Getting Started with Cisco Network Assistant

Version 4.1

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-6194-05

Getting Started with Cisco Network Assistant

Preface v

Audience v

Purpose v

Obtaining Documentation v

Cisco.com v

Product Documentation DVD vi

Ordering Documentation vi

Documentation Feedback vi

Cisco Product Security Overview vi

Reporting Security Problems in Cisco Products vii

Obtaining Technical Assistance viii

Cisco Technical Support & Documentation Website viii

Submitting a Service Request viii

Definitions of Service Request Severity ix

Obtaining Additional Publications and Information ix

CHAPTER 1 **What Is Network Assistant?** 1-1

CHAPTER 2 **Network Assistant Features** 2-1

Front Panel View 2-2

Topology View 2-3

Menu Bar, Toolbar, and Feature Bar 2-4

Menu Bar 2-4

Toolbar 2-4

Feature Bar 2-5

Interaction Modes 2-7

Guide Mode 2-7

Expert Mode 2-8

Wizards 2-8

Smartports Advisor 2-8

Privilege Levels 2-8

Searching for a Network Assistant Update 2-9

Online Help 2-9

CHAPTER 3 **Installing, Starting, and Connecting Network Assistant** 3-1

Installation Requirements 3-1

Installing Network Assistant 3-1

Starting Network Assistant 3-2

Connecting Network Assistant to a Community or a Cluster 3-2

Access Modes in Network Assistant 3-3

Event Notification 3-3

CHAPTER 4 **Planning and Creating Communities** 4-1

Planning a Community 4-1

Candidate and Member Characteristics 4-1

Community Limits 4-2

Automatic Discovery of Candidates and Members 4-3

Community Names 4-3

Hostnames 4-3

Passwords 4-3

Communication Protocols 4-4

Community Information 4-4

Creating a Community 4-4

Discovering and Adding Devices 4-4

Manually Adding Members 4-5

Converting a Cluster to a Community 4-5

Verifying a Community 4-5

INDEX

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 Network Assistant makes it easy to manage devices and networks.

Installing, Launching, and Connecting Network Assistant—How to install Network Assistant on your workstation, launch 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. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

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

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

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

Ordering Documentation

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

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

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

Documentation Feedback

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

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

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

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

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

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

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

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

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

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.
- For Nonemergencies—psirt@cisco.com

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

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

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

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

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

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

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

Obtaining Technical Assistance

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

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

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

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

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

  or view the digital edition at this URL:

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

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

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

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

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

What Is Network Assistant?

Network Assistant is an application that manages 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 perform 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 20 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; therefore, 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 that can belong to a community, see the release notes. For information on community limitations, see the "Community Limits" 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 20, 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."

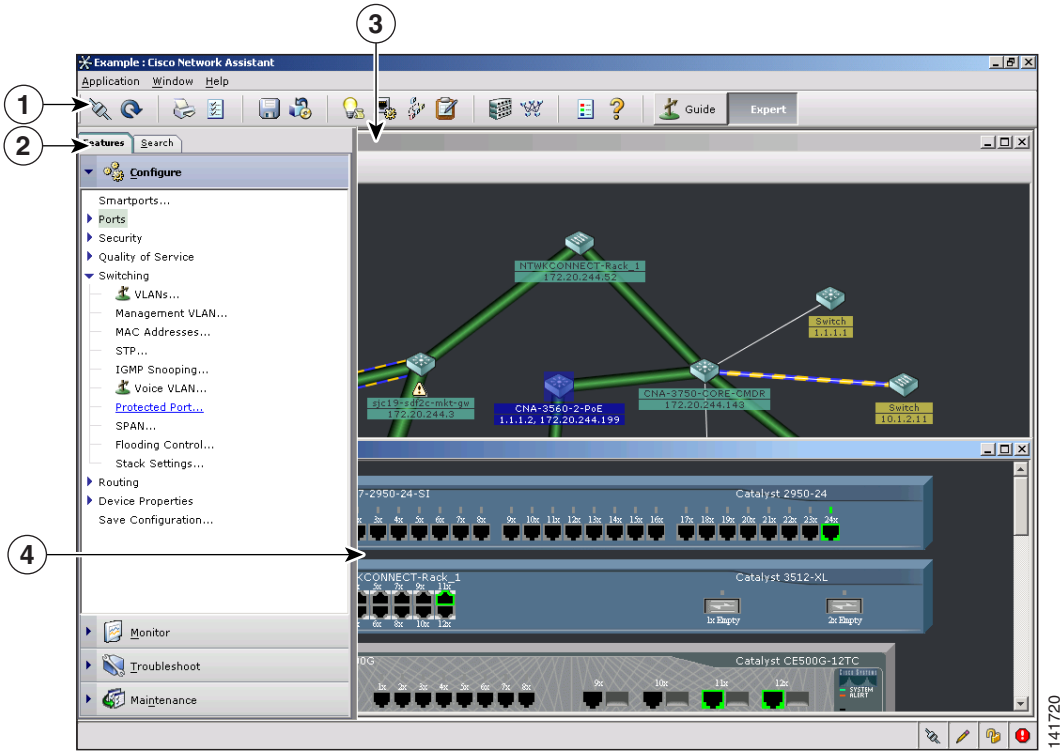
For information on setting up device clusters, see Chapter 4, "Planning and Creating Clusters" of the Getting Started with Cisco Network Assistant document, version 1.0.

