Cisco Edge 300 Series Switch Software Configuration Guide, Release 1.3

June 20, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-26743-01

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco Edge 300 Series Switch Software Configuration Guide, Release 1.3

CONTENTS

APPENDIX D

Preface

This document describes how to configure the Cisco Edge 300 Series switch in your network.

This guide does not describe how to install your switch. For information, see the hardware installation guide for your switch.

Conventions

This publication uses these conventions to convey instructions and information:

For command descriptions

- Commands and keywords are in **boldface** text.
- Arguments for which you supply values are in *italic*.
- Square brackets ([ ]) mean optional elements.
- Braces ({ }) group required choices, and vertical bars (|) separate the alternative elements.
- Braces and vertical bars within square brackets ([{ | }]) mean a required choice within an optional element.

For interactive examples

- Terminal sessions and system displays are in `screen` font.
- Information that you enter is in **`boldface screen`** font.
- Nonprinting characters, such as passwords or tabs, are in angle brackets (< >).

Notes, cautions, and warnings use these conventions and symbols:

Note Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

⚠ Warning **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Related Publications

- Cisco Smart Install Configuration Guide
- Cisco Edge 300 Series Switch Installation Guide
- Release notes for the Cisco Edge 300 Series Switch

Obtaining Documentation and Submitting a Service Request

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

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

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

CHAPTER 1

Cisco Edge 300 Series Switch

Cisco Edge 300 Series Switch Overview

The Cisco Edge 300 series switch delivers cloud-based services to a room environment as part of a Smart Install network. The switch allows in-room devices and applications to fully utilize network infrastructure intelligence.

A Cisco Edge 300 series switch functions as a key component in a cloud network:

In-room client switch

The Cisco Edge 300 series switch functions as the in-room client switch in class rooms, hotel rooms, hospital rooms, and offices. The switch is a hybrid platform that provides PC, switching, and routing capabilities. It provides various interfaces for these components:

- Input devices such as a keyboard, mouse, microphone, camera, and so on
- Output devices such as a monitor, television, projector, speakers, headphones, and so on

The switch also integrates a wireless access point to allow 802.11b/g/n clients to connect to the network over a wireless connection.

Network aggregator

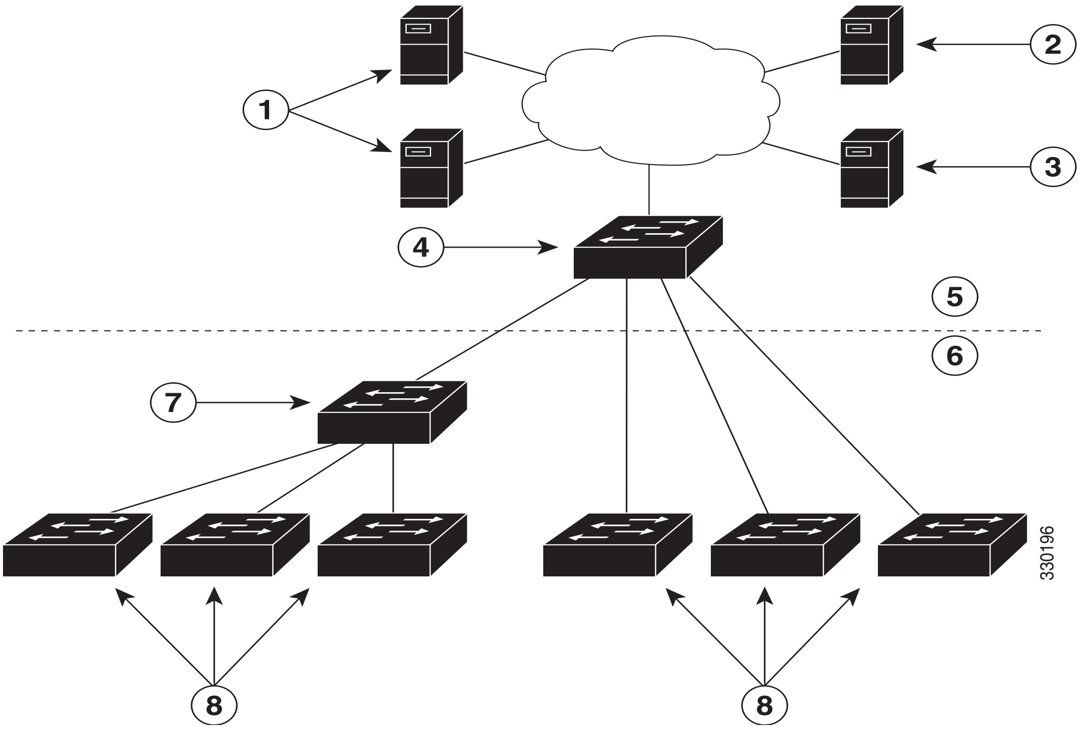
An Ethernet switch such as a Catalyst 3000 series switch functions as a Smart Install director and securely manages the Cisco Edge 300 switches. Intelligent services on medianet and security in Catalyst switches enhance the quality of cloud service delivery.

Cloud and application delivery servers

Data center servers provide environment-specific content, computing power, storage and hosting, and other cloud applications, including third-party applications for use in the client switches.

Figure 1-1 shows a typical Smart Install configuration in which the Cisco Edge 300 series switches function as client switches.

Figure 1-1 Typical Smart Install Edge Network Diagram



1	Cloud and application delivery servers	**5**	Aggregation layer
2	DHCP server	**6**	Access layer
3	TFTP server	**7**	Intermediate switch
4	Director	**8**	Client switches

Cisco Edge 300 Series Switch Features and Applications

Note These features and applications are not documented in this guide.

The Cisco Edge 300 series switch provides these features and applications:

- Cisco Edge Surveillance
- Cisco Edge Video Conference
- Video streaming
- Display of Adobe Flash files
- Display of Windows Office files
- Display of PDF files
- MP3 and AAC audio support
- AVI, WAV, and MPG4 video support and H.264/AVC encode and decode video support
- JPG support

- WebEx meeting
- Software upgrade capability
- Screen capture capability

Central Management and Configuration

Cisco Edge 300 series switches function exclusively in a Smart Install network. Smart Install is a plug-and-play configuration and image-management feature. This means that you can ship a switch to a location, place it in the network, and power it on with no local configuration required.

Smart Install Network

A network using Smart Install includes a group of networking devices, known as clients, that are served by a common Layer 3 switch or a router that acts as a director.

All Cisco Edge 300 series switches function as Smart Install client switches in a Smart Install network. End users do not configure the client switches: all switches are centrally configured through a GUI that is installed on a TFTP server and managed by the director.

Smart Install Director

The Smart Install director provides a single management point for images and configuration of client switches. When a client switch is first installed in the network, the director automatically detects the new switch and identifies the correct image and configuration files to download. It can allocate an IP address and hostname to a client. If a standalone switch in the network is replaced by another switch of the same SKU, that is, a switch with the same product ID, it automatically gets the same configuration and image as the previous one.

The Smart Install director supports these functions in the network:

- Configuration management for Edge configuration files
- Cisco Discovery Protocol (CDP) information consolidation from neighbors and client switches
- DHCP snooping

The director can also support these functions in the network, or other devices in the network could provide them:

- DHCP server
- TFTP server for storage of image and configuration files

For information about configuring the director, see the "Configuring the Smart Install Director" section on page 2-6.

DHCP and TFTP Servers

DHCP is the backbone of a Smart Install network: a Smart Install client switch uses DHCP to get an IP address and the Smart Install director snoops DHCP messages. All DHCP communication passes through the director so that it can snoop all DHCP packets from client switches.

The director can function as a DHCP and TFTP server and can store the configuration and image files. However, in a large network, there are third-party DHCP and TFTP servers for the director to use. The client switch downloads the image and configuration files from the TFTP server.

The DHCP server provides the client switches with an IP address, and DHCP options are used to send information and files:

- The TFTP server IP address to the client switches
- Configuration file names to the client switches
- Image filenames and locations to the client switches
- Hostnames to the client switches
- The director IP address to other switches in the network

For information about configuring the DHCP server, see the "Configuring the DHCP Server" section on page 2-2. For information about configuring the TFTP server, see the "Configuring the TFTP Server" section on page 2-8.

Note In networks that do not use DHCP to assign IP addresses to the clients, you can configure a static IP address on the client switch. See the "Using Static IP Addresses" section on page 2-5 for more information.

GUI and Configuration Files

You use a GUI to centrally configure the Cisco Edge 300 series switch as a Smart Install client. You need to install the GUI on the TFTP server (see the "Setting Up the GUI on the CentOS/Fedora Server" section on page 2-10).

The director requires information to manage the client switches. Using the GUI, you can create these files that the director can retrieve from the TFTP server:

Image List File

Specifies the images that need to be loaded on the client switch:

- Root file system image—Specifies the critical files and subdirectories for the switch. The root file system is located on the same partition as the root directory. When a switch starts up, all file systems are attached to the root file system.
- Bootable Linux kernel image—Specifies the Linux operating system kernel that runs on the switch.
- Cisco applications image—Specifies the Cisco applications that run on the switch.
- Third-party applications image—Specifies the third-party applications that run on the switch.
- Fonts image—Specifies the languages on the desktop and GUI.

You configure the image list file as part of the Smart Install director configuration file.

Cisco Edge Configuration File

Specifies a common configuration that applies to all client switches in a group and an individual configuration that applies to a single client switch in a group and that includes components such as the SSID, wireless security settings, and wireless radio settings. You use a CLI to enter Cisco Edge 300 series switch-specific commands in the GUI to create the Edge configuration file (see the "Managing Cisco Edge Configuration Files" section on page 2-23 and Chapter 4, "Using CLI Mode").

Smart Install Director Configuration File

Specifies which image list file and Cisco Edge configuration file to load on a group of client switches.

Applying and Upgrading Images and Configuration Files

When the switch starts up, it connects to the director. If the switch detects any new images or configuration files, it automatically restarts in factory-default mode and then downloads and installs the new images or configuration files.

These are the supported types of image and configuration upgrades:

- Upgrade initiated by the user—For a single client switch that is in the network and connected to the director. The user can turn the switch off and on or can press and hold the Reset button for 5 seconds to start from factory-default mode. In either case, the switch connects to the director and can detect any new images or configuration files.
- Upgrade initiated by the administrator—For a single client switch that is in the network and connected to the director. The administrator initiates the upgrade by rebooting the switch using the GUI or by connecting to the switch, for example, over a Telnet connection.

For more information, see "Switch Image and Configuration Upgrades" section on page 2-34.

Note On-demand upgrades and scheduled downloads are not supported. You cannot upgrade switches from the director by using the **write erase** and **reload**, **vstack download-image**, **vstack download-config**, or **archive download-sw** privileged EXEC commands.

CHAPTER 2

Configuring the Smart Install Network

Configuring the Director and DHCP Server

The director manages the switches in the network. For each group of switches, a director configuration file specifies the image list file and the Cisco Edge configuration file.

The director manages these Cisco Edge configuration files:

- Startup configuration—The configuration that a client switch uses when it starts.
- Backup configuration—An exact copy of a client switch startup configuration stored in the director.
- Seed configuration—A configuration on the director that is the basis for the client switch startup configuration. If the startup and backup configuration cannot be located, the director supplies the seed configuration to the client switch.

For information about managing and creating Cisco Edge configuration files, see the "Managing Cisco Edge Configuration Files" section on page 2-23.

DHCP and Smart Install

Note If your Smart Install network does not use DHCP, see the "Using Static IP Addresses" section on page 2-5.

Note This section explains some of the basic tasks for configuring the director and DHCP server in a Smart Install network. For extensive information about Smart Install and the Smart Install director, see the *Smart Install Configuration Guide, Release 12.2(58)SE*.

A typical Smart Install network uses the DHCP protocol and a DHCP server. In a DHCP network, DHCP snooping is automatically enabled on the director. The director snoops DHCP offers and requests to and from the client switches and uses DHCP snooping to insert the DHCP options used in the Smart Install operation.

A DHCP server in a Smart Install network can be positioned in one of these ways:

- The Smart Install director can act as the DHCP server in the network. When the DHCP offer goes to the client switches, the director allocates the IP addresses and assigns configurations, images, and the hostname as DHCP options in the offer and the acknowledgement. DHCP snooping is enabled by default.
- The DHCP server can be another device (third-party server) in the Smart Install network. In this case, DHCP packets between the clients and the DHCP server pass through the director.

Note You can configure a join-window time period so that the director can modify the DHCP offer and send the image and configuration files to the client only during the window. The join window restricts Smart Install for a specified period of time and acts as a security precaution to control when a client can receive these files. See the "Using a Join Window" section in the *Smart Install Configuration Guide, Release 12.2(58)SE*.

- A third-party server and the director DHCP server can coexist in a network. In this case, the director is responsible only for the DHCP requests of the switches in the Smart Install network. The director maintains the Smart Install database and pool. The third-party server maintains the other DHCP database functions.

Configuring the DHCP Server

The DHCP server can be the director, another Cisco device running Cisco IOS, or a third-party server. You can also have the director act as the Smart Install DHCP server and have another device perform all other DHCP server functions.

Either way, use one of these procedures to set up a Cisco device as DHCP server. If you choose to configure a third-party device as DHCP server, follow the instructions in the product documentation for configuring a network address and a TFTP server.

- Configuring the Director as the DHCP Server, page 2-3
- Configuring Another Device as DHCP Server, page 2-4

DHCP Server Configuration Guidelines

- If the director (or another device running Cisco IOS) is the DHCP server and the network reloads, the server could assign new IP addresses to the switches, which then might no longer be reachable. If the director IP address changes, it is no longer the Smart Install director. To prevent this occurrence, you should enable *DHCP remembering* by entering the **ip dhcp remember** global configuration command or the **remember** DHCP-pool configuration command on the DHCP server.
- If you use an external device as the DHCP server, you can configure the DHCP server to send option 125/suboption 16 for the director IP address to avoid the possibility of fake DHCP servers.
- A third-party DHCP servers require an IP-address-to-MAC-address binding to ensure that the same IP address is given to a switch on a reload.

