

Configuring the Catalyst 4500 Series Switch with Cisco Network Assistant

This chapter describes how to install Network Assistant on the workstation and configure the Catalyst 4500 (or 4900) series switch to communicate with Network Assistant. (Heretofore, the term *Catalyst 4500 series switch* will be used to refer to both switch types.) It also describes how to create communities and clusters. These are two technologies used by Network Assistant to manage a group of network devices, including the Catalyst 4500 series switch.

Network Assistant is a free network management tool that enables you to configure and manage Catalyst 4500 series switches using a Graphical User Interface (GUI). Network Assistant works in both secure and unsecure environments. Network Assistant manages standalone devices or groups of devices or switches (in communities or clusters) from anywhere in your intranet. Using Network Assistant, you can perform multiple configuration tasks without having to remember commands.

**Note**

For complete syntax and usage information for the switch commands used in this chapter, first look at the *Cisco Catalyst 4500 Series Switch Command Reference* and related publications at this location:

<http://www.cisco.com/en/US/products/hw/switches/ps4324/index.html>

If the command is not found in the Catalyst 4500 Series Switch Command Reference, it will be found in the larger Cisco IOS library. Refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at this location:

<http://www.cisco.com/en/US/products/ps6350/index.html>

Configuring and Using the Network Assistant

This chapter contains these topics:

- [Network Assistant-Related Features and Their Defaults, page 12-2](#)
- [Overview of the CLI Commands, page 12-2](#)
- [Configuring Your Switch for Network Assistant, page 12-3](#)

- [Managing a Network using Community, page 12-5](#)
- [Converting a Cluster into a Community, page 12-9](#)
- [Managing a Network using Cluster, page 12-10](#)
- [Configuring Network Assistant in Community or Cluster Mode, page 12-13](#)

**Note**

The Network Assistant is not bundled with an online software image on Cisco.com. You can download the Network Assistant at this location:

<http://www.cisco.com/en/US/products/ps5931/index.html>

**Note**

For information on software and hardware requirements, installing Network Assistant, launching Network Assistant, and connecting Network Assistant to a device refer to *Getting Started with Cisco Network Assistant*, available at the URL:

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

Network Assistant-Related Features and Their Defaults

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

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

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

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

Overview of the CLI Commands

Table 2 is an overview of the Network Assistant-related CLI commands.

Table 2 CLI Commands

Command	Functions
[no] cluster enable	Names the cluster.
[no] cluster run	Enables clustering. Note This command is used strictly for clustering.
[no] ip http server	Configures the HTTP on a switch.
[no] ip http port <i>port_number</i>	Configures the HTTP port.
[no] ip domain-name <i>domain_name</i>	Configures the domain on the switch.
[no] ip http secure-server	Configures and enable HTTPS on a switch.
[no] ip http secure-port <i>port_number</i>	Configures the HTTPS port.
[no] ip http max-connections <i>connection_number</i>	Configures the maximum concurrent connections to the HTTP server.
[no] ip http timeout-policy <i>idle idle_time life life_time requests requests</i>	Configures the HTTPS port. A idle value of 180 seconds is recommended. A life value of 180 seconds is recommended. The recommended maximum number of requests allowed is 25.
line vty	Configures additional VTYS for use by CNA.
show version	Displays the Cisco IOS release.
show running-config	Displays the switch configuration.
vtp domain	Creates a VTP domain to manage VLANs.
vtp mode	Sets the behavior for VTP management of the VLANs.

Configuring Your Switch for Network Assistant

The following topics are discussed:

- [\(Minimum\) Configuration Required to Access Catalyst 4500 Accessible from CNA, page 12-3](#)
- [\(Additional\) Configuration Required to use Community, page 12-4](#)
- [\(Additional\) Configuration Required to use Cluster, page 12-5](#)

