CHAPTER 9

Configuring Switches with Web-based Tools

This chapter describes how to install and configure the Network Assistant and Embedded CiscoView on the Catalyst 4500 series switch. It also provides an overview of the concepts and procedures used to create and manage a cluster of Catalyst 4500 series switches.

This chapter describes these topics:

Note For complete syntax and usage information for the switch commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at http://www.cisco.com/go/NetworkAssistant.

Configuring and Using the Network Assistant

This chapter contains these topics:

Note The Network Assistant is not bundled with an online software image on Cisco.com. You can download the Network Assistant from this URL: at http://www.cisco.com/go/NetworkAssistant

Understanding How the Network Assistant Works

Network Assistant is an application that manages standalone devices and clusters of devices from anywhere in your intranet. Using its graphical user interface, you can perform multiple configuration tasks without having to remember command-line interface commands. Network Assistant enables you to apply VLAN settings, link and device monitoring, and other networking features to multiple devices and ports at the same time.

Network Assistant is a client-server application that sends Cisco IOS commands to configure and manage the Catalyst 4500 series switch over HTTP. The client opens a connection to the HTTP server and sends a request. The HTTP server receives the request, sends a response back to the client, and closes the connection.

By default, the HTTP server is disabled on the Catalyst 4500 series switch. To connect the switch to the Network Assistant, you must enable the HTTP server.

After you enable the HTTP server, it listens for requests on port number 80. Through the CLI, you can change the TCP/IP port number to any number from 1 to 65,535. If you do not use the port number 80, you will need to ensure that the new port number matches the number that is configured on the switch.

Although the HTTP server uses HTTP Version 1.0, it also supports HTTP Version 1.1 messaging.

Installation Requirements

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

- Processor speed: Pentium 300 MHz
- DRAM: 128 MB
- Number of colors: 65536
- Resolution: 1024 x 768
- Font size: Small

The following client platforms are supported by Network Assistant:

- Windows NT 4.0, with Service Pack 6 or later
- Windows 2000 Professional SP3+
- Windows XP Professional SP1+

Software and Hardware Requirements

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

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

Table 1 Hardware Supported for Network Assistant 1.0 Support

Type	Part Number
Chassis	WS-C4503
	WS-C4506
Power supplies	PWR-C45-1300AC
	PWR-C45-1000AC

Table 1 Hardware Supported for Network Assistant 1.0 Support (continued)

Type	Part Number
Supervisors	WS-X4013+
	WS-X4515
	WS-X4013+TS
Modules	WS-X4124-RJ45
	WS-X4148-RJ
	WS-X4224-RJ45V
	WS-X4248-RJ45V
	WS-X4548-GB-RJ45
	WS-X4424-GB-RJ45
	WS-X4306-GB

Network Assistant-related Default Configuration

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
HTTP server	Disabled	Enabled[1]
TCP/IP port number	80	Optional[2]
Authentication	Disabled	Optional
Cluster	Disabled	Enabled[3]

1. Required for Network Assistant to access the device.
2. Port number on the Network Assistant and the Catalyst 4500 series switch must match.
3. Enabled only if you want to manage a cluster of devices.

Installing the Network Assistant

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

Step 1 Go to this Web address: 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 Network Assistant installer, cna-1 0-windows-k9-installer.1-0-1a.exe

Step 4 Download the Network Assistant Installer and initiate 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.

Overview of the CLI Commands

Table 3 is an overview of the Network Assistant-related CLI commands.

[

Table 3 CLI Commands

Command	Functions
[no] ip http server	Configures the HTTP server on the switch.
[no] ip http port *port_number*	Configures the HTTP port.
show version	Displays the Cisco IOS version.
show running-config	Displays the switch configuration.
[no] ip http authentication {enable | local | tacacs}	Configures the HTTP authentication.
cluster run	Enables clustering.

Configuring the Cisco Device for Use with Network Assistant

Before you can access the Network Assistant, you need to perform the following tasks:

- Enable Communication with Network Assistant, page 9-4
- Enable Intra-Cluster Communication, page 9-7

Enable Communication with Network Assistant

Network Assistant communicates with a Catalyst 4500 series switch by sending Cisco IOS commands over a HTTP connection.

To enable Network Assistant to connect to a Catalyst 4500 series switch, perform this task on the switch:

	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)# interface {vlan` *vlan_ID* `| {fastethernet | gigabitethernet} slot/interface | Port-channel` *number*`}`	Selects an interface.

