



Getting Started with Cisco Network Assistant

Version 1.0

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-6194-01



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.

CCSP, the Cisco Square Bridge logo, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO 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. (0406R)

Getting Started with Cisco Network Assistant

Copyright ©2004 Cisco Systems, Inc. All rights reserved.



Preface	v
Audience	v
Purpose	v
Obtaining Documentation	v
Cisco.com	v
Ordering Documentation	vi
Documentation Feedback	vi
Obtaining Technical Assistance	vi
Cisco Technical Support Website	vii
Submitting a Service Request	vii
Definitions of Service Request Severity	vii
Obtaining Additional Publications and Information	viii

CHAPTER 1

What Is Network Assistant? 1-1

CHAPTER 2

Network Assistant Features 2-1

Front Panel View	2-2
Topology View	2-2
Menu Bar, Toolbar, and Feature Bar	2-3
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
Privilege Levels	2-8
Searches for New Packages	2-8
Online Help	2-9

CHAPTER 3

Installing, Launching, and Connecting Network Assistant 3-1

- Installation Requirements 3-1
- Installing Network Assistant 3-1
- Launching Network Assistant 3-2
- Connecting Network Assistant to a Device 3-2

CHAPTER 4

Planning and Creating Clusters 4-1

- Planning a Cluster 4-1
 - Command Device Characteristics 4-1
 - Standby Command Device Characteristics 4-1
 - Candidate and Member Characteristics 4-2
 - Automatic Discovery of Candidates and Members 4-2
 - Discovery through CDP Hops 4-3
 - Discovery through Non-CDP-Capable and Noncluster-Capable Devices 4-4
 - Discovery through Different VLANs 4-5
 - Discovery through Different Management VLANs 4-5
 - Discovery through Routed Ports 4-6
 - Discovery of Newly Installed Devices 4-7
 - HSRP and Standby Command Devices 4-8
 - Virtual IP Addresses 4-8
 - Other Considerations for Standby Groups 4-9
 - Automatic Recovery of Cluster Configuration 4-10
- IP Addresses 4-10
- Host Names 4-10
- Passwords 4-11
- SNMP Community Strings 4-11
- Clusters and Stacks 4-11
- TACACS+ and RADIUS 4-13
- Access Modes in Network Assistant 4-13
- LRE Profiles 4-13
- Creating a Cluster 4-13
 - Enabling a Command Device 4-14
 - Adding Cluster Devices 4-14
 - Creating a Standby Group 4-14
 - Verifying a Cluster 4-15

INDEX



Preface

Audience

This guide is for system administrators, network managers, and other users who want to manage standalone network devices and device clusters through a GUI. It presents Cisco Network Assistant, known as Network Assistant for short, 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 Clusters—The concepts and procedures to plan and to create clusters by using Network Assistant.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/index.shtml>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

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

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

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year at this URL:

<http://www.cisco.com/techsupport>

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

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

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 automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

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

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

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

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553 2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

<http://cisco.com/univercd/cc/td/doc/pcat/>

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

<http://www.ciscopress.com>

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

<http://www.cisco.com/packet>

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

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

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

<http://www.cisco.com/ipj>

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

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



What Is Network Assistant?

Network Assistant is an application that manages standalone devices and clusters of devices 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 cluster:

- A topology view, showing devices that are eligible to join the 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 port LEDs.

A cluster can contain up to 16 connected, cluster-capable Catalyst devices. The devices belong exclusively to the 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 is the single point of access that Network Assistant uses to configure, manage, and monitor the command device and the *member devices*.

The main reasons for creating a cluster are

- You can manage Cisco cluster-capable devices regardless of their interconnection media and physical locations. The devices can be in the same location, or they can be distributed across a Layer 2 or Layer 3 network.
- You can designate devices to take the place of a failed command device. Having *standby command devices* safeguards against a loss of contact with cluster members.

Network Assistant features can identify a device as the command device, add members to the cluster, and identify standby command devices. See [Chapter 2, “Network Assistant Features,”](#) for more information.

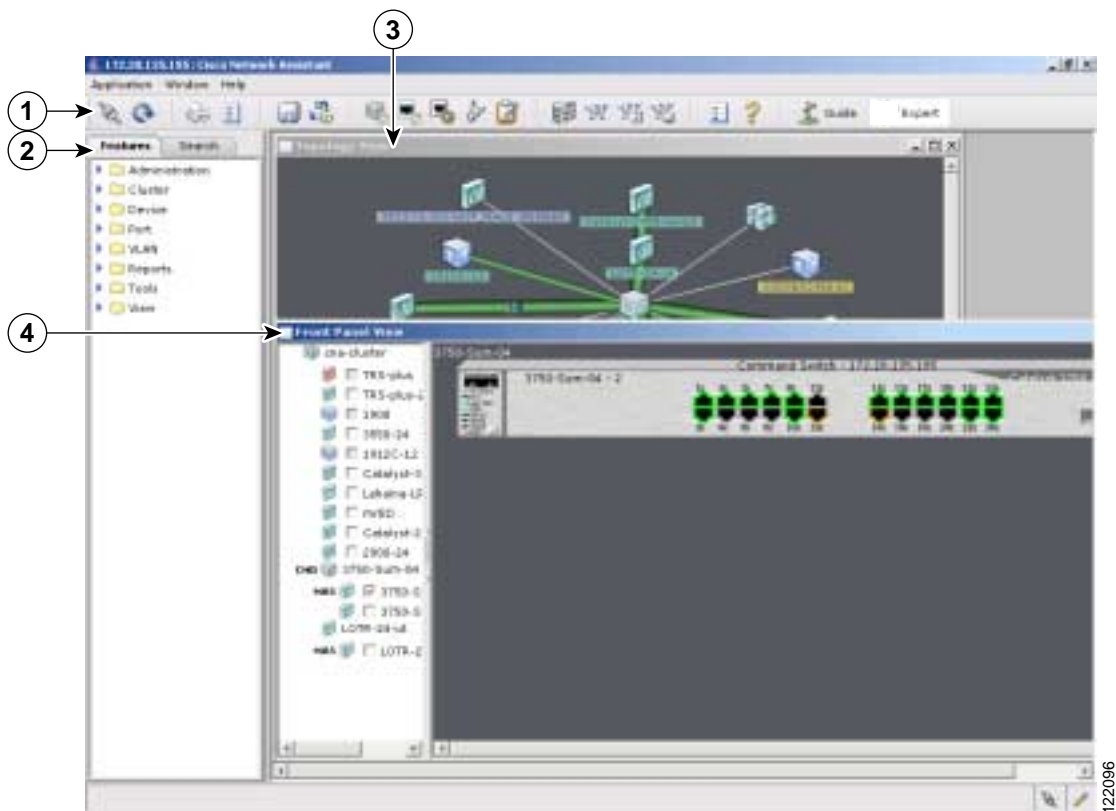
For information on setting up device clusters, see [Chapter 4, “Planning and Creating Clusters.”](#)



Network Assistant Features

Network Assistant simplifies cluster management by offering an intuitive GUI, alternative modes for configuring network devices, two levels of access, and comprehensive online help. [Figure 2-1](#) shows the main features of the user interface.

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 device, you can display the Front Panel view by clicking the Front Panel icon on the toolbar or by choosing **View > Front Panel** from the feature bar. You see the front-panel image of the device. If the device commands a cluster, you also see the cluster members that were selected the last time the view was displayed.

