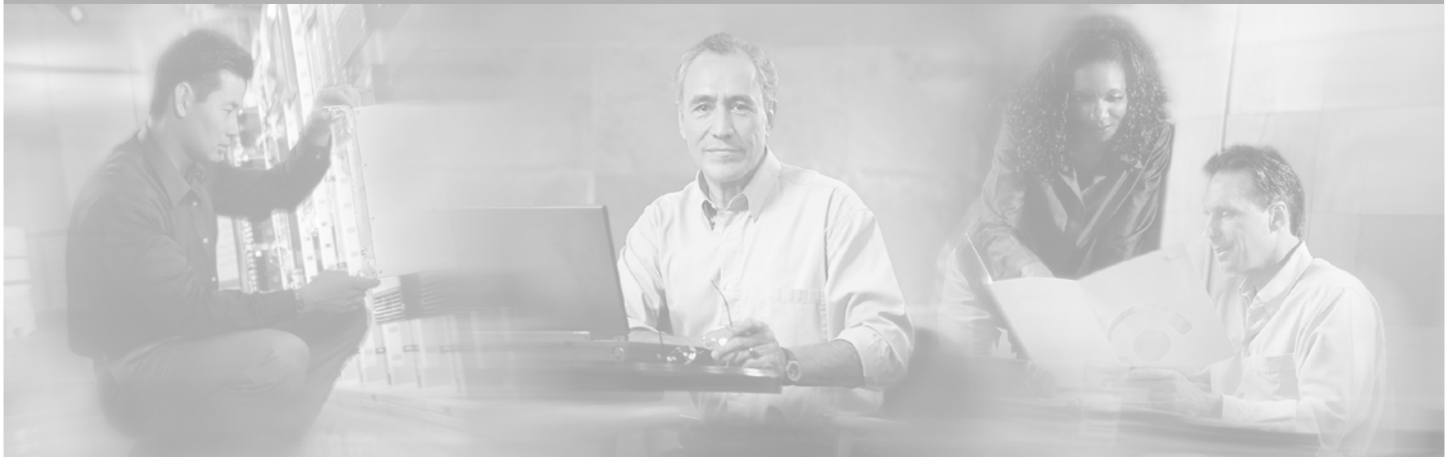


Getting Started with Cisco Network Assistant

Version 5.1

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

Text Part Number: OL-6194-06

Getting Started with Cisco Network Assistant

CONTENTS

Preface

Audience

This guide is for system administrators, network managers, and other users who want to manage standalone network devices and device groups through a GUI. It presents Cisco Network Assistant, known as Network Assistant, as a solution.

Purpose

The purpose of this guide is to give users information to start using Network Assistant. It consists of these chapters:

Introduction—What Network Assistant is and what it does.

Network Assistant Features—How to use Network Assistant to manage devices and networks.

Installing, Starting, and Connecting Network Assistant—How to install Network Assistant on your workstation, start it, and connect it to a network device.

Planning and Creating Communities—The concepts and procedures for planning and creating communities by using Network Assistant. The concept of clusters is supported for backward compatibility.

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 and released regularly. 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 Support 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 these announcements 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. Registered users can access the tool at this URL:

http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

To register as a Cisco.com user, go to this URL:

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

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Support 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 Support Website

The Cisco 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 at this URL:

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

Access to all tools on the Cisco 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 Before you submit a request for service online or by phone, use the **Cisco Product Identification Tool** to locate your product serial number. You can access this tool from the Cisco Support website by clicking the **Get 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. After using the Search box on the Cisco.com home page, click the **Advanced Search** link next to the Search box on the resulting page 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 Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

  http://www.cisco.com/offer/subscribe

- 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

- *Internet Protocol Journal* is a quarterly journal published by Cisco 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, 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

CHAPTER 1

What Is Network Assistant?

Network Assistant is an application that you can use to manage standalone devices and device groups—communities and clusters—from anywhere in your intranet. Using its GUI, you can perform multiple configuration tasks without using command-line interface (CLI) commands. You can apply actions to multiple devices and ports at the same time for VLAN and quality of service (QoS) settings, inventory and statistics reports, link and device monitoring, software upgrades, and many other networking features.

Network Assistant gives you two graphical views of a device group:

- A topology view, which shows devices that are in a community, a cluster, or that are eligible to join the community or cluster, link information between devices, and other connected clusters.
- A front-panel view, from which you can monitor the real-time status of the devices and do many configuration tasks. The devices and port LEDs in the view look like the physical devices and the port LEDs.

A community is a device group that can contain up to 40 connected network devices. Network Assistant uses the Cisco Discovery Protocol (CDP) automatic discovery capability to find eligible network devices and to add them to a community. When a network device is added to a community, it becomes a *member device*. Network Assistant manages, configures, and monitors each member on an individual basis. Each member must have an IP address assigned to it.

Most Cisco network devices that have IP addresses, such as routers, switches, and access points, can belong to a community. For a specific list of network devices, see the release notes. For information on community limitations, see the "Community Device Limit" section on page 4-2.