	Command	Purpose
Step 4	`Switch(config-if)# ip address ip_address address_mask`	(Optionally) Assigns an IP address to the Catalyst 4500 series **Note** This step is mandatory if the switch is a cluster command switch candidate. This step is optional if the switch is a cluster member candidate.
Step 5	`Switch(config)# ip http port port_number`	(Optionally) Configures the HTTP port. **Note** Perform this step only if you want to change the default setting (80) for the TCP/IP port number on the server.
Step 6	`Switch(config)# ip http authentication [enable | local | tacacs]`	Configures HTTP authentication on the switch. The Catalyst 4500 series switch software allows you to authenticate console, Telnet, and HTTP logins using the TACACS or Local database. When you log in to the switch using HTTP, a dialog box appears and prompts you for your username and password. After you provide your username and password, the system authenticates your login with the HTTP user-authentication method. The system denies access unless the username and password are valid.
Step 7	`Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 8	`Switch# show running-config| include http`	Verifies that the HTTP server is enabled.

This example shows how to configure the HTTP server:

```
Switch# configure terminal
Switch(config)# interface GigabitEthernet 3/21
Switch(config-if)# ip address 10.77.209.183 255.255.255.0
Switch(config)# ip http server
Switch(config)# ip http port 80
Switch(config)# end
Switch# show running-config
Building configuration...
!
ip http server
!
```

This example shows how to configure the TCP/IP port number to the default (80):

```
Switch(config)# default ip http port
```

This example shows how to configure the TCP port number to 2398:

```
Switch(config)# ip http port 2398
```

This example shows how to configure the authentication login to use local passwords and to verify the configuration:

```
Switch(config)# ip http authentication local
Switch(config)# end
Switch# show running-config | include http
ip http server
ip http authentication local
```

This example illustrates the sample configuration files for the cluster command switch candidate:

```
Current configuration : 2481 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service compress-config
!
hostname Switch
!
!
vtp domain switch
vtp mode transparent
ip subnet-zero
!
cluster run
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
power redundancy-mode redundant
!
!
!
vlan internal allocation policy ascending
!
vlan 17,100,110,117,120,200
!
interface FastEthernet1
 ip address 4.4.4.4 255.255.255.0
 speed auto
 duplex auto
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface GigabitEthernet3/1
 no switchport
 ip address 3.3.3.3 255.255.255.0
!
interface GigabitEthernet3/3
!
interface GigabitEthernet3/4
!
interface GigabitEthernet3/5
!
interface GigabitEthernet3/6
!
interface GigabitEthernet3/7
!
```

```
interface GigabitEthernet3/8
!
interface GigabitEthernet3/9
 shutdown
!
interface GigabitEthernet3/10
 shutdown
!
interface GigabitEthernet3/11
 shutdown
interface Vlan1
 no ip address
!
interface Vlan100
 no ip address
!
ip http server
```

Enable Intra-Cluster Communication

You can use the following interfaces for intra-cluster communication: a router, an switched virtual interface (SVI), an access port, or a trunk port. If you employ an access port or trunk port, the VLAN used for inter-cluster communication must have an SVI in the *no shut* state.

To enable inter-cluster communication, perform this task on each of the Catalyst 4500 series switches that will serve as cluster member candidates.

	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)# vlan vlan_id`	Specifies a VLAN used to communicate with the cluster command switch.
Step 4	`Switch(config-vlan)# no shutdown`	Enables a VLAN interface.
Step 5	`Switch(config)# interface {vlan vlan_ID | {fastethernet | gigabitethernet} slot/interface | Port-channel number}`	Selects an interface.
Step 6	`Switch(config-if)# no shutdown`	Enables the interface.
Step 7	`Switch(config)# interface {vlan vlan_ID | {fastethernet | gigabitethernet} slot/interface | Port-channel number}`	Selects a port interface.
Step 8	`Switch(config-if)# switchport mode access`	Configures the port interface as an access port.
Step 9	`Switch(config-if)# switchport access vlan vlan-id`	Assigns the port interface to a VLAN.
Step 10	`Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 11	`Switch# show running-config`	Verifies the configuration.