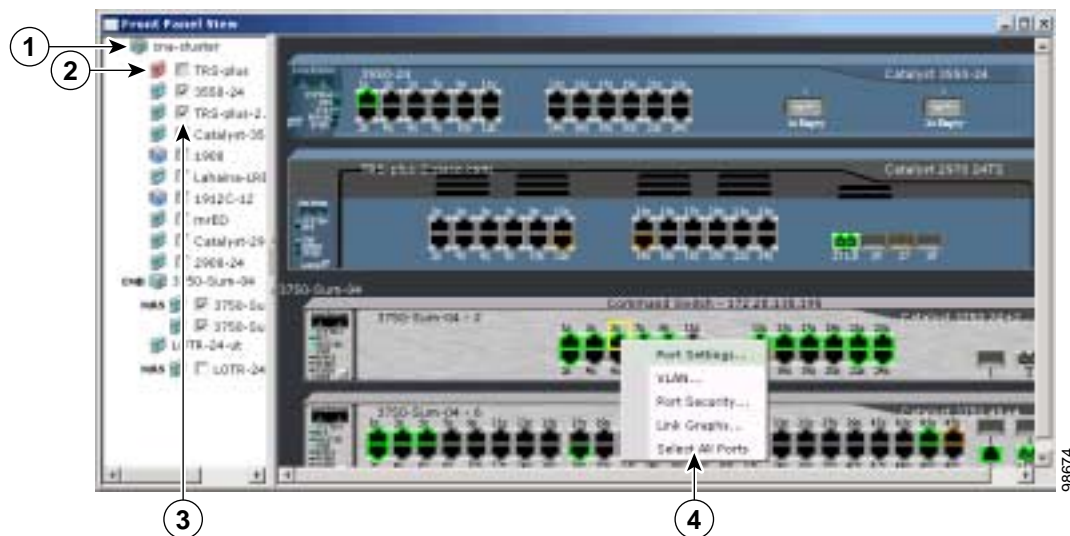
If Network Assistant connects to a device that does not command a cluster, the Front Panel view appears by default. You see only the front panel of that device.

By using the Front Panel view, you can

- Drag and re-arrange the devices that appear.
- Select and configure the devices.
- Right-click on 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 cluster with a Catalyst 3750 switch as the command device.

Figure 2-2 Front Panel View and Port Popup Window



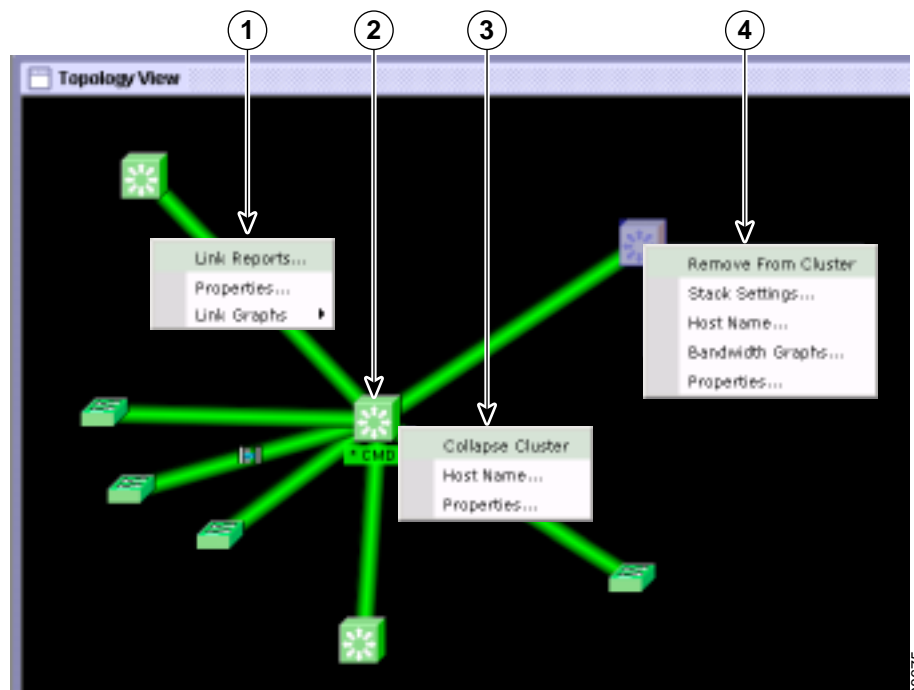
1	Cluster tree	3	Check boxes to show devices
2	Command device	4	Port settings popup window

Topology View

When Network Assistant connects to a device that commands a cluster, the Topology view appears by default. When Network Assistant connects to another device, you can see the Topology view by clicking the Topology view icon on the toolbar or by choosing **View > Topology**.

The Topology view displays a command device (shown by the **CMD** label) and the devices that are connected to it, as shown in Figure 2-3. When you right-click on a device or link icon, a popup window appears.

Figure 2-3 Topology View and Device Popup Windows



1	Link popup window	3	Command device popup window
2	Command device	4	Cluster member popup window

The Topology view shows how the devices within a device cluster are connected and how the cluster is connected to other clusters and devices. You can add and remove cluster members from this view.

You can see the network topology at two levels of detail:

- **Collapse Cluster**—When you right-click a command-device icon and select **Collapse Cluster**, the cluster collapses and is represented by a single icon. The view shows how the cluster connects to other clusters, candidate switches, and devices that are not eligible to join the cluster (such as routers, access points, IP phones, and so on).
- **Expand Cluster**—When you right-click a cluster icon and select **Expand Cluster**, the Topology view displays the cluster in detail. You see the command device, member devices, and candidate devices that can join the cluster. This view does not show the details of any neighboring clusters.



Note

The Topology view displays only the cluster and 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 for configuring devices and device clusters are available from the menu bar, the toolbar, and the feature bar.

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, and show or hide the feature bar.
- **Window**—Navigate to Network Assistant windows that are open.
- **Help**—Launch the online help.

Toolbar

The toolbar has icons for commonly used device and cluster configuration options and for information windows like the legend and 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 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 new packages.
Save Configuration ^{2,3}		Save the configuration of the cluster or a device to flash memory.
Software Upgrade ^{2,4}		Upgrade the software for the cluster or a device.
Port Settings ^{1,4}		Display and configure port parameters on a device.
Smartports Device Macros ⁴		Display or configure Smartports macros on a device.
Smartports Port Macros ⁴		Display or configure Smartports macros on a port.
VLAN ¹		Display VLAN membership, assign ports to VLANs, and change the administration mode.

Table 2-1 Toolbar Icons (continued)

Toolbar Option	Icon	Task
Inventory ⁴		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.
Topology Options		Select the information to be displayed in the Topology view.
Save Topology Layout ²		Save your arrangement of the cluster icons in the Topology view to flash memory.
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.
3. The Catalyst 4500 series switch saves the configuration to the user’s PC, not to flash memory.
4. The Catalyst 4500 series switch does not support this option.