Configuring the Director as the DHCP Server

You can configure the director as the DHCP server and create DHCP server pools directly from the Smart Install director.

Beginning in privileged EXEC mode, follow these steps on the director to configure it as the DHCP server:

	Command	Purpose
Step 1	**config terminal**	Enters global configuration mode.
Step 2	**vstack director** *ip_ address*	Configures the device as the Smart Install director by entering the IP address of an interface on the device.
Step 3	**vstack basic**	Enables the device as the Smart Install director.
Step 4	**vstack dhcp-localserver** *poolname*	Creates a name for the Smart Install DHCP server address pool, and enters vstack DHCP pool configuration mode.
Step 5	**address-pool** *network-number mask prefix-length*	Specifies the subnet network number and mask of the DHCP address pool. **Note** The prefix length specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/).
Step 6	**default-router** *ip_address*	Specifies the IP address of the DHCP default router for the pool. **Note** We recommend that the default router address for DHCP be on VLAN 1. Newly installed devices search VLAN 1 for DHCP and TFTP.
Step 7	**file-server** *address*	Specifies the IP address of the TFTP server. **Note** If the director is also the TFTP server, you must enable it. See the "Configuring the TFTP Server" section on page 2-8.
Step 8	**exit**	Returns to global configuration mode.
Step 9	**ip dhcp remember**	(Optional) Configures the DHCP server to remember the IP bindings of a device. If the network or device reloads, the DHCP server issues the same IP address to a client that it had before the reload.

	Command	Purpose
Step 10	**end**	Returns to privileged EXEC mode.
Step 11	**copy running-config startup config**	(Optional) Saves your entries in the configuration file.
Step 12	**show dhcp server**	Verifies the configuration by displaying the DHCP servers recognized by the device.

This example shows how to configure the Smart Install director as the DHCP server:

```
Director# configure terminal
Director(config)# vstack director 1.1.1.20
Director(config)# vstack basic
Director(config)# vstack dhcp-localserver pool1
Director(config-vstack-dhcp)# address-pool 1.1.1.0 255.255.255.0
Director(config-vstack-dhcp)# default-router 1.1.1.30
Director(config-vstack-dhcp)# file-server 1.1.1.40
Director(config-vstack-dhcp)# exit
Director(config)# ip dhcp remember
Director(config)# end
```

DHCP snooping is enabled by default on the director.

Configuring Another Device as DHCP Server

If the Smart Install director is not the DHCP server, you can use the Cisco IOS DHCP commands to configure a server pool outside the Smart Install network. The director must have connectivity to the DHCP server. For procedures to configure other DHCP server options, see the “Configuring DHCP” section of the “IP Addressing Services” section of the *Cisco IOS IP Configuration Guide, Release 12.2* or the “IP Addressing Services” section of the *Cisco IOS IP Configuration Guide, Release 15.1* on Cisco.com.

Beginning in privileged EXEC mode, follow these steps:

	Command	Purpose
Step 1	**config terminal**	Enters global configuration mode.
Step 2	**ip dhcp pool** *poolname*	Creates a name for the DHCP server address pool, and enters DHCP pool configuration mode.
Step 3	**bootfile** *filename*	Specifies the name of the configuration file to be used.
Step 4	**network** *network-number mask prefix-length*	Specifies the subnet network number and mask of the DHCP address pool. **Note** The prefix length specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/).
Step 5	**option 150** *address*	Specifies the IP address of the TFTP server.

	Command	Purpose
Step 6	**remember**	(Optional) Configures the DHCP pool to remember the IP bindings of a device. If the network or device reloads, the DHCP server issues the same IP address to the device that it had before the reload.
Step 7	**end**	Returns to privileged EXEC mode.

This example shows how to configure another device as a DHCP server:

```
Switch # configure terminal
Switch(config)# ip dhcp pool pool1
Switch(dhcp-config)# network 10.10.10.0 255.255.255.0
Switch(dhcp-config)# bootfile config-boot.text
Switch(dhcp-config)# option 150 10.10.10.1
Switch(dhcp-config)# remember
Switch(config-if)# end
```

When the director is a Layer 3 switch, DHCP snooping is enabled by default. When there is a relay agent between the DHCP server and the director, you must enable DHCP snooping on the relay agent.

To enable DHCP snooping on a Cisco DHCP relay device, enter these global configuration commands:

ip dhcp snooping

ip dhcp snooping vlan 1

ip dhcp snooping vlan *vlan-id* for any other configured Smart Install VLANs

no ip dhcp snooping information option (if the DHCP server is running Cisco IOS)

You must also enter the **ip dhcp snooping trust** interface configuration command on the director interface that is connected to the server.

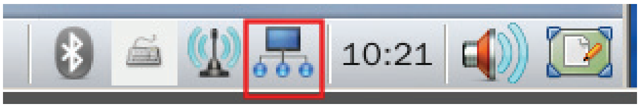
If the director and the DHCP server are on different VLANs, you must enable IP routing on the VLAN interface connected to the client switches, and enter this command:

ip helper *address* (IP address of the DHCP server)

Using Static IP Addresses

In a Smart Install network that uses static IP addresses, you need to configure the IP address on the client switches from the local desktop GUI.

Step 1 From the local desktop, double-click the Wired Network icon on the status bar.



Note If the Wired Network icon is not on the status bar, click the **Home** button and go to Settings > Wired Network.

Step 2 In the Wired Network window, click the **Net Configuration** button.

Step 3 In the User Authentication window, enter the root user name and password.

Step 4 In the Network Configuration window, choose Manual (Static) from the Net Type drop-down list.

Step 5 Enter the IP address (required), netmask (required), gateway (optional), DNS server, and IBD director (optional) IP address.

Note If you do not configure a gateway, enter the following Linux command to add a host route to the IBD and network file system (NFS) server:

```
# route add -net ip_address netmask subnet_mask gw gateway_ip_address
```

Step 6 Click **OK**.

Configuring the Smart Install Director

The director in a Smart Install network must be a Layer 3 switch running Cisco IOS release 12.2(58)SE or later or a router running Cisco IOS Release 15.1(3)T or later.

To configure a device as director, enter the IP address of one of its Layer 3 interfaces in the **vstack director** *ip_ address* global configuration command, and enable it as director by entering the **vstack basic** command.

Note If you entered the **no vstack** global configuration command to disable Smart Install on a device, the **vstack director** *ip_ address* and **vstack basic** global configuration commands are not supported on the device. To reenable Smart Install on a device, enter the **vstack** global configuration command.

When a device is configured as director, DHCP snooping is automatically enabled by default on VLAN 1, and the director builds the director database.

The database lists the client devices in the Smart Install network and includes this information for each switch:

- Product identifier (PID)
- MAC address
- IP address
- Hostname
- Network topology including neighbors interfacing with the switch
- Serial number

Note When the director is a switch, DHCP snooping is enabled by default on VLAN 1. It is also enabled on any other Smart Install management VLANs configured by entering the **vstack vlan** *vlan-range* global configuration command. We recommend using the VLAN 1 interface as the director IP address because newly installed clients use VLAN 1 to broadcast DHCP requests.

In a Smart Install network that uses DHCP to assign IP addresses, you only need to configure the director. Client switches do not require any configuration.

There can be only one director for a set of clients, and you cannot configure a backup director. If the director fails:

- The director database must be rebuilt.
- Any upgrade being performed for a non-Smart Install-capable switch might fail.
- The accumulated download status is lost.
- A configuration backup might not occur before the director restarts.

The director can change status and become a client switch if:

- The director interface that has the director IP address shuts down.
- The director interface that has the director IP address is deleted.
- The director IP address is changed.

If the director becomes a client, DHCP snooping is disabled, and the director database is no longer used.

If the director IP address is provided by DHCP and you configure a different director IP address on a client switch, the client is longer part of the Smart Install network of the director.

Smart Install relies on a TFTP server to store image and configuration files. The TFTP server can be an external device, or the director can act as a TFTP server. If the director is the TFTP server, the available flash file space on the director must be able to accommodate the client Cisco IOS image and configuration files. See the "Configuring the TFTP Server" section on page 2-8.

In a Smart Install network using DHCP, the DHCP server can be an external device, or the director can act as the DHCP server. See the "DHCP Server Configuration Guidelines" section on page 2-3. The director snoops all DHCP packets that pass through it on VLAN 1 and on any other VLANs configured as Smart Install management VLANs. All network DHCP packets from intermediate or client switches or from an external DHCP server must pass through the director, which must be able to snoop all DHCP packets from clients.

Note Smart Install options in the DCHP offer are option 125, suboption 5 (the image list file), option 125 suboption 16 (the director IP address), and option 67 (the configuration file).

The director builds a topology director database for the network by collecting information from the network Smart Install switches. The director uses the database:

- To assign a configuration file and image to a client.
- As a reference to obtain the PID, the image name, and the configuration file for an on-demand upgrade of network switches.

The director periodically updates the director database based on CDP updates from neighbor switches and from Smart Install messages sent to the director by Smart Install-capable clients. The updates contain information about the client neighbors.

Configuring the TFTP Server

Smart Install stores image and configuration files on the TFTP server.

If you use an external device as the TFTP server, the image list and configuration files are stored at these locations on the TFTP server:

Files	Location on the TFTP Server
Image list file	/opt/Tftproot/imglist
Edge configuration file	/opt/Tftproot/sb_conf
Group association file	/opt/Tftproot/

If you use an external device as the TFTP server, the files that are part of the image list file are stored at these locations on the TFTP server:

Files	Location on the TFTP Server
Factory mode operating system	/opt/Tftproot/images/FM_OS
Operating system file (includes the root file system image and bootable Linux kernel image)	/opt/Tftproot/images/OS
Cisco application files	/opt/Tftproot/images/CiscoApp
Third-party application files	/opt/Tftproot/images/Partner
Fonts applications	/opt/Tftproot/images/Fonts

The director can function as the server, eliminating the need for an external TFTP-serving device. If the director is the TFTP server, image and configuration files are stored in the director flash memory. If the director does not have available memory storage space, you can store the files on a third-party server and point to that location.

If the TFTP server is a third-party device, disable the server option to change the name of a file if another file is created with the same name. Otherwise, duplicate image list files might be created.

When you specify **flash**: as the location from which to retrieve the files, the director automatically gets the required image and configuration files and acts as the TFTP server.

Guidelines when selecting the director to be the TFTP server:

- The total flash memory space (used and free) on the director must be large enough to contain the director image and configuration file and the image and configuration files required for client switches.
- There must be enough available flash memory on the director to hold the client Cisco IOS images and configuration files. The Cisco IOS image files vary in size, depending on the PIDs and size of the images.
- A copy of each client configuration file is stored in the root directory of the flash file system on the director. There must be enough space for each planned client.

- Most director devices have enough flash memory to hold one client Cisco IOS image and a small number of client configuration files. For example, a Catalyst 3750 switch can have a maximum flash size of 64 MB, which accommodates only four or five images, based on the image size.
- If the director is a switch and the Smart Install network includes client switches with more than one product ID, you should use an external TFTP server.

Installing and Using the GUI

- GUI Introduction
- Setting Up the GUI on the CentOS/Fedora Server
- Accessing the GUI
- Managing Switch Groups
- Managing Cisco Edge Configuration Files

GUI Introduction

You can configure and deploy the Cisco Edge 300 series switch in different switch groups for different audiences. For example, a primary school can offer one set of applications for first graders and another set of applications for second graders. You would use the GUI to create two switch groups, associate the switches for the first graders with one switch group and the switches for the second graders with the other switch group, and then generate and push a different switch client configuration file to each switch group.

You use the GUI to configure and manage the Cisco Edge 300 series switches in the Smart Install network. You can

- Create switch groups (see the "Creating Switch Groups" section on page 2-16).
- Add individual switches to the GUI or import lists of switches into the GUI (see the "Managing the Edge Switch List" section on page 2-16).
- Add switches to switch groups by creating a Smart Install group-device association file based on one or more of these components:
  - MAC address
  - Product identifier (PID)
  - Location

  For more information, see the "Adding Members to a Switch Group" section on page 2-19.
- Create a Cisco Edge configuration file (see the "Managing Cisco Edge Configuration Files" section on page 2-23).

Setting Up the GUI on the CentOS/Fedora Server

Note Setting up the GUI requires familiarity with Linux distribution and Linux shell commands.

Note The Internet must remain connected during the GUI installation.

Before you set up the GUI, download and install the following software:

- Internet Explorer version 9.0 or Firefox Mozilla 8.0.1 or later.
- CentOs 6.2/Fedora 14, 15, and 16.
- Software Package Manager—This software should be part of the Fedora pre-installed software package. If you do not install a software package manager during the Fedora installation, you can download a software package manager from the Internet. For example, you can download Yum from http://yum.baseurl.org/.

To install the GUI, associated software components, and images on the TFTP server, run the installUI.sh Linux shell script that is part of the SMI_GUI_release_v1.3.tar.gz release package or a later release package.

To run the Linux shell script to install the GUI, follow these steps:

Step 1 Switch to super user (root) by entering the **su** Linux command.

Step 2 Enter your root password.

Step 3 Change the directory to the one that contains the release package (in this procedure, SMI_GUI_release_v1.3.tar.gz).

Step 4 Unzip the release package to the tmp directory by entering the **tar zxvf SMI_GUI_release_v1.3.tar.gz -C /tmp** Linux command.

Step 5 Change the directory to /tmp/SMI_GUI by entering the **cd /tmp/SMI_GUI/** Linux command.