The main reason for creating a community is so that you can manage Cisco cluster-capable devices as well as noncluster-capable devices in the same logical group, regardless of their physical locations and the software installed on the devices. Network Assistant supports the creation, modification, deletion, and management of multiple communities.

A cluster is a device group that can contain up to 16 connected network devices, but they have to be cluster-capable Catalyst devices. The devices belong exclusively to one cluster; they do not participate in other clusters. You assign an IP address to a device that will become the *command device*. The IP address of the command device is the single point of access that Network Assistant uses to configure, manage, and monitor the command device and the member devices.

A community offers these benefits that a cluster does not:

- Communities can manage routers, access points, and switches. Clusters can only manage switches.
- The device limit for communities is 40, but the device limit for clusters is 16.

- Network Assistant can communicate securely with every member in a community. In a cluster, Network Assistant communicates with member devices through the command device, but the communication is secure only between Network Assistant and the command device. It is not secure from the command device to member devices.
- If a community member fails, Network Assistant can continue to manage the other members. If a cluster command device fails, Network Assistant cannot manage the other members of the cluster unless a cluster standby device has been configured.
- Communities have fewer restrictions than clusters about where members are located and how they are connected to each other. For more information on cluster member restrictions, see the online help.
- If candidate devices do not have CDP enabled, you can still create a community and manually add the devices. Clusters cannot be created unless CDP is enabled on all the candidate devices.

Network Assistant features include front panel and topology views of device groups. See Chapter 2, “Network Assistant Features,” for more information.

For information on setting up communities, see Chapter 4, “Planning and Creating Communities.”

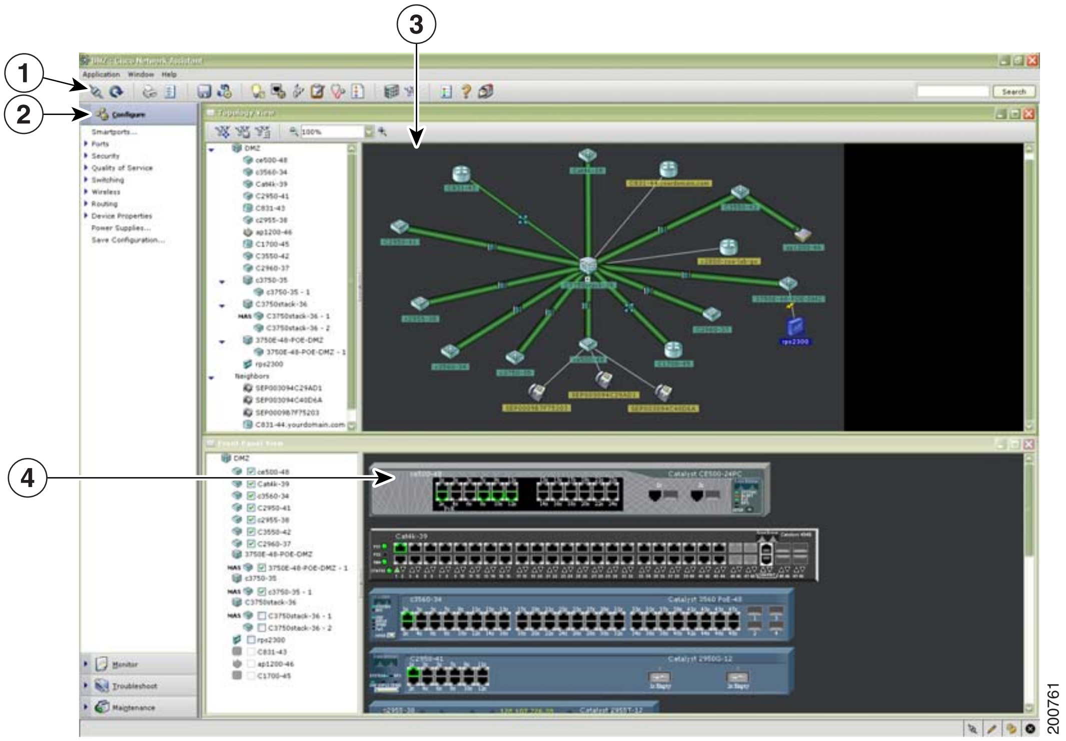
For information on setting up device clusters, see Chapter 4, “Planning and Creating Clusters” of the Getting Started with Cisco Network Assistant document, version 1.0.

CHAPTER 2

Network Assistant Features

Network Assistant simplifies the management of communities or clusters by offering a GUI, alternative modes for configuring network devices, two levels of access, and comprehensive online help. Figure 2-1 shows the main features of the GUI.

Figure 2-1 Network Assistant GUI



1	Toolbar	**3**	Topology view
2	Feature bar	**4**	Front Panel view

The following sections describe the Network Assistant features.