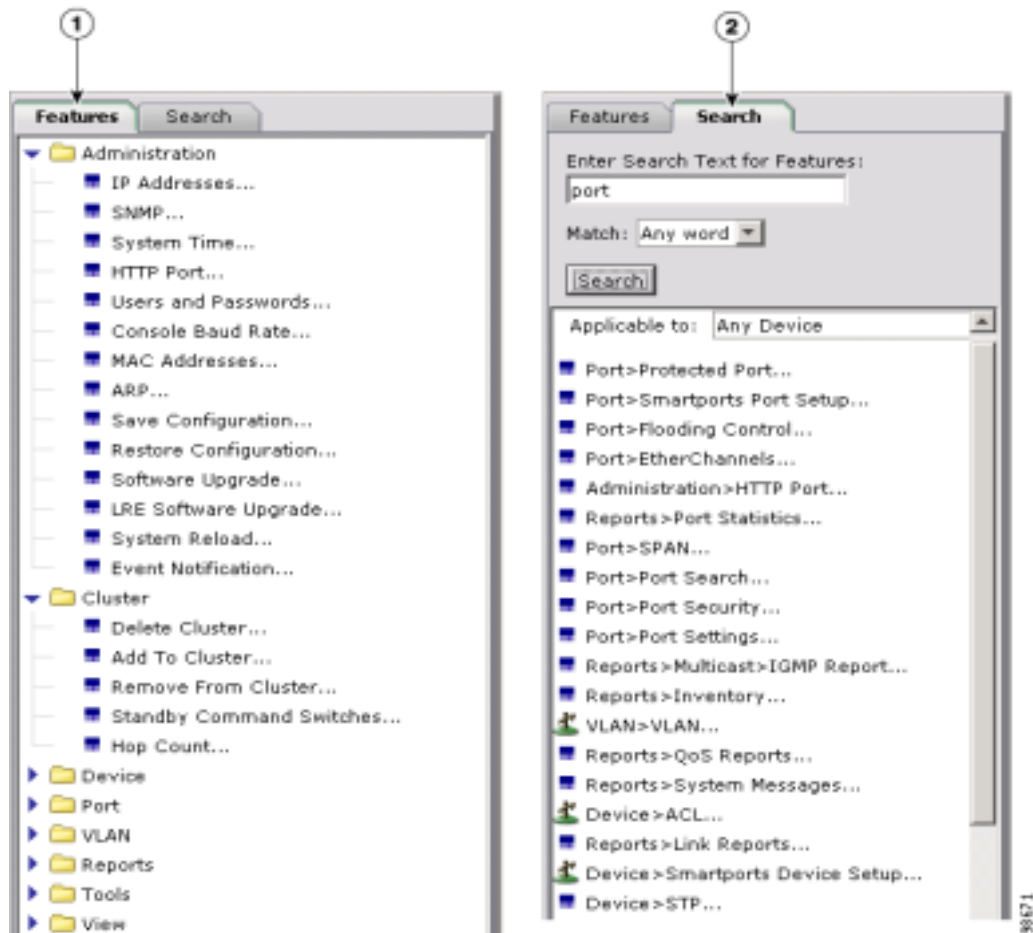
Feature Bar

The feature bar shows the networking features that are available for the devices in your cluster. By default, the feature bar is in standard mode. In this mode, the feature bar 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 for a sample cluster.

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](#).

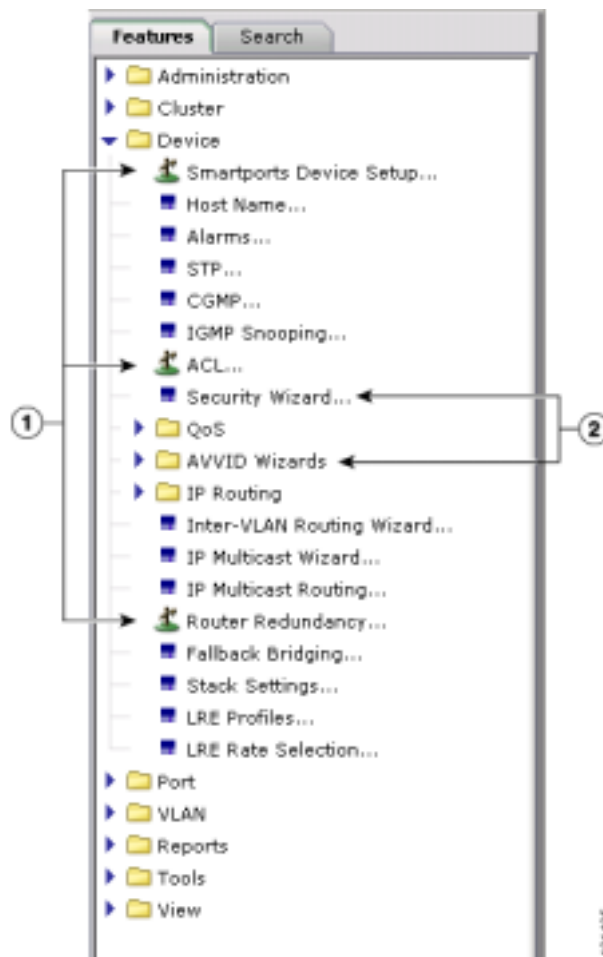
Interaction Modes

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 guide mode by default. When you choose a feature on the feature bar with a signpost icon (see [Figure 2-5 on page 2-7](#)), 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 and Wizards



1	Guide mode icon	2	Wizards
---	-----------------	---	---------

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 are shown with a signpost on the feature bar will 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

Like guide mode, wizards provide a step-by-step approach for completing a specific configuration task. Unlike guide mode, a wizard does not prompt you to provide information for all of the feature options. Instead, it prompts you to provide minimal information and then uses the default settings of the remaining options to set up default configurations.

When you select a feature that has *Wizard* in its name, as shown in [Figure 2-5](#), the wizard launches.

Wizards are not available for read-only access levels. For more information about the read-only access mode, see the [“Privilege Levels”](#) section.

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 or cluster configuration are not shown for read-only access.

If your privilege level is not 15, you must specify it in the Connect window that appears when you launch Network Assistant. If you do not specify it, you are denied access to Network Assistant.



Note

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

Searches for New Packages

Network Assistant is made up of *packages*. They are components that support devices or features or correct defects. 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**. Network Assistant does an immediate search for new packages.

If a new package 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 cluster devices. In these cases, the right pane of the Help window contains all the versions of the topic, each labeled with the host names of the cluster 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, Launching, and Connecting Network Assistant

This chapter describes what you need to install Network Assistant, how to install it, how to launch it, and how to connect it to a device.

Installation Requirements

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

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

Network Assistant is supported on these operating systems:

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



Note

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

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 access privileges.
2. Find the Network Assistant installer, cna-1_0-windows-installer.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 Network Assistant installation.

Launching Network Assistant

After Network Assistant is installed, you see its icon on your desktop, a Network Assistant entry under **Start > Programs**, and a Network Assistant executable file in the installation directory. When you click any of these, you see the Network Assistant GUI (see [Figure 2-1 on page 2-1](#)) and the Connect window.

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

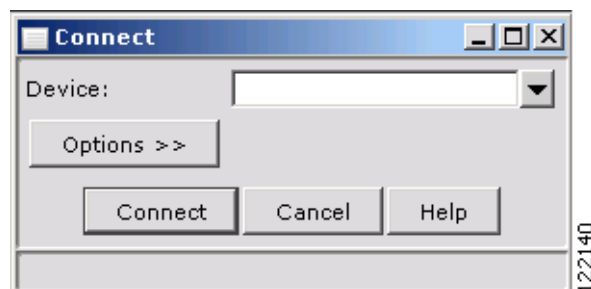
Connecting Network Assistant to a Device

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 that you want to connect to. Click **Options** if you want to

- Communicate with the device by using HTTPS (secure HTTP) instead of HTTP.
- Use an HTTP port other than 80 on the device.
- Connect with read-only access.