Step 6 Run./installUI.sh or double-click the installUI.sh file. The GUI is installed in the /var/www/html/smartinstall directory on the TFTP server.

Step 7 When you see "Do you want to reboot the system now to finish the installation", enter **y** and then press **enter** to reboot the system.

Step 8 Verify that you can open the GUI by opening a browser (make sure that JavaScript is enabled) and entering **http://***ip-address***/smartinstall**, in which *ip-address* is the IP address of the TFTP server.

After you have run the script, the TFTP and HTTP server package is automatically added from the Internet. Users can then copy the images (all of which have a delivery.tar.gz suffix) to the TFTP server in these directories:

- Operating system file in /opt/Tftproot/images/OS
- Factory mode operating system file in /opt/Tftproot/images/FM_OS
- Cisco applications in /opt/Tftproot/images/CiscoApp
- Third-party applications in /opt/Tftproot/images/Partner
- Fonts applications in /opt/Tftproot/images/Fonts

Note Director configuration files that you create with the GUI are saved in the /opt/Tftproot directory.

Accessing the GUI

You can access the GUI through Microsoft Internet Explorer or Mozilla Firefox. Make sure that JavaScript is enabled on the browser.

To access the GUI, follow these steps:

Step 1 Open a browser, and enter the **http://***ip-address***/smartinstall** URL, in which *ip-address* is the IP address of the GUI server.

Step 2 Enter your user name and password.

The default user name and password are **cisco**. For security, you should change the user name and password (see the "Changing GUI Login Credentials" section on page 2-12).

Step 3 Click **OK**. The Home screen opens. The Home screen provides an introduction to the GUI.

Step 4 (Optional) In the upper right of the screen, from the drop-down list, select a language.

Note The GUI server must support the Chinese character set.

Changing GUI Login Credentials

To change your GUI login credentials, follow these steps:

Step 1 On the menu, click **Admin Information**. The Change Admin Info screen opens.

The Original User Name field shows your existing user name.

Step 2 In the Original Password field, enter your existing password.

Step 3 In the New User Name field, enter a new user name.

Step 4 In the New Password and the Confirm New Password fields, enter a new password.

The new password should follow these rules:

- The password should contain characters from at least three of the following classes: a-z, A-Z, 0-9, and !@#$%^&*().
- No character in the password should be repeated more than three times consecutively.
- The password should not be 'cisco', or any variant obtained by changing the capitalization of letters, or by substituting 1,l or ! for i, or substituting 0 for o, or substituting $ for s.
- The password should not be \'ocsic\', or any variant obtained by changing the capitalization of letters, or by substituting 1,l or ! for i, or substituting 0 for o, or substituting $ for s.

Step 5 Click **Submit**.

Note If you forget your password, you can reset both the user name and password to *cisco* by double-clicking the reset.sh file in the Smart Install root directory.

Managing Image Servers

- Creating Image Servers
- Importing a List of Image Servers
- Cloning, Modifying, and Deleting Image Servers
- Using the Search Function to Clone, Modify, and Delete Image Servers
- Distributing Groups to Image Servers

The images and configuration files for Cisco Edge switches are stored on an image server. By default, the image server is the same server that is running the GUI, but it can also be running on a separate server.

Cisco Edge images (OS, FM_OS, CiscoApp, PARTNER, and FONTS images), image list files, director configuration file, and Cisco Edge configuration files are stored on distributed image servers in each site.

To add image servers to the GUI, take one of the following actions:

- Manually add image servers to the GUI Image Server List screen.
- Import a list of image servers into the GUI Image Server List screen.
- In the GUI, clone an existing image server, and edit the image server.

Creating Image Servers

To run a separate image server, you should add this server to the GUI. To add a separate image server, follow these steps:

Step 1 On the menu, choose **Manage > Manage Image Servers**. The Manage Image Servers screen opens.

Step 2 Click **Add an Image Server** above the table. The Add an Image Server screen opens.

Step 3 In the Server Name field, enter the name of the image server that you want to add. The server name should be unique and less than 30 characters.

Step 4 In the IP Address field, enter a valid IPv4 or IPv6 address of the image server.

Step 5 In the Username and Password fields, enter the samba account information for the image server.

Step 6 Click the **Add** button. The Image Server List screen opens, and the image server is added to the Image Server List table. The Image Server List table also shows a row ID for the image server and the date that the image server was created.

The far-right column of the Image Server List table provides these links to manage the image server:

- **Edit—**Opens the Edit Image Server screen. This screen contains the same fields as the Add an Image Server screen. You use it to make any changes to the image server except for the server name, which is used to identify the image server. For more information, see the "Cloning, Modifying, and Deleting Image Servers" section on page 2-14.
- **Clone—**Adds an image server in fast mode if there is any existing image server added to GUI. For more information, see the "Cloning, Modifying, and Deleting Image Servers" section on page 2-14.
- **Del**—Deletes an image server.
- **Members**—Opens a screen that you use to distribute groups to image servers. For more information, see the "Distributing Groups to Image Servers" section on page 2-15.

Importing a List of Image Servers

You can import a Microsoft Excel spreadsheet with image server information into the GUI. Follow these spreadsheet requirements:

- The spreadsheet can have any name but must be saved with a .csv extension and cannot exceed 2 MB.
- The first row of the spreadsheet must be the title row and cannot include any image server information. The image server information can start on the second row.
- The title row must consist of these titles: image server name, IP address of the server, username, and password.

To import a spreadsheet into the GUI, follow these steps:

Step 1 On the menu, choose **Manage > Manage Image Servers**. The Manage Image Servers screen opens.

Step 2 To the right of the Upload a spreadsheet field, click the icon with the black arrow.

Step 3 Navigate to a spreadsheet file, and follow the browser instructions to place the file directory and name into the Upload a spreadsheet field.

Step 4 Click **Upload** to upload the information into the table on the Image Server List screen.

Note If the spreadsheet contains an IP address that is not in the required format or is a duplicate of a IP address that exists in the table on the Image Server List screen, the GUI rejects this record with an error message.

Cloning, Modifying, and Deleting Image Servers

To clone, modify, or delete image servers from the GUI, follow these steps:

Step 1 On the menu, choose **Manage > Manage Image Servers**. The Manage Image Servers screen opens.

The Action column of the Manage Image Servers table provides the links for editing, cloning, or deleting image servers from the GUI.

Step 2 Take one of these actions:

- To edit an image server, click the corresponding **Edit** link in the Action column. The Edit Image Server screen opens. You can change the IP Address, Username, and Password fields. When you are done, click **Update**.
- To clone an image server row, click the corresponding **Clone** link in the Action column. The Add an Image Server screen opens. You must modify the Server name and IP Address fields. As an option, you can modify the Username and Password fields. When you are done, click **Add**.
- To delete an image server from the GUI, click the corresponding **Del** link in the Action column. The deletion is confirmed, and the screen reloads.

Using the Search Function to Clone, Modify, and Delete Image Servers

To use the search function to clone, modify, or delete image servers from the GUI, follow these steps:

Step 1 On the menu, choose **Manage > Manage Image Servers**. The Manage Image Servers screen opens.

Step 2 Click **Search Image Servers**. The Search Image Servers screen opens.

Step 3 Check a check box to specify the type of search condition, and then enter the condition in the corresponding field.

For example, you can check the **Server name** check box and enter **server1** to search for all the image servers that contain server1 in the server name. You can also check the **IP Address** check box and enter the IP address in the corresponding field to search for the image server.

Step 4 Click **Search by Above**. The search results appear in a table at the bottom of the screen. By default, all image servers are automatically selected (checked) in the table.

Step 5 Take one of these actions:

- To edit an image server, click the corresponding **Edit** link in the Action column. The Edit Image Server screen opens. You can change the IP Address, Username, and Password fields. When you are done, click **Update**.
- To clone an image server row, click the corresponding **Clone** link in the Action column. The Add an Image Server screen opens. You must modify the Server name and IP Address fields. As an option, you can modify the Username and Password fields. When you are done, click **Add**.

- To delete an image server from the GUI, click the corresponding **Del** link in the Action column. The deletion is confirmed, and the screen reloads.
- To delete all the image servers that are selected in the search results, click **Delete the selected Image Servers**. If you do not want to delete all the image servers, clear the check boxes for the image servers that you do not want to delete.

Distributing Groups to Image Servers

Groups can be distributed to an image server. Each group can only use one image server. You can change the members (that is, the groups) of each image server, by the following procedure:

Step 1 On the menu, choose **Manage > Manage Image Servers**. The Manage Image servers screen opens.

Step 2 For the image server to which you want to distribute groups, in the far right column (Action) of the Image Server List table, click **Member**. The Group Assignment screen opens.

Step 3 In the Groups Without an Image Server field, choose the groups that you want to assign to the image server by pressing the **Crtl** key on your keyboard and clicking group names.

Step 4 Click the left angle brackets (**<<**) to move the groups to the Groups that use <image server name> field or the right angle brackets (**>>**) to move clients back to the Groups Without an Image Server field.

Step 5 Click **Submit Changes**. The table in the lower half of the screen displays the details of the groups that you have distributed to the image server.

Managing Switch Groups

- Creating Switch Groups
- Managing the Edge Switch List
- Adding Members to a Switch Group
- Using the Cisco IOS CLI to Configure Smart Install Groups

You can group client switches in the Smart Install network for configuration and manageability. These groups are based on one of these switch components:

- MAC address
- Product identifier (PID)
- Location

You use the GUI to generate Smart Install group-device association files that the director uses to configure the switches in groups rather than individually. This file is stored on the TFTP server in the /opt/Tftproot/ directory. Although you can manually enter MAC addresses, PIDs, and locations, you can also import a spreadsheet with switch information into the GUI.

Note You can use the CLI to organize client switches into groups based on MAC address or PID (see the "Using the Cisco IOS CLI to Configure Smart Install Groups" section on page 2-20). We recommend, however, that you use the GUI to organize the client switches into groups and use the CLI only if the GUI is not available.

Note If you change any member of the group whose configuration is already downloaded to the director, an update bar will be displayed at the bottom of the page. You can click the **update** button to update the new member information to the director.

Creating Switch Groups

To create a switch group to which you can add switches, follow these steps:

Step 1 On the menu, choose **Manage > Manage Groups**. The Manage Group screen opens.

Step 2 Click **Add a Group** above the table. The Add a Group screen opens.

Step 3 In the Group Name field, enter a name that is meaningful to you.

Step 4 From the Image Server drop-down list, choose an image server.

Step 5 (Optional) In the Description field, enter a description that provides details about the group.

Step 6 Click the **Add** button. The Group List screen opens, and the group is added to the Group List table. The Group List table also shows a row ID for the group and the date that the group was created.

The far right column of the Group List table provides these links to manage the group:

- **Edit—**Opens the Edit a Group screen. This screen contains the same field as the Add a Group screen. You use it to make changes to the group name and description.
- **Del—**Deletes a group.
- **Members—**Opens a screen that you use to add Smart Install switch clients to the group, or to remove them from the group. For information, see the "Adding Members to a Switch Group" section on page 2-19.

Managing the Edge Switch List

The Smart Install director discovers switch clients and adds them to the director database. However, the discovered client switches do not appear on the GUI. To add client switches to the GUI:

- Import a list of client switches into the GUI Cisco Edge List screen.
- Manually add client switches to the GUI Cisco Edge List screen.
- In the GUI, clone an existing client switch, and edit the client switch.

Importing a List of Client Switches

You can import a Microsoft Excel spreadsheet or a text file with client switch information into the GUI. Follow these spreadsheet requirements:

- The spreadsheet can have any name but must be saved with a .csv or .txt extension and cannot exceed 2 MB. A text file must also have comma-separated values.
- The first row of the spreadsheet must be the title row and cannot include any switch information. The switch information can start on the second row.
- The title row must consist of these titles: MAC, PID, LOCATION. Do not include group information: groups are assigned through the GUI.

- The MAC address must consist of six groups of two hexadecimal digits, separated by colons. For example, AA:01:BB:02:CC:03.
- The PID must be alphanumerical and can consist of a maximum of 49 characters.

Note A spreadsheet should not contain group information. You must use the GUI to allocate a switch to a group.

To import a spreadsheet into the GUI, follow these steps:

Step 1 On the menu, choose **Manage > Manage Cisco Edges**. The Manage Cisco Edges screen opens.

Step 2 To the right of the Upload a spreadsheet field, click the icon with the black arrow.

Step 3 Navigate to a spreadsheet or text file, and follow the browser instructions to place the file directory and name into the Upload a spreadsheet field.

Step 4 Click **Upload** to upload the information into the table on the Cisco Edge List screen.

Note If the spreadsheet or text file contains a MAC address that is not in the required format or is a duplicate of a MAC address that exists in the table on the Cisco Edge List screen, the GUI rejects this record with an error message.

Note For more information, see Appendix B, "Importing a Spreadsheet with Client Switch Information."

Manually Adding Client Switches

To manually add a client switch to the GUI, follow these steps:

Step 1 On the menu, choose **Manage > Manage Cisco Edges**. The Manage Cisco Edges screen opens.

Step 2 Click the **Add a Cisco Edge** tab. The Add a Cisco Edge screen opens.

Step 3 Enter this information:

- MAC field: Enter the MAC address in the format of six groups of two hexadecimal digits, separated by colons. For example, AA:01:BB:02:CC:03.

  Note If you enter a MAC address that is not in the required format or is a duplicate of a MAC address that already exists in the table on the Cisco Edge List screen, the GUI rejects your entry with an error message.

- PID field: Enter the PID, which must be alphanumerical and can consist of a maximum of 49 characters.
- LOCATION field: Enter the location, which is a name that is meaningful to you. The location must be alphanumerical and can consist of a maximum of 49 characters
- GROUP field: From the drop-down list, select the group to which the switch should belong. If there is no existing group, the admin can click on the Create a group link on the right of the drop-down list to create one.