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 sections that follow describe the Network Assistant features.

Front Panel View

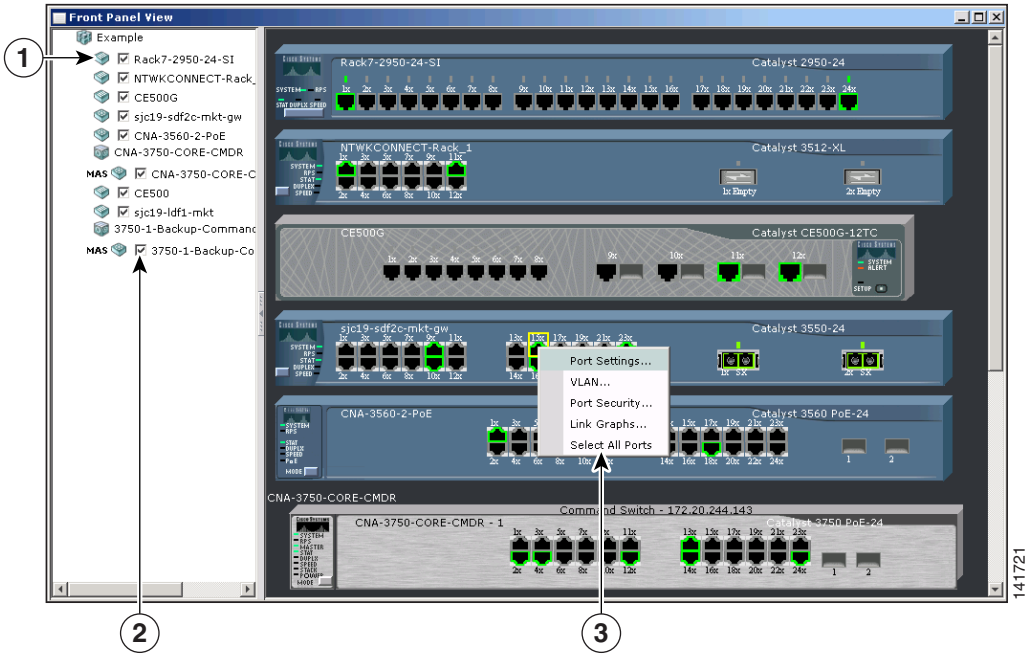
When Network Assistant connects to a community or a cluster, you can display the Front Panel view by clicking Front Panel on the toolbar or by choosing **Monitor > View > Front Panel** from the feature bar. You see the front-panel image of the device. If the device belongs to a community, you see all 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 Catalyst 3560, 2955, 2924, and 3750 switches as member devices.