When you click **Connect**, you are either connected to the device directly, or you are prompted for a username and password and then connected.

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.



Planning and Creating Clusters

This chapter provides the concepts and procedures to plan and create clusters with Network Assistant. For information on using Network Assistant to configure clusters, refer to its online help.



Note

You can also create clusters through the command-line interface (CLI), but less easily. For the CLI cluster commands, refer to the command reference for the command device.

Planning a Cluster

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

Command Device Characteristics

A command device must meet these requirements:

- It has an IP address.
- Clustering and the HTTP server are enabled (the default except on Catalyst 4500 series switches).
- Cisco Discovery Protocol (CDP) version 2 is enabled (the default).
- It is not a command device or a member in another cluster.
- It is connected to standby command devices through the management VLAN and to cluster members through a common VLAN.



Note

Standby command devices are not required in a cluster, and they are not supported by Catalyst 4500 series switches.

Standby Command Device Characteristics

A standby command device must meet these requirements:

- It has an IP address.
- It has CDP version 2 enabled.

- It is connected to the command device and to other standby command devices through its management VLAN.
- It is connected to all other cluster members through a common VLAN.
- It is redundantly connected to the cluster so that connectivity to members is maintained.
- It is not a command device or a member in another cluster.

Standby command devices must be the same type of device as the command device. For example, if the command device is a Catalyst 3750 switch, the standby command devices must also be Catalyst 3750 switches. If you want to maintain the same level of feature support when a standby command device takes over, it should run the same release of Cisco IOS that the command device runs.

Candidate and Member Characteristics

Candidates are cluster-capable devices that have not yet been added to a cluster. Members are devices that have actually been added to a cluster. Although not required, a candidate or member can have its own IP address and password.

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

- It is running cluster-capable software.
- It has CDP version 2 enabled.
- It is not a command device or a member of another cluster.
- If a standby group exists, it is connected to every standby command device through at least one common VLAN. The VLAN to each standby command device can be different.
- It is connected to the command device through at least one common VLAN.

**Note**

Catalyst 2900 XL, Catalyst 2950, and Catalyst 3500 XL candidates and members must be connected through their management VLAN to the command device and the standby command devices.

This requirement does not apply if you have a Catalyst 2970, Catalyst 3550, Catalyst 3560, Catalyst 3750, or Catalyst 4500 command device. Candidates and members can connect through any VLAN in common with the command device.

A Catalyst 4500 switch can be a cluster member only if another Catalyst 4500 switch is the command device.

Automatic Discovery of Candidates and Members

The command device uses CDP to discover members, candidates, neighboring clusters, and edge devices across multiple VLANs and in star or cascaded topologies.

**Note**

Do not disable CDP on the command device, on members, or on any cluster-capable devices that you might want a command device to discover.

Following these connectivity guidelines ensures automatic discovery of the cluster, cluster candidates, connected clusters, and neighboring edge devices:

- [Discovery through CDP Hops, page 4-3](#)
- [Discovery through Non-CDP-Capable and Noncluster-Capable Devices, page 4-4](#)
- [Discovery through Different VLANs, page 4-5](#)
- [Discovery through Different Management VLANs, page 4-5](#)
- [Discovery through Routed Ports, page 4-6](#)
- [Discovery of Newly Installed Devices, page 4-7](#)

Discovery through CDP Hops

By using CDP, a command device can discover devices up to seven CDP hops away (the default is three hops) from the edge of the cluster. The edge of the cluster is where the last members are connected to the cluster and to candidate devices. For example, members 9 and 10 in [Figure 4-1](#) are at the edge of the cluster.

You can set the number of hops the command device searches for candidates and members by selecting **Cluster > Hop Count**. When new candidates are added to the network, the command device discovers them and adds them to the list of candidates.

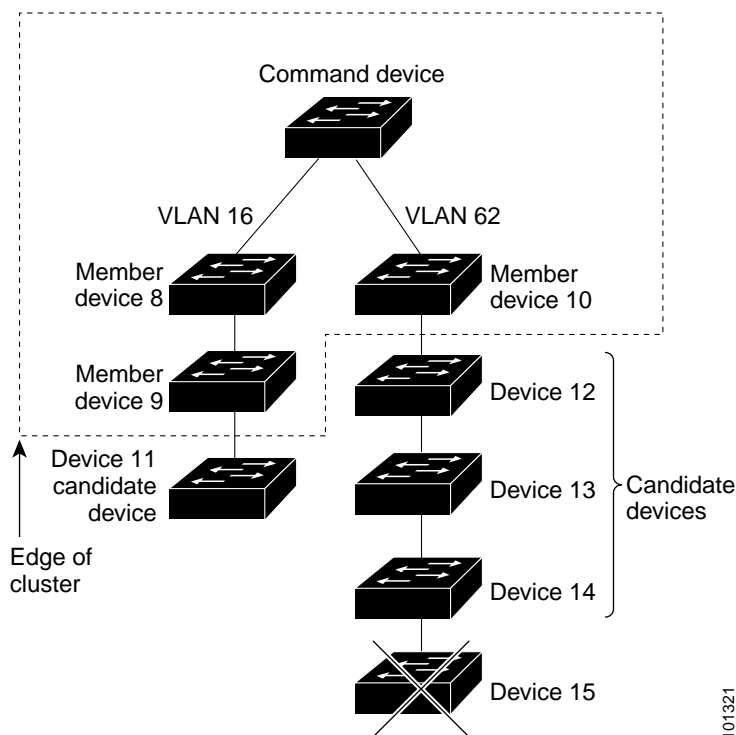


Note

A stack in a cluster functions as a single member device. See the [“Clusters and Stacks” section on page 4-11](#) if you plan to use a stack in a cluster.

In [Figure 4-1](#), the command device has ports assigned to VLANs 16 and 62. The CDP hop count is three. The command device discovers devices 11, 12, 13, and 14 because they are within three hops from the edge of the cluster. It does not discover device 15 because it is four hops from the edge of the cluster.

Figure 4-1 Discovery through CDP Hops

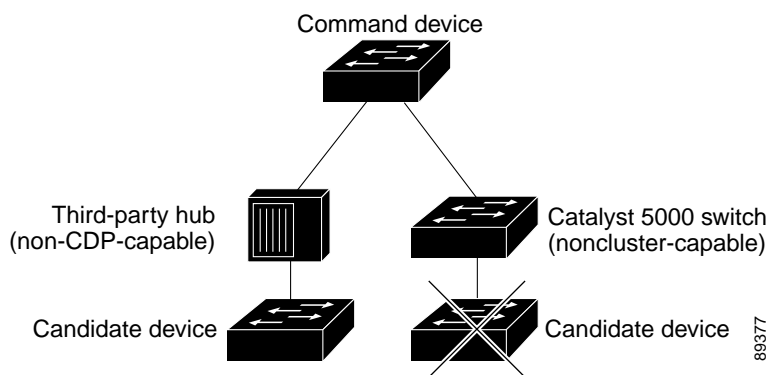


Discovery through Non-CDP-Capable and Noncluster-Capable Devices

If a command device is connected to a *non-CDP-capable third-party hub* (such as a non-Cisco hub), it can discover cluster-enabled devices connected to that hub. However, if the command device is connected to a *noncluster-capable Cisco device*, it cannot discover a cluster-enabled device connected beyond the noncluster-capable Cisco device.