Note A switch can belong to only one group.

Step 4 Click **Add** to save your changes and return to the Cisco Edge List screen, or click **Back** to cancel your changes and return to the Cisco Edge List screen.

Cloning, Modifying, and Deleting Client Switches

To clone, modify, or delete client switches from the GUI, follow these steps:

Step 1 On the menu, choose **Manage > Manage Cisco Edges**. The Manage Cisco Edges screen opens.

The Action column of the Manage Cisco Edge table provides the links for modifying, cloning, or deleting client switches from the GUI.

Step 2 Take one of these actions:

- To edit a switch, click the corresponding **Edit** link in the Action column. The Edit Cisco Edge screen opens. This screen contains the same fields as the Add a Cisco Edge screen. You can change the MAC, PID, and LOCATION fields, and allocate the switch to another group. When you are done, click **Update**.
- To clone a switch row, click the corresponding **Clone** link in the Action column. The Add a Cisco Edge screen opens. You must modify the MAC fields (no two switches can have the same MAC address). As an option, you can modify the PID and LOCATION fields and allocate the switch to another group. When you are done, click **Add**.
- To delete a switch from the GUI, click the corresponding **Del** link in the Action column. The deletion is confirmed, and the screen reloads.

Using the Search Function to Clone, Modify, and Delete Switches

To use the search function to clone, modify, or delete client switches from the GUI, follow these steps:

Step 1 On the menu, choose **Manage > Manage Cisco Edges**. The Manage Cisco Edges screen opens.

Step 2 Click **Search Cisco Edges**. The Search Cisco Edge screen opens.

Step 3 Check a check box to specify the type of search condition, and either enter the condition in the corresponding field, or click the condition that is shown in the field.

For example, check the **Location** check box to search by location. You could also check the MAC check box and enter 1 in the corresponding field to search only for the switches with a MAC address that includes 1.

Step 4 Click **Search by Above**. The search results appear in a table at the bottom of the screen. By default, all switches are automatically selected (checked) in the table.

Step 5 Take one of these actions:

- To edit a switch, click the corresponding **Edit** link in the Action column. The Edit Cisco Edge screen opens. This screen contains the same fields as the Add a Cisco Edge screen. You can change the MAC, PID, and LOCATION fields and allocate the switch to another group. When you are done, click **Update**.

- To clone a switch row, click the corresponding **Clone** link in the Action column. The Add a Cisco Edge screen opens. You must modify the SN and MAC fields (no two switches can have the same MAC address). As an option, you can modify the PID and LOCATION fields and allocate the switch to another group. When you are done, click **Add**.
- To delete a switch from the GUI, click the corresponding **Del** in the Action column. The deletion is confirmed, and the screen reloads.
- To delete all switches that are selected in the search results, click **Delete the selected Cisco Edge**. If you do not want to delete all switches, clear the check boxes for the switches that you do not want to delete.

Adding Members to a Switch Group

You can use the GUI to add members to a switch group or modify the members in a switch group.

Note You can also use the CLI to add custom groups of switches based on MAC addresses or PIDs (see the "Using the Cisco IOS CLI to Configure Smart Install Groups" section on page 2-20). We recommend that you use the GUI to organize the client switches into groups and use the CLI only when the GUI is not available.

Using the Group Assignment Screen to Add Members to a Switch Group

To add clients to a switch group in the GUI (see the "Managing Switch Groups" section on page 2-15), follow these steps:

Step 1 On the menu, choose **Manage > Manage Group**. The Manage Group screen opens.

Step 2 For the group to which you want to add clients, in the far right column (Action) of the Group List table, click **Member**. The Group Assignment screen opens.

Step 3 In the Available Cisco Edges field, choose the clients that you want to assign to the group by pressing the **Crtl** key on your keyboard and clicking client names.

Step 4 Click the left angle brackets (**<<**) to move the clients to the Group field or the right angle brackets (**>>**) to move clients back to the Available Cisco Edges field.

Step 5 Click **Submit Changes**. The table in the lower half of the screen displays the details of the clients that you have added to the group.

Using the Search Function to Assign Members to or Change Members of a Switch Group

To use the search function to assign members to a switch group or change members from one switch group to another, follow these steps:

Step 1 On the menu, choose **Manage > Manage Cisco Edges**. The Manage Cisco Edges screen opens.

Step 2 Click the **Group Cisco Edge** button. The Select Group Condition screen opens.

Step 3 Check a check box to specify the type of search condition. Either enter the condition in the corresponding field, or click the condition that is shown in the field.

For example, check the **Location** check box to search by location. You could also check the MAC check box and enter 1 in the corresponding field to search for only the switches with a MAC address that includes 1.

Step 4 Click **Search by Above**. The search results appear in a table at the bottom of the screen. By default, all switches are selected (checked).

Step 5 From the drop-down list to the right of the Group Selected Cisco Edge To button, choose a switch group for the selected switches. If you do not want to reassign some of the switches, uncheck the check boxes for those switches.

Step 6 Click the **Group Selected Cisco Edge To** button to complete the assignment.

Using the Cisco IOS CLI to Configure Smart Install Groups

You can use the CLI to organize client switches into groups based on MAC address or product ID. We recommend that you use the GUI to organize the client switches into groups, and use the CLI only when the GUI is not available.

Note For information about using the GUI to organize the client switches into groups, see the "Creating Switch Groups" section on page 2-16 and the "Adding Members to a Switch Group" section on page 2-19.

Note The Cisco Edge 300 series switch does not support a mixed combination of CLI-generated and GUI-generated group files. You must use *only* the GUI or *only* the CLI to generate group files.

Custom Group Based on MAC Address

You can configure a custom group based on the MAC addressees. A MAC address match takes priority over other matches. The switches that do not match the MAC addresses in the group can get the configuration and image for another group or get the default configuration.

Beginning in privileged EXEC mode, follow these steps on the director to configure a group based on MAC addresses:

	Command	Purpose
Step 1	**config terminal**	Enters global configuration mode.
Step 2	**vstack group custom** *group_name* **mac**	Identifies a custom group based on a MAC address match, and enters Smart Install group configuration mode for the group.
Step 3	**match** *mac_address*	Enters the MAC address of the client switch to be added to the custom group. Repeat the command for each MAC address to be added. **Note** To see MAC addresses of switches in the Smart Install network, enter the **show vstack neighbors all** privileged EXEC command. Switches added to the group use the same image and configuration file.

	Command	Purpose
Step 4	**image** *location image_name*-**imglist.txt**	Enters the location and image list file for the custom group. • *location*—Enter **flash:** if the TFTP server is the director and the file is in the director flash memory, or enter **tftp:** and the location of the image. You can also enter **flash0:**, **flash1:**, or **usb:**. **Note** Although visible in the command-line help, these options are not supported: **flash1:**, **ftp:**, **http:**, **https:**, **null:**, **nvram:**, **rcp:**, **scp:**, **system:**, **tmpsys:.** • *image_name*-**imglist.txt** is the image list file that you want to download.
Step 5	**config** *location* **config.text.***config_filename*	Enters the location and configuration file for the custom group. • *location*—Enter **flash:** if the TFTP server is the director and the file is in the director flash memory, or enter **tftp:** and the location of the configuration file. You can also enter **flash0:**, **flash1:**, or **usb:**. **Note** Although visible in the command-line help, these options are not supported: **flash1:**, **ftp:**, **http:**, **https:**, **null:**, **nvram:**, **rcp:**, **scp:**, **system:**, **tmpsys:.** • **config.text.***config_filename*—Enter the filename of the configuration file for the group.
Step 6	**end**	Returns to privileged EXEC mode.
Step 7	**copy running-config startup config**	(Optional) Saves your entries in the configuration file.
Step 8	**show vstack group custom detail**	Verifies the configuration.

Note The director automatically creates a director configuration file for the new group and saves it on the TFTP server.

This example creates a custom group named testgroup3 that includes the three switches identified by MAC address and configures the group to use the specified image file (global-imglist.txt) and configuration file (config.text.classroom).

```
Director# configure terminal
Director(config)# vstack group custom textgroup3 mac
Director(config-vstack-group)# match mac 0023.34ca.c180
Director(config-vstack-group)# match mac 001a.a1b4.ee00
Director(config-vstack-group)# match mac 00:1B:54:44:C6:00
Director(config-vstack-group)# image tftp://101.122.33.10/global-imglist.txt
Director(config-vstack-group)# config tftp://101.122.33.10/config.text.classroom
Director(config-vstack-group)# exit
Director(config)# end
```

The director configuration file that is created for this group is testgroup3-imagelist.txt.

Custom Group Based on Product ID

You can configure a custom group based on the product IDs (PIDs). The switches that do not match the group PID can get the configuration and image for another group or get the default configuration.

Beginning in privileged EXEC mode, follow these steps on the director to configure a group based on a PID:

	Command	Purpose
Step 1	**config terminal**	Enters global configuration mode.
Step 2	**vstack group custom** *group_name* **product-id**	Identifies a custom group based on a product-ID match, and enters Smart Install group configuration mode for the group.
Step 3	**match** *product-id*	Enters the product ID of the client switches in the custom group.
Step 4	**image** *location image_name*-**imglist.txt**	Enters the location and image list file for the custom group. • *location*—Enter **flash:** if the TFTP server is the director and the file is in the director flash memory, or enter **tftp:** and the location of the image. You can also enter **flash0:**, **flash1:**, or **usb:**. **Note** Although visible in the command-line help, these options are not supported: **flash1:**, **ftp:**, **http:**, **https:**, **null:**, **nvram:**, **rcp:**, **scp:**, **system:**, **tmpsys:.** • *image_name*-**imglist.txt** is the image list file that you want to download.
Step 5	**config** *location* **config.text.***config_filename*	Enters the location and configuration file for the custom group. • *location*—Enter **flash:** if the TFTP server is the director and the file is in the director flash memory, or enter **tftp:** and the location of the configuration file. You can also enter **flash0:**, **flash1:**, or **usb:**. **Note** Although visible in the command-line help, these options are not supported: **flash1:**, **ftp:**, **http:**, **https:**, **null:**, **nvram:**, **rcp:**, **scp:**, **system:**, **tmpsys:.** • **config.text.***config_filename*—Enter the filename of the configuration file for the group.
Step 6	**end**	Returns to privileged EXEC mode.
Step 7	**copy running-config startup config**	(Optional) Saves your entries in the configuration file.
Step 8	**show vstack group custom detail**	Verifies the configuration.

Note The director automatically creates a director configuration file for the new group and saves it on the TFTP server.

This example creates a custom group named testgroup4 that includes the switches identified by the product ID and configures the group to use the specified image file (global.imglist.txt) and configuration file (config.text.classroom).

```
Director# configure terminal
Director(config)# vstack group custom testgroup4 product-id
Director(config-vstack-group)# match EDGE_300
Director(config-vstack-group)# image tftp://101.122.33.10/global-imglist.txt
Director(config-vstack-group)# config tftp://101.122.33.10/config.text.classroom
Director(config-vstack-group)# exit
Director(config)# end
```

The director configuration file that is created for this group is testgroup4-imagelist.txt.

Managing Cisco Edge Configuration Files

- Configuring a Group Using the GUI
- Configuring a Cisco Edge Using the GUI
- Configuring a Cisco Edge or Group Using CLI Mode
- Modifying a Group or Cisco Edge Using CLI Mode
- Using Auto-Complete to Enter Commands

Note On the GUI, a client switch is referred to as a Cisco Edge.

Cisco Edge Configuration File

The Cisco Edge configuration file is the client switch configuration file that is on the TFTP server and managed by the director. The Cisco Edge configuration file consists of these parts:

- A common configuration that applies to all client switches in a group and that includes GUI fields that configure the root password, set all switches to default settings, and configure interface characteristics for all switches in the group. You can also switch to CLI mode to configure the group.
- An individual configuration that applies to a single client switch and that includes GUI fields that configure the interface characteristics for only the single client switch, the Bluetooth settings, the SSID, the wireless security settings, and so on. An individual switch is identified by its MAC address. You can also switch to CLI mode to configure the Cisco Edge.

Configuring a Group Using the GUI

To configure a group using the GUI, follow these steps:

Step 1 On the menu, choose **Configure > Configure Groups**. The Configure Groups screen opens.

Step 2 Click the Configure link from the Action column for the group.

Note The value of each field is set to the default value when the page is loaded for your first-time configuration. The administrator can click **Restore default settings** button to restore the default values.

Step 3 Click the following tabs to configure the group:

Basic Settings	
Group name	Display the name of the group. You can change the name of the group.
Password of root	Enter the root (admin) password for the group. This is a required field.
Password of student	Enter the default user password for the group.
Login GUI	Enable or disable access to the GUI without entering the username and password.
OS version	Choose the operating system image from the drop-down list.
Factory mode OS version	Choose the factory mode operating system image from the drop-down list.
Cisco Software version	Choose the Cisco application image from the drop-down list.
Partner Software version	Choose the partner application image from the drop-down list.
Fonts	Choose the fonts file from the drop-down list.
Resolution	Choose the video resolution from the drop-down list.
Bluetooth	Enable or disable Bluetooth.
Language	Choose the language from the drop-down list.
Time zone	Choose the time zone from the drop-down list.
NTP Server	Enter the IP address of the NTP server.
Number of Cisco Edges	Show the number of Cisco Edge switches.

