Configuring Switches with Web-Based Tools

This chapter describes how to install and configure the Network Assistant on the Catalyst 4500 (or Catalyst 4948) series switch. (Heretofore, the term *Catalyst 4500 series switch* will be used to refer to both switch types.) It also describes how to create and manage a group of devices or Catalyst 4500 series switches using communities or clusters.

Network Assistant is a Windows-based Java application that sends Cisco IOS commands to configure and manage the Catalyst 4500 series switch over HTTP. 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.

This chapter also describes how to install and configure the Embedded CiscoView network management system to provide a graphical representation of a Catalyst 4500 series switch and to provide a GUI-based management and configuration interface.

This chapter describes these topics:

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

Configuring and Using the Network Assistant

This chapter contains these topics:

Installation Requirements

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

- Processor speed: Pentium 1 GHz
- DRAM: 256 MB
- Number of colors: 65536
- Resolution: 1024 x 768
- Font size: Small

Network Assistant supports the following client platforms:

- Windows 2000 Professional SP4
- Windows XP Professional SP2

Software and Hardware Requirements

The minimum Cisco IOS software required on the Catalyst 4500 series switch is Cisco IOS Release 12.2(20)EWA.

Table 1 lists the hardware required to support the Network Assistant.

Table 1 Hardware Supported for Network Assistant 2.0 Support

Type	Part Number
Chassis	WS-C4503
	WS-C4506
	WS-C4507R
	WS-C4948
Power supplies	PWR-C45-1000AC
	PWR-C45-1300ACV
	PWR-C45-2800AC
Supervisors	WS-X4013+
	WS-X4013+TS
	WS-X4515
Modules	WS-X4124-RJ45
	WS-X4148-RJ
	WS-X4224-RJ45V

Table 1 Hardware Supported for Network Assistant 2.0 Support (continued)

Type	Part Number
	WS-X4248-RJ45V
	WS-X4306-GB
	WS-X4424-GB-RJ45
	WS-X4506-GB-T
	WS-X4524-GB-RJ45V
	WS-X4548-GB-RJ45
	WS-X4548-GB-RJ45V

Network Assistant-Related Features and Their Defaults

Table 2 lists the Network Assistant-related configuration parameters on a Catalyst 4500 series switch.

Table 2 Network Assistant-Related Configuration on a Catalyst 4500 Series Switch

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

1. Does not require any configuration work besides enabling the HTTP server and ensuring that an IP address is defined on a Catalyst 4500 series switch interface port.
2. You need to set an IP address in each switch for community device discovery and for the cluster commander.
3. Port number on the Network Assistant and the Catalyst 4500 series switch must match.
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 3 is an overview of the Network Assistant-related CLI commands.

Table 3 CLI Commands

Command	Functions
cluster enable	Names the cluster.
cluster run	Enables clustering.[1]

Table 3 CLI Commands

Command	Functions
[**no**] **ip http authentication** {**enable** | **local** | **tacacs**}	Configures the HTTP authentication.
[no] ip http server	Configures the HTTP server on the switch.
[no] ip http port *port_number*	Configures the HTTP port.
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.

1. This command is used strictly for clustering.

Installing Network Assistant

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

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

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

Step 2 Click on Free Download.

Step 3 Find the latest version of the Network Assistant installer.

Step 4 Download the Network Assistant Installer and install the application. (You can operate the installer 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 initiate the installer, follow the displayed instructions. In the final panel, click **Finish** to complete the installation of Network Assistant.

Getting Started with Network Assistant

If you use the default configuration, access the Catalyst 4500 series switch and enter the **ip http server** global configuration command:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# ip http server`	Enables the HTTP server on the switch. By default, the HTTP server is disabled.
Step 3	`Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 4	`Switch# show running-config`	Verifies the configuration.

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 vlan_ID | {fastethernet | gigabitethernet} slot/interface | Port-channel number}`	Selects an interface.
Step 3	`Switch(config-if)# ip address ip_address address_mask`	(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.
Step 4	`Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 5	`Switch# show running-config`	Verifies the configuration.