This example shows how to enable intra-cluster communication:

```
Switch# configure terminal
Switch(config)# cluster run
Switch(config)# vlan 100
Switch(config-vlan)# no shutdown
Switch(config)# interface vlan 100
Switch(config-if)# no shutdown
witch(config-if)# interface Gigabit Ethernet 3/24
Switch(config-if)# switchport mode access
SSwitch(config-if)# switchport access vlan 100
Switch(config)# end
Switch# show running-config
Building configuration...

Current configuration : 3954 bytes
!
version 12.2
!
hostname Switch
!
cluster run
!
!
vlan 100
!
interface GigabitEthernet3/24
 switchport access vlan 100
 switchport mode access
!
interface Vlan100
 ip address 100.100.100.1 255.255.255.0
!
ip http server
!
end

Switch#
```

This example illustrates the sample configuration files for the cluster member candidate:

```
Building configuration...
Current configuration : 1492 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service compress-config
!
hostname g5-7
!
!
vtp domain switch
vtp mode transparent
ip subnet-zero
!
cluster run
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
vlan 2-3,5,17,100,200-201,300-301,555
```

```
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface FastEthernet3/1
 switchport access vlan 100
 switchport mode access
!
interface Vlan1
 no ip address
!
interface Vlan100
 no ip address
ip http server
```

Displaying the Network Assistant-Related Configuration

To display the Network Assistant configuration, perform this task:

Command	Purpose
`Switch# show running-config`	Displays the Network Assistant-related configuration.

This example shows how to display the Network Assistant-related configuration:

```
Switch# show running-config
.....
Building configuration...

Current configuration : 3647 bytes
!
version 12.2
...
!
hostname Switch
!
boot system flash bootflash:cat4000-i5s-mz.122_20_EWA
!
...
!
cluster run
cluster enable sample-cluster 0
...
!
...
ip http server
ip http port 800
!
...
end
```

Launching the Network Assistant

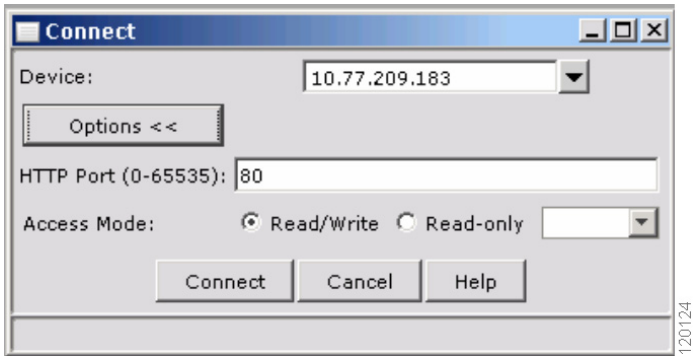
After installing Network Assistant, you will see its icon on your desktop. You will also use a Network Assistant entry under **Start > Programs** and a Network Assistant executable file in the installation directory. When you select any of these items, two windows will appear: the Network Assistant window, 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 Figure 1. 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. 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.

Figure 1 Connect Window



When the connection occurs, the Network Assistant window is in the 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.

Note For information on how to use Network Assistant, refer to *Getting Started with Cisco Network Assistant*, available at the URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cna/v1_0/gsg/index.htmCisco.com

Clustering Switches

This section provides an overview of the concepts and of the procedures used to create and manage Catalyst 4500 series switches. Unless otherwise noted, the term *device* refers to a standalone switch.

You can create and manage switch clusters by using the standalone Network Assistant application or the command-line interface (CLI). Configuring switch clusters is performed more easily from the Network Assistant than through the CLI.

Note For complete procedures about using Network Assistant to configure switch clusters, refer to *Getting Started with Cisco Network Assistant*, available at: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cna/v1_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/ios122/122cgcr/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. Refer to the "Enable Intra-Cluster Communication" section on page 9-7 for details on how to enable clustering.

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.

In a switch cluster, one switch must be the *cluster command 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 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 15 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.