(Minimum) Configuration Required to Access Catalyst 4500 Accessible from CNA

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

	Command	Purpose
Step 1	Switch# configure terminal	Enters global configuration mode.
Step 2	Switch(config)# ip http server or Switch(config)# ip domain-name <i>domain_name</i>	(HTTP only) Enables the HTTP server on the switch. By default, the HTTP server is disabled. Enables the domain name on the switch to configure HTTPS.
Step 3	Switch(config)# ip http secure-server	Enables 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>	Configures the maximum concurrent connections to the HTTP server. <i>A connection_number</i> of 16 is recommended.
Step 5	Switch(config)# ip http timeout-policy idle <i>idle_time</i> life <i>life_time</i> requests <i>requests</i>	Configures the HTTPS port. The idle keyword specifies the maximum amount of time a connection can stay idle. A idle value of 180 seconds is recommended. The life keyword specifies the maximum amount of time a connection can stay open since it was established. A life value of 180 seconds is recommended. The requests keyword specifies the maximum amount of requests on a connection. The recommended maximum number of requests allowed is 25.
Step 6	Switch(config-if)# end	Returns to privileged EXEC mode.
Step 7	Switch# show running-config	Verifies the configuration.

**Note**

If you have enabled clustering, disable clustering before configuring a community (see [Table 2](#)).

(Additional) Configuration Required to use Community

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

	Command	Purpose
Step 1	Switch# configuration terminal	Enters global configuration mode.
Step 2	Switch(config)# interface { vlan <i>vlan_ID</i> { fastethernet gigabitethernet } <i>slot/interface</i> port-channel <i>number</i> }	Selects an interface.
Step 3	Switch(config-if)# ip address <i>ip_address</i> <i>address_mask</i>	(Optional) Assigns 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.

	Command	Purpose
Step 4	Switch(config-if)# end	Returns to privileged EXEC mode.
Step 5	Switch# show running-config	Verifies the configuration.

(Additional) Configuration Required to use 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	Enters global configuration mode.
Step 2	Switch(config)# cluster run	Enables clustering.
		 <p>Note Enable clustering on all switches that are part of the potential cluster.</p>
Step 3	Switch(config)# cluster enable	Names the cluster.
Step 4	Switch(config)# interface { vlan <i>vlan_ID</i> { fastethernet gigabitethernet } <i>slot/interface</i> Port-channel <i>number</i> }	Selects an interface.
Step 5	Switch(config-if)# ip address <i>ip_address address_mask</i>	(Optional) Assigns an IP address to the Catalyst 4500 series switch cluster master.
		 <p>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.</p>
Step 6	Switch(config-if)# end	Returns to privileged EXEC mode.
Step 7	Switch# show running-config	Verifies the configuration.

Managing a Network using Community

This section describes how to use communities to manage *devices* (including Catalyst 4500 series switches, routers, access points, and PIX firewalls) using the Network Assistant application.

When you use communities to group the switches in your network, the only requirements are an HTTP server and that you configure an IP address on each switch.

The total number of devices in the community cannot exceed 20 total devices (including up to 4 Catalyst 4500 series switches (modular), 16 Catalyst 2900/3500 or Catalyst 4948/4948-10GE switches ((non-modular), 2 routers, and 2 PIX firewalls).



Note

Access points have been eliminated from the device limits. There is no current limit for the number of access points that can be managed by CNA.

**Note**

The **Add to Community** dialog display any number of devices, but only allows you to select 20 devices. If you try to add a 21st device, the dialog displays the 21st device and prompts you to select the unwanted device.

**Note**

For complete procedures for using Network Assistant to configure switch communities, refer to *Getting Started with Cisco Network Assistant*, available at:

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

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

- [Candidate and Member Characteristics](#), page 12-6
- [Automatic Discovery of Candidates and Members](#), page 12-7
- [Community Names](#), page 12-7
- [Hostnames](#), page 12-7
- [Passwords](#), page 12-8
- [Access Modes in Network Assistant](#), page 12-8
- [Community Information](#), page 12-8

Candidate and Member Characteristics

Candidates are network devices that have IP addresses but are not part of a community. Members are network devices that are currently part of a community.

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

- It has an IP address.
- Cisco Discovery Protocol (CDP) version 2 is enabled (the default) - if you want the device to be autodiscovered.
- It has HTTP (or HTTPS) enabled.

**Note**

A cluster member can be added to a community, but the reverse is not possible.