Figure 4-2 shows that the command device discovers the device that is connected to a third-party hub. However, the command device does not discover the device that is connected to a Catalyst 5000 switch.

Figure 4-2 Discovery through Non-CDP-Capable and Noncluster-Capable Devices



Discovery through Different VLANs

If the command device is a Catalyst 2970, Catalyst 3550, Catalyst 3560, Catalyst 3750, or Catalyst 4500 switch, the cluster can have members in different VLANs. As members, they must be connected through at least one VLAN in common with the command device. The command device in [Figure 4-3](#) has ports assigned to VLANs 9, 16, and 62 and therefore discovers the devices in those VLANs. It does not discover the device in VLAN 50. It also does not discover the device in VLAN 16 in the first column because the command device has no VLAN connectivity to it.

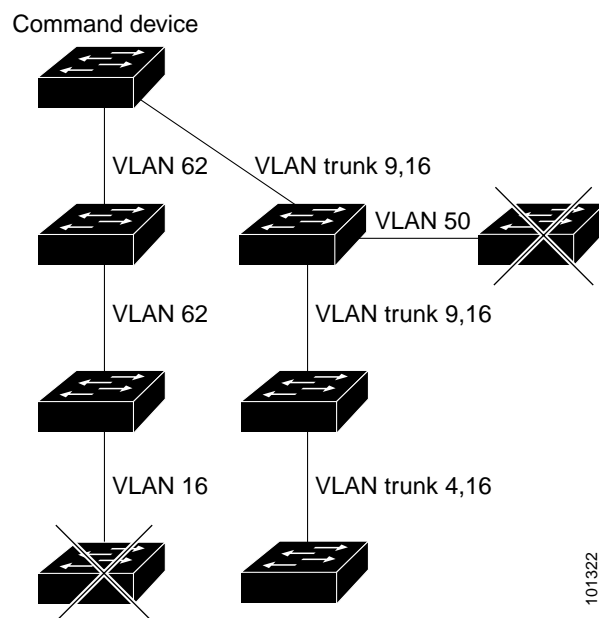
Catalyst 2900 XL, Catalyst 2950, and Catalyst 3500 XL members must be connected to the command device through their management VLAN. For information about discovery through management VLANs, see the [“Discovery through Different Management VLANs”](#) section on page 4-5.



Note

For additional considerations about VLANs in stacks, see the [“Clusters and Stacks”](#) section on page 4-11.

Figure 4-3 Discovery through Different VLANs



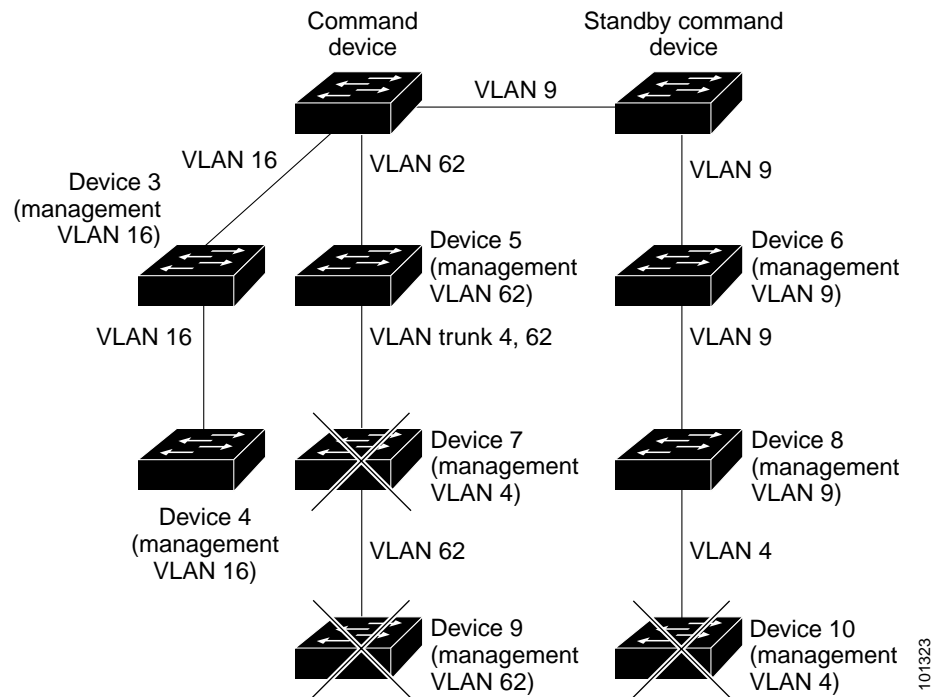
Discovery through Different Management VLANs

As command devices, Catalyst 2970, Catalyst 3550, Catalyst 3560, Catalyst 3750, and Catalyst 4500 switches can discover and manage members in different VLANs and different management VLANs. As members, they must be connected through at least one VLAN in common with the command device. They do not need to be connected to the command device through their management VLAN. The default management VLAN is VLAN 1.

The command device and standby command device in [Figure 4-4](#) (assuming they are Catalyst 2970, Catalyst 3550, Catalyst 3560, Catalyst 3750, or Catalyst 4500 switches) have ports assigned to VLANs 9, 16, and 62. The management VLAN on the command device is VLAN 9. Each command device discovers the devices in the different management VLANs except these:

- Devices 7 and 10 (devices in management VLAN 4) because they are not connected through a common VLAN (meaning VLANs 62 and 9) with the command device
- Device 9 because automatic discovery does not extend beyond a noncandidate, which is device 7

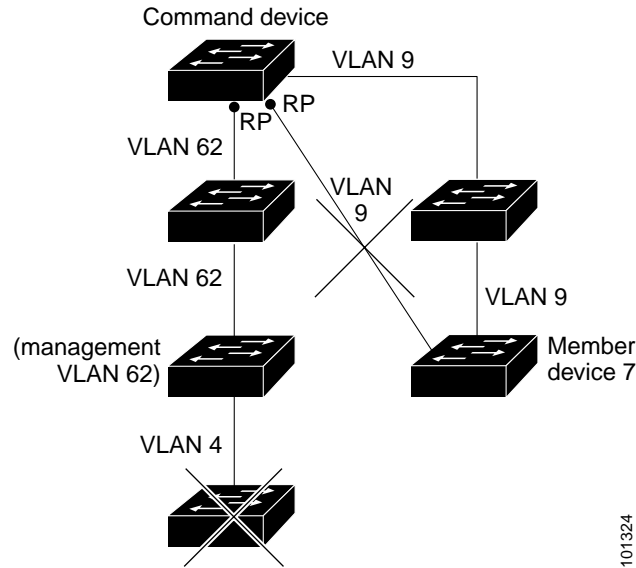
Figure 4-4 Discovery through Different Management VLANs



Discovery through Routed Ports

If the command device has a routed port (RP) configured, it discovers only candidates and members in the *same* VLAN as the routed port.

