



Getting Started with Cisco Network Assistant

Version 5.4

Americas 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: 408 527-0883

Text Part Number: OL-6194-07

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

Getting Started with Cisco Network Assistant
© 2004-2008 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface v

Audience i-v

Purpose i-v

Obtaining Documentation and Submitting a Service Request i-v

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 2-5

Feature Bar 2-6

Network Assistant Modes 2-8

Wizards 2-9

Smartports 2-9

Privilege Levels 2-9

Updates for Network Assistant 2-9

Online Help 2-10

CHAPTER 3

Installing Cisco Network Assistant 3-1

Installing Network Assistant 3-1

Starting Network Assistant 3-1

Connecting to Network Assistant 3-2

Event Notification 3-3

CHAPTER 4

Planning and Creating Communities 4-1

Planning a Community 4-1

Candidate and Member Characteristics 4-1

Community Device Limit 4-2

Automatic Discovery of Candidates and Members 4-2

Community Names 4-2

Hostnames	4-2
Passwords	4-3
Communication Protocols	4-3
Community Information	4-3
Creating a Community	4-3
Discovering and Adding Devices	4-3
Manually Adding Members	4-4
Converting a Cluster to a Community	4-4
Verifying a Community	4-4

APPENDIX A

Configuring a Catalyst 4500 Series Switch for Network Assistant Management A-1

Network Assistant-Related Features and Their Defaults	A-1
Configuring Your Switch for Network Assistant	A-2
Minimum Configuration to Access Catalyst 4500 from Network Assistant	A-2
Additional Configuration Required to Manage a Community	A-3
Additional Configuration Required to Manage a Cluster	A-3

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 to use Network Assistant to manage devices and networks.
- Installing 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 and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.





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. You can perform multiple configuration tasks without using command-line interface (CLI) commands. You can also 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 graphical user interface (GUI) provides these views:

- Topology view—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.
- Front-panel view—allows you to 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 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](#).

You can create a community to 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. With Network Assistant you can create, modify, delete, and manage 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.

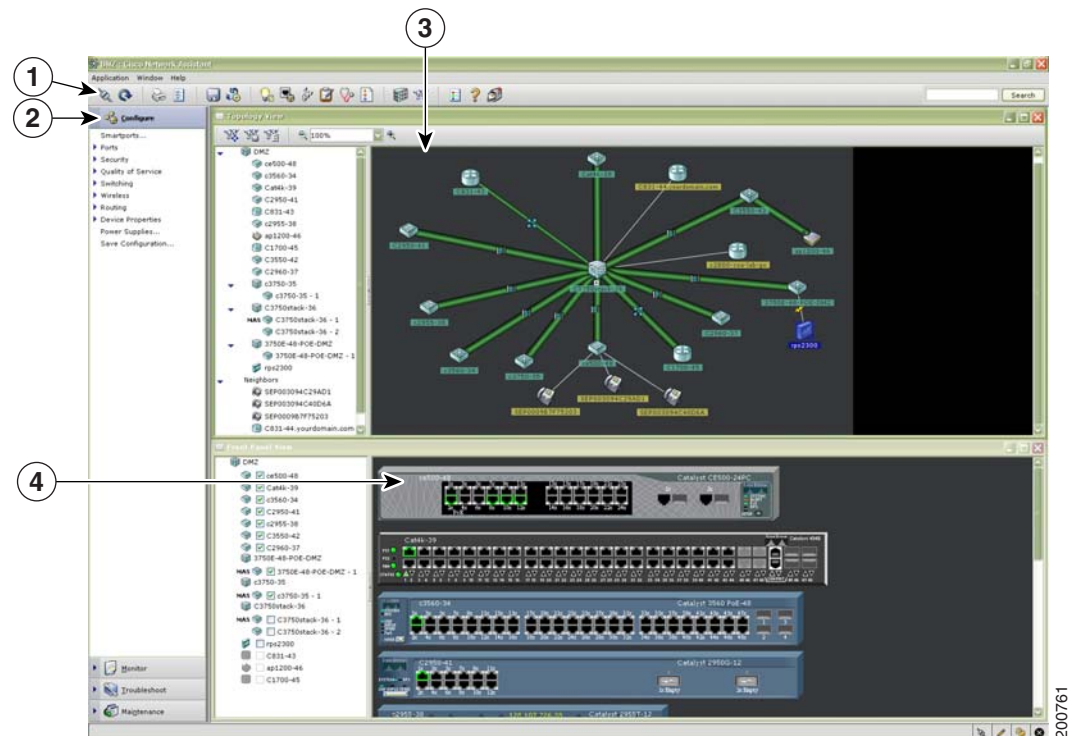


CHAPTER 2

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

These sections describe the Network Assistant features:

- [Front Panel View](#), page 2-2
- [Topology View](#), page 2-3

- [Menu Bar, Toolbar, and Feature Bar, page 2-4](#)
- [Network Assistant Modes, page 2-8](#)
- [Wizards, page 2-9](#)
- [Smartports, page 2-9](#)
- [Privilege Levels, page 2-9](#)
- [Updates for Network Assistant, page 2-9](#)
- [Online Help, page 2-10](#)

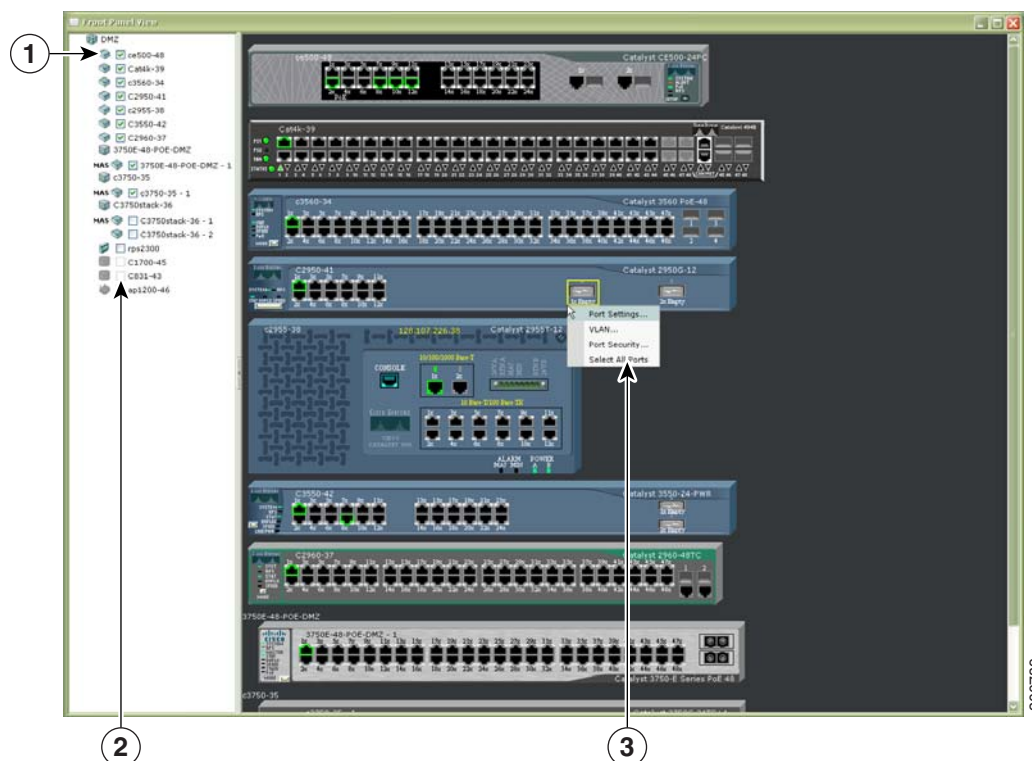
Front Panel View

When Network Assistant connects to a community or a cluster, you can display the Front Panel view of your device by clicking the Front Panel on the toolbar or by choosing **Monitor > View > Front Panel** on the feature bar. 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 is 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**.