WiFi	
SSID	Enter the SSID name.
Broadcast SSID	Enable or disable broadcast of the SSID name.
Radio	Enable or disable the wireless radio.
Wireless Mode	Choose a mode from the drop-down list. • 802.11b/g—Devices in the network support 802.11b and 802.11g. • 802.11b—All devices in the wireless network only support 802.11b. • 802.11g—All devices in the wireless network only support 802.11g. • 802.11n—All devices in the wireless network only support 802.11n. • 802.11g/n—Devices in the network support 802.11g and 802.11n. • 802.11b/g/n—Devices in the network support 802.11b, 802.11g, and 802.11n.
Channel	Choose the channel number (which sets the frequency) for the access point.
Transmit power	Choose the power at which the access point radio transmits its wireless signal.
Channel Bandwidth	Choose the channel width when the access point functions in 802.11n mode.
Encryption mode	Choose the encryption mode. Depending on the mode, you will also have to select an encryption type and enter a key.
Wifi > Advanced	
AP isolation	Configure wireless separation for clients that are connected to the same SSID.
Operating mode	Configure greenfield or mixed mode when the access point functions in 802.11n mode.
Guard interval	Configure the period between packets when the access point functions in 802.11n mode or 802.11n mixed mode.
MCS	Configure the high throughput Modulation and Coding Schemes (MCS) rate when the access point functions in 802.11n mode or 802.11n mixed mode.
RDG	Configure the Reverse Direction Grant (RDG) when the access point functions in 802.11n mode or 802.11n mixed mode.
APSD capable	Configure Wi-Fi Multimedia (WMM) power save mode for the access point.
WMM capable	Configure Wi-Fi Multimedia (WMM) for the access point.
Beacon interval	Configure the beacon interval for the access point.
Bg protection	Configure the CTS-to-self protection for the access point.
Channel allocation	Configure the channel width when the access point functions in 802.11n mode or 802.11n mixed mode.
Data beacon rate	Configure the Delivery Traffic Indication Message (DTIM) interval for the access point.

Extension channel	Configure the control side band that is used for the extension or secondary channel when the access point functions in 802.11n mode or 802.11n mixed mode.
Packet aggregation	Configure Aggregate MAC Service Data Unit (A-MSDU) packet aggregation when the access point functions in 802.11n mode or 802.11n mixed mode.
Short slot	Configure the short-slot time when the access point functions in 802.11g mode or 802.11g mixed mode.
Transmit burst	Configure the transmit burst (Tx burst) for the access point.
Transmit preamble	Configure the preamble for the access point.
IGMP snoop	Enable or disable Internet Group Management Protocol (IGMP) snooping.
Multicast MSC	Configure the high throughput Modulation and Coding Schemes (MCS) rate on multicast frames.
Multicast phy mode	Configure PHY mode on multicast frames.
Ethernet Port	
MAC address-table aging time	Enter the number of seconds (from 15 to 3825) that a dynamic MAC address remains in the MAC address table after the address is used or updated.
Interface Gi1/Fe1/Fe2/Fe3/Fe4	Click the + icon next to the Interface to configure the interface.
Status	Enable or disable the port. **Note** The Gi1 port is enabled and cannot be disabled.
Output-queue-strategy	Choose the type of output traffic scheduling on an interface from the drop-down list.
Pause	Enable or disable auto-negotiation flow control on an interface. **Note** This option is available on the Gi1 interface.
Priority	Choose the QoS priority for incoming traffic on an interface.
Rate-limit	Choose the rate-limit and rate for broadcast and unknown unicast traffic on an interface.
Speed	Choose the speed for an interface.
Duplex Mode	Choose the duplex mode for an interface.

NFS	
Note Change the status to ON to enter NFS settings.	
NFS Server	Enter the IP address of the network file system (NFS) server.
NFS Server Path	Enter the path of the NFS server.
Cisco Edge Path	Enter the path of the Cisco Edge.
Status	Choose ON or OFF.
Members	
Display information about the Cisco Edge switches in the group. **Note** You can click the links in the Operation column to configure, power off, or reboot the Cisco Edge switch.	

Step 4 Click the **Apply changes** button. The Apply Settings window appears.

Step 5 Enter the Smart Install Director IP address, user name, Telnet password, and Privileged EXEC mode password.

Step 6 Click the **Apply** button.

Note When you click the Apply button, the configuration file is downloaded to the director switch and all Cisco Edge switches in the group that are powered on reboot with the new configuration. Cisco Edge switches in the group that are not powered on are configured when powered on.

Note After the first-time configuration is applied, the Cisco Edge 300 switches send their IP addresses to the GUI. When the GUI has the IP addresses of Edge 300 switches, it could help to clear the /apps folder. This operation is useful as you need to clear the old application before upgrading images. The administrator can clear the /apps folder by checking the **clear /apps** checkbox in the Apply Settings window. The clear /apps operation will only be applied to those switches that are up and running, and in the group. The switches that are powered off or not in the group will not be affected.

Configuring a Cisco Edge Using the GUI

To configure a Cisco Edge using the GUI, follow these steps:

Step 1 On the menu, choose **Configure > Configure Cisco Edge**. The Configure Cisco Edge screen opens.

Step 2 Click the **Configure** link from the Action column for the Cisco Edge. The Cisco Edge Config screen opens.

Step 3 Click one of the following tabs to configure the group:

Basic Settings	
MAC	Display the MAC address.
PID	Display the product identifier.

Location	Display the location.
Group	Display the group to which the Cisco Edge switch belongs.
Status	Display the current status of the Cisco Edge switch (on, off).
IP	Display the IP address of the Cisco Edge switch.
Password of root	Display the root (admin) password for the group.
Password of student	Display the default user password for the group.
OS version	Display the operating system image.
Factory mode OS version	Display the factory mode operating system image version.
Cisco Software version	Display the Cisco application image version.
Partner Software version	Display the partner software version.
Fonts	Display the fonts file.
Hostname	Enter the hostname of the switch.
Login GUI	Enable or disable access to the GUI without entering the username and password.
Resolution	Choose the video resolution from the drop-down list.
Bluetooth	Enable or disable.
Language	Choose the language from the drop-down list.
Time zone	Choose the time zone from the drop-down list.
NTP Server	Enter the IP address of the NTP server.
WiFi	
SSID	Enter the SSID name.
Broadcast SSID	Enable or disable broadcast of the SSID name.
Radio	Enable or disable the wireless radio.
Wireless Mode	Choose a mode from the drop-down list. • 802.11b/g—Devices in the network support 802.11b and 802.11g. • 802.11b—All devices in the wireless network only support 802.11b. • 802.11g—All devices in the wireless network only support 802.11g. • 802.11n—All devices in the wireless network only support 802.11n. • 802.11b/g/n—Devices in the network support 802.11b, 802.11g, and 802.11n.
Channel	Choose the channel number (which sets the frequency) for the access point.
Transmit power	Choose the power at which the access point radio transmits its wireless signal.
Channel Bandwidth	Choose the channel width when the access point functions in 802.11n mode.
Encryption mode	Choose the encryption mode. Depending on the mode, you will also have to select an encryption type and enter a key.
Wifi > Advanced	

AP isolation	Configure wireless separation for clients that are connected to the same SSID.
Operating mode	Configure greenfield or mixed mode when the access point functions in 802.11n mode.
Guard interval	Configure the period between packets when the access point functions in 802.11n mode or 802.11n mixed mode.
MCS	Configure the high throughput Modulation and Coding Schemes (MCS) rate when the access point functions in 802.11n mode or 802.11n mixed mode.
RDG	Configure the Reverse Direction Grant (RDG) when the access point functions in 802.11n mode or 802.11n mixed mode.
APSD capable	Configure Wi-Fi Multimedia (WMM) power save mode for the access point.
WMM capable	Configure Wi-Fi Multimedia (WMM) for the access point.
Beacon interval	Configure the beacon interval for the access point.
Bg protection	Configure the CTS-to-self protection for the access point.
Channel allocation	Configure the channel width when the access point functions in 802.11n mode or 802.11n mixed mode.
Data beacon rate	Configure the Delivery Traffic Indication Message (DTIM) interval for the access point.
Extension channel	Configure the control side band that is used for the extension or secondary channel when the access point functions in 802.11n mode or 802.11n mixed mode.
Packet aggregation	Configure Aggregate MAC Service Data Unit (A-MSDU) packet aggregation when the access point functions in 802.11n mode or 802.11n mixed mode.
Short slot	Configure the short-slot time when the access point functions in 802.11g mode or 802.11g mixed mode.
Transmit burst	Configure the transmit burst (Tx burst) for the access point.
Transmit preamble	Configure the preamble for the access point.
IGMP snoop	Enable or disable Internet Group Management Protocol (IGMP) snooping.
Multicast MSC	Configure the high throughput Modulation and Coding Schemes (MCS) rate on multicast frames.
Multicast phy mode	Configure PHY mode on multicast frames.

Ethernet Port	
MAC address-table aging time	Enter the number of seconds (from 15 to 3825) that a dynamic MAC address remains in the MAC address table after the address is used or updated.
Interface Gi1/Fe1/Fe2/Fe3/Fe4	Click the + icon next to the Interface to configure the interface.
Status	Enable or disable the port. The Gi1 port cannot be disabled.
Output-queue-strategy	Choose the type of output traffic scheduling on an interface from the drop-down list.
Pause	Enable or disable auto-negotiation flow control on an interface. **Note** This option is available on the Gi1 interface.
Priority	Choose the QoS priority for incoming traffic on an interface.
Rate-limit	Choose the rate-limit and rate for broadcast and unknown unicast traffic on an interface.
Speed	Choose the speed for an interface.
Duplex Mode	Choose the duplex mode for an interface.
NFS **Note** Change the status to ON to enter NFS settings.	
NFS Server	Enter the IP address of the network file system (NFS) server.
NFS Server Path	Enter the path of the NFS server.
Cisco Edge Path	Enter the path of the Cisco Edge.
Status	Choose ON or OFF.

Step 4 Click the **Apply changes** button. The Apply Settings window appears.

Step 5 Enter the Smart Install Director IP address, user name, Telnet password, and Privileged EXEC mode password.

Step 6 Click the **Apply** button.

Note When you click the Apply button, the configuration file is downloaded to the director switch. The configuration takes effect when the switch is rebooted.

Configuring a Cisco Edge or Group Using CLI Mode

Note Use the information in this section together with the CLI commands that are described in Chapter 4, "Using CLI Mode."

To use CLI mode to configure a Cisco Edge or a group, follow these steps:

Step 1 Do one of the following:

- On the menu, choose **Configure > Configure Cisco Edges**. The Configure Cisco Edges screen opens.
- On the menu, choose **Configure > Configure Groups**. The Configure Groups screen opens.

Step 2 Click the **Configure** link from the Action column for the Cisco Edge or group.

Step 3 Click the **Switch to CLI Mode** link.

Step 4 In the Image selection window, make your image selections:

- OS Images—Choose an operating system image from the drop-down list.
- Factory mode OS version—Choose the factory mode operating system image from the drop-down list.
- Cisco Application Images—Choose a Cisco application image from the drop-down list.
- Partner Application Images—Choose a third-party application image from the drop-down list.
- Fonts—Choose the fonts file from the drop-down list.
- IP Address of Director—Enter the IP address of the director (required).
- User Name or Director—Enter your user name to access the director name (optional).
- Telnet Password of Director—Enter your Telnet password of the director switch (optional).

  Note If you entered a director user name, enter the Telnet password for the director user name. Otherwise, enter the switch Telnet login password.

- Privileged EXEC Mode Password—Enter your password to access Privileged EXEC mode (optional).

Step 5 In the Configuration File field, enter CLI commands or use auto-completion to enter CLI commands (see the "Using Auto-Complete to Enter Commands" section on page 2-33). For information about CLI commands, see Chapter 4, "Using CLI Mode."

Step 6 Click **Parse Configuration File and Save**. The file is saved. The *Configuration file has been downloaded to the tftp server* message appears. An error message appears if the file was not saved.

Modifying a Group or Cisco Edge Using CLI Mode

To use CLI mode to modify a Cisco Edge or a group, follow these steps:

Step 1 Do one of the following:

- On the menu, choose **Configure > Configure Cisco Edges**. The Configure Cisco Edges screen opens.
- On the menu, choose **Configure > Configure Groups**. The Configure Groups screen opens.

Step 2 Click the **Configure** link from the Action column for the Cisco Edge or group.

Step 3 Click the **Switch to CLI Mode** link.

Step 4 In the Image selection window, make these selections:

- OS Images—Choose an operating system image from the drop-down list.
- Factory mode OS version—Choose the factory mode operating system image from the drop-down list.
- Cisco Application Images—Choose a Cisco application image from the drop-down list.
- 3rd Party Application Images—Choose a third-party application image from the drop-down list.
- IP Address of Director—Enter the IP address of the director (required).
- Fonts—Choose the fonts file from the drop-down list.
- User Name or Director—Enter your user name to access the director name (optional).
- Telnet Password of Director—Enter your Telnet password of the director switch (optional).

Note If you entered a director user name, enter the Telnet password for the director user name. Otherwise, enter the switch Telnet login password.

- Privileged EXEC Mode Password—Enter your password to access Privileged EXEC mode (optional).

Step 5 In the Configuration File field, change CLI commands or enter new CLI commands. You can also use auto-complete to enter new CLI commands (see the "Using Auto-Complete to Enter Commands" section on page 2-33).

Step 6 When you are done, take one of these actions:

- Save the file under the same name:

  Click **Parse Configuration File and Save** to save the file under the same name. The file is saved. The "Configuration file has been downloaded to the tftp server" message appears. An error message appears if the file was not saved.

Using Auto-Complete to Enter Commands

When you create or edit a Cisco Edge configuration file, you can use auto-complete. It can reduce command syntax errors by providing valid choices. The syntax check occurs only when you click **Parse Configuration File and Save** or **OK**.

To use auto-complete, follow these steps:

Step 1 In the smart input field (with a pound sign [#]), enter a few initial letters of a command. The available commands appear under the smart input field.

(You can also place the cursor in an empty smart input field and press **Space**. Auto-complete shows the commands for the command mode that you are in under the smart input field.)