Front Panel View

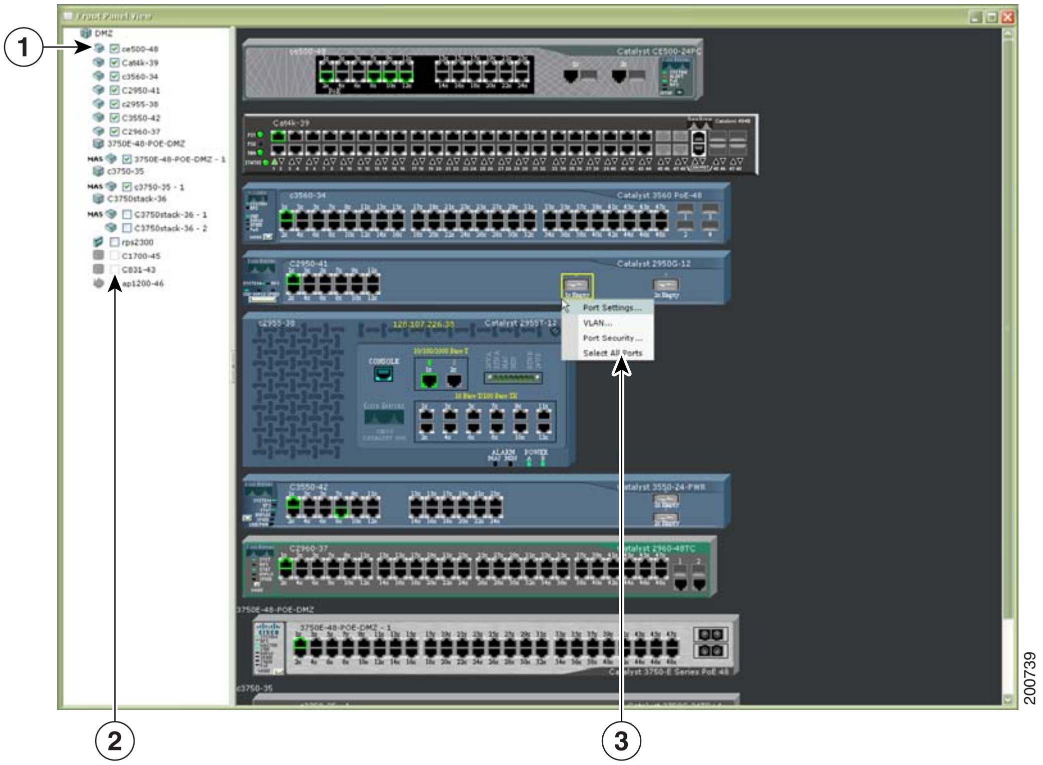
When Network Assistant connects to a community or a cluster, you can display the Front Panel view by clicking Front Panel on the toolbar or by choosing **Monitor > View > Front Panel** on the feature bar. You see the front-panel image of the device. If the device belongs to a community, you see all of the devices that were selected the last time that the front panel view appeared for that community. If the device commands a cluster, you see the cluster members that were selected the last time that the view was displayed.

By using the Front Panel view, you can

- Drag and re-arrange the devices that appear.
- Select and configure the devices.
- Right-click a port and configure it.
- Select multiple ports, on the same device or on different devices, and configure the ports at the same time.

Figure 2-2 shows a community with these members: Catalyst 4948, 3750, 3560, 3550, 2960, 2955, and 2950 switches and a Catalyst Express 500 switch.

Figure 2-2 Front Panel View and Port Popup Window



1	Member devices	**3**	Settings popup window
2	Check boxes to show devices		

Topology View

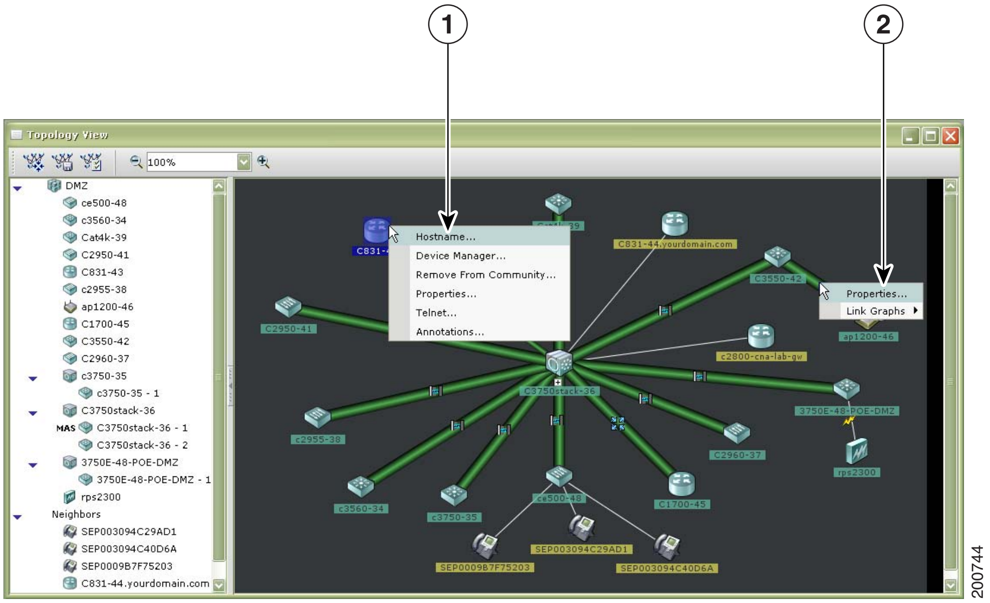
When Network Assistant connects to a community or a cluster, the Topology view appears by default. If you change this default, you can see the Topology view by clicking Topology view on the toolbar or by choosing **Monitor > Views > Topology**.