The Layer 3 command device in [Figure 4-5](#) can discover the devices in VLANs 9 and 62 but not the device in VLAN 4. If the routed port path between the command device and member 7 is lost, the redundant path through VLAN 9 maintains connectivity with member 7.

Figure 4-5 *Discovery through Routed Ports*

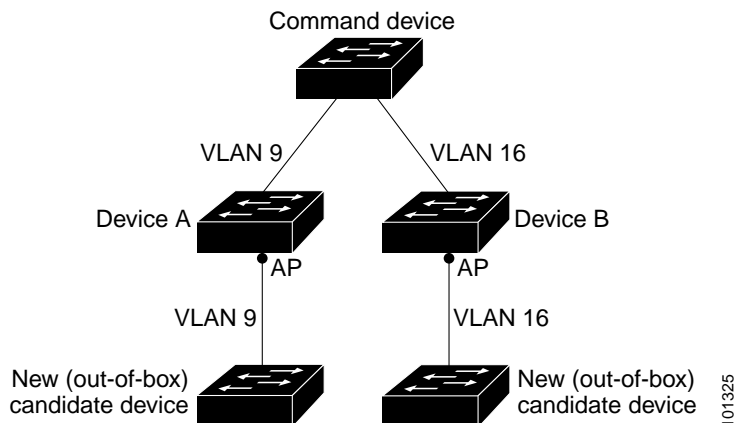
Discovery of Newly Installed Devices

To join a cluster, a new, out-of-the-box device must be connected to the cluster through one of its access ports. An access port (AP) carries the traffic of and belongs to only one VLAN. By default, the new device and its access ports are assigned to VLAN 1.

When the new device joins a cluster, its default VLAN changes to the VLAN of the immediately upstream neighbor. The new device also configures its access port to belong to the VLAN of the immediately upstream neighbor.

The command device in [Figure 4-6](#) belongs to VLANs 9 and 16. When new cluster-capable devices join the cluster:

- One cluster-capable device and its access port are assigned to VLAN 9.
- The other cluster-capable device and its access port are assigned to management VLAN 16.

Figure 4-6 *Discovery of Newly Installed Devices*

HSRP and Standby Command Devices

You can configure a group of standby command devices on devices that support Hot Standby Router Protocol (HSRP). Because a command device manages the forwarding of all communication and configuration information to all the members, we strongly recommend the following:

- If the command device is a stack, configure a standby command device to take over in case the entire stack fails. (If only the stack master fails, the stack elects a new stack master, and the stack resumes its role as the command device.)
- If a command device is a standalone device, configure a standby command device to take over if the command device fails.

Devices in the standby group are ranked according to HSRP priorities. The device with the highest priority in the group is the *active command device*. The device with the next highest priority is the *standby command device*. The other devices in the standby group are the *passive command devices*. If the active command device and the standby command device fail *at the same time*, the passive command device with the highest priority becomes the active command device.



Note

The HSRP standby hold time interval should be greater than or equal to three times the hello time interval. The default HSRP standby hold time interval is 10 seconds. The default HSRP standby hello time interval is 3 seconds.

These connectivity guidelines ensure automatic discovery of the cluster, candidates, connected clusters, and neighboring edge devices. These topics also provide more detail about standby command devices:

- [Virtual IP Addresses, page 4-8](#)
- [Other Considerations for Standby Groups, page 4-9](#)
- [Automatic Recovery of Cluster Configuration, page 4-10](#)

Virtual IP Addresses

You must assign a unique virtual IP address and group number and name to the standby group. Configure this information on a specific VLAN or a routed port on the active command device. The active command device receives traffic destined for the virtual IP address. To manage the cluster, you must access the active command device through the virtual IP address, not through the command-device IP address. This is in case the IP address of the active command device is different from the virtual IP address of the standby group.

If the active command device fails, the standby command device assumes ownership of the virtual IP address and becomes the active command device. The passive devices in the standby group compare their assigned priorities to decide the new standby command device. The passive standby device with the highest priority then becomes the standby command device. If the previously active command device becomes active again, it resumes its role as the active command device, and the current active command device again becomes the standby command device. For more information about IP addresses in device clusters, see the [“IP Addresses” section on page 4-10](#).

Other Considerations for Standby Groups

These requirements also apply:

- Standby command devices must be the same type of device as the command device. For example, if the command device is a Catalyst 3750 switch, the standby command devices must also be Catalyst 3750 switches.
- Only one standby group can be assigned to a cluster. You can have more than one router-redundancy standby group.

An HSRP group can be both a standby group and a router-redundancy group. However, if a router-redundancy group becomes a standby group, router redundancy becomes disabled on that group.

- All standby-group members must be members of the cluster.

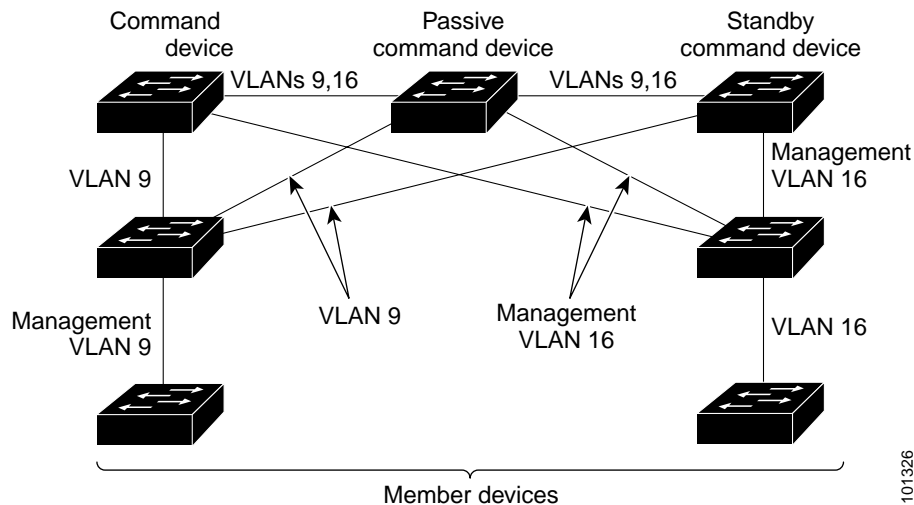


Note

There is no limit to the number of devices that you can assign as standby command devices. However, the total number of devices in the cluster—which would include the active command device, standby-group members, and other members—cannot be more than 16.

- Each standby-group member (Figure 4-7) must be connected to the command device through the same VLAN. In this example, the command device and standby command devices are Catalyst 2970, Catalyst 3550, Catalyst 3560, or Catalyst 3750 command switches. Each standby-group member must also be redundantly connected to each other through at least one VLAN in common with the cluster.

Figure 4-7 VLAN Connectivity between Standby-Group Members and Other Members



Note

For additional considerations about standby groups in stacks, see the “Clusters and Stacks” section on page 4-11.

Automatic Recovery of Cluster Configuration

The active command device continually forwards cluster-configuration information (but not device-configuration information) to the standby command device. This ensures that the standby command device can take over the cluster immediately if the active command device fails.

Automatic discovery has these limitations:

- (This limitation applies only to clusters that have Catalyst 2950, Catalyst 3550, Catalyst 3560, and Catalyst 3750 command and standby devices command devices.) If the active command device and the standby command device fail *at the same time*, the passive command device with the highest priority becomes the active command device. However, because it was a passive standby command device, the previous command device *did not* forward cluster-configuration information to it. The active command device only forwards cluster-configuration information to the standby command device. You must therefore rebuild the cluster.
- If the active command device fails and there are more than two devices in the cluster standby group, the new command device does not discover Catalyst 2916M XL members. You must re-add these members to the cluster.
- If the active command device fails and becomes active again, it does not discover Catalyst 2916M XL members. You must re-add these members to the cluster.

