 series, models 1701, 1711, 1710, 1712, 1721, 1751, 1751-V, and 1760

- Cisco 800 series, models 831, 836, 837, 851, 857, 876, 877, and 878

- Cisco 850 series, models 851W, 857W, 871, 871W, 876W, 877W, and 878W

Switches

- Catalyst 4900 series

    - Catalyst 4948 (WS-C4948)

    - Catalyst 4948-10GE (WS-C4948-10GE)

- Catalyst 4500 series

    - Chassis:
      Catalyst 4006 (WS-C4006)
      Catalyst 4503 (WS-C4503)
      Catalyst 4506 (WS-C4506)
      Catalyst 4507R (WS-C4507R)
      Catalyst 4510R (WS-C4510R)

    - Supervisors:
      Supervisor Engine II-Plus (WS-X4013+)
      Supervisor Engine IV (WS-X4515)
      Supervisor II-Plus-TS (WS-X4013+TS)
      Supervisor Engine V (WS-X4516)
      10-Gigabit Supervisor Engine V (WS-X4516-10GE)

    - Supervisor Daughter Card: NetFlow Services daughter card (WS-F4531)

- Switching modules:
24-port 10/100 with RJ-45 connectors (WS-X4124-RJ45)
24-port Fast Ethernet 100BASE-FX, multimode fiber with MT-RJ connectors (WS-X4124-FX-MT)
48-port Fast Ethernet 100BASE-FX, multimode fiber with MT-RJ connectors (WS-X4148-FX-MT)
48-port Fast Ethernet 100BASE-LX10, single-mode fiber with MT-RJ connectors (WS-X4148-FE-LX-MT)
48-port 10/100 with RJ-45 connectors (WS-X4148-RJ)
48-port Ethernet 10/100-Mbps with 4 telco connectors (WS-X4148-RJ21)
24-port 10/100 PoE 802.3af compliant with RJ-45 connectors (WS-X4224-RJ45V)
32-port Ethernet 10/100 and 2 GBIC uplinks (WS-X4232-GB-RJ)
48-port 10/100 PoE 802.3af compliant with telco connectors (WS-X4248-RJ21V)
48-port 10/100 PoE 802.3af compliant with RJ-45 connectors (WS-X4248-RJ45V)
2 GBIC ports (WS-X4302-GB)
24-port 10/100/1000 with RJ-45 connectors (WS-X4424-GB-RJ45)
18 GBIC ports (WS-X4418-GB)
48-port Ethernet 10/100/100 with RJ-45 connectors (WS-X4448-GB-RJ45)
48-port 1000BASE-X, SFP-based with LC connectors—SFP optics included (WS-X4448-LX)
48-port 1000BASE-X ports, SFP-based with LC connectors (WS-X4448-SFP)
Enhanced 48-port 10/100/1000 with RJ-45 connectors (WS-X4548-GB-RJ45)
24-port 10/100/1000 PoE 802.3af compliant with RJ-45 connectors (WS-X4524-GB-RJ45V)
48-port 10/100/1000 PoE 802.3af compliant with RJ-45 connectors (WS-X4548-GB-RJ45V)
6 GBIC ports (WS-X4306-GB)
6-port 10/100/1000 PoE 802.3af compliant or SFP-based (WS-X4506-GB-T)

- Power supplies:
PWR-C45-1000 AC
PWR-C45-1300 ACV
PWR-C45-1400 AC
PWR-C45-1400 DC-P
PWR-C45-2800 ACV
PWR-C45-4200 ACV

- Catalyst 3750 switches, all models

- Catalyst 3560 switches, all models

- Catalyst 3550 switches, all models

- Catalyst 3500 XL switches, all models

- Catalyst 2970 switches, all models

- Catalyst 2960 switches, all models

- Catalyst 2955 switches, all models

- Catalyst 2950 switches, all models

- Catalyst 2940 switches, all models

- Catalyst 2900 XL switches, all models

- Catalyst Express 500 switches, all models

- Cisco EtherSwitch service modules:
  - NME-16ES-1G
  - NME-16ES-1G-P
  - NME-X-23ES-1G
  - NME-X-23ES-1G-P
  - NME-XD-24ES-1S-P
  - NME-XD-48ES-2S-P

Note The Topology view of Network Assistant supports Catalyst 6500 switches. You cannot add these devices to a community or cluster, but you can launch device manager for them from the Topology view.