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. **Note** Enable clustering on all switches that are part of the potential cluster.
Step 3	`Switch(config)# interface {vlan vlan_ID | {fastethernet | gigabitethernet} slot/interface | Port-channel number}`	Selects an interface.
Step 4	`Switch(config-if)# ip address ip_address address_mask`	(Optional) Assigns an IP address to the Catalyst 4500 series switch cluster master. **Note** This step is mandatory if the switch is part of a community or is a cluster command switch. This step is optional if the switch is a cluster member candidate.
Step 5	`Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 6	`Switch# show running-config`	Verifies the configuration.

Launching the Network Assistant

After installing Network Assistant, you will see its icon on your desktop. You will also see a Network Assistant entry under **Start > Programs** and a Network Assistant executable file in the installation directory. When you select any of these items, two windows will appear: the Network Assistant window, in disconnect mode, and the Connect window.

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

Connecting Network Assistant to a Device

To connect the Network Assistant to a device, use the Connect window, shown in. In this window, enter the IP address of the device to which you want to connect. If you are authorized to configure the device and the HTTP port of the device is 80, you can ignore the settings in the **Options** button.

Note The HTTP port cannot be configured on a Catalyst 4500 series switch running Network Assistant with Release 12.2(20)EWA.

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

When the connection occurs, the Network Assistant window is in the connect mode. The toolbar adds icons that represent device features. The disconnected icon changes to connected.

Similarly, the feature bar fills with menus that list the device features that Network Assistant manages.

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.

Using Community Mode to Manage a Network of Switches

This section describes how to use communities to create and manage Catalyst 4500 series switches (called *devices*) using the standalone Network Assistant application.

Beginning with Network Assistant 2.0, you can use communities to group the switches in your network. In contrast with clusters (described next), communities do not require a special IOS configuration. The only requirement is that you configure an IP address on each switch. Be aware that management of routers and access points is supported only in communities.

The total number of devices in the community does not exceed 20 total devices (including up to 4 Catalyst 4500 series switches (modular), 16 Catalyst 2900/3500 or Catalyst 4948 switches (non-modular), 2 routers, and 12 access points). 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.

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

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

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

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

Note A cluster member can be added to a community, but a cluster cannot.

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

Beginning with the IP address for a starting device and the port numbers for HTTP 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 4 hops away.

See the "Candidate and Member Characteristics" section on page 9-7 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.

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 via the IP management address.

Community Names

When you apply the community configuration information to the list of member devices, Network Assistant requests that you enter a name 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 via an IP address. When you select a name it is always for the community.

Host Names

You do not need to assign a host name 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 host name, 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 protocols to communicate with network devices. It attempts communication with HTTP 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, host name, 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 > 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) 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 **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.

Using Cluster Mode to Manage a Network of Switches

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).

Beginning with Network Assistant 1.0 and 2.0, 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 Catalyst 4500 series switches 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 and communities, refer to *Getting Started with Cisco Network Assistant*, available at:
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cna/v2_0/gsg/index.htmCisco.com.
For the CLI cluster commands, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122sr/cr/index.htm

This section contains the following topics:

Understanding Switch Clusters

These sections describe:

Note Clustering is disabled by default on the Catalyst 4500 series switch.

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 7 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 chose a Catalyst 4500 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 server enabled.
- It has 16 VTY lines.
- 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 have not yet been added to a cluster. Cluster member switches are switches that have been added to a switch cluster. Although not required, a candidate or cluster member switch can have its own IP address and password.

Note The host name 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.
- 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.

  Catalyst 4500 candidate and cluster member switches must be configured 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 connection.