Step 2 Press **Tab** to auto-complete the command.

(You can also click a command that is shown under the smart input field, and it appears in the smart input field.)

Step 3 Press **Enter**. The command moves to the Configuration File field.

Note The prompt of the smart input field changes according to the command mode that you are in. For example, when the **configure terminal** command moves to the Configuration File field, the command mode changes: (config)#.

This is an example of how you can edit a Cisco Edge configuration file:

Step 1 In the Configuration File field, place the cursor where you want to change or add a CLI command.

Step 2 To make your edits, take one of these actions:

- Manually make an adjustment to the command without using the smart input field. You can edit the command in the Configuration File field as you would do in a regular text box.
- Enter a command in the smart input field and press **Enter** to add the command. The last location of the cursor in the Configuration File field determines where the command is inserted:
  - If you placed the cursor at the beginning of a command line, the new command is inserted above the line.
  - If you placed the cursor in a command line, the new command is inserted to the right of the cursor position.
  - If you placed the cursor at the end of a command line, the new command is inserted below the line.

Step 3 Click **Parse Configuration File and Save** to save your changes. The file is saved. The “Configuration file has been downloaded to the tftp server” message appears. An error message appears if the file was not saved.

Switch Image and Configuration Upgrades

This section describes the upgrade methods.

Caution Before upgrading from software release 1.0 to release 1.1, remove the Factory Mode OS Version and Fonts selections from the GUI and apply the changes. See the "Managing Cisco Edge Configuration Files" section on page 2-23.

Note If there are any problems with an upgrade, see the "Troubleshooting Software Upgrades" section on page D-2.

Upgrade Initiated by the User

In the room where the switch is located, a user can initiate an upgrade by one of these methods:

- Pressing the Reset button—The switch starts up in factory-default mode, connects to the director, and then downloads and installs the latest images and configuration files.
- Turning the switch off and on—The switch starts up in normal mode, connects to the director, and detects whether or not new images and configuration files are available. If new images and configuration files are available, the switch restarts in factory-default mode and automatically downloads and installs the new images and configuration files.

In either case, the switch saves a copy of the existing images and configuration files before installing the new images and files. If the installation fails, the switch restores the old configuration.

Upgrade Initiated by the Administrator

Using the GUI, you can reboot the switch to initiate an upgrade.

Step 1 Do one of the following:

- On the menu, choose **Configure > Configure Cisco Edges**. The Configure Cisco Edges screen opens.
- On the menu, choose **Monitor > Monitor Cisco Edges**. The Monitor Cisco Edges screen opens.

Step 2 Click the **Reboot** link from the Operation column for the Cisco Edge.

Note If the Status of the Cisco Edge is off, the Operation links are not available.

Using the CLI, you can connect to a switch, for example over a Telnet or secure shell (SSH) connection, and restart the switch to initiate an upgrade.

Note On-demand upgrades and scheduled downloads are not supported. You cannot upgrade switches from the director by using the **write erase** and **reload**, **vstack download-image**, **vstack download-config**, or **archive download-sw** privileged EXEC commands.

CHAPTER 3

Monitoring Cisco Edge Switches

To monitor a Cisco Edge switch, follow these steps:

Step 1 Do one of the following:

a. On the menu, choose **Monitor > Monitor Groups**. The Monitor Groups screen opens.

b. Click the **Members** link in the Operation column for the group. The members list opens.

or

On the menu, choose **Monitor > Monitor Cisco Edges**. The Monitor Cisco Edges screen opens.

Step 2 Click the **Details** link in the Operation column for the Cisco Edge to display the Cisco Edge Details screen.

Note If the Status of the Cisco Edge is off, the Operation links are not available.

The Cisco Edge Details page displays the following information:

System	
Status	On or Off.
Hostname	Displays the configured hostname.
CPU and Memory usage	Displays CPU and memory usage information by clicking the **Show details** button.
Disk Usage	Displays the amount of used and available disk space on the different file systems.
Bluetooth status	On or Off.
Startup Config	Displays the startup configuration file by clicking the **Show details** button.
Hosts file	Displays the hosts file information.

Software Version	
OS Version	Displays the operating system image.
Factory Mode OS Version	Displays the factory mode operating system image.
Cisco Software Version	Displays the Cisco application image.
Partner Software Version	Displays the partner application image.

Network	
IP Mode	STATIC or DHCP.
IP Address	Displays the switch IP address.
Mask	Displays the net mask.
DNS Server	Displays the DNS server addresses by clicking the **Show DNS file** button.
MAC address	Displays the MAC address.
Bcast	Displays the broadcast address of the subnet.
Gateway	Displays the gateway IP address.

WiFi	
Status	On or Off.
SSID	Displays the SSID.
Channel	Displays the wireless channel.
Mode	Displays the 802.11 wireless mode for the access point.
Encryption	Displays the authentication and associated encryption for the access point.
Key	Displays the encryption key.
Access devices	Displays the WiFi-connected devices.

Ethernet Port	
Status	Enabled, Disabled, Connected.
Speed	Displays the configured speed.
Duplex mode	Displays the configured duplex mode.
Port statistics	Displays the receive and transmit counts for the port.
QoS	Displays the QoS information of all switch ports
MAC address learned	Displays the list of learned MAC addresses.

NFS Server	
Status	Success or Failure.
Remote Path	Displays the IP address and remote path.
Mount Point	Displays the mount point.

CHAPTER 4

Using CLI Mode

- Configuration Guidelines
- Switch Command Reference

Configuration Guidelines

You can switch to CLI mode to create a Cisco Edge configuration file on the GUI. The CLI uses only commands that are specific to the Cisco Edge 300 series switch. Although the syntax is similar to the Cisco IOS CLI, the commands are *incompatible* with Cisco IOS commands.

Use the CLI to configure these switch settings:

- Basic switch settings—hostname, MAC address, Bluetooth settings, password, Network Time Protocol (NTP) server, and switch language
- Ethernet interface settings—status, speed, and quality of service (QoS)
- Wireless interface settings—status, radio, wireless mode, channel, wireless separation, transmission power, Wi-Fi Multimedia (WMM), and advanced wireless settings
- SSID security settings—broadcast, authentication, and encryption

Note For information about how to enter the CLI in the GUI to create a Cisco Edge configuration file, see the "Managing Cisco Edge Configuration Files" section on page 2-23.

Follow these configuration guidelines:

- Create one Cisco Edge configuration file for each switch group. This file is used to configure *all* switches in the group. When a switch that is part of the group is rebooted, it is configured as defined in the Cisco Edge configuration file. Any changes that were made locally to the switch are lost after the switch reboots.
- Start a Cisco Edge configuration file with the **configure terminal** global command. End the Cisco Edge configuration file with the **exit** global command.
- Within a Cisco Edge configuration file, start each individual switch configuration with the **system identifier** *mac_address* system configuration command. End each individual switch configuration with the **done** system configuration command.

Note We recommend that you use the **system identifier default** system configuration command to configure all the switches in the group to default settings before you configure each switch individually.

- From the system configuration mode, you can enter these configuration modes:
  - Ethernet configuration mode

    Use the **interface** system configuration command to enter this mode. Use the **exit** global configuration command to return to the system configuration mode.
  - WiFi interface configuration mode

    Use the **interface** system configuration command to enter this mode. We recommend that before you configure any wireless settings, that you first use the **wireless-mode** WiFi configuration command to set the 802.11 wireless mode. Use the **exit** global configuration command to return to the system configuration mode.
  - SSID configuration mode

    Use the **ssid** system configuration command to enter this mode. Use the **exit** global configuration command to return to the system configuration mode.
- All commands must be entered in lowercase letters. Arguments can include uppercase letters.
- If there is a configuration conflict, the most recent configuration takes precedence. In this example, the SSID is not broadcast:

```
ssid NEWAP1
    broadcast ssid on
    broadcast ssid off
exit
```

Example of a Cisco Edge Configuration File

This is an example of a Cisco Edge configuration file with two switches: one with the hostname switch333 and MAC address 1111.1111.1211 and the other with the hostname switch344 and MAC address 1111.1111.1213.

```
configure terminal
system identifier default
done
system identifier 1111.1111.1211
   hostname switch333
   mac address-table aging-time 3825
   mac address-table static 1234.1111.1111 interface gi1 default
   interface gi1
       speed 10
   exit
   interface fe3
       speed 10
   exit
   ssid NEWAP1
   exit
done
system identifier 1111.1111.1213
   hostname switch 344
   mac address-table aging-time 3825
   mac address-table static 1111.1111.1111 interface cpu default
   mac address-table static port-count-2 1111.1111.1111 interface cpu fe3 default
```

```
    mac address-table static port-count-3 1111.1111.1111 interface cpu fe3 fe2 critical
    mac address-table static port-count-4 1111.1111.1111 interface cpu fe3 fe2 fe1 default
    mac address-table static port-count-5 1111.1111.1111 interface cpu fe3 fe2 fe1 fe4
    critical
    mac address-table static port-count-6 1111.1111.1111 interface cpu fe3 fe2 fe1 fe4 gi1
    critical
    interface fe3
        priority normal
        output-queue-strategy wrr
        speed 10
    exit
    ssid NEWAP2
        broadcast ssid on
        encryption mode wpapsk type tkip pass-phrase better33safe990-than12sorry_
    exit
    interface bvi1
        wireless-mode 9
        radio on
        channel number 12
        ap-isolation off
        operating-mode greenfield
        channel bandwidth 20/40
        guard-interval 800
        mcs 33
        rdg on
        extension channel upper
        bg-protection on
        beacon-interval 1000
        data-beacon-rate 255
        transmit power 99
        transmit preamble auto
        transmit burst off
        short-slot on
        packet aggregation on
    exit
done
exit
```

Switch Command Reference

Note A syntax description, the command default mode, usage guidelines, and examples are provided *only* for commands that are not self-explanatory.

- Global Configuration Mode
- System Configuration Mode
- Ethernet Interface Configuration Mode
- WiFi Interface Configuration Mode
- SSID Configuration Mode

Global Configuration Mode

Table 4-1 Global Configuration Commands

Command	Function
configure terminal	Starts the Cisco Edge configuration file, and enters global configuration mode.
exit	Exits global configuration mode.
password root	Configures the root password to access and configures all Cisco Edge 300 switches in the network.
system identifier	Sets all switches to their default setting or enters system configuration mode to configure an individual switch.

configure terminal

To start the Cisco Edge configuration file and enter the global configuration mode, use the **configure terminal** global configuration command.

```
configure terminal
```

Usage Guidelines

Each Cisco Edge configuration file must start with the **configure terminal** command.

exit

To exit the configuration mode that you are in, use the **exit** command in any configuration mode.

```
exit
```

Command Modes

Global configuration

Switch configuration

Ethernet Interface configuration

WiFi Interface configuration

SSID configuration

Usage Guidelines

Use **exit** to leave a configuration mode and return to the previous configuration mode.

At the end of a Cisco Edge configuration file, use **exit** after the done system configuration command.

password root

To configure the root password in order to access and configure all Cisco Edge 300 switches in the network, use the **password root** command in global configuration mode.

password root *password*

Syntax Description

password	Specifies the password. Must be alphanumerical, can include the : ~ ! @ # $ % ^ & * ( ) - _ = + , . ? and ; characters, and have a maximum of 30 characters.

Command Default

The default password is cisco.

Command Modes

Global configuration

system identifier

To set all switches to their default setting or to enter the system configuration mode to configure an individual switch, use the **system identifier** global configuration command.

system identifier {*mac_address* | **default**}

Syntax Description

mac_address	Identifies the MAC address of the switch.
default	Sets the configuration of the switches to default settings.

Usage Guidelines

Use the **default** keyword to set the configuration for all switches in a group to the default settings before you configure each switch individually.

Note We recommend that you first set all switches to default settings before you configure each switch individually.

Use the *mac_address* argument to identify a switch by its MAC address and start the configuration for that switch. Use the **done** command to specify the end of the configuration for that switch.

Examples

This example configures the switches to their default settings and identifies the switch with MAC address 1111.1111.1211 so that you can configure it:

```
system identifier default
system identifier 1111.1111.1211
```

System Configuration Mode

Table 4-2 System Configuration Commands

Command	Function
bluetooth	Enables or disables Bluetooth on the switch.
data-store	Configures the system data storage location.
desktop resolution	Configures the desktop parameter.
done	Defines the end of an individual switch configuration and returns to the global configuration mode.
exit	Exits system configuration mode.
hostname	Configures the hostname of the switch.
interface	Enters Ethernet interface configuration mode to configure a Fast Ethernet interface or the Gigabit Ethernet interface, or enters WiFi interface configuration mode to configure the wireless interface.
language support	Configures the language of the switch.
locale	Configures the time zone of the switch.
mac address-table aging-time	Configures the period that a dynamic MAC address remains in the MAC address table after the address is used or updated.
mac address-table static	Adds a static MAC address to one or more interfaces and sets the default QoS mode.
ntp server	Configures the IP address of the NTP server that is used by the switch.
ssid	Sets the SSID name, and enters SSID configuration mode to configure the security settings for the switch access point.

bluetooth

To enable or disable Bluetooth on the switch, use the **bluetooth** system configuration command.

bluetooth {**on** | **off**}

Command Default

Bluetooth is on.

data-store

To set the network file system (NFS) server location, use the **data-store** command.

data-store *remote_ip_addr remote_path destination_path*

Syntax Description

remote_ip_addr	Configures the IP address of the NFS server.
remote_path	Configures the directory path.
destination_path	Configures the destination directory.

Usage Guidelines

Do not mount the server to local system directories other than **/mnt**.