Access Points

Cisco Aironet 350, 1100, and 1200 series. Network Assistant supports them only if they run a Cisco IOS image.

Firewalls

Cisco PIX 515E Firewalls. PIX Firewalls do not support the Cisco Discovery Protocol, so they are not automatically shown as neighbors in the Topology view. They are shown only after you add them to a community by using a Create Community or Modify Community window. To see a PIX Firewall link to another community member, you must add the link manually by selecting Add Link in a Topology popup menu.

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/en/US/products/ps5931/prod_installation_guides_list.html

Updating Network Assistant

To update Network Assistant to a later release in the language you are using, 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 in two ways:

- Drag and drop a software-image file from your PC, mapped drive, or network drive to a device icon in the Topology view.

- Select **Maintenance** > **Software Upgrade** from the feature bar.

For detailed instructions, click **Help**.

Minimum Cisco IOS Release

Table 1 lists the minimum software releases required for the devices that Network Assistant manages.

Table 1   Minimum Cisco IOS Release Required

Device	Minimum Software Release
All supported Cisco routers	12.2(15)T9
Catalyst 4500 series switches	12.2(20)EWA
Catalyst 3750 switches	12.1(11)AX
Catalyst 3560 switches	12.1(19)EA1b
Catalyst 3550 switches	12.1(4)EA1
Catalyst 2970 switches	12.1(11)AX
Catalyst 2960 switches	12.2(25)FX

Table 1 *Minimum Cisco IOS Release Required (continued)*

Device	Minimum Software Release
Catalyst 2955 switches	12.1(12c)EA1
Catalyst 2950 switches	12.0(5.2)WC(1)
Catalyst 2950 LRE[1] switches	12.1(11)JY
Catalyst 2940 switches	12.1(13)AY
Catalyst 3500 XL switches	12.0(5.1)XU
Catalyst 2900 XL switches (8-MB)	12.0(5.1)XU
Catalyst Express 500 switches	12.2(25)FY
Cisco EtherSwitch service modules	12.2(25)EZ (switch software) 12.3(14)T (router software)
All supported Cisco access points	12.2(15)JA
Cisco PIX Firewalls	6.3(4)

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

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)

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 3:

- CNA supports the standard ASCII character set. Do not enter characters from extended ASCII character sets in GUI fields for feature options.

- 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)

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

  The workaround is to open the Port Settings window from the feature bar. (CSCee96650)

- 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)

- When there are more than one neighbor devices of same device type and they have same hostname, the Topology view displays only one neighbor device instead of displaying all the neighbor devices.

  The workaround is to not have same hostname for more than one device. (CSCsb50280).

Catalyst 4500 Series Switches

On Catalyst 4500 series switches, Network Assistant supports only the features shown in Table 2:

Table 2   Features Supported by Catalyst 4500 Series Switches

Menu Path	Features
Configure	Smartports, Save Configuration
Configure > Ports	Port Settings
Configure > Security	Security Wizard, Port Security
Configure > Switching	VLANs, MAC Addresses, Voice VLAN
Configure > Device Properties	IP Addresses, Hostname, System Time, HTTP Port, Users and Passwords, SNMP
Configure > Clusters	Cluster Conversion Wizard, Create Cluster, Delete Cluster, Add To Cluster, Remove From Cluster, Hop Count
Monitor	Event Notification, System Messages
Monitor > Reports	Inventory, Bandwidth Graphs, Link Graphs, ARP
Monitor > Views	Front Panel, Topology
Troubleshoot	Ping and Trace
Maintenance	Software Upgrade, Configuration Archive, System Reload

This limitation applies to the Catalyst 4500 Series Switches:

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

  The workaround is to close Network Assistant and restart it. (CSCef67553)

Community Limitations

These limitations apply only to communities:

- A community can contain up to 20 devices. This limit is enforced whenever you add devices to a community.