The following topics are discussed:

Configuring Network Assistant in Community Mode

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

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# vtp domain name`	Creates a VTP domain to manage VLAN.
Step 3	`Switch(config)# vtp mode transparent`	Establishes the behavior for VTP management of the VLANs.
Step 4	`Switch(config)# vlan vlan_id`	Creates a VLAN.
Step 5	`Switch(config)# interface {vlan vlan_ID | {fastethernet | gigabitethernet} slot/interface | Port-channel number}`	Selects an interface.
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)# exit`	Returns to global configuration mode.
Step 8	`Switch(config)# interface {vlan vlan_ID | {fastethernet | gigabitethernet} slot/interface | Port-channel number}`	Creates an SVI for the selected VLAN.
Step 9	`Switch(config-if)# ip address ip_address`	Assigns an IP address to the SVI.
Step 10	`Switch(config-if)# exit`	Returns to global configuration mode.
Step 11	`Switch(config)# ip http server`	Starts the http server so that Network Assistant can talk to the switch.
Step 12	`Switch(config)# line vty x y`	Opens *y-x* VTY lines.
Step 13	`Switch(config)# exec-timeout x y`	Configures an automatic session logout if no keyboard input or output is displayed on the terminal.
Step 14	`Switch(config)# password password`	Specifies a password for a range of lines.
Step 15	`Switch(config)# login`	Prompts you for a set VTY line password.

	Command	Purpose
Step 16	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 17	`Switch# show running-config`	Verifies the configuration.

This example shows how to configure Network Assistant in community mode:

```
Switch# configure terminal
Switch(config)# vtp domain cnadoc
Switch(config)# vtp mode transparent
Switch(config)# vlan 10
Switch(config)# interface GigabitEthernet 2/1
Switch(config-if)# switchport access vlan 10
Switch(config)# interface vlan10
Switch(config-if)# ip address aa.bb.cc.dd
Switch(config)# ip http server
Switch(config)# line vty 5 15
Switch(config)# exec-timeout 0 0
Switch(config)# password keepout
Switch(config)# login
Switch# show running-config
Building configuration...
```

This example illustrates the configuration file examples for the cluster command switch candidate:

```
Building configuration...

Current configuration : 1560 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log datetime
no service password-encryption
service compress-config
service sequence-numbers
!
hostname Switch
!
boot-start-marker
boot system flash bootflash:cat4000-i9s-mz.122-25.EWA.bin
boot-end-marker
!
enable password stayout
!
no aaa new-model
vtp domain cnadoc
vtp mode transparent
ip subnet-zero
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
power redundancy-mode redundant
!
!
!
vlan internal allocation policy ascending
!
vlan 10
!
interface GigabitEthernet1/1
```

```
 switchport access vlan 10
!
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 Vlan10
 ip address abc.abc.abc.abc abc.abc.abc.abc
!
ip route 0.0.0.0 0.0.0.0 abc.abc.abc.abc
ip http server!
!
!
line con 0
 exec-timeout 0 0
 password keepout
 login
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 password keepout
 login
line vty 5 15
 exec-timeout 0 0
 password keepout
 login
!
```

```
!
end

switch#
```

Configuring Network Assistant in Cluster Mode

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

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# cluster run`	Launches the cluster on the cluster commander.
Step 3	`Switch(config)# cluster enable cluster_name`	Names the cluster.
Step 4	`Switch(config)# vtp domain name`	Creates a VTP domain to manage VLANs and names.
Step 5	`Switch(config)# vtp mode transparent`	Establishes the behavior for VTP management of the VLANs
Step 6	`Switch(config)# vlan vlan_id`	Creates a VLAN.
Step 7	`Switch(config)# interface {vlan vlan_ID | {fastethernet | gigabitethernet} slot/interface | Port-channel number}`	Selects an interface.
Step 8	`Switch(config-if)# switchport access vlan vlan_id`	Enables the physical port to be in the specified VLAN.
Step 9	`Switch(config)# interface vlan_ID`	Creates an SVI for the selected VLAN.
Step 10	`Switch(config-if)# ip address ip_address`	Assigns an IP address to the SVI.
Step 11	`Switch(config)# ip http server`	Starts the http server so that Network Assistant can talk to the switch.
Step 12	`Switch(config)# line vty x y`	Opens *y*-*x* VTY lines.
Step 13	`Switch(config)# exec-timeout x y`	Configures an automatic session logout if no keyboard input or output is displayed on the terminal.
Step 14	`Switch(config)# password password`	Specifies a password for a range of lines.
Step 15	`Switch(config)# login`	Prompts you for a set VTY line password.
Step 16	`Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 17	`Switch# show running-config| include http`	Verifies that the HTTP server is enabled.