**Note**

If the cluster commander is added to a community, the other member devices of the cluster are not added automatically. The cluster members must be added to the community on an individual basis in order to be managed.

Automatic Discovery of Candidates and Members

Network Assistant forms a community using CDP to locate or discover all the available devices in the network. Beginning with the IP address for a starting device and the port numbers for HTTP (or HTTPS) protocols, Network Assistant uses CDP to compile a list of community candidates that neighbor the starting device. Network Assistant can discover candidate and member devices across multiple networks and VLANs as long as they have valid IP addresses.

**Note**

By default, Network Assistant in community mode discovers up to four hops away.

See the [“Candidate and Member Characteristics”](#) section on page 12-6 for a list of requirements that network devices must meet in order to be discovered.

**Note**

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

**Note**

PIX firewalls do not support the CDP, so they are not automatically shown as neighbors in the Topology view. They are shown only after you add them to a community with the Create Community or Modify Community window. To see a PIX firewall link to another community member, you must add the link manually by selecting ADD Link in a Topology popup menu.

You can edit the list of discovered devices to fit your needs and add them to the community. As each device is added to the community, its neighbors are discovered and added to the list of candidate devices. If Network Assistant fails to discover a device you can add it manually through the IP management IP address.

Community Names

When you apply the community configuration information to the list of member devices, Network Assistant requests that you enter a name (or IP address) for the community. You need to assign a name to the community before you can manage it. Network Assistant saves the name to your PC.

The community name can consist of the characters 0-9, a-z and A-Z, with spaces allowed between the characters.

**Note**

You can connect to a cluster only through an IP address. When you select a name it is always for the community.

Hostnames

You do not need to assign a hostname to a starting device or a community member. However, Cisco recommends it and Network Assistant does not assign one by default. If a discovered device does have a hostname, Network Assistant saves it to your PC as identifying information for that device along with its IP address, communication protocol, and designated protocol port.

Passwords

Although you do not need to assign a password to a device if it will become a community member, Cisco recommends that you do so.

Community members can have different passwords.

Communication Protocols

Network Assistant uses the HTTP (or HTTPS) protocols to communicate with network devices. It attempts communication with HTTP (or HTTPS) when using CDP to discover candidate devices.

Access Modes in Network Assistant

When Network Assistant is connected to a community or cluster, two access modes are available: read-write and read-only, depending on the password.

Community Information

Network Assistant saves all community configuration information and individual device information such as IP address, hostname, and 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 attempt to use a different PC to manage an existing community, the member device information will not be available. You will need to create the community again and add the same member devices.

Adding Devices

There are three ways to add members to a community.

The first uses the Devices Found window on Network Assistant to add devices that you discovered to a new community:

- a. In the Devices Found window, select candidate devices that you wish to add.
To add 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 **Add**.

The second way uses the Modify Community window to add devices to an existing community:

- a. Choose **Application > Communities** to open the Communities window.
- b. In the Communities window, select the name of the community to which you would like to add a device, and click **Modify**.
- c. To add a single device manually, enter the IP address for the desired device in the Modify Community window, and click **Add**.
- d. To discover candidate devices, enter the IP address for the starting device, and click **Discover**.
- e. 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 device in a range.

The third way to add a device uses the Topology view:

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

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

When a community has 20 members, the **Add to Community** option is not available for that community. In this case, you must remove a member before adding a new one.



Note

If you are logged into a community and you delete that community from some other CNA instance, then unless you close that community session, you can perform all the configurations through that session. After you close that session (and thereby delete the community), you will not be able to connect to that community.

Converting a Cluster into a Community

The Cluster Conversion wizard helps you convert a cluster into a community. When you complete the conversion, you can immediately manage the device group as a community. The benefits of managing a community is that the communication with the devices in a community is more secure (through multiple passwords and HTTPS) than in a cluster. Moreover, device availability is greater, and the range of devices that can be members is broader.



Note

The Cluster Conversion wizard does not alter your cluster definition. This means that you can still manage the devices as a cluster.