Note You can change the preferences in Network Assistant to show the Front Panel view by default by choosing **Application > Preferences > Show Front Panel View when connected to network**. If you no longer want Network Assistant to show the Topology view by default, deselect **Show Topology View when connected to a network**.

The Topology view shows how the devices within a community or a cluster are connected. If you manage a community, you can see the VLAN links by highlighting them. You can make neighboring devices members of the community or cluster, or you can remove members.

The Topology view in Figure 2-3 shows the members of a community and the neighboring devices discovered by Network Assistant. When you right-click a device or a link icon, a popup window appears.

Figure 2-3 Topology View and Device Popup Windows



1	Device popup window	**2**	Link popup window

Note When you are managing a community, the Topology view displays all the devices in that community. To display a different community, you must connect to that community.

When you are managing a cluster, the Topology view displays only the cluster and the network neighborhood of the specific command or member device that you access. To display a different cluster, you must access the command device or a member device of that cluster.

Menu Bar, Toolbar, and Feature Bar

Configuration and monitoring options are available on the menu bar, the toolbar, and the feature bar. The menu bar provides options for configuring communities and Network Assistant itself. The options on the feature bar are for configuring devices, ports and VLANs, for monitoring, and for getting reports.

Menu Bar

The menu bar provides these options for managing Network Assistant, navigating among windows, and accessing online help:

- Application—Choose printing options, select interaction modes, set user preferences, search for and install Network Assistant updates, show or hide the feature bar, create and modify communities, and request system message notifications.
- Window—Navigate to open Network Assistant windows.
- Help—Open the online help.

Toolbar

The toolbar has icons and buttons for commonly used configuration options and for information windows such as the legend and the online help. Table 2-1 lists the toolbar options from left to right on the toolbar.

Table 2-1 Toolbar Icons and Buttons

Toolbar Option	Icon	Task
Connect	🔌	Connect Network Assistant to a community, a cluster, or a standalone device.
Refresh	🔄	Update the views with the latest status.
Print	🖨	Print a Network Assistant window or help topic.
Preferences	📋	Set Network Assistant display properties, choose the views to open when Network Assistant is connected, and choose how often Network Assistant searches for an update.
Save Configuration[1]	💾	Save the configuration of the devices to your PC.
Software Upgrade[1]		Upgrade the software on one or more devices.
Smartports[1]	💡	Display or configure Smartports setup on a device.
Port Settings[2]	⚙	Display and configure port parameters on a device.

Table 2-1 Toolbar Icons and Buttons (continued)

Toolbar Option	Icon	Task
VLANs[1]		Display VLAN membership, assign ports to VLANs, and change the administration mode.
Inventory	📋	Display the device type, the software version, the IP address, and other information about a device.
Health	🩺	Monitor measurements that show the health of your managed devices.
Event Notification		Display messages about network and device events.
Front Panel		Display the Front Panel view.
Topology		Display the Topology view.
Legend	☰	Display the legend, which describes the icons, labels, and links.
Help for Active Window	?	Display the help topic for the active, open window. You can also click **Help** from the active window or press the **F1** key.
Feedback	📬	Open a Web page where you can leave feedback about your experience with Network Assistant.
Search	Search	Enter terms in the field at the right of the toolbar, and click the **Search** button to search the online help.

[1] Not available in read only mode. For more information about the read only and read-write access modes, see the "Privilege Levels" section on page 2-8.

[2] Some options from this menu option are not available in read only mode.

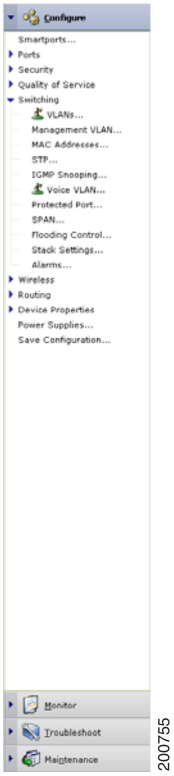
Feature Bar

The feature bar shows the networking features that are available for the devices in your community or cluster. By default, the feature bar is in standard mode. In this mode, it is always visible, and you can reduce or increase its width. In autohide mode, the feature bar appears only when you move the cursor to the left edge of the Network Assistant workspace.

- To see the feature bar in standard mode, click **Application > Feature Bar**, and select **Standard Mode**.
- To hide the feature bar, click **Application > Feature Bar**, and select **Autohide Mode**.

Figure 2-4 shows a feature bar.