This example shows how to configure Network Assistant in community mode:

```
Switch# configure terminal
Switch(config)# cluster run
Switch(config)# cluster enable cnadoc
Switch(config)# vtp domain cnadoc
Switch(config)# vtp mode transparent
Switch(config)# vlan 10
Switch(config)# interface GigabitEthernet 2/1
Switch(config-if)# switchport access vlan 10
Switch(config)# interface vlan10
Switch(config-if)# ip address aa.bb.cc.dd
```

```
Switch(config)# ip http server
Switch(config)# line vty 5 15
Switch(config)# exec-timeout 0 0
Switch(config)# password keepout
Switch(config)# login
Switch# show running-config
Building configuration...

Current configuration : 1560 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log datetime
no service password-encryption
service compress-config
service sequence-numbers
!
hostname Switch
!
boot-start-marker
boot system flash bootflash:cat4000-i9s-mz.122-25.EWA.bin
boot-end-marker
!
enable password stayout
!
no aaa new-model
vtp domain cat4500vtpdomain
vtp mode transparent
ip subnet-zero
!
cluster run
!
cluster enable switchcluster
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
power redundancy-mode redundant
!
!
!
vlan internal allocation policy ascending
!
vlan 10
!
interface GigabitEthernet1/1
 switchport access vlan 10
!
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 Vlan10
 ip address abc.abc.abc.abc abc.abc.abc.abc
!
ip route 0.0.0.0 0.0.0.0 abc.abc.abc.abc
ip http server
!
!
line con 0
 exec-timeout 0 0
 password keepout
 login
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 password keepout
 login
line vty 5 15
 exec-timeout 0 0
 password keepout
 login
!
!
end

switch#
```

Configuring Embedded CiscoView Support

The Catalyst 4500 series switch supports CiscoView web-based administration through the Catalyst Web Interface (CWI) tool. CiscoView is a device management application that can be embedded on the switch flash and provides dynamic status, monitoring, and configuration information for your switch.

CiscoView displays a physical view of your switch chassis with color-coded modules and ports and monitoring capabilities that display the switch status, performance, and other statistics. Configuration capabilities allow comprehensive changes to devices, if the required security privileges have been granted. The configuration and monitoring capabilities for the Catalyst 4500 series of switches mirror those available in CiscoView in all server-based CiscoWorks solutions, including CiscoWorks LAN Management Solution (LMS) and CiscoWorks Routed WAN Management Solution (RWAN).

These sections describe the Embedded CiscoView support available with Cisco IOS Release 12.1(20)EW and later releases:

Understanding Embedded CiscoView

The Embedded CiscoView network management system is a web-based interface that uses HTTP and SNMP to provide a graphical representation of the switch and to provide a GUI-based management and configuration interface. You can download the Java Archive (JAR) files for Embedded CiscoView at this URL at http://www.cisco.com/cgi-bin/tablebuild.pl/cview-cat4000

Installing and Configuring Embedded CiscoView

To install and configure Embedded CiscoView, perform this task:

	Command	Purpose
Step 1	`Router# dir device_name`	Displays the contents of the device. If you are installing Embedded CiscoView for the first time, or if the CiscoView directory is empty, skip to Step 5.
Step 2	`Switch# delete device_name:cv/*`	Removes existing files from the CiscoView directory.
Step 3	`Switch# squeeze device_name:`	Recovers the space in the file system.
Step 4	`Switch# copy tftp bootflash`	Copies the tar file to bootflash.

Step 5	`Switch# archive tar /xtract tftp://`
	`ip address of tftp server/ciscoview.tar`
	`device_name:cv`
		Extracts the CiscoView files from the tar file on the TFTP server to the CiscoView directory.

Step 6	`Switch# dir device_name:`	Displays the contents of the device. In a redundant configuration, repeat Step 1 through Step 6 for the file system on the redundant supervisor engine.
Step 7	`Switch# configure terminal`	Enters global configuration mode.
Step 8	`Switch(config)# ip http server`	Enables the HTTP web server.
Step 9	`Switch(config)# snmp-server community string ro`	Configures the SNMP password for read-only operation.
Step 10	`Switch(config)# snmp-server community string rw`	Configures the SNMP password for read/write operation.