To launch the Cluster Conversion Wizard, follow these steps:

- Step 1** Start Network Assistant and connect to an existing cluster through its commander IP address.
- Step 2** In the feature bar, click **Configure > Cluster > Cluster Conversion Wizard**.
You will see the query "Do you want to convert this cluster to a community?"
- Step 3** Select **Yes** to proceed or **No** if you want to manually bring up the Cluster Conversion Wizard.
If you select **Yes**, the Welcome screen appears, providing information about clusters, communities, and their benefits.
Next, a table appears listing the devices in the cluster starting with those that have no IP address and subnet mask. Be aware that all the devices in the cluster must have an IP address and subnet mask to be members of a community.
- Note** If a device has more than one interface with an IP address and subnet mask, you see more than one interface listed when you click in the cell. You can choose a different interface from the one originally shown.
- Step 4** In the IP Address column, enter an IP address for each device that does not have one.
- Step 5** In the Subnet Mask column, click in the cell for each device that does not have a subnet mask and select one.

Step 6 Enter a name for the community.

Step 7 Click **Finish** to begin the conversion.

When the conversion completes, Network Assistant restarts and automatically connects to the newly created community.



Note

If you have enabled clustering, you should disable clustering before configuring a community (see [Table 2](#)).

Managing a Network using Cluster

This section describes how to use clustering to create and manage Catalyst 4500 series switches using the standalone Network Assistant application or the command-line interface (CLI).

You can use clustering to group the switches in your network. You must enter the cluster run command on each switch to be managed. The major advantage is that you can manage 16 devices with one IP address.



Note

Clustering is the auto- discovering mechanism used in CNA 1.0.



Note

For complete procedures for using Network Assistant to configure switch clusters, refer to *Getting Started with Cisco Network Assistant*, available at:

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

This section contains the following topics:

- [Understanding Switch Clusters, page 12-10](#)
- [Using the CLI to Manage Switch Clusters, page 12-12](#)

Understanding Switch Clusters

These sections describe:

- [Clustering Overview, page 12-10](#)
- [Cluster Command Switch Characteristics, page 12-11](#)
- [Candidate Switch and Cluster Member Switch Characteristics, page 12-12](#)

Clustering Overview

A *switch cluster* is a set of up to 16 connected, cluster-capable Catalyst switches that are managed as a single entity. The switches in the cluster use the switch clustering technology so that you can configure and troubleshoot a group of different Catalyst 4500 series switch platforms through a single IP address.

Using switch clusters simplifies the management of multiple switches, regardless of their physical location and platform families.

**Note**

By default, Network Assistant in clustering mode discovers up to seven hops away.

In a switch cluster, one switch must be the *cluster commander switch*, and up to 15 other switches can be *cluster member switches*. The total number of switches in a cluster cannot exceed 16 switches. The cluster command switch is the single point of access used to configure, manage, and monitor the cluster member switches. Cluster members can belong to only one cluster at a time.

**Note**

Always choose a Catalyst 4500 or 4948 series switch as the cluster command switch.

Cluster Command Switch Characteristics

A cluster command switch must meet these requirements:

- It is using Cisco IOS Release 12.2(20)EWA or later.
- It has an IP address.
- It has Cisco Discovery Protocol (CDP) version 2 enabled (the default).
- It is using cluster-capable software and has clustering enabled.
- It has IP HTTP (or HTTPS) server enabled.

**Note**

On a Catalyst 4500 series switch, neither HTTP or HTTPS is enabled by default.

- It has 16 VTY lines.

**Note**

On a Catalyst 4500 series switch, the default is 4 lines. You configure the switch to set the value to 16.

- It is not a command or cluster member switch of another cluster.

**Note**

If your switch cluster contains a Catalyst 4500 series switch, the cluster command switch must also be a Catalyst 4500 series switch.

Network Assistant and VTY

Network Assistant uses virtual terminal (VTY) lines to communicate with the cluster command device. Catalyst 4500 series switches have 5 VTY lines configured by default. Network Assistant can employ an additional 8 lines. Therefore, you should configure the maximum number of lines (or at least, $8 + 5 = 13$) so that Network Assistant can communicate with the switch and not use VTY lines that might be needed for telnet.