Figure 2-4 ***Feature Bar***



The features are grouped under menus. When you click a menu item, the configuration window for the feature appears.

Access modes affect the availability of features; some are not available in read only mode. For more information about how access modes affect Network Assistant, see the "Privilege Levels" section on page 2-8.

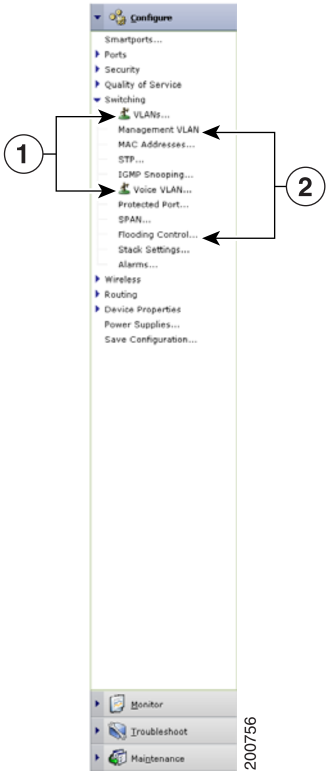
Interaction Modes

There are two modes for interacting with the Network Assistant GUI: guide mode and expert mode. Guide mode presents feature options one step at a time, with accompanying help information. Expert mode presents all the options for configuring a feature in a single window. For help, click **Help** in the window.

Guide Mode

Network Assistant is in expert mode by default. When you choose a feature on the feature bar with a signpost icon (see Figure 2-5), you see a series of configuration steps—guide mode. If you choose a feature without this icon, you see a configuration window—expert mode.

Figure 2-5 Guide Mode Signposts



1	Guide mode icon	**2**	Menu items that support only the expert mode

Guide mode is not available if your switch access level is read only. For more information about the read only access mode, see the "Privilege Levels" section on page 2-8.

Expert Mode

If you prefer to see a configuration window for every feature, choose **Expert** in the **Application** menu, or click **Expert** on the toolbar. Even the features that appear with a signpost on the feature bar appear in expert mode. If you want to see guide mode again, choose **Guide** in the **Application** menu, or click **Guide** on the toolbar.

To start a guide-mode feature in **Expert** mode, you must choose **Expert** *before* selecting the feature.

Wizards

All wizards contain *Wizard* in their names on the feature bar. Like guide mode, wizards provide a step-by-step approach for completing a specific configuration task. Unlike guide mode, wizards do not prompt you to enter information for all of the feature options. Instead, they prompt you to enter minimal information and use the default settings of the remaining options to set default configurations.

Wizards are not available for read only access levels. For more information about the read only access mode, see the "Privilege Levels" section.

Smartports

Network Assistant detects where you have not used Smartports to configure a device connection and provides this information in the Event Notification window. You can configure the connection either manually or based on suggestions provided by Network Assistant. Open the Smartports window to either select a role to apply or use Smartports to suggest a role to apply. See the online help for more information on Smartports.

Privilege Levels

Network Assistant provides two types of access to configuration options: read write and read only. Your access type is determined by your privilege level, a number from 1 to 15. Privilege levels correspond to these access types:

- Level 15 provides read write access.
- Levels 1 to 14 provide read only access. Any options in the Network Assistant windows, feature bar, toolbar, and popup windows that change the device, community, or cluster configuration are enabled for read only access. This means that you cannot modify the configuration shown in the windows started by these items.

By default, Network Assistant tries to log you on with privilege level 15. However, this normally requires that you pass the authentication with a proper username and password. Lower levels do not generally impose this requirement.

Note You must have privilege level 15 to access Network Assistant through a TACACS+ or a RADIUS server.

Searching for a Network Assistant Update

Network Assistant can search Cisco.com to see whether new packages are available. Use either of these actions to request a search:

- Choose **Application > Preferences**, and use the Preferences window to request an automatic search every week or every month.
- Choose **Application > Application Updates** to request an immediate search for updates.

If an update is found, you can install it through Network Assistant.

Online Help

Network Assistant provides comprehensive online help that explains configuration and monitoring tasks.

Sometimes the information in a help topic differs for different devices. In these cases, the right pane of the Help window contains all the versions of the topic, each labeled with the hostnames of the devices it applies to.

Online help includes these features:

- Conceptual help that gives background information on networking features
- Window help that gives procedures for performing tasks
- An index of online help topics
- A tab for requesting a search of all the online help topics
- A glossary of terms used in the online help

CHAPTER 3

Installing, Starting, and Connecting Network Assistant

This chapter describes installation requirements for Network Assistant, how to install it, how to start it, and how to connect it to a device or an existing community.

Installation Requirements

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

- Processor speed: 1 GHz
- DRAM: 512 MB minimum, 1024 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

Network Assistant is supported on these operating systems:

- Windows XP, Service Pack 1 or later
- Windows 2000, Service Pack 3 or later (Windows Server 2003 SP1+ is also supported)

64-bit Windows versions are not tested or officially supported. You will need write permission to your home directory and to the Network Assistant installation directory so Network Assistant can create the necessary log files and preference files.