Note The default password for accessing the switch web page is the enable-level password of the switch.

The following example shows how to install and configure Embedded CiscoView on your switch:

```
Switch# dir
Directory of bootflash:/
    1  -rw-     9572396  Dec 30 2002 01:05:01 +00:00  cat4000-i9k2s-mz.121-19.EW
    2  -rw-     9604192   Jan 3 2003 07:46:49 +00:00  cat4000-i5k2s-mz.121-19.EW
    3  -rw-     1985024  Jan 21 2003 03:31:20 +00:00  Cat4000IOS.v4-0.tar
    4  -rw-     1910127  Jan 23 2003 04:23:39 +00:00  cv/Cat4000IOS-4.0.sgz
    5  -rw-        7258  Jan 23 2003 04:23:46 +00:00  cv/Cat4000IOS-4.0_ace.html
    6  -rw-         405  Jan 23 2003 04:23:46 +00:00  cv/Cat4000IOS-4.0_error.html
    7  -rw-        2738  Jan 23 2003 04:23:46 +00:00  cv/Cat4000IOS-4.0_install.html
    8  -rw-       20450  Jan 23 2003 04:23:46 +00:00  cv/Cat4000IOS-4.0_jks.jar
    9  -rw-       20743  Jan 23 2003 04:23:46 +00:00  cv/Cat4000IOS-4.0_nos.jar
   10  -rw-       12383  Jan 23 2003 04:23:46 +00:00  cv/applet.html
   11  -rw-         529  Jan 23 2003 04:23:46 +00:00  cv/cisco.x509
   12  -rw-        2523  Jan 23 2003 04:23:46 +00:00  cv/identitydb.obj
   13  -rw-        1173  Mar 19 2003 05:50:26 +00:00  post-2003.03.19.05.50.07-passed.txt


32578556 bytes total (38199688 bytes free)

Switch#
Switch# del cv/*
Delete filename [cv/*]?
Delete bootflash:cv/Cat4000IOS-4.0.sgz? [confirm]y
Delete bootflash:cv/Cat4000IOS-4.0_ace.html? [confirm]y
Delete bootflash:cv/Cat4000IOS-4.0_error.html? [confirm]y
Delete bootflash:cv/Cat4000IOS-4.0_install.html? [confirm]y
Delete bootflash:cv/Cat4000IOS-4.0_jks.jar? [confirm]y
Delete bootflash:cv/Cat4000IOS-4.0_nos.jar? [confirm]y
Delete bootflash:cv/applet.html? [confirm]y
Delete bootflash:cv/cisco.x509? [confirm]y
Delete bootflash:cv/identitydb.obj? [confirm]y
Switch#

Switch# squeeze bootflash:
All deleted files will be removed. Continue? [confirm]y
Squeeze operation may take a while. Continue? [confirm]y
Squeeze of bootflash complete
Switch#
Switch# copy tftp bootflash
Address or name of remote host []? 10.5.5.5
Source filename []? Cat4000IOS.v5-1.tar
Destination filename [Cat4000IOS.v5-1.tar]?
Accessing tftp://10.5.5.5/Cat4000IOS.v5-1.tar...
Loading Cat4000IOS.v5-1.tar from 10.5.5.5 (via FastEthernet2/1):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 2031616 bytes]

2031616 bytes copied in 11.388 secs (178400 bytes/sec)
Switch#
Switch# dir


Directory of bootflash:/
1  -rw-     9572396  Dec 30 2002 01:05:01 +00:00  cat4000-i9k2s-mz.121-19.EW
    2  -rw-     9604192   Jan 3 2003 07:46:49 +00:00  cat4000-i5k2s-mz.121-19.EW
    3  -rw-     1985024  Jan 21 2003 03:31:20 +00:00  Cat4000IOS.v4-0.tar
    4  -rw-        1173  Mar 19 2003 05:50:26 +00:00  post-2003.03.19.05.50.07-passed.txt
    5  -rw-     2031616  Mar 26 2003 05:33:12 +00:00  Cat4000IOS.v5-1.tar
```

```
32578556 bytes total (38199688 bytes free)
Switch#
Switch# archive tar /xtract Cat4000IOS.v5-1.tar /cv
extracting Cat4000IOS-5.1.sgz (1956591 bytes)
extracting Cat4000IOS-5.1_ace.html (7263 bytes)
extracting Cat4000IOS-5.1_error.html (410 bytes)