You can configure the Catalyst 4500 series switch to support an appropriate number of VTY lines with the **line vty** configuration command. For example, the **line vty 6 15** command configures the switch to include 9 VTY lines.

**Note**

If your existing VTY lines have non-default configurations, you might want to apply those configurations to the new VTY lines.

Candidate Switch and Cluster Member Switch Characteristics

Candidate switches are cluster-capable switches that are not part of a cluster. Cluster member switches are switches that are currently part of a switch cluster. Although not required, a candidate or cluster member switch can have its own IP address and password.



Note

The hostname of a candidate should not be in the form [a-zA-Z0-9]-*n*, where *n* is 0-16. These names are reserved.

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

- It is running cluster-capable software and has clustering enabled.
- It has CDP version 2 enabled.
- It has HTTP server enabled.



Note

Even when HTTP is enabled on the commander switch, communication between the commander switch and member switch is still carried over HTTP. So, it is not secure.

- It has 16 VTY lines.
- It is not a command or cluster member switch of another cluster.
- It is connected to the cluster command switch through at least one common VLAN.

It is recommended that you configure the Catalyst 4500 candidate and cluster member switches with an SVI on the VLAN connection to the cluster command switch.

Using the CLI to Manage Switch Clusters

You can configure cluster member switches from the CLI by first logging in to the cluster command switch. Enter the **rcommand** user EXEC command and the cluster member switch number to start a Telnet session (through a console or Telnet connection) and to access the cluster member switch CLI. The command mode changes and the Cisco IOS commands operate as usual. Enter the **exit** privileged EXEC command on the cluster member switch to return to the command-switch CLI.

This example shows how to log in to member-switch 3 from the command-switch CLI:

```
switch# rcommand 3
```

If you do not know the member-switch number, enter the **show cluster members** privileged EXEC command on the cluster command switch. For more information about the **rcommand** command and all other cluster commands, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference*.

The Telnet session accesses the member-switch CLI at the same privilege level as on the cluster command switch. The Cisco IOS commands then operate as usual. For instructions on configuring the switch for a Telnet session, see the [“Accessing the CLI Through Telnet”](#) section on page 2-2.



Note

CISCO-CLUSTER_MIB is not supported.

Configuring Network Assistant in Community or Cluster Mode

This section provides a detailed explanation of the CLI used to configure Network Assistant to work in a community or cluster. Network Assistant communicates with a Catalyst 4500 series switch by sending Cisco IOS commands over an HTTP (or HTTPS) connection.

The following topics are discussed:

- [Configuring Network Assistant in on a Networked Switch in Community Mode, page 12-13](#)
- [Configuring Network Assistant in a Networked Switch in Cluster Mode, page 12-17](#)

Configuring Network Assistant in on a Networked Switch in Community Mode

To configure Network Assistant on a networked switch in community mode, follow these steps:

	Command	Purpose
Step 1	Switch# configure terminal	Enters global configuration mode.
Step 2	Switch(config)# enable password name	Enables password protection of configuration mode.
Step 3	Switch(config)# vtp domain name	Creates a VTP domain to manage VLAN.
Step 4	Switch(config)# vlan vlan_id	Creates a VLAN.
Step 5	Switch(config-vlan)# interface {vlan vlan_ID {fastethernet gigabitethernet} slot/interface Port-channel number}	Selects the interface that will connect to your CNA-enabled PC.
Step 6	Switch(config-if)# switchport access vlan vlan_id	Enables the selected interface to be in the specified VLAN.
Step 7	Switch(config-if)# interface {vlan vlan_ID slot/interface Port-channel number}	Select the VLAN instance for configuration.
Step 8	Switch(config-if)# ip address ip_address	Assigns an IP address to the SVI.
Step 9	Switch(config-if)# no shutdown	Enables the interface.
Step 10	Switch(config-if)# ip http server	Starts the HTTP server so that Network Assistant can talk to the switch.
Step 11	Switch(config)# ip domain-name domain_name	Enables the domain name on the switch to configure HTTPS.
Step 12	Switch(config)# ip http secure-server	Enables the HTTPS server on the switch. By default, the HTTPS server is disabled.
Step 13	Switch(config)# ip http max-connections connection_number	Configures the maximum concurrent connections to the HTTP server. A <i>connection_number</i> of 16 is recommended.