Installing Network Assistant

To install Network Assistant on your PC, follow these steps:

1. Go to this web address: http://www.cisco.com/go/NetworkAssistant.

   You must be a registered Cisco.com user, but you need no other access privileges.

2. Find the Network Assistant installer file , cna-windows-k9-installer-5-0-en.exe.
3. Download the Network Assistant installer, and run it. (You can run it directly from the web if your browser offers this choice.)

   Network Assistant is free—there is no charge to download, install, or use it.

When you run the installer, follow the displayed instructions. In the final panel, click **Finish** to complete the Network Assistant installation.

Starting Network Assistant

After Network Assistant is installed, you see its icon on your desktop, a Network Assistant shortcut under the **Start** menu, and a Network Assistant entry under **Start > Programs**. When you click any of these, you see a partial Network Assistant GUI and the Connect window.

In disconnect mode, Network Assistant is not connected to a device or a community; it cannot manage a standalone device, a community, or the command device of a cluster. Its menu bar and toolbar support only the tasks that customize Network Assistant itself. The feature bar, which usually lists device features, is empty.

Connecting Network Assistant to a Community or a Cluster

To connect Network Assistant to a device, use the Connect window shown in Figure 3-1. In it, enter the IP address of the device to which you want to connect. For an existing community, select its name from the pull-down menu. For an existing cluster, select the IP address. Click **Options** if you want to

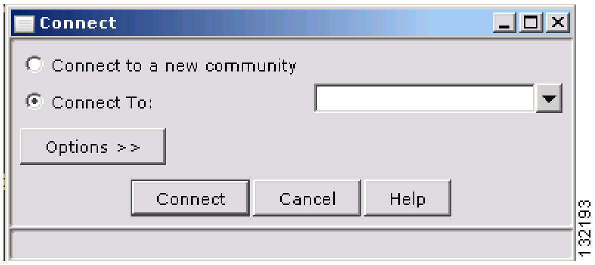
- Communicate with a cluster command device or standalone device by using HTTPS (secure HTTP) instead of HTTP.
- Use an HTTP port other than 80 on cluster command devices or standalone devices.
- Connect with read-only access.

Note To learn about HTTPS and HTTP options in a community, see the "Communication Protocols" section on page 4-3.

Because Catalyst 4500 series switches ship with HTTP and HTTPS disabled by default, you must enable them as needed. HTTPS v3.0 is supported in Cisco IOS 12.2(25)SG cryptographic versions and later.

For instructions on how to use the **Connect to a new community** option to create a community, see the "Creating a Community" section on page 4-3. When you click **Connect**, you are either connected to the community directly, or you are prompted for a username and password and then connected. When you connect to a cluster, Network Assistant asks if you want to convert the cluster to a community. For more information on converting a cluster to a community, see the "Converting a Cluster to a Community" section on page 4-4.

Figure 3-1 Connect Window



When the connection occurs, the Network Assistant window is in *connect* mode. The toolbar adds icons that represent device features. Similarly, the feature bar fills with menus that list the device features that Network Assistant manages.

Access Modes in Network Assistant

When you select a community to manage, you can set the access mode and access level. If you do not set the access mode before connecting to the community, Network Assistant applies the read/write access mode to all the devices in the community.

Event Notification

Network Assistant informs you of events that it detects by putting an event icon on the status bar and under devices in the Topology view. Clicking an event icon opens a window that describes the event and, whenever possible, connects you to the windows where you can take the needed actions.

CHAPTER 4

Planning and Creating Communities

This chapter provides the concepts and procedures for planning and creating communities by using Network Assistant. For information on using Network Assistant to configure communities, refer to the online help.

Planning a Community

This section describes the guidelines, requirements, and caveats that you should understand before you create a community.

Candidate and Member Characteristics

Candidates are network devices that have IP addresses but that have not been added to a community. Members are network devices that have been added to a community.

To join a community, a candidate must meet these requirements:

- It has an IP address.
- It has HTTP or HTTPS enabled on the default ports.

Note You cannot add clusters to a community. You can add cluster members individually.

If you add a cluster command device to a community, the other members of the cluster are not added automatically. To manage the cluster members, you must add them individually to the community.

If you add a Catalyst 3750 switch stack master to a community, the individual stack members are automatically added to the community, even though the stack members do not appear in the Modify Community or Discover windows. However, when you connect to the community, the stack members do appear in the Front Panel and Topology views.

Community Device Limit

The combined number of Catalyst switches, Cisco access routers, and PIX firewalls in a community cannot exceed 40. There are no limits on individual device types. There is no limit on the number of Cisco Aironet Access Points.

Note Even though the devices in a Catalyst 3750 switch stack function as a single switch, they count as individual switches against the combined limit and individual device limits.

If the limit of 40 devices is exceeded, you cannot manage a community. You need to remove devices so that the total is not more than 40.

There is no limit to the number of communities that Network Assistant can manage.