  Furthermore, a community cannot contain more than 16 nonmodular switches, 4 modular switches, and 2 routers. These limits are checked during the launch of Network Assistant; you receive a warning if they are exceeded.

- Changes to the topology or network do not propagate across all open Network Assistant sessions connected to the same community. You see this inconsistency when multiple Network Assistant sessions are open on one desktop, and they point to the same community.

  Open one Network Assistant session per desktop per community. (CSCeh53619)

- The Topology view sometimes displays duplicate devices and links. There is no workaround. (CSCeh61352)

- In the Topology view, the horizontal scrollbar sometimes does not scroll far enough left to show the complete topology. The workaround is to right-click the Topology view and to select Automatic Topology Layout from the popup menu. (CSCeh56952)

- In the Topology view, if there are multiple links between community members and one of the links is blocked, it is shown in green, not in gray. There is no workaround. (CSCeh60050)

- In the Topology view, the redundant link for an HSRP group is not shown. There is no workaround. (CSCeh54526)

- If a community has members that are connected to a member through a hub or a Gigastack module, the Topology view shows all the connections. But if nonmembers are connected to a community member through a hub or a Gigastack module, the Topology view shows only the connection of the first nonmember.

- Accessing a community through a router running NAT (Network Address Translation) is not supported.

Cluster Limitations

These limitations apply only to clusters:

- 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)

- 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 restart 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)

- 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)

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

  There is no workaround. (CSCee93695)

Community and Cluster Limitations

These limitations apply to both communities and clusters:

- Network Assistant fails when a device is running the cryptographic software image and the vty lines have been configured with the **transport input ssh** and **line vty 0 15** global configuration commands to use only SSH. The workaround is to use the **transport input ssh telnet** and **line vty 0 15** global configuration commands to allow SSH and Telnet access through the vty lines. (CSCdz01037)

- 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)

- 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)

- Hostnames 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 hostnames 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.

- 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. (CSCee91784)

- When you reload a device with Network Assistant, it saves the running configuration. If you want to reload without saving the running configuration, use the CLI. (CSCeh24259)

- If a dual-media port on a Catalyst 4500 switch, model WS-C4948 or model WS-X4506-GB-T, is configured to RJ-45 and you apply a Smartports port role, the port is changed to SFP, the default setting. The connection to the port is lost.

  Reconfigure the media type to RJ-45 through the Port Settings window. (CSCeh31699)

- If you open the Modify Port Settings or the Modify Port Mode window twice in succession from the Front Panel view by right-clicking a port, selecting Port Settings or VLAN from the popup menu, and repeating these actions for another port, the windows display the settings for the port that you selected first.

  Ensure that the **Interface** field in these windows applies to the port that you selected. Be sure to close these windows between port selections. (CSCei17154)

- After you perform a search, the TAB key moves the focus in the search results. If you press the TAB key enough to reach the end of the results, the next TAB keystroke moves the focus out of the search results and into the next-in-focus window on the Network Assistant desktop.

  Press **ALT-s** to return to the search results. (CSCei68648)

- Network Assistant does not verify if the VLAN and the native VLAN are the same on the access point and the switch port that is connected to the access point. VLAN differences might cause wireless connectivity problems when you use the Secure Wireless feature.

  The workaround is to ensure that the VLANs and the native VLAN are the same on the access point and the switch port. (CSCsb77434)

Important Notes

These sections contain important notes related to Network Assistant:

Compatibility with Cisco IOS

If you run Cisco IOS 12.2(25)SEE or later, Cisco IOS 12.2(25)SEG or later, or Cisco IOS 12.1(22)EA7 or later, you must run Network Assistant 4.0 or later.