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 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, given that 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 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# a 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-     8620304  Dec 23 2002 23:27:49 +00:00  wickwire.EW1
    2  -rw-     9572396  Dec 30 2002 01:05:01 +00:00  cat4000-i9k2s-mz.121-19.EW
    3  -rw-     9604192   Jan 3 2003 07:46:49 +00:00  cat4000-i5k2s-mz.121-19.EW
    4  -rw-     1985024  Jan 21 2003 03:31:20 +00:00  Cat4000IOS.v4-0.tar
    5  -rw-     1910127  Jan 23 2003 04:23:39 +00:00  cv/Cat4000IOS-4.0.sgz
    6  -rw-        7258  Jan 23 2003 04:23:46 +00:00  cv/Cat4000IOS-4.0_ace.html
    7  -rw-         405  Jan 23 2003 04:23:46 +00:00  cv/Cat4000IOS-4.0_error.html
    8  -rw-        2738  Jan 23 2003 04:23:46 +00:00  cv/Cat4000IOS-4.0_install.html
    9  -rw-       20450  Jan 23 2003 04:23:46 +00:00  cv/Cat4000IOS-4.0_jks.jar
   10  -rw-       20743  Jan 23 2003 04:23:46 +00:00  cv/Cat4000IOS-4.0_nos.jar
   11  -rw-       12383  Jan 23 2003 04:23:46 +00:00  cv/applet.html
   12  -rw-         529  Jan 23 2003 04:23:46 +00:00  cv/cisco.x509
   13  -rw-        2523  Jan 23 2003 04:23:46 +00:00  cv/identitydb.obj
   14  -rw-     9630880  Feb 27 2003 01:25:16 +00:00  kurt70.devtest-enh
   15  -rw-        1173  Mar 19 2003 05:50:26 +00:00  post-2003.03.19.05.50.07-passed.txt
   16  -rw-    10511956  Mar 26 2003 04:24:12 +00:00  kurt_alpha_bas_crypto_103

61341696 bytes total (9436548 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 FastEthernet1):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 2031616 bytes]

2031616 bytes copied in 11.388 secs (178400 bytes/sec)
Switch#
Switch# dir
Directory of bootflash:/

    1  -rw-     8620304  Dec 23 2002 23:27:49 +00:00  wickwire.EW1
    2  -rw-     9572396  Dec 30 2002 01:05:01 +00:00  cat4000-i9k2s-mz.121-19.EW
    3  -rw-     9604192   Jan 3 2003 07:46:49 +00:00  cat4000-i5k2s-mz.121-19.EW
    4  -rw-     1985024  Jan 21 2003 03:31:20 +00:00  Cat4000IOS.v4-0.tar
    5  -rw-     9630880  Feb 27 2003 01:25:16 +00:00  kurt70.devtest-enh
    6  -rw-        1173  Mar 19 2003 05:50:26 +00:00  post-2003.03.19.05.50.07-passed.txt
    7  -rw-    10511956  Mar 26 2003 04:24:12 +00:00  kurt_alpha_bas_crypto_103
    8  -rw-     2031616  Mar 26 2003 05:33:12 +00:00  Cat4000IOS.v5-1.tar

61341696 bytes total (9383128 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# dir
Directory of bootflash:/

    1  -rw-     8620304  Dec 23 2002 23:27:49 +00:00  wickwire.EW1
    2  -rw-     9572396  Dec 30 2002 01:05:01 +00:00  cat4000-i9k2s-mz.121-19.EW
    3  -rw-     9604192   Jan 3 2003 07:46:49 +00:00  cat4000-i5k2s-mz.121-19.EW
    4  -rw-     1985024  Jan 21 2003 03:31:20 +00:00  Cat4000IOS.v4-0.tar
```

```
  5  -rw-     9630880  Feb 27 2003 01:25:16 +00:00  kurt70.devtest-enh
  6  -rw-        1173  Mar 19 2003 05:50:26 +00:00  post-2003.03.19.05.50.07-passed.txt
  7  -rw-    10511956  Mar 26 2003 04:24:12 +00:00  kurt_alpha_bas_crypto_103
  8  -rw-     2031616  Mar 26 2003 05:33:12 +00:00  Cat4000IOS.v5-1.tar
  9  -rw-     1956591  Mar 26 2003 05:36:11 +00:00  cv/Cat4000IOS-5.1.sgz
 10  -rw-        7263  Mar 26 2003 05:36:19 +00:00  cv/Cat4000IOS-5.1_ace.html
 11  -rw-         410  Mar 26 2003 05:36:19 +00:00  cv/Cat4000IOS-5.1_error.html
 12  -rw-        2743  Mar 26 2003 05:36:19 +00:00  cv/Cat4000IOS-5.1_install.html
 13  -rw-       20450  Mar 26 2003 05:36:19 +00:00  cv/Cat4000IOS-5.1_jks.jar
 14  -rw-       20782  Mar 26 2003 05:36:19 +00:00  cv/Cat4000IOS-5.1_nos.jar
 15  -rw-       12388  Mar 26 2003 05:36:19 +00:00  cv/applet.html
 16  -rw-         529  Mar 26 2003 05:36:19 +00:00  cv/cisco.x509
 17  -rw-        2523  Mar 26 2003 05:36:19 +00:00  cv/identitydb.obj

61341696 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/ios122/122cgcr/fun_c/fcprt1/fcd105.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#
```