When a previously active command device resumes its active role, it receives a copy of the latest cluster configuration from the active command device, including members that were added while it was down. The active command device sends a copy of the cluster configuration to the standby group.

IP Addresses

You must assign IP information to a command device. You can assign more than one IP address to the command device, and you can access the cluster through any of the IP addresses. If you configure a standby group, you must use the standby-group virtual IP address to manage the cluster from the active command device. Using the virtual IP address ensures that you retain connectivity to the cluster if the active command device fails and that a standby command device becomes the active command device.

If the active command device fails and the standby command device takes over, you must use either the standby-group virtual IP address or any of the IP addresses available on the new active command device to access the cluster.

You can assign an IP address to a cluster-capable device, but it is not necessary. A member is managed and communicates with other members through the command-device IP address. If a member leaves the cluster and it does not have its own IP address, you then must assign IP information to it to manage it as a standalone device.



Note

Changing the IP address of the command device ends your Network Assistant session on the device.

Host Names

You do not need to assign a host name to either a command device or a member. However, a host name assigned to the command device can help to identify the cluster. The default host name for a device is *Switch*.

If a device joins a cluster and it does not have a host name, the command device appends a unique member number to its own host name and assigns it sequentially as each device joins the cluster. The number shows the order in which the device was added to the cluster. For example, a command device named *eng-cluster* would name the fifth cluster member *eng-cluster-5*.

If a device has a host name, it retains that name when it joins a cluster. It retains that host name even after it leaves the cluster.

If a device received its host name from the command device, was removed from the cluster, and was added to a new cluster with the same member number (such as 5), the old host name (such as *eng-cluster-5*) is overwritten with the host name of the command device in the new cluster (such as *mkg-cluster-5*). If the member number changes in the new cluster (such as 3), the device retains the previous name (*eng-cluster-5*).

Passwords

You do not need to assign passwords to a device if it will be a cluster member. When a device joins a cluster, it inherits the command-device password and retains it when it leaves the cluster. If no command-device password is configured, the member inherits a null password. Members only inherit the command-device password.

If you change the member password to be different from the command-device password and save the change, the member cannot be managed by the command device until you change the member password to match the command-device password. Rebooting the member does not change the password back to the command-device password. We recommend that you do not change the member password after it joins a cluster.

SNMP Community Strings

A member inherits the first read-only (RO) and read-write (RW) community strings of the command device, with *@esN* appended to the community strings. *N* is the member number.

If the command device has multiple read-only or read-write community strings, only the first read-only and read-write strings are propagated to the member.

Clusters and Stacks

A cluster can have one or more Catalyst 3750 stacks. Each stack can act as the command device or as a single member. [Table 4-1](#) compares stacks and clusters.

Table 4-1 Comparison of Stacks and Clusters

Stack	Cluster
Made up of only Catalyst 3750 switches.	Made up of cluster-capable devices, such as Catalyst 2950, Catalyst 3550, Catalyst 3750, and Catalyst 4500 switches.
Stack members are connected through StackWise ports.	Cluster members are connected through LAN ports.
Requires one <i>stack master</i> and supports up to eight other <i>stack members</i> .	Requires 1 command device and supports up to 15 other members.
Can be a command device or a member.	Cannot be a stack master or stack member.

Table 4-1 Comparison of Stacks and Clusters (continued)

Stack	Cluster
Stack master is the single point of <i>complete</i> management for all stack members.	Command device is the single point of <i>some</i> management for all members of a cluster.
Back-up stack master is automatically determined in case the stack master fails.	Standby command device must be pre-assigned in case the command device fails. Note This does not apply if a Catalyst 4500 switch is the command device.
Supports up to eight simultaneous stack master failures.	Supports only one command device failure at a time.
Stack members behave and are presented as a single, unified system in the network.	Cluster members are independent devices that are neither managed as nor behave as a unified system.
Integrated management of stack members is through a single configuration file.	Each member has its own configuration file.
Stack- and interface-level configurations are stored on each stack member.	Cluster configuration is stored on the command device and the standby command device.
New stack members are automatically added to the stack.	New members are manually added to the cluster.

Stack members work together to behave as a unified system in the network and are presented to the network as such by Layer 2 and Layer 3 protocols. Therefore, a cluster recognizes an entire stack as an eligible cluster member. Individual stack members cannot join a cluster or participate as separate members. Because a cluster must have 1 command device and can have up to 15 members, a cluster can potentially have up to 16 stacks, totalling 144 devices.

Stacks are configured through the stack master.

**Note**

From the CLI, you can configure a cluster to contain up to 16 stacks. However, from Network Assistant, the maximum number of devices in a cluster is 16, counting the individual devices in a stack. For example, Network Assistant counts a stack with three stack members as three separate devices.

If you use the CLI to configure a cluster of more than 16 actual devices and then try to display the cluster from Network Assistant, you will have to remove members until the Network Assistant limit of 16 separate devices is reached.

Keep these considerations in mind if you have stacks in clusters:

- If the command device is not a Catalyst 3750 switch or a stack and a new stack master is elected, the stack loses its connectivity to the cluster if there are no redundant connections between the stack and the command device. You must add the stack to the cluster.
- If the command device is a stack and new stack masters are simultaneously elected in that stack and in member stacks, connectivity between the stacks is lost if there are no redundant connections between them. You must add the stacks to the cluster, including the stack that is the command device.
- All stack members should have redundant connectivity to all the VLANs in the cluster. Otherwise, if a new stack master is elected, stack members connected to any VLANs not configured on the new stack master lose their connectivity to the cluster. You must change the VLAN configuration of the stack master or the stack members and add the stack members back to the cluster.

- If a stack in the role of a member reloads and a new stack master is elected, the stack loses connectivity with the command device. You must add the stack back to the cluster.
- If a stack that is acting as the command device reloads and the original stack master is not re-elected, you must rebuild the entire cluster.

TACACS+ and RADIUS

Inconsistent authentication configurations in clusters cause Network Assistant to continually prompt for a username and password. If TACACS+ is configured on a member, it must be configured on all members. Similarly, if RADIUS is configured on a member, it must be configured on all members. Further, the same cluster cannot have some members configured with TACACS+ and other members configured with RADIUS.

Access Modes in Network Assistant

Some configuration windows display incomplete information if you have read-only access to a cluster with these devices and Cisco IOS releases:

- Catalyst 2900 XL or Catalyst 3500 XL members running Cisco IOS Release 12.0(5)WC2 or earlier



Note Catalyst 2900 XL switches with 4-MB CPU DRAM do not support read-only mode.

- Catalyst 2950 members running Cisco IOS Release 12.0(5)WC2 or earlier
- Catalyst 3550 members running Cisco IOS Release 12.1(6)EA1 or earlier

In read-only mode, these devices appear as unavailable and cannot be configured from Network Assistant.