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

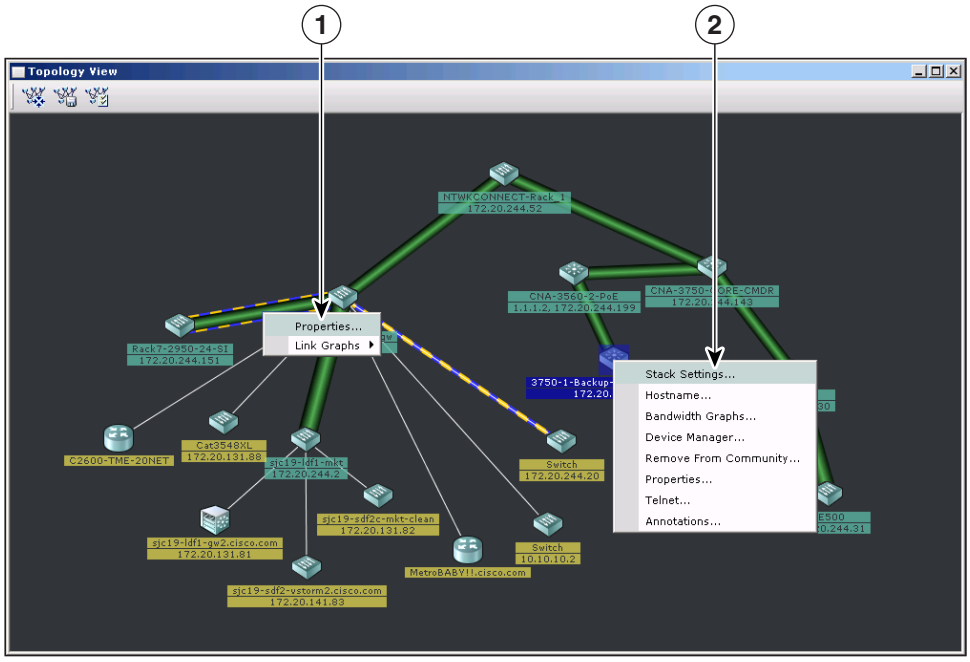
When Network Assistant connects to a community or a cluster, the Topology view appears by default. If you change this default, you can see the Topology view by clicking Topology view on the toolbar or by choosing **Monitor > Views > Topology**.

Note You can change the preferences in Network Assistant to also display 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	Link popup window	**2**	Device 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 from 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 for commonly used configuration options and for information windows like 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

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[1]		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[2]		Save the configuration of the devices to your PC.
Software Upgrade[2]		Upgrade the software on one or more devices.
Smartports		Display or configure Smartports setup on a device.
Port Settings[1]		Display and configure port parameters on a device.

Table 2-1 Toolbar Icons (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.
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.

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.

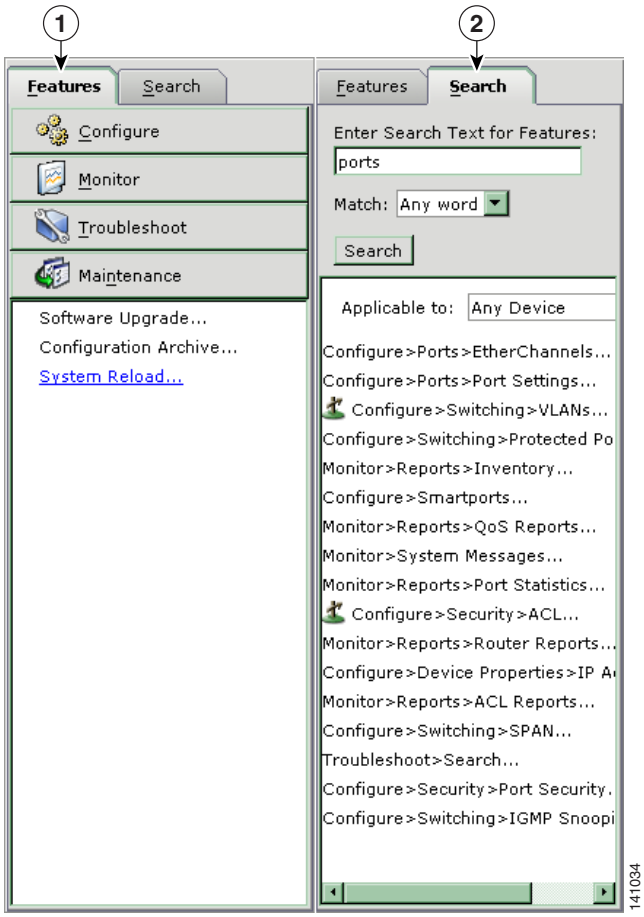
Feature Bar

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



1	Features tab	**2**	Search tab

On the Features tab, the features are grouped under menus. When you click a menu item, the configuration window for the feature appears. On the Search tab, you can launch a configuration window by entering search text, clicking **Search**, and selecting from the search results.

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.