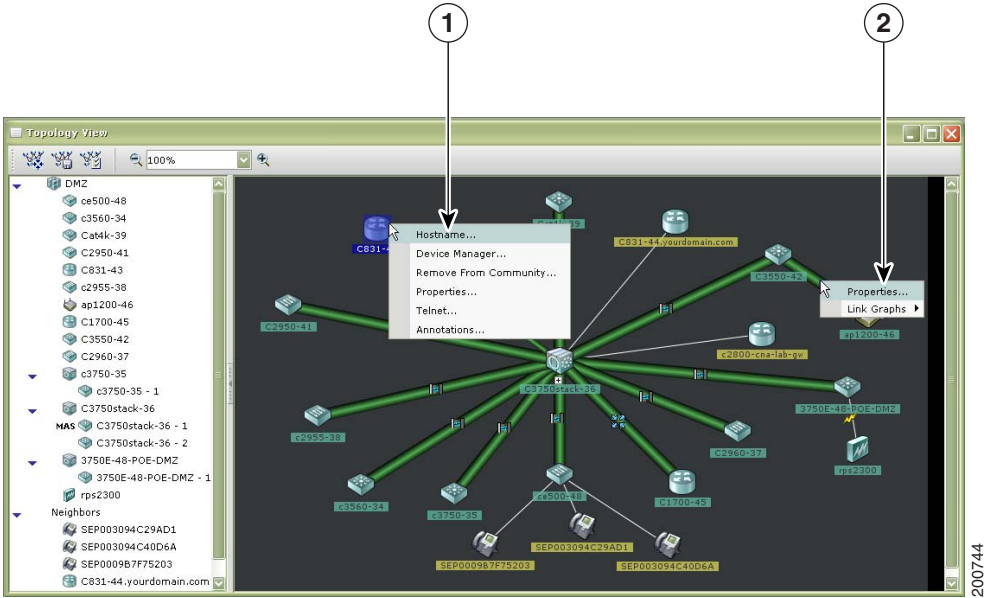
Note

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 do not 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

These menu bar, toolbar, and feature bar has these options:

- Menu bar—use to configure communities and Network Assistant.
- Toolbar—contains icons and buttons for commonly used configuration options and for information windows such as the legend and the online help.
- Feature bar—use to configure devices, ports and VLANs, perform monitoring, and access reports.

Menu Bar

The menu bar has these options:

- 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 the Network Assistant windows.
- Help—open the online help.

Toolbar

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.
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.

Table 2-1 *Toolbar Icons and Buttons (continued)*

Toolbar Option	Icon	Task
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		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 2-9](#).
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 the 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 opens.

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 2-9](#).

Network Assistant Modes

You can use Network Assistant in these modes:

- **Expert Mode**—Configures a feature in a single window. Network Assistant is in expert mode by default. To run a feature in expert mode choose **Expert** in the **Application** menu. To access the online help in expert mode, click **Help** in the window.
- **Guide Mode**—Configures a feature one step at a time and displays the corresponding help information for the window that is appearing. Features that appear with a signpost icon on the feature bar (see [Figure 2-5](#)) means that you can run them in guide mode. When you select the feature, a series of steps guides you through the configuration for that feature.

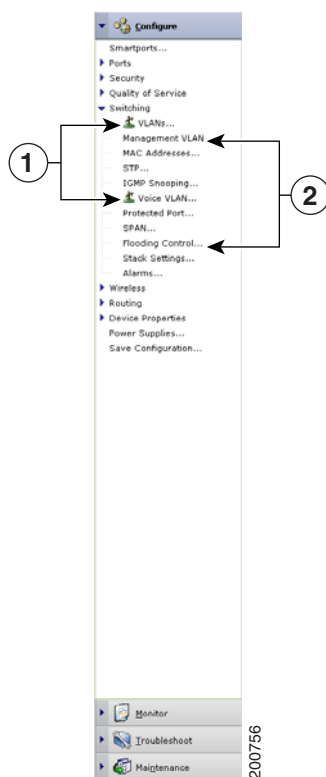
To run guide mode, choose **Guide** in the **Application** menu. To run a guide-mode feature in **Expert** mode, you must choose **Expert** before selecting the feature.



Note

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 2-9.

Figure 2-5 Guide Mode Signposts



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

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.

Updates for Network Assistant

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 Cisco Network Assistant

This chapter describes how to install Cisco Network Assistant and how to connect it to a device or an existing community.

For information about the requirements needed to install Network Assistant, see the Release Notes at: http://www.cisco.com/en/US/products/ps5931/prod_release_notes_list.html

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 to access this site. You do not need any 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.)

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



Note Network Assistant is free. There is no charge to download, install, or use it.

Starting Network Assistant

After you install Network Assistant, you will 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 to Network Assistant

Use the Connect window in Network Assistant to connect to a community or cluster. [Figure 3-1](#) shows the Connect window.

To connect Network Assistant to a device:

Step 1 From the Connect window, enter the IP address of the device.

- For an existing community, select its name from the pull-down menu. For an existing cluster, select the IP address.

When you select a community, you can also 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.

- For HTTP and Access Mode options, click the **Options** button.
 - In the HTTP protocol field, select HTTP or HTTPS. To communicate with a clustered or a standalone device, use HTTPS (secure HTTP) instead of HTTP.
 - Select an HTTP port. Use an HTTP port other than 80 on cluster command devices or standalone devices.
 - Select an access mode. Read-only access mode is the default.
 - Click **OK** to return to the Connect Window.
- You can also use this window to connect to a new community. 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.