Examples

```
data-store 10.10.11.201 /var/ftp/upload /mnt
```

desktop resolution

To configure the resolution on the desktop, use the **desktop resolution** command.

desktop resolution {**1** | **2** | **3** | **4** | **5** | **6**}

Syntax Description

1	1280 x 960p85
2	720p
3	1024 x 768p60
4	1080p
5	720p50
6	1080p50

Command Default

1024x768p60

Usage Guidelines

Changing the desktop resolution requires a reboot.

done

To define the end of an individual switch configuration and return to the global configuration mode, use the **done** system configuration command.

done

Usage Guidelines

Each individual switch configuration must end with the **done** command.

hostname

To configure the hostname of the switch, use the **hostname** system configuration command.

hostname *name*

Syntax Description

name	The name that you assign to the switch.

Command Default

The default hostname is intel_ce_linux.

Usage Guidelines

Changing the hostname requires a reboot.

interface

To enter Ethernet interface configuration mode to configure a Fast Ethernet or the Gigabit Ethernet interface or to enter WiFi interface configuration mode to configure the wireless interface, use the **interface** system configuration command.

interface {**fe1** | **fe2** | **fe3** | **fe4** | **gi1** | **bvi1**}

Syntax Description

fe1	Configures the Fast Ethernet 1 interface.
fe2	Configures the Fast Ethernet 2 interface.
fe3	Configures the Fast Ethernet 3 interface.
fe4	Configures the Fast Ethernet 4 interface.
gi1	Configures the Gigabit Ethernet interface.
bvi1	Configures the wireless interface.

Usage Guidelines

Use the **interface** command to enter the Ethernet interface configuration mode or WiFi interface configuration mode.

Related Commands

Use the **exit** command to leave Ethernet interface configuration mode or WiFi interface configuration mode.

Table 4-3 on page 4-13 lists the Ethernet interface configuration commands.

Table 4-4 on page 4-18 lists the WiFi interface configuration commands.

language support

To configure the switch language, use the **language support** system configuration command.

```
language support {1 | 3 | 4 | 6 | 8}
```

Syntax Description

1	English (US).
3	Spanish (Mexico).
4	Simplified Chinese.
6	Traditional Chinese.
8	Portuguese.

Command Default

The default is English.

Usage Guidelines

Changing the language requires a reboot.

locale

To configure the time zone, use the **locale** system configuration command.

```
locale value
```

Syntax Description

value	Time Zone
0	GMT0
1	GMT+1
2	GMT+2
3	GMT+3
4	GMT+4
5	GMT+5
6	GMT+6

value	Time Zone
7	GMT+7
8	GMT+8
9	GMT+9
10	GMT+10
11	GMT+11
12	GMT+12
13	GMT-1
14	GMT-2
15	GMT-3
16	GMT-4
17	GMT-5
18	GMT-6
19	GMT-7
20	GMT-8
21	GMT-9
22	GMT-10
23	GMT-11
24	GMT-12
25	GMT+13
26	GMT+14

Command Default

The default time zone is GMT0.

mac address-table aging-time

To configure the period that a dynamic MAC address remains in the MAC address table after the address is used or updated, use the **mac address-table aging-time** system configuration command.

mac address-table aging-time *aging-time*

Syntax Description

aging-time	The period in seconds after which a dynamic MAC address is no longer available in the MAC address table. The range is from 15 to 3825 seconds.

Command Default

The default period is 330 seconds.

Usage Guidelines

When no packets arrive within the aging time period for a MAC address, it is removed from the MAC address table. If packets arrive for the MAC address after it has been removed from the table, the packets are forwarded to all interfaces except to the one on which they arrived. If the MAC address is received again, it is added to the table.

Configure 0 seconds to disable the timer and to prevent MAC addresses from being removed from the MAC address table.

mac address-table static

To add a static MAC address to one or more interfaces and set the default QoS mode, use the **mac address-table static** system configuration command.

mac address-table static *mac-address* [**port-count** *count*] **interface** *interface id* [**default** | **critical**]

Syntax Description

mac_address	Identifies the switch by its MAC address in the xxxx.xxxx.xxxx format.
port-count *count*	(Optional) If you configure only one interface or only the CPU, do not use the **port-count** *count* keyword and argument. If you configure more than one interface, the value that you enter for the *count* argument determines the number of interfaces that you need to enter. The minimum value is 2. The maximum value is 6.
interface *interface id*	Identifies the interface or interfaces to which the static MAC address is applied. If you use the **port-count** *count* keyword and argument, you can enter more than one interface for the *interface id* argument. Use a space to separate the values. These are the possible values for the *interface id* argument: • fe1—Fast Ethernet interface 1 • fe2—Fast Ethernet interface 2 • fe3—Fast Ethernet interface 3 • fe4—Fast Ethernet interface 4 • gi1—Gigabit Ethernet interface • cpu—CPU of the switch
default	(Optional) Configures the interface or interfaces for default QoS mode.
critical	(Optional) Configures the interface or interfaces for critical QoS mode.

Usage Guidelines

To prevent flooding, you can add a static MAC address to an interface. For example, you can configure a static MAC address for an attached uplink switch to prevent packet flooding to the Cisco Edge 300 series switch.

Configure critical QoS for an interface that receives relative important information in relation to the other interfaces. For example, to ensure high video quality, you can configure critical QoS for an interface that is connected to a surveillance camera.

Examples

This example assigns the abcd.abcd.abcd static MAC address to all Ethernet interfaces and the CPU on a switch and sets the QoS mode to default:

```
mac address-table static port-count-6 abcd.abcd.abcd interface fe1 fe2 fe3 fe4 gi1 cpu
default
```

ntp server

To configure the IP address of the NTP server that is used by the switch, use the **ntp server** system configuration command.

ntp server *ip address*

Syntax Description

ip address	The IP address of the NTP server.

ssid

To set the SSID name and enter SSID configuration mode to configure the security settings for the access point of the switch, use the **ssid** system configuration command.

ssid *ssid*

Syntax Description

ssid	The SSID name for the access point. The name can consist of up to 32 characters.

Command Default

The default SSID name is CISCO_EDGE.

Related Commands

Use the **exit** command to leave SSID configuration mode.

Table 4-5 on page 4-32 lists the SSID configuration commands.

Ethernet Interface Configuration Mode

Table 4-3 Ethernet Interface Configuration Commands

Command	Function
disable	Disables an interface.
duplex	Configures the duplex mode for an interface.
enable	Enables an interface.
exit	Exits Ethernet interface configuration mode.
output-queue-strategy	Configures the type of output traffic scheduling on an interface.
pause	Configures auto-negotiation flow control on the Gi1 interface.
priority	Configures the QoS priority for incoming traffic on an interface.
rate-limit	Configures rate-limiting for broadcast and unknown unicast traffic on an interface.
speed	Configures the speed for an interface.

disable

To disable an interface, use the **disable** command in Ethernet interface configuration mode.

disable {**fe1** | **fe2** | **fe3** | **fe4** | **gi1**}

Syntax Description

fe1	Disables the Fast Ethernet 1 interface.
fe2	Disables the Fast Ethernet 2 interface.
fe3	Disables the Fast Ethernet 3 interface.
fe4	Disables the Fast Ethernet 4 interface.
gi1	Disables the Gigabit Ethernet interface.

Defaults

All interfaces are enabled.

Related Commands

The **enable** command enables an interface.

duplex

To configure the duplex mode for an interface, use the **duplex** Ethernet configuration command.

duplex {auto | **half** | **full**}

Syntax Description

auto	Configures automatic duplex mode sensing.
half	Configures half-duplex mode.
full	Configures full-duplex mode.

Defaults

The defaults is automatic duplex mode sensing.

enable

To disable an interface, use the **enable** command in Ethernet interface configuration or WiFi interface configuration mode.

enable {**fe1** | **fe2** | **fe3** | **fe4**}

Syntax Description

fe1	Enables the Fast Ethernet 1 interface.
fe2	Enables the Fast Ethernet 2 interface.
fe3	Enables the Fast Ethernet 3 interface.
fe4	Enables the Fast Ethernet 4 interface.

Defaults

All interfaces are enabled.

Related Commands

The **disable** command disables an interface.

output-queue-strategy

To configure the type of output traffic scheduling on an interface, use the **output-queue-strategy** Ethernet configuration command.

output-queue-strategy {**strict** | **wrr**}

Syntax Description

strict	Configures traffic scheduling based on the queue priority.
wrr	Configures traffic scheduling based on weighted round robin (WRR).

Defaults

The default traffic scheduling is **wrr**.

pause

To configure auto-negotiation flow control on the Gi1 interface, use the **pause** Ethernet configuration command.

pause {**on** | **off**}

Syntax Description

on	Enables flow control. Pause frames are advertised when congestion occurs. Incoming pause frames are accepted.
off	Disables flow control. No pause frames are advertised, and incoming pause frames are discarded.

Defaults

Flow control is off.

Usage Guidelines

This command is supported on the Gi1 interface.

priority

To configure the QoS priority for incoming traffic on an interface, use the **priority** Ethernet interface configuration command.

priority {**high** | **normal**}

Syntax Description

high	Configures incoming traffic as high priority.
normal	Configures incoming traffic as normal priority.

Defaults

Incoming traffic is treated as normal priority.

rate-limit

To configure rate-limiting for broadcast and unknown unicast traffic on an interface, use the **rate-limit** Ethernet interface configuration command.

rate-limit {**none** | **set broadcast** | **set unknown-unicast** | **set both**} *rate*

Syntax Description

none	Disables rate-limiting.
set broadcast	Configures rate-limiting for broadcast traffic.
set unknown-unicast	Configures rate-limiting for unknown unicast traffic.
set both	Configures rate-limiting for both broadcast traffic and unknown unicast traffic.
rate	A value between 1 MB and 100 MB.

Defaults

Rate-limiting is disabled.

speed

To configure the speed for an interface, use the **speed** Ethernet configuration command.

speed {**auto** | **10** | **100** | **1000**}

Syntax Description

auto	Configures automatic speed sensing.
10	Configures 10 Mb/s speed.
100	Configures 100 Mb/s speed.
1000	Configures 1000 Mb/s speed and full-duplex mode. **Note** 1000 Mb/s speed is supported only on the Gi1 interface.

Defaults

The defaults are automatic speed sensing.

WiFi Interface Configuration Mode

Table 4-4 WiFi Interface Configuration Commands

Command	Function
ap-isolation	Configures wireless separation for clients that are connected to the same SSID.
apsd	Configures Wi-Fi Multimedia (WMM) power save mode for the access point.
beacon-interval	Configures the beacon interval for the access point.
bg-protection	Configures the CTS-to-self protection for the access point.
channel bandwidth	Configures the channel width when the access point functions in 802.11n mode or 802.11n mixed mode.
channel number	Configures the channel number (which sets the frequency) for the access point.
data-beacon-rate	Configures the Delivery Traffic Indication Message (DTIM) interval for the access point.
exit	Exits WiFi interface configuration mode.
extension channel	Configures the control side band that is used for the extension or secondary channel when the access point functions in 802.11n mode or 802.11n mixed mode.
guard-interval	Configures the period between packets when the access point functions in 802.11n mode or 802.11n mixed mode.
igmp-snoop	Enables or disables Internet Group Management Protocol (IGMP) snooping.
mcs	Configures the high throughput Modulation and Coding Schemes (MCS) rate when the access point functions in 802.11n mode or 802.11n mixed mode.
multicast-mcs	Configures the high throughput Modulation and Coding Schemes (MCS) rate on multicast frames.
multicast-phy-mode	Configures PHY mode on multicast frames.
operating-mode	Configures greenfield or mixed mode when the access point functions in 802.11n mode.
packet aggregation	Configures Aggregate MAC Service Data Unit (A-MSDU) packet aggregation when the access point functions in 802.11n mode or 802.11n mixed mode.
radio	Turns the access point wireless radio on or off.
rdg	Configures the Reverse Direction Grant (RDG) when the access point functions in 802.11n mode or 802.11n mixed mode.
short-slot	Configures the short-slot time when the access point functions in 802.11g mode or 802.11g mixed mode.
transmit burst	Configures the transmit burst (Tx burst) for the access point.
transmit preamble	Configures the preamble for the access point.

Table 4-4 WiFi Interface Configuration Commands (continued)

Command	Function
transmit power	Configures the power at which the access point radio transmits its wireless signal.
wireless-mode	Configures the 802.11 wireless mode for the access point.
wmm	Configures Wi-Fi Multimedia (WMM) for the access point.

ap-isolation

To configure wireless separation for clients that are connected to the same SSID, use the **ap-isolation** WiFi interface configuration command.

ap-isolation {**on** | **off**}

Syntax Description

on	Enables wireless separation. This prevents wireless clients that are connected to the same SSID from communicating with each other.
off	Disables wireless separation. This allows wireless clients that are connected to the same SSID to communicate with each other.

Related Commands

WiFi interface configuration

apsd

To configure Wi-Fi Multimedia (WMM) power save mode for the access point, use the **apsd** WiFi interface configuration command.

apsd {**on** | **off**}

Syntax Description

on	Enables WMM power save mode.
off	Disables WMM power save mode.

Command Default

WMM power save mode is disabled.

Usage Guidelines

You can configure the **apsd** command only when the Wi-Fi Multimedia (WMM) is enabled.

Related Commands

Use the wmm command to enable WMM.

beacon-interval

To configure the beacon interval for the access point, use the **beacon-interval** WiFi interface configuration command.

beacon-interval *interval*

Syntax Description

interval	A period between 20 and 1000 milliseconds.

Command Default

The default period is 100 milliseconds.

Usage Guidelines

The default setting should work well for most networks.

Configure a long interval to

- Increase the access point throughput performance.
- Decrease the discovery time for clients and decrease the roaming efficiency.
- Decrease the power consumption of the clients.

Configure a short interval to

- Minimize the discovery time for clients and improve the roaming efficiency
- Decrease the access point throughput performance.
- Increase the power consumption of the clients.

bg-protection

Note This command applies to 802.11b/g mixed mode, 802.11n/g mixed mode, and 802.11b/g/n mixed mode.