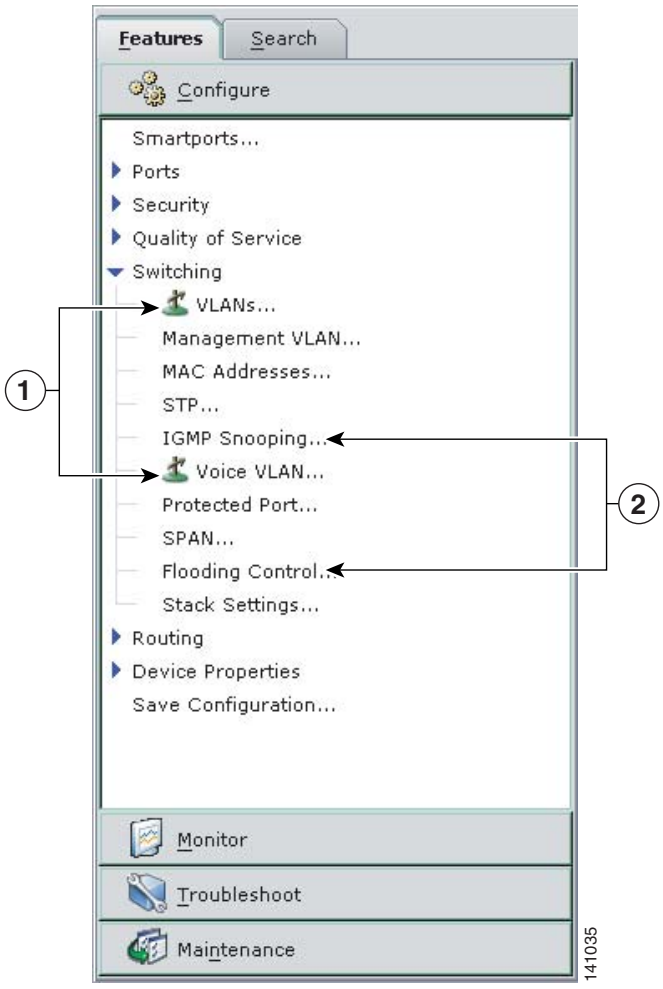
Interaction Modes

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; to get help, you 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 launch 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 Advisor

When Network Assistant detects that you have not used Smartports to configure a device connection, it recommends that you do so in the Event Notification window. From this window, you can start Smartports Advisor and configure the device connection. Smartports Advisor asks whether you want to use Smartports to apply Cisco-recommended configurations, or *roles*, to configure a port for optimal communication with the linked device.

Device connections are optimized wherever Smartports roles have been applied. Applying a role helps you configure the essential security, availability, quality of service (QoS), and manageability features on a device.

Smartports Advisor displays the front panels of devices to which you are connected. On the front panels, Smartports Advisor displays the ports to which Smartports roles have already been applied and the ports to which Smartports roles can be applied.

You apply roles to the port connections by accepting the role suggestions that Smartports Advisor makes, and then you enter the VLAN information. See the online help for more information on Smartports Advisor.

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 access types as follows:

- 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 users cannot modify the configuration shown in the windows launched 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. Take 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 glossary of terms used in the online help

You can send us feedback about the online help. Click **Feedback** on the Help window to display an online form. After completing the form, click **Submit** to send your comments to Cisco Systems Inc. We appreciate and value your comments.

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: 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

Network Assistant is supported on these operating systems:

- Windows XP, Service Pack 1 or later
- Windows 2000, Service Pack 3 or later

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, cna-windows-k9-installer-4-1-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

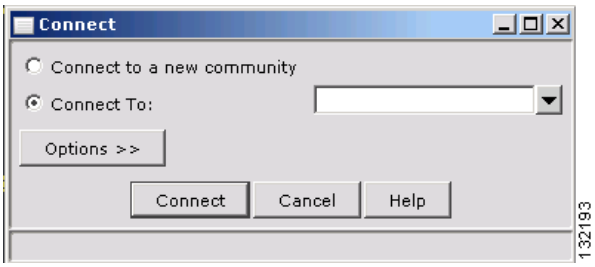
- Communicate with a cluster command device or standalone device by using HTTPS (secure HTTP) instead of HTTP.
- Use an HTTP port other than 80 on cluster command devices or standalone devices.
- Connect with read-only access.

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

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 4-4. 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 4-5.

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 default access mode to all the devices in the community.

Event Notification

Network Assistant informs you of events that it detects by putting a clickable 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.

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 its 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 have not been added to a community. Members are network devices that have actually 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 added to the community automatically, 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 Limits

The combined number of Catalyst switches, Cisco access routers, and PIX firewalls in a community cannot exceed 20.