Note

For information about using the 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.

Figure 3-1 *Connect Window*



Step 2 Click **Connect**.

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.

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.

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. It contains these sections:

- [Planning a Community, page 4-1](#)
- [Creating a Community, page 4-3](#)

For information about using Network Assistant to configure communities, see 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 starts 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, see 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, see 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 A-1](#) lists the Network Assistant-related configuration parameters on a Catalyst 4500 series switch.

Table A-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

This section describes how to configure your switch for Network Assistant. It includes these sections:

- [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	(HTTP only) Enable the HTTP server on the switch. By default, the HTTP server is disabled.
	or Switch(config)# ip domain-name <i>domain_name</i>	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 <i>connection_number</i>	Configure the maximum concurrent connections to the HTTP server. We recommend using 16 as the <i>connection_number</i> .
Step 5	Switch(config)# ip http timeout-policy idle <i>idle_time</i> life <i>life_time</i> requests <i>requests</i>	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 recommend 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.

REVIEW DRAFT—CISCO CONFIDENTIAL**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 <i>vlan_ID</i> { fastethernet gigabitethernet } <i>slot/interface</i> Port-channel <i>number</i> }	Select an interface.
Step 3	Switch(config-if)# ip address <i>ip_address</i> <i>address_mask</i>	(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 <i>vlan_ID</i> { fastethernet gigabitethernet } <i>slot/interface</i> Port-channel <i>number</i> }	Select an interface.
Step 5	Switch(config-if)# ip address <i>ip_address</i> <i>address_mask</i>	(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

A

accessing
 communities [4-2](#)
automatic discovery
 adding members [4-3](#)
 considerations
 connectivity [4-2](#)
 non-CDP-capable devices [4-4](#)
 in communities [4-2](#)
 See also CDP

C

candidates
 automatic discovery in communities [4-3](#)
Catalyst 4500 switches
 cluster configuration [A-3](#)
 community configuration [A-3](#)
 default settings [A-1](#)
 minimum configuration [A-2](#)
CDP
 automatic discovery in communities [4-2](#)
Cisco Discovery Protocol
 See CDP
Cluster Conversion Wizard [4-4](#)
clusters
 Cluster Conversion Wizard [4-4](#)
 converting to a community [4-4](#)
 definition [1-1](#)
 size limitation [1-1](#)
communities
 accessing [4-2](#)

 adding members [4-3](#)
 automatic discovery [4-2 to 4-3](#)
 candidates
 adding [4-3](#)
 automatic discovery of members [4-2 to 4-3](#)
 defined [4-1](#)
 discovering [4-3](#)
 requirements [4-1](#)
 See also community member
 communication protocols [4-3](#)
 community information [4-3](#)
 community names [4-2](#)
 composition [4-2](#)
 converting a cluster to a community [4-4](#)
 creating [4-3](#)
 definition [1-1 to 1-2](#)
 limits [4-2](#)
 management
 local PC [4-3](#)
 members
 adding [4-4](#)
 automatic discovery [4-2 to 4-3](#)
 hostnames [4-2](#)
 requirements [4-1](#)
 planning considerations
 hostnames [4-2](#)
 identifying information [4-3](#)
 passwords [4-3](#)
 saving identification information [4-3](#)
 verifying [4-4](#)
connecting Network Assistant [3-2](#)
converting a cluster to a community [4-4](#)

D

device limits in a community [4-2](#)
discovery, communities
 See automatic discovery

F

features
 Front Panel view [2-2](#)
 menu bar [2-4](#)
 online help [2-10](#)
 privilege levels [2-9](#)
 Topology view [2-3](#)
 wizards [2-9](#)

H

hostnames
 in communities [4-2](#)

I

installing Network Assistant
 procedure [3-1](#)
IP addresses
 community candidates [4-1](#)

M

manually adding members to communities [4-4](#)
members
 adding [4-3](#)
 adding to a community [4-4](#)
menu bar [2-4](#)

N

Network Assistant
 connecting [3-2](#)
 installing
 procedure [3-1](#)
 introduced [1-1](#)
 starting [3-1](#)

O

online help [2-10](#)

P

passwords
 in communities [4-3](#)
privilege levels [2-9](#)

S

Smartports Advisor [2-9](#)
starting Network Assistant [3-1](#)

T

Topology view [2-3](#)

W

wizards [2-9](#)