LRE Profiles

A configuration conflict occurs if a cluster has Long-Reach Ethernet (LRE) switches that use both private and public profiles. If one LRE switch in a cluster is assigned a public profile, all LRE switches in that cluster must have that same public profile. Before you add an LRE switch to a cluster, make sure that you assign it the same public profile used by other LRE switches in the cluster.

A cluster can have a mix of LRE switches that use different private profiles.

Creating a Cluster

To create a cluster, you enable a command device and add cluster members. To ensure that you have a backup command device in case the primary one fails, you should also create a standby group. Finally, you should verify that the cluster contains the devices that you think it contains. This section tells you how to perform these tasks.



Note

Refer to the release notes for the list of devices eligible for clustering, including which ones can be command devices and which ones can only be members.

Enabling a Command Device

Follow these steps to enable a command device:

1. During the setup of the device, assign an IP address and a password to the device. For information about using the setup program, refer to the release notes.
2. Launch Network Assistant, and enter the assigned IP address in the Connect window.
3. Choose **Cluster > Create Cluster** on the feature bar.
4. Use the Create Cluster window to enter a cluster number (the default is 0) and a cluster name.

Adding Cluster Devices

There are two ways to add members to a cluster. The first uses the Add to Cluster window:

1. On the feature bar, choose **Cluster > Add to Cluster** to open the Add to Cluster window.
2. Select a candidate device from the list, click **Add**, and click **OK**.

To add more than one candidate, press **Ctrl** and make your choices, or press **Shift** and choose the first and last switch in a range.

The second way uses the Topology view:

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

Candidates are cyan; members are green. To add more than one candidate, press **Ctrl** and left-click the candidates that you want to add.

You can select 1 or more devices so long as the total number of devices in the cluster does not exceed 16 (including the command device). When a cluster has 16 members, the **Add to Cluster** option is not available for that cluster. In this case, you must remove a member before adding a new one.

If a password has been configured on a candidate switch, you are prompted to enter it before it can be added to the cluster. If the candidate switch does not have a password, any entry is ignored.

If multiple candidates have the same password, you can select them as a group and add them at the same time. If a candidate in the group has a different password from the others, it is not added to the cluster with the others.

When a candidate joins a cluster, it inherits the command-device password.

Creating a Standby Group

Standby group members must meet the requirements described in the [“Standby Command Device Characteristics”](#) section on page 4-1 and the [“HSRP and Standby Command Devices”](#) section on page 4-8.



Note

The Catalyst 4500 series switch does not support standby groups.

Follow these steps to create a standby group:

1. From the feature bar, choose **Cluster > Standby Command Devices**, and use the Standby Command Devices window.
2. Enter a virtual IP address for the standby group. It must be in the same subnet as the IP addresses of the device.
3. Enter a group number that is unique within the IP subnet.
4. Enter a group name of up to 31 characters.

Verifying a Cluster

Follow these steps to verify the cluster:

1. Choose **View > Topology** to display the Topology view.
2. Choose **Reports > Inventory** to display an inventory of the devices in the cluster.
This summary includes device model numbers, serial numbers, software versions, IP information, and location.
3. Display port and device statistics from **Reports > Port Statistics** and **Port > Port Settings > Runtime Status**.



A

accessing

- clusters [4-10](#)
- command devices [4-8](#)
- members [4-10](#)

access ports, cluster connection points [4-7](#)

automatic discovery

- adding members [4-14](#)
- considerations
 - beyond a noncandidate device [4-6](#)
 - connectivity [4-2](#)
 - different VLANs [4-5](#)
 - management VLANs [4-5](#)
 - new devices [4-7](#)
 - non-CDP-capable devices [4-4](#)
 - noncluster-capable devices [4-4](#)
 - routed ports [4-6](#)
- creating standby groups [4-14](#)
- in clusters [4-2](#)
- See also CDP

automatic recovery, clusters

See also HSRP

automatic recovery of clusters [4-8](#)

C

candidates

- adding [4-14](#)
- automatic discovery [4-2](#)
- defined [4-2](#)
- requirements [4-2](#)
- standby group [4-14](#)

candidates (continued)

See also command device, standby group, and members

CDP, automatic discovery in clusters [4-2](#)

clusters

- accessing [4-10](#)
- adding members [4-14](#)
- advantages of [1-1](#)
- automatic discovery [4-2](#)
- automatic recovery [4-8](#)
- creating [4-13](#)
- creating standby groups [4-14](#)
- IP addresses [4-10](#)
- LRE profile considerations [4-13](#)
- planning considerations
 - host names [4-10](#)
 - passwords [4-11](#)
 - RADIUS [4-13](#)
 - SNMP [4-11](#)
 - TACACS+ [4-13](#)
- redundancy [4-14](#)
- size limitation [1-1](#)
- stack considerations [4-11](#)
- verifying [4-15](#)

cluster standby group

See also HSRP

command device

- accessing [4-8](#)
- active [4-8](#)
- passive [4-8](#)
- priority [4-8](#)
- recovery from failure [4-8](#)
- redundant [4-8, 4-14](#)
- requirements [4-1](#)

command device (continued)

standby [4-8](#)

community strings

configuring [4-11](#)

in clusters [4-11](#)

SNMP [4-11](#)

connecting Network Assistant [3-2](#)

D

discovery, clusters

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 [2-2](#)

wizards [2-8](#)

Front Panel view [2-2](#)

G

guide mode [2-7](#)

H

host names in clusters [4-10](#)

HSRP

automatic cluster recovery [4-10](#)

standby group considerations [4-9](#)

See also clusters, cluster standby group, and standby command switch

installing Network Assistant

procedure [3-1](#)

requirements [3-1](#)

interaction modes [2-7](#)

IP addresses

candidate or member [4-2, 4-10](#)

command device [4-10](#)

redundant clusters [4-8](#)

standby command device [4-10](#)

virtual [4-8](#)

See also IP information

L

launching Network Assistant [3-2](#)

LRE profiles, considerations in clusters [4-13](#)

M

management VLAN

considerations in clusters [4-5](#)

discovery through different management VLANs [4-5](#)

members

adding [4-14](#)

automatic discovery [4-2](#)

passwords [4-10](#)

requirements [4-2](#)

menu bar [2-4](#)

N

Network Assistant

- connecting [3-2](#)
- installing
 - new packages [2-8](#)
 - procedure [3-1](#)
 - requirements [3-1](#)
- introduced [1-1](#)
- launching [3-2](#)
- new packages, searching for [2-8](#)

O

- online help [2-9](#)

P

- passwords in clusters [4-11](#)
- privilege levels [2-8](#)

R

- RADIUS in clusters [4-13](#)
- redundant clusters
 - See standby group
- routed ports in clusters [4-6](#)

S

- searching for updates [2-8](#)
- SNMP in clusters [4-11](#)
- stacks in clusters [4-11](#)
- standby command device
 - configuring [4-14](#)
 - considerations [4-9](#)
 - priority [4-8](#)
 - requirements [4-1](#)

standby command device (continued)

- virtual IP address [4-8](#)

standby group

- automatic recovery [4-10](#)
- considerations [4-9](#)
- creating [4-14](#)
- requirements [4-1](#)
- virtual IP address [4-8](#)

T

- TACACS+ in clusters [4-13](#)
- toolbar [2-4](#)
- Topology view [2-2](#)

U

- updates, searching for [2-8](#)

V

- virtual IP address
 - command device [4-8](#)
 - standby group [4-8](#)

W

- wizards [2-8](#)