	Command	Purpose
Step 14	Switch(config)# ip http timeout-policy idle <i>idle_time life life_time requests requests</i>	Configures the HTTPS port. The idle keyword specifies the maximum amount of time a connection can stay idle. A idle value of 180 seconds is recommended. The life keyword specifies the maximum amount of time a connection can stay open since it was established. A life value of 180 seconds is recommended. The requests keyword specifies the maximum number of requests on a connection. A requests value of 25 recommended.
Step 15	Switch(config-if)# ip http secure-server	(Optionally) Enables the switch to accept HTTPS connections from Network Assistant.
Step 16	Switch(config)# ip route <i>a.b.c</i>	Establishes the route to the default router, usually supplied by the local Internet Provider. Note This line represents the only difference between the configuration for a standalone and a networked switch.
Step 17	Switch(config)# line con 0	Select the console port to perform the configuration.
Step 18	Switch(config-line)# exec-timeout <i>x y</i>	Configures an automatic session logout if no keyboard input or output is displayed on the terminal.
Step 19	Switch(config-line)# password <i>password</i>	Specifies a password for the console port.
Step 20	Switch(config-line)# login	Allows login to the console port.
Step 21	Switch(config-line)# line vty <i>x y</i>	Creates additional VTY lines for CNA to access the switch.
Step 22	Switch(config-line)# password <i>password</i>	Specifies a password for the switch.
Step 23	Switch(config-line)# login	Allows login to the switch.
Step 24	Switch(config-line)# line vty <i>x y</i>	Creates additional VTY lines for CNA to access the switch.
Step 25	Switch(config-line)# password <i>password</i>	Specifies a password for the switch.
Step 26	Switch(config-line)# login	Allows login to the switch.
Step 27	Switch(config-line)# end	Returns to privileged EXEC mode.
Step 28	Switch# show running-config	Verifies the configuration.

This example shows how to configure Network Assistant on a networked switch in community mode:

```
Switch# configure terminal
Switch(config)# vtp domain cnadoc
Changing VTP domain name from cisco to cnadoc
Switch(config)# vlan 2
Switch(config-vlan)# exit
Switch(config)# interface GigabitEthernet 2/1
Switch(config-if)# switchport access vlan 2
Switch(config-if)# exit
Switch(config)# interface vlan 2
Switch(config-if)# ip address 123.123.123.1 255.255.255.0
Switch(config-if)# no shutdown
```

```

Switch(config-if)# exit
Switch(config)# ip http server
Switch(config)# ip domain-name cisco.com
Switch(config)# ip http secure-server
Switch(config)# ip http max-connections 16
Switch(config)# ip http timeout-policy idle 180 life 180 requests 25
Switch(config)# ip route 0.0.0.0 0.0.0.0 123.123.123.2
Switch(config)# line con 0
Switch(config-line)# exec-timeout 0 0
Switch(config-line)# password keepout
Switch(config-line)# login
Switch(config-line)# line vty 5 15
Switch(config-line)# password keepout
Switch(config-line)# login
Switch(config-line)# line vty 5 15
Switch(config-line)# end
Switch# show running-config
Building configuration...

Current configuration : 1426 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service compress-config
!
hostname Switch
!
boot-start-marker
boot-end-marker
!
enable password cna
!
no aaa new-model
ip subnet-zero
ip domain-name cisco.com
!
vtp domain cnadoc
vtp mode transparent
!
crypto pki trustpoint TP-self-signed-913087
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-913087
  revocation-check none
  rsakeypair TP-self-signed-913087
!!
crypto pki certificate chain TP-self-signed-913087
certificate self-signed 01
  3082028E 308201F7 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  52312B30 29060355 04031322 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 39313330 38373123 30210609 2A864886 F70D0109 02161456
  61646572 2D343531 302E6369 73636F2E 636F6D30 1E170D30 36303432 30323332
  3435305A 170D3230 30313031 30303030 30305A30 52312B30 29060355 04031322
  494F532D 53656C66 2D536967 6E65642D 43657274 69666963 6174652D 39313330
  38373123 30210609 2A864886 F70D0109 02161456 61646572 2D343531 302E6369
  73636F2E 636F6D30 819F300D 06092A86 4886F70D 01010105 0003818D 00308189
  02818100 F2C86FEA 49C37856 D1FA7CB2 9AFF748C DD443295 F6EC900A E83CDA8E
  FF8F9367 0A1E7A20 C0D3919F 0BAC2113 5EE37525 94CF24CF 7B313C01 BF177A73
  494B1096 B4D24729 E087B39C E44ED9F3 FCCD04BB 4AD3C6BF 66E0902D E234D08F