Automatic Discovery of Candidates and Members

Beginning with the IP address for a starting device and the port numbers for the HTTPS and HTTP protocols, Network Assistant uses CDP to compile a list of community candidates that are within four CDP hops of the starting device. Network Assistant can discover candidate and member devices across multiple networks and VLANs if they have valid IP addresses. See the "Candidate and Member Characteristics" section on page 4-1 for a list of requirements that network devices must meet in order to be discovered.

Note Do not disable CDP on candidates, members, or any network devices that you might want Network Assistant to discover.

You can edit the list of discovered devices to fit your needs and to add them to the community. If Network Assistant does not discover a network device, you can manually add the device.

For instructions on adding discovered devices to a community or manually adding devices to a community, see the "Manually Adding Members" section on page 4-4.

Community Names

When you create a community, Network Assistant requires that you assign a name to it. The name can contain up to 64 alphanumeric characters and is not case sensitive.

Note When you select a name in the Connect window and a cluster and a community share that name, Network Assistant connects to the community.

Hostnames

You do not need to assign a hostname to a community member, and Network Assistant does not assign one by default. However, Cisco IOS assigns the hostname *Switch* to switches without a hostname. Therefore, you might want to assign hostnames to switches to avoid confusing them.

Passwords

When connecting to a community, Network Assistant prompts you for each unique password that has already been assigned for members of the community. Network Assistant attempts to use these passwords to connect to other devices. You are prompted for a password only if the previously entered password does not work for a device.

For example, if a community has ten members, and five members share one password and the other five share a different password, Network Assistant prompts you twice, once for each password. Network Assistant does not save the passwords to your PC, so it prompts you for the passwords each time that you attempt to connect to a community.

Communication Protocols

Network Assistant uses HTTPS and HTTP to communicate with community members. It first tries to use HTTPS when using CDP to discover neighboring devices and when devices are added manually. If HTTPS fails, it tries again with HTTP.

The HTTPS port is fixed at 443; the HTTP port defaults to 80. You can specify a different HTTP port when you create a community. Afterward, you use the HTTP Port window to change the HTTP port. The port settings for both HTTPS and HTTP must be the same for all the members of a community.

Community Information

Network Assistant saves all individual device information, such as the IP address, the hostname, and the communication protocol, to your local PC. When Network Assistant connects to a community, it uses the locally saved data to rediscover the member devices.

If you try to use a different PC to manage an existing community, none of the member device information is available. You need to create the community again and add the same member devices.

Creating a Community

There are three ways to create a community:

- By discovering candidates that you can add to the community
- By manually adding devices
- By using the Cluster Conversion Wizard to convert a cluster into a community

You should verify that the community contains the devices that you think it contains. This section tells you how to perform these tasks.

Discovering and Adding Devices

Follow these steps to compile a list of candidate devices and to add them to a community:

1. Start Network Assistant, and select **Connect to a new community** in the Connect window. Click **Connect**.
2. In the Create Community window, enter a name for the community.

3. Click the **Advanced** button if you want to set an HTTP port other than 80, the default port. Enter the HTTP port number that you want to use. Click **OK**.
4. Enter the IP address for the starting device, and click **Discover Neighbors**.
5. In the Devices Found list, select candidate devices that you want to remove.
    a. To remove more than one candidate, press **Ctrl** and make your choices, or press **Shift** and choose the first and last device in a range.
    b. Click **Remove**.
6. Click **Add All To Community** to add the remaining devices in the list to the community.

Manually Adding Members

Network Assistant provides two ways to manually add devices to a community.

1. In the Create Community window, enter the IP address for the device that you want to add.
2. Click **Add to Community**.

The second way to manually add a device uses the Topology view:

1. If the Topology view does not appear, choose **View > Topology** from the feature bar.
2. Right-click a candidate icon, and select **Add to Community**.

    Candidate device labels are cyan; member labels are green.

Converting a Cluster to a Community

The Cluster Conversion Wizard creates a community by using the information available for the cluster. The wizard prompts you to enter an IP address and from the pulldown lists to select an interface name and subnet mask for each device that does not have them. Network Assistant does not delete the cluster upon creating the community.

There are two ways to start the Cluster Conversion Wizard. When you connect to a cluster command device, the wizard startes and asks if you want to convert the cluster into a community. You can also start the wizard from the feature bar by choosing **Configure > Cluster > Cluster Conversion Wizard**.

Verifying a Community

Follow these steps to verify the community:

1. Choose **Monitor > View > Topology** to display the Topology view.
2. Choose **Monitor > Reports > Inventory** to display an inventory of the devices in the community.

    This summary includes device model numbers, serial numbers, software versions, IP information, and location.
3. Choose **Monitor > View > Front Panel** to display the Front Panel view.

APPENDIX A

Configuring a Catalyst 4500 Series Switch for Network Assistant Management

This appendix describes how to configure a Catalyst 4500 series switch for Network Assistant. It also lists the Network Assistant feature defaults for the switch.

Note For complete information on configuring Network Assistant on the Catalyst 4500 series switch, refer to the "Configuring the Catalyst 4500 Series Switch with Cisco Network Assistant" chapter in the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*.