For each of these device types, there are these individual limits:

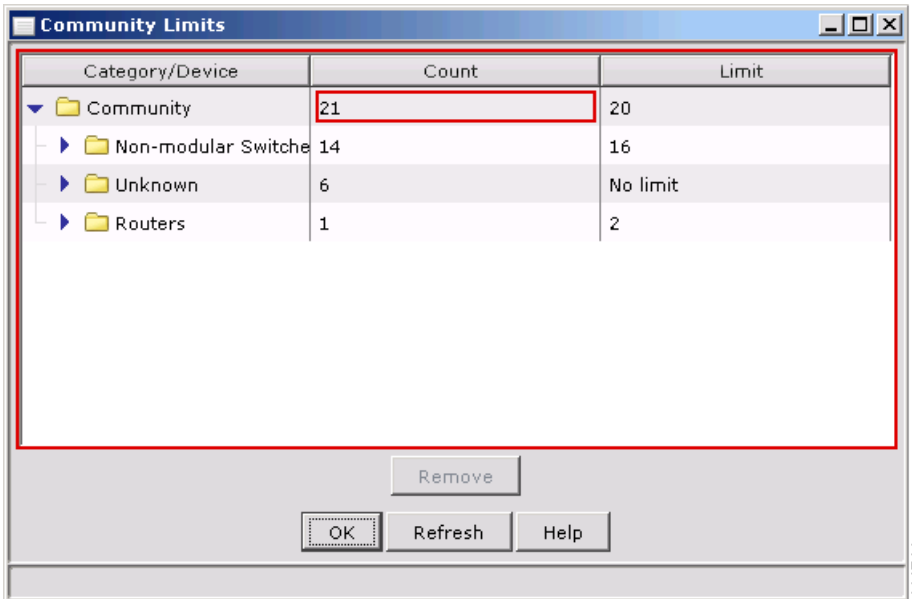
- 16 nonmodular Catalyst switches
- 4 modular Catalyst switches
- 2 Cisco access routers
- 2 PIX Firewalls

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.

When you create a community or add devices to a community, you cannot exceed the combined limit of 20 devices. Individual device limits are enforced when you connect to a community. If the combined or individual limits are exceeded, the window shown in Figure 4-1 appears. You cannot manage a community until you remove enough devices of the types that exceed the individual limits.

Figure 4-1 Community Limits Window



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 4-5.

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 launch the Cluster Conversion Wizard. When you connect to a cluster command device, the wizard launches and asks if you want to convert the cluster into a community. You can also launch 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.

A

accessing
  communites 4-3
automatic discovery
  adding members 4-4
  considerations
    connectivity 4-3
    non-CDP-capable devices 4-5
  in communities 4-3
  See also CDP

C

candidates
  automatic discovery in communities 4-4
CDP
  automatic discovery in communities 4-3
Cisco Discovery Protocol
  See CDP
Cluster Conversion Wizard 4-5
clusters
  Cluster Conversion Wizard 4-5
  converting to a community 4-5
  definition 1-1
  size limitation 1-1
communities
  accessing 4-3
  adding members 4-4
  advantages of 1-1
  automatic discovery 4-3, 4-4
communities (continued)
  candidates
    adding 4-4
    automatic discovery of members 4-3
    defined 4-1
    discovering 4-4
    requirements 4-1
    See also community member
  communication protocols 4-4
  community information 4-4
  community names 4-3
  composition 4-2
  converting a cluster to a community 4-5
  creating 4-4
  definition 1-1, 1-2
  limits 4-2
  management
    local PC 4-4
  members
    adding 4-5
    automatic discovery 4-3
    hostnames 4-3
    requirements 4-1
  planning considerations
    hostnames 4-3
    identifying information 4-4
    passwords 4-3
  saving identification information 4-4
  verifying 4-5
connecting Network Assistant 3-2
converting a cluster to a community 4-5

D

device limits in a community 4-2
discovery, communities
  See automatic discovery

E

expert mode 2-8

F

features
  expert mode 2-8
  Front Panel view 2-2
  guide mode 2-7
  menu bar 2-4
  online help 2-9
  privilege levels 2-8
  toolbar 2-4
  Topology view 2-3
  wizards 2-8
Front Panel view 2-2

G

guide mode 2-7

H

hostnames
  in communities 4-3

I

installing Network Assistant
  procedure 3-1
  requirements 3-1
interaction modes 2-7
IP addresses
  community candidates 4-1

L

launching Network Assistant 3-2

M

manually adding members to communities 4-5
members
  adding 4-4
  adding to a community 4-5
  automatic discovery 4-4
menu bar 2-4

N

Network Assistant
  connecting 3-2
  installing
    procedure 3-1
    requirements 3-1
  introduced 1-1
  launching 3-2

O

online help 2-9

P

passwords
  in communities 4-3
privilege levels 2-8

S

Smartports Advisor 2-8

T

toolbar 2-4
Topology view 2-3

W

wizards 2-8