To configure the CTS-to-self protection for the access point, use the **bg-protection** WiFi interface configuration command.

bg-protection {**auto** | **on** | **off**}

Syntax Description

auto	Configures automatic selection of CTS-to-self protection.
on	Enables CTS-to-self protection.
off	Disables CTS-to-self protection.

Command Default

The default is automatic selection of CTS-to-self protection.

Usage Guidelines

CTS-to-self protection minimizes collisions among clients in a mixed mode environment but reduces throughput performance.

channel bandwidth

Note This command applies to 802.11n mode or 802.11n mixed mode.

To configure the channel width when the access point functions in 802.11n mode, use the **channel bandwidth** WiFi interface configuration command.

channel bandwidth {**20** | **20/40**}

Syntax Description

20	Configures a 20-MHz channel width.
20/40	Configures automatic selection of 20-MHz or 40-MHz channel width.

Command Default

The default is automatic selection of 20-MHz or 40-MHz channel width.

Usage Guidelines

The default setting should work well for most networks.

A 40-MHz channel provides a higher throughput performance for 802.11n clients.

802.11b and 802.11g clients can function only with a 20-MHz channel.

Related Commands

The setting of the **channel bandwidth** command affects the options for the **mcs** command.

channel number

To configure the channel number (which sets the frequency) for the access point, use the **channel number** WiFi interface configuration command.

channel number {**auto** | *number*}

Syntax Description

auto	Configures automatic selection of the channel number.
number	A value between 1 and 14, or 0 (automatic selection).

Command Default

The default channel number is 6.

Usage Guidelines

We recommend that you either use the default channel number or the automatic selection of the channel number and only change the channel number if you experience interference in the network.

If you need to change the channel number, use the following numbers based on your location:

- China and Europe: 1 to 13
- America: 1 to 11
- Japan: 14 (for 11b only)

data-beacon-rate

To configure the Delivery Traffic Indication Message (DTIM) interval for the access point, use the **data-beacon-rate** WiFi interface configuration command.

data-beacon-rate *rate*

Syntax Description

rate	A value between 1 and 255 milliseconds.

Command Default

The default rate is 1 millisecond.

Usage Guidelines

The DTIM interval is a multiple of the beacon interval. Before you change the DTIM interval, consider the types of clients in the network: laptops might function better with a short interval, but mobile phones might function better with a long interval.

A long interval allows clients to save power but can delay multicast and broadcast traffic.

A short interval decreases delivery time of multicast and broadcast traffic but can increase power consumption by clients.

Related Commands

The setting of the **beacon-interval** command affects the **data-beacon-rate** command.

extension channel

Note This command applies to 802.11n mode or 802.11n mixed mode.

To configure the control sideband that is used for the extension or secondary channel when the access point functions in 802.11n mode, use the **extension channel** WiFi interface configuration command.

extension channel {**upper** | **lower**}

Syntax Description

upper	Configures the upper extension channel.
lower	Configures the lower extension channel.

Command Default

The lower extension channel is configured.

Usage Guidelines

This command has effect only when you configure a 40-MHz channel width.

When the main channel number is in the lower range (for example, in the 1–4 range), use the upper extension channel.

When the main channel number is in the upper range (for example, in the 10–13 range), use the lower extension channel.

When the main channel number is in the middle range (for example, in the 5–9 range), use either the upper or lower extension channel.

Related Commands

Use the **channel bandwidth** command to configure the channel width.

Use the **channel number** command to configure the main channel number.

guard-interval

Note This command applies to 802.11n mode or 802.11n mixed mode.

To configure the period between packets when the access point functions in 802.11n mode, use the **guard-interval** WiFi interface configuration command.

guard-interval {**400** | **800**}

Syntax Description

400	Configures a short guard interval of 400 nanoseconds.
800	Configures a long guard interval of 800 nanoseconds.

Command Default

The default is 400 nanoseconds (ns).

Usage Guidelines

Use a 400-ns interval to increase the throughput performance for 802.11n clients but risk some packet errors and multipath interference.

Use an 800-ns interval to minimize packet errors and multipath interference but decrease the throughput performance for 802.11n clients.

Related Commands

The setting of the **guard-interval** command affects the options for the **mcs** command.

igmp-snoop

To enable or disable IGMP snooping on the wireless interface, use the **igmp-snoop** WiFi interface configuration command.

igmp-snoop {**on** | **off**}

Command Default

IGMP snooping is off.

mcs

Note This command applies to 802.11n mode or 802.11n mixed mode.

To configure the high throughput Modulation and Coding Schemes (MCS) rate when the access point functions in 802.11n mode, use the **mcs** WiFi interface configuration command.

mcs *index_number*

Syntax Description

index_number	A value between 0 and 15, or 33 (automatic selection).

Command Default

The default is 33 (automatic rate configuration).

Usage Guidelines

This table shows the MCS index numbers with their potential data rates in Mb/s based on MCS, guard interval, and channel width.

Index Number	**Guard Interval of 800 ns**		**Guard Interval of 400 ns**	
	20-MHz Channel Width	**40-MHz Channel Width**	**20-MHz Channel Width**	**40-MHz Channel Width**
0	6.5	13.5	7 2/9	15
1	13	27	14 4/9	30
2	19.5	40.5	21 2/3	45
3	26	54	28 8/9	60
4	39	81	43 1/3	90
5	52	109	57 5/9	120
6	58.5	121.5	65	135
7	65	135	72 2/9	152.5
8	13	27	14 4/9	30
9	26	54	28 8/9	60
10	39	81	43 1/3	90

11	52	108	57 7/9	120
12	78	162	86 2/3	180
13	104	216	115 5/9	240
14	117	243	130	270
15	130	270	144 4/9	300
33	Configures automatic selection of the MCS index number.			

We recommend that you use automatic selection of the MCS index number. Change the MCS index to a fixed number only if the Received Signal Strength Indication (RSSI) for the clients in the network can support the selected MCS index number.

Related Commands

The setting of the **channel bandwidth** command affects the options for the **mcs** command.

The setting of the **guard-interval** command affects the options for the **mcs** command.

multicast-mcs

Note This command applies to 802.11n mode or 802.11n mixed mode.

To configure the high throughput Modulation and Coding Schemes (MCS) rate on multicast frames when the access point functions in 802.11n mode, use the **multicast-mcs** WiFi interface configuration command.

multicast-mcs *index_number*

Syntax Description

index_number	A value between 0 and 15.

Command Default

The default is 2.

Usage Guidelines

This table shows the MCS index numbers with their potential data rates in Mb/s based on MCS, guard interval, and channel width.

Index Number	**Guard Interval of 800 ns**		**Guard Interval of 400 ns**	
	20-MHz Channel Width	**40-MHz Channel Width**	**20-MHz Channel Width**	**40-MHz Channel Width**
0	6.5	13.5	7 2/9	15
1	13	27	14 4/9	30
2	19.5	40.5	21 2/3	45
3	26	54	28 8/9	60

4	39	81	43 1/3	90
5	52	109	57 5/9	120
6	58.5	121.5	65	135
7	65	135	72 2/9	152.5
8	13	27	14 4/9	30
9	26	54	28 8/9	60
10	39	81	43 1/3	90
11	52	108	57 7/9	120
12	78	162	86 2/3	180
13	104	216	115 5/9	240
14	117	243	130	270
15	130	270	144 4/9	300

multicast-phy-mode

To configure PHY mode on multicast frames when the access point functions in 802.11n mode, use the **multicast-phy-mode** WiFi interface configuration command.

multicast-phy-mode {**0** | **1** | **2** | **3**}

Syntax Description

0	Disabled
1	CCK (802.11b)
2	OFDM (802.11g)
3	HTMIX (802.11b/g/n)

Command Default The default is 2.

operating-mode

Note This command applies to 802.11n mode.

To configure greenfield or mixed mode when the access point functions in 802.11n mode, use the **operating-mode** WiFi interface configuration command.

operating-mode {**greenfield** | **mixed**}

Syntax Description

greenfield	Configures greenfield mode, which improves 802.11n throughput performance but prevents 802.11b and 802.11g clients in the coverage area from recognizing the 802.11n traffic.
mixed	Configures mixed mode, which allows the 802.11b and 802.11g clients in the coverage area to recognize the 802.11n traffic.

Command Default

The default is mixed mode.

Usage Guidelines

Use greenfield mode if there are only 802.11n clients in the coverage area. If you use greenfield mode when 802.11b, 802.11g, and 802.11n clients coexist in the same coverage area, packet collisions might occur.

Use mixed mode when 802.11b, 802.11g, and 802.11n clients coexist in the same coverage area.

packet aggregation

Note This command applies to 802.11n mode or 802.11n mixed mode.

To configure Aggregate MAC Service Data Unit (A-MSDU) packet aggregation when the access point functions in 802.11n mode, use the **packet aggregation** WiFi interface configuration command.

packet aggregation {**on** | **off**}

Syntax Description

on	Enables packet aggregation.
off	Disables packet aggregation.

Command Default

Packet aggregation is off.

Usage Guidelines

Enable packet aggregration if network traffic consists primarily of data.

Disable packet aggregration if network traffic consists primarily of voice, video, or other multimedia traffic.

radio

To turn the access point wireless radio on or off, use the **radio** WiFi interface configuration command.

radio {**on** | **off**}

Syntax Description

on	Enables the wireless radio.
off	Disables the wireless radio.

Command Default

The wireless radio is enabled.

Usage Guidelines

If you do not intend to use the access point, turn off the radio.

rdg

Note This command applies to 802.11n mode or 802.11n mixed mode.

To configure the Reverse Direction Grant (RDG) when the access point functions in 802.11n mode, use the **rdg** WiFi interface configuration command.

rdg {**on** | **off**}

Syntax Description

on	Enables RDG.
off	Disables RDG.

Command Default

RDG is disabled.

Usage Guidelines

When RDG is enabled, a transmitter that has reserved the channel transmission opportunity allows the receiver to send packets in the reserved direction. When RDG is disabled, packets can be transmitted only in one direction during the channel transmission opportunity reservation.

Enable RDG for better throughput performance for 802.11n traffic.

short-slot

Note This command applies to 802.11g mode or 802.11g mixed mode.

To configure the short-slot time when the access point functions in 802.11g mode or 802.11g mixed mode, use the **short-slot** WiFi interface configuration command.

short-slot {**on** | **off**}

Syntax Description

on	Enables short-slot time.
off	Disables short-slot time.

Command Default

Short-slot time is enabled.

Usage Guidelines

Enable the short-slot time for better throughput performance for 802.11g clients.

If there are mostly 802.11b clients in the network, disable the short-slot time.

transmit burst

To configure the transmit burst (Tx burst) for the access point, use the **transmit burst** WiFi interface configuration command.

transmit burst {**on** | **off**}

Syntax Description

on	Enables Tx burst.
off	Disables Tx burst.

Command Default

Tx burst is enabled.

Usage Guidelines

Leave Tx burst on for better throughput performance.

Disable Tx burst if you notice wireless interference in the network.

transmit preamble

To configure the preamble for the access point, use the **transmit preamble** WiFi interface configuration command.

transmit preamble {**long** | **short** | **auto**}

Syntax Description

long	Configures a long preamble.
short	Configures a short preamble.
auto	Configures automatic preamble selection.

Command Default

The default is a long preamble.

Usage Guidelines

Use the long preamble setting for compatibility with legacy 802.11 systems operating at 1 and 2 Mb/s.

Configure a short preamble setting to improve throughput performance.

transmit power

To configure the power at which the access point radio transmits its wireless signal, use the **transmit power** WiFi interface configuration command.

transmit power *percentage*

Syntax Description

percentage	A value between 1 and 100.

Command Default

The default is 100 percent.

Usage Guidelines

For transmission of the wireless signal over a long distance, use the 100 percent setting.

For transmission of the wireless signal over a short distance, for example, when all clients are in a small room, lower the percentage.

wireless-mode

To configure the 802.11 wireless mode for the access point, use the **wireless-mode** WiFi interface configuration command.

wireless-mode {**0** | **1** | **4** | **6** | **7** | **9**}

Syntax Description

0	Configures 802.11b/g mixed mode.
1	Configures 802.11b mode.
4	Configures 802.11g mode.
6	Configures 802.11n mode.
7	Configures 802.11n/g mixed mode.
9	Configures 802.11b/g/n mixed mode.

Command Default

The default is 802.11b/g/n mixed mode.

Usage Guidelines

802.11b/g mixed mode—Select this mode if you have devices in the network that support 802.11b and 802.11g.

802.11b mode—Select this mode if all devices in the wireless network only support 802.11b.

802.11g mode—Select this mode if all devices in the wireless network only support 802.11g.

802.11n mode—Select this mode if all devices in the wireless network only support 802.11n.

802.11b/g/n mixed mode—Select this mode if you have devices in the network that support 802.11b, 802.11g, and 802.11n.

wmm

To configure Wi-Fi Multimedia (WMM) for the access point, use the **wmm** WiFi interface configuration command.

wmm {**on** | **off**}

Syntax Description

on	Enables WMM.
off	Disables WMM.

Command Default

WMM is disabled.

Usage Guidelines

WMM provides QoS for wireless traffic. If there is a lot of mixed media traffic (voice, video, data), enable WMM.

Related Commands

Use the **apsd** command to configure WMM power save mode.

SSID Configuration Mode

Table 4-5 SSID Configuration Commands

Command	Function
broadcast ssid	Enables or disables broadcast of the SSID name.
encryption mode (open, shared, or WEP configuration)	Configures open, shared, or Wired Equivalency Privacy (WEP) authentication and associated encryption for the access point.
encryption mode (WPA configuration)	Configures Wi-Fi Protected Access