Note For complete syntax and usage information for the switch commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at this location: http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/index.htm.

This appendix contains these topics:

- Network Assistant-Related Features and Their Defaults, page A-1
- Configuring Your Switch for Network Assistant, page A-2

Network Assistant-Related Features and Their Defaults

Table 1 lists the Network Assistant-related configuration parameters on a Catalyst 4500 series switch.

Table 1 Network Assistant-Related Configuration on a Catalyst 4500 Series Switch

Feature	Default Value	Recommended Value
Authentication	Disabled	Optional
IP address	Depends on community or discovery option[1]	User selectable
IP HTTP port number	80	Optional[2]
IP HTTPS port number	443	Optional[3]
IP HTTP server	Disabled	Enabled[4]
Cluster run	Disabled	Enabled[5]

1. You need to set an IP address in each switch for community device discovery and for the cluster commander.
2. Port number on the Network Assistant and the Catalyst 4500 series switch must match.
3. You can only change this value for a cluster of devices. Port number on the Network Assistant and on the Catalyst 4500 series switch must match. Value can be changed to any non-default number above 1024.
4. Required for Network Assistant to access the device.
5. Enabled only if you want to manage a cluster of devices.

Configuring Your Switch for Network Assistant

These topics are discussed:

- Minimum Configuration to Access Catalyst 4500 from Network Assistant, page A-2
- Additional Configuration Required to Manage a Community, page A-3
- Additional Configuration Required to Manage a Cluster, page A-3

Minimum Configuration to Access Catalyst 4500 from Network Assistant

If you use the default configuration, access the Catalyst 4500 series switch, and enter the **ip http server** (for HTTP) or the **ip http secure-server** (for HTTPS) global configuration command:

	Command	Purpose
Step 1	Switch# **configure terminal**	Enter global configuration mode.
Step 2	Switch(config)# **ip http server** or Switch(config)# **ip domain-name** *domain_name*	(HTTP only) Enable the HTTP server on the switch. By default, the HTTP server is disabled. Enable the domain name on the switch to configure HTTPS.
Step 3	Switch(config)# **ip http secure-server**	Enable the HTTPS server on the switch. By default, the HTTPS server is disabled.
Step 4	Switch(config)# **ip http max-connections** *connection_number*	Configure the maximum concurrent connections to the HTTP server. We recommend using 16 as the *connection_number*.
Step 5	Switch(config)# **ip http timeout-policy idle** *idle_time* **life** *life_time* **requests** *requests*	Configure the HTTPS port. The **idle** keyword specifies the maximum amount of time a connection can stay idle. We recommend an idle value of 180 seconds. The **life** keyword specifies the maximum amount of time that a connection can stay open since it was established. We recomend a life value of 180 seconds. The **requests** keyword specifies the maximum amount of requests on a connection. We recommend a maximum of 25 requests.
Step 6	Switch(config-if)# **end**	Return to privileged EXEC mode.
Step 7	Switch# **show running-config**	Verify the configuration.

Additional Configuration Required to Manage a Community

Note If you have enabled clustering, disable clustering before configuring a community.

If you plan to use a community, define an IP address on each switch:

	Command	Purpose
Step 1	Switch# **configuration terminal**	Enter global configuration mode.
Step 2	Switch(config)# **interface** {**vlan** *vlan_ID* | {**fastethernet** | **gigabitethernet**} *slot/interface* | **Port-channel** *number*}	Select an interface.
Step 3	Switch(config-if)# **ip address** *ip_address address_mask*	(Optional) Assign an IP address to the Catalyst 4500 series. **Note** This step is mandatory if the switch is part of community or is a cluster command switch. This step is optional if the switch is a cluster member candidate.
Step 4	Switch(config-if)# **end**	Return to privileged EXEC mode.
Step 5	Switch# **show running-config**	Verify the configuration.

Additional Configuration Required to Manage a Cluster

If you plan to use clustering, enter the **cluster run** global configuration command on each device, and enter the **ip address** interface configuration command on the cluster commander:

	Command	Purpose
Step 1	Switch# **configuration terminal**	Enter global configuration mode.
Step 2	Switch(config)# **cluster run**	Enable clustering. **Note** Enable clustering on all switches that are part of the potential cluster.
Step 3	Switch(config)# **cluster enable**	Name the cluster.
Step 4	Switch(config)# **interface** {**vlan** *vlan_ID* | {**fastethernet** | **gigabitethernet**} *slot/interface* | **Port-channel** *number*}	Select an interface.
Step 5	Switch(config-if)# **ip address** *ip_address address_mask*	(Optional) Assign an IP address to the Catalyst 4500 series switch cluster master. **Note** This step is mandatory if the switch is part of a community or is a cluster command switch. This step is optional if the switch is a cluster member candidate.

	Command	Purpose
Step 6	`Switch(config-if)# end`	Return to privileged EXEC mode.
Step 7	`Switch# show running-config`	Verify the configuration.

INDEX