Community Notes

This note applies to community on all the devices described in the :

All the devices for the topology of a community are derived from the CDP (Cisco Device Protocol) table of Cisco IOS. Therefore, the Topology view shows duplicate devices when CDP discovers duplicate devices. This happens for a single device when the command **show cdp neighbor** is entered. Two devices are displayed: one with the actual hostname (for example, *abc*), the other with hostname.domainname (for example, *abc.cisco.com*).

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 3:

- 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 that could create possibly unexpected activity in this software release.

These caveats apply to all the devices described in the "Devices Supported" section on page 3:

- 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.

  After you click Finish, you see the commands that are actually applied to the device.

- CSCeh32160

  If you change a hostname while a Network Assistant window is open, the window might not display the new hostname, even if you refresh the window.

  To see the new hostname, close the window and then reopen it.

- CSCeh37933

  The Media Type column in the Port Settings window appears even if the modules of a Catalyst 4500 switch do not support AWP (alternate wired ports). If this case, the column fields display as *N/A*.

  There is no workaround. The other columns in the window are not affected.

- CSCeh43889

  In the Port Settings window, you must apply a change to some speed settings before you can change a duplex setting.

  After you configure a speed setting, click **Apply**; then configure a duplex setting.

- CSCeh54393

  In a Topology view for a community, the link icons for routed, trunk, and Gigastack links are not shown.

  There is no workaround.

- CSCeh59451

  Even if you see the message `Port security is only supported on static access interfaces`, it is also supported on ISL trunk ports and IEEE 802.1Q trunk ports if these ports are supported by the Cisco IOS image.

  The Port Security window lists all the ports that are eligible for port security. If a port is not listed, configure the port as necessary through the VLAN window, and return to Port Security window to configure the port security settings.

- CSCeh72079

  When the media type is changed on a S-X4506-GB-T linecard through the CLI or through another instance of Network Assistant, your instance of Network Assistant might be put into an inconsistent state, resulting in a blank Port Settings window.

  The workaround is to close your instance of Network Assistant and then restart it. You can then use the Port Settings window without a problem.

- CSCeh75133

  You cannot see the PoE columns in the Port Settings window for Catalyst 4503, 4506, or 4507R switches that run Cisco IOS 12.2(20)EWA and have a WS-4548, WS-4524, or WS-4506-GB-T PoE line card.

  The workaround is to upgrade the software on the switch to a later version of Cisco IOS.

- CSCej02776

  Zooming in or zooming out on the time axis of a bandwidth graph when the axis approaches noon or midnight might cause the time increments to be incorrectly labeled.

  Close the Bandwidth Graph window, reopen it, and zoom in or out again.

- CSCsb77153

  On Catalyst 4500 and 4900 series switches, you cannot edit flow control values from the Port Settings window; they are read-only.

  The workaround is to open the Front Panel view, right-click on the port to be configured, and select **Port Settings** from the drop-down list. From the Modify Port Settings window, you can configure the flow control values.

- CSCsb88555

  On a Catalyst 4500 or Catalyst 4900 series switch, when you select **Security** > **Port Security** and try to associate a secure address with a trunk port, an "Invalid input detected" error is displayed.

  There is no workaround for a trunk port. Open the VLANs window, select the device and port, click **Modify**, and select an administrative mode that is not for a trunk port.

- CSCsb88566

  When you connect to Network Assistant in read-only mode, choose **Configure** > **Port** > **Port Settings** on the feature bar, and select a Catalyst 4500 series switch, you are prompted to request level-15 access. This is the read/write access level, which is incompatible with read-only mode. You cannot view the Port Settings window.

  The only workaround is to get permission from your administrator to connect to Network Assistant in read/write mode.

- CSCsd64494

  For a stack of Catalyst 3750 switches, the **Hostname** list in the Bandwidth Graphs window has an entry for an entire stack and for each of the devices in the stack. The window shows valid data only for the entire stack.

  There is no workaround. Ignore the data that is shown for stack members.