```

```

E6F6C001 BAC80854 D4668160 9299FC73 C14A33F3 51A17BF5 8C0BEA07 3AC03D84
889F2661 02030100 01A37430 72300F06 03551D13 0101FF04 05300301 01FF301F
0603551D 11041830 16821456 61646572 2D343531 302E6369 73636F2E 636F6D30
1F060355 1D230418 30168014 BB013B0D 00391D79 B628F2B3 74FC62B4 077AD908
301D0603 551D0E04 160414BB 013B0D00 391D79B6 28F2B374 FC62B407 7AD90830
0D06092A 864886F7 0D010104 05000381 81002963 26762EFA C52BA4B3 6E641A9D
742CE404 E45FECB1 B5BD2E74 6F682476 A7C3DAA5 94393AE3 AA103B6E 5974F81B
09DF16AE 7F9AE67C 5CB3D5B1 B945A5F3 36A8CC8C 8F142364 F849344D 5AE36410
51182EB9 24A9330B 3583E1A3 79151470 D304C157 3417E240 52BE2A91 FC7BBEDE
562BEDAD E6C46D9A F7FF3148 4CE9CEE1 5B17
quit
!
!
!
power redundancy-mode redundant
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 2
!
interface GigabitEthernet1/1
 switchport access vlan 2
!
interface GigabitEthernet1/2
!
interface GigabitEthernet1/3
!
interface GigabitEthernet1/4
!
interface GigabitEthernet1/5
!
interface GigabitEthernet1/6
!
interface GigabitEthernet1/7
!
interface GigabitEthernet1/8
!
interface GigabitEthernet1/9
!
interface GigabitEthernet1/10
!
interface GigabitEthernet1/11
!
interface GigabitEthernet1/12
!
interface GigabitEthernet1/13
!
interface GigabitEthernet1/14
!
interface GigabitEthernet1/15
!
interface GigabitEthernet1/16
!
interface GigabitEthernet1/17
!
interface GigabitEthernet1/18
!

```

```

interface GigabitEthernet1/19
!
interface GigabitEthernet1/20
!
interface Vlan1
no ip address
!
interface Vlan2
ip address 123.123.123.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 123.123.123.2
ip http server
ip http secure-server
ip http max-connections 16
ip http timeout-policy idle 180 life 180 requests 25
!
line con 0
password cna
login
stopbits 1
line vty 0 4
password cna
login
line vty 5 15
password cna
login
!
!
end

Switch#

```

Configuring Network Assistant in a Networked Switch in Cluster Mode

To configure Network Assistant on a networked switch in cluster mode, perform this task on the switch:

	Command	Purpose
Step 1	Switch# configure terminal	Enters global configuration mode.
Step 2	Switch(config)# enable password name	Enables password protection of configuration mode.
Step 3	Switch(config)# vtp domain name	Creates a VTP domain to manage VLANs and names.
Step 4	Switch(config)# cluster run	Launches the cluster on the cluster commander.
Step 5	Switch(config)# cluster enable cluster_name	Makes the switch the cluster commander.
Step 6	Switch(config)# vlan vlan_id	Creates a VLAN.
Step 7	Switch(config-vlan)# interface {vlan vlan_ID {fastethernet gigabitethernet} slot/interface Port-channel number}	Selects the interface that will connect to your CNA-enabled PC.
Step 8	Switch(config-if)# switchport access vlan vlan_id	Enables the physical port to be in the specified VLAN.
Step 9	Switch(config-if)# interface {vlan vlan_ID slot/interface Port-channel number}	Select the VLAN instance for configuration.
Step 10	Switch(config-if)# ip address ip_address	Assigns an IP address to the SVI.
Step 11	Switch(config-if)# no shut	Enables the interface.