extracting Cat4000IOS-5.1_install.html (2743 bytes)
extracting Cat4000IOS-5.1_jks.jar (20450 bytes)
extracting Cat4000IOS-5.1_nos.jar (20782 bytes)
extracting applet.html (12388 bytes)
extracting cisco.x509 (529 bytes)
extracting identitydb.obj (2523 bytes)
Switch#
Switch# dirDirectory of bootflash:/

1  -rw-     9572396  Dec 30 2002 01:05:01 +00:00  cat4000-i9k2s-mz.121-19.EW
    2  -rw-     9604192   Jan 3 2003 07:46:49 +00:00  cat4000-i5k2s-mz.121-19.EW
    3  -rw-     1985024  Jan 21 2003 03:31:20 +00:00  Cat4000IOS.v4-0.tar
    4  -rw-        1173  Mar 19 2003 05:50:26 +00:00  post-2003.03.19.05.50.07-passed.txt
    5  -rw-     2031616  Mar 26 2003 05:33:12 +00:00  Cat4000IOS.v5-1.tar
    6  -rw-     1956591  Mar 26 2003 05:36:11 +00:00  cv/Cat4000IOS-5.1.sgz
    7  -rw-        7263  Mar 26 2003 05:36:19 +00:00  cv/Cat4000IOS-5.1_ace.html
    8  -rw-         410  Mar 26 2003 05:36:19 +00:00  cv/Cat4000IOS-5.1_error.html
    9  -rw-        2743  Mar 26 2003 05:36:19 +00:00  cv/Cat4000IOS-5.1_install.html
   10  -rw-       20450  Mar 26 2003 05:36:19 +00:00  cv/Cat4000IOS-5.1_jks.jar
   11  -rw-       20782  Mar 26 2003 05:36:19 +00:00  cv/Cat4000IOS-5.1_nos.jar
   12  -rw-       12388  Mar 26 2003 05:36:19 +00:00  cv/applet.html
   13  -rw-         529  Mar 26 2003 05:36:19 +00:00  cv/cisco.x509
   14  -rw-        2523  Mar 26 2003 05:36:19 +00:00  cv/identitydb.obj

32578556 bytes total (7358284 bytes free)
Switch#
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip http server
Switch(config)# snmp-server community public ro
Switch(config)# snmp-server community public rw
Switch(config)# exit
Switch# wr
Building configuration...
Compressed configuration from 2735 bytes to 1169 bytes[OK]
Switch# show ciscoview ?
  package  ADP Package Details
  version  ADP version
  |        Output modifiers
  <
```

For more information about web access to the switch, refer to the "Using the Cisco Web Browser" chapter in the *Cisco IOS Configuration Fundamentals Configuration Guide* at this URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hcf_c/index.htm

Displaying Embedded CiscoView Information

To display the Embedded CiscoView information, enter the following commands:

Command	Purpose
`Switch# show ciscoview package`	Displays information about the Embedded CiscoView files.
`Switch# show ciscoview version`	Displays the Embedded CiscoView version.

The following example shows how to display the Embedded CiscoView file and version information:

```
Switch# show ciscoview package
File source:
CVFILE                          SIZE(in bytes)
-------------------------------------------------
Cat4000IOS-5.1.sgz               1956591
Cat4000IOS-5.1_ace.html          7263
Cat4000IOS-5.1_error.html        410
Cat4000IOS-5.1_install.html      2743
Cat4000IOS-5.1_jks.jar           20450
Cat4000IOS-5.1_nos.jar           20782
applet.html                      12388
cisco.x509                       529
identitydb.obj                   2523

Switch# show ciscoview version
Engine Version: 5.3.4 ADP Device: Cat4000IOS ADP Version: 5.1 ADK: 49
Switch#
```