- CSCsd80600

  When you open the Modify Port Settings window from the Front panel view and change the duplex, speed, or power (PoE switches only) setting, the old setting is shown when you close the window and open it again. The Port Settings window and command-line interface do show the change.

  The change appears in the Modify Port Settings window if you click the Refresh icon on the toolbar.

- CSCse58716

  In the Bandwidth Graphs window of the Spanish version of Network Assistant, the legend label *Bandwidth Utilization* is cut off on the right.

  Enlarge the window to see the full label.

- CSCse80505

  In non-English versions of Network Assistant, the letter bar at the top of the glossary contains some letters for which there are no corresponding glossary entries. Clicking these letters takes you to the bottom of the glossary. In the Japanese and Chinese versions, the glossary bar does not contain Chinese and Japanese characters.

  You can find Japanese and Chinese terms by browsing the glossary.

- CSCsf09989

  When you scroll from right to left in a text field, the far left characters are sometimes cut off.

  There is no workaround.

These caveats apply to Cisco EtherSwitch service modules:

- CSCei55046

  The Front Panel view on EtherSwitch service modules NME-16ES-1G-P, NME-X-23ES-1G-P, NME-XD-24ES-1S-P, and NME-XD-48ES-2S-P shows the EN-LED as not enabled.

  There is no workaround.

- CSCsd04956

  The Topology view does not show the internal Gigabit Ethernet link between routers and the EtherSwitch service modules NME-16ES-1G and NME-X-23ES-1G.

  There is no workaround.

- CSCsd06275

  The Smartports window shows the NME-XD-24ES-1S-P EtherSwitch service module with two Mode buttons instead of one

  There is no workaround.

Resolved Caveats

This section describes the resolved caveats.

Caveats Resolved in Network Assistant 4.1

This caveat was resolved in Network Assistant 4.1:

- CSCse65622

  You can now manage Cisco 870 Series Integrated Services Routers, models 871 and 877W, in communities.

Caveats Resolved in Network Assistant 4.0

These caveats were resolved in Network Assistant 4.0:

- CSCeh17771

  Access points and routers are not supported in the Front Panel view. Their check boxes are grayed out and now do not appear with a check mark.

- CSCei78959

  If you set the configuration bits through the CLI to 0x2100 or 0x2101 and then restore a configuration with the Configuration Archive window, you can now reload the device.

- CSCej00845

  If a device has multiple IP addresses and more than one of these IP addresses is added to a community, the device is now counted only once in determining whether the community limits have been exceeded.

- CSCsb60066

  If you change the hostname of a community member in a Network Assistant session and change it in a session with a different community, you no longer see a message that the name change failed.

- CSCsb90846

  Upgrading the Cisco IOS software on a device to a cryptographic image from an noncryptographic image is now sufficient to make an HTTPS connection with the device.

Related Documentation

This online document provides complete information about Network Assistant:

Getting Started with Cisco Network Assistant

http://www.cisco.com/en/US/products/ps5931/prod_installation_guides_list.html

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

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

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 library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

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

The Product Documentation DVD is created monthly and is released in the middle of the month. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

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

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

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

If you do not have a user ID or password, you can register at this URL:

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

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Technical Support & Documentation site area by entering your comments in the feedback form available in every online document.

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 do the following:

- 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 encryption key 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 to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. (To register as a Cisco.com user, go to this URL: http://tools.cisco.com/RPF/register/register.do) Registered users can access the tool at this URL: http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

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 Tool** to locate your product serial number before submitting a request for service online or by phone. You can access this tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This 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.

Tip Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. On the Cisco.com home page, click the **Advanced Search** link under the Search box and then click the **Technical Support & Documentation**.radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

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 channel product 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 magazine for Cisco networking professionals. 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 subscribe to *Packet* magazine at this URL:

  http://www.cisco.com/packet

- *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 where networking professionals 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

- "What's New in Cisco Documentation" is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of "What's New in Cisco Documentation" at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- 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.