	Command	Purpose
Step 12	Switch(config-if)# ip http server	Starts the HTTP server so that Network Assistant can talk to the switch.
Step 13	Switch(config)# ip http secure-server	(Optionally) Enables the switch to accept HTTPS connections from Network Assistant.
Step 14	Switch(config)# ip route a.b.c	Establishes the route to the default router, usually supplied by the local Internet Provider. Note This line represents the only difference between the configuration for a standalone and a networked switch.
Step 15	Switch(config)# line con 0	Select the console port to perform the configuration.
Step 16	Switch(config-line)# exec-timeout x y	Configures an automatic session logout if no keyboard input or output is displayed on the terminal.
Step 17	Switch(config-line)# password password	Specifies a password for the console port.
Step 18	Switch(config-line)# login	Allows login to the console port.
Step 19	Switch(config-line)# line vty x y	Creates additional VTY lines for CNA to access the switch.
Step 20	Switch(config-line)# password password	Specifies a password for the switch.
Step 21	Switch(config-line)# login	Allows login to the switch.
Step 22	Switch(config-line)# line vty x y	Creates additional VTY lines for CNA to access the switch.
Step 23	Switch(config-line)# password password	Specifies a password for the switch.
Step 24	Switch(config-line)# login	Allows login to the switch.
Step 25	Switch(config-line)# end	Returns to privileged EXEC mode.
Step 26	Switch# show running-config include http	Verifies that the HTTP server is enabled.

This example shows how to configure Network Assistant on a networked switch in cluster mode:

```
Switch# configure terminal
Switch(config)# vtp domain cnadoc
Switch(config)# cluster run
Switch(config)# cluster enable cnadoc
Switch(config)# vlan 10
Switch(config-vlan)# interface GigabitEthernet 2/1
Switch(config-if)# switchport access vlan 10
Switch(config-if)# interface vlan10
Switch(config-if)# ip address aa.bb.cc.dd
Switch(config-if)# no shut
Switch(config-if)# ip http server
Switch(config-if)# ip http secure-server
Switch(config)# ip route 0.0.0.0 0.0.0.0 123.123.123.2
Switch(config)# line con 0
Switch(config-line)# exec-timeout 0 0
Switch(config-line)# password keepout
Switch(config-line)# login
Switch(config-line)# line vty 5 15
Switch(config-line)# password keepout
Switch(config-line)# login
Switch(config-line)# line vty 5 15
Switch(config-line)# end
Switch# show running-config
Building configuration...
```

```
Current configuration : 1469 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service compress-config
!
hostname Switch
!
boot-start-marker
boot-end-marker
!
enable password cna
!
no aaa new-model
ip subnet-zero
!
vtp domain cnadoc
vtp mode transparent
cluster run
cluster enable cnadoccluster 0
!
!
!
!
power redundancy-mode redundant
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 2
!
interface GigabitEthernet1/1
    switchport access vlan 2
!
interface GigabitEthernet1/2
!
interface GigabitEthernet1/3
!
interface GigabitEthernet1/4
!
interface GigabitEthernet1/5
!
interface GigabitEthernet1/6
!
interface GigabitEthernet1/7
!
interface GigabitEthernet1/8
!
interface GigabitEthernet1/9
!
interface GigabitEthernet1/10
!
interface GigabitEthernet1/11
!
```

```
interface GigabitEthernet1/12
!
interface GigabitEthernet1/13
!
interface GigabitEthernet1/14
!
interface GigabitEthernet1/15
!
interface GigabitEthernet1/16
!
interface GigabitEthernet1/17
!
interface GigabitEthernet1/18
!
interface GigabitEthernet1/19
!
interface GigabitEthernet1/20
!
interface Vlan1
  no ip address
!
interface Vlan2
  ip address 123.123.123.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 123.123.123.2
ip http server
no ip http secure-server
!
!
!
line con 0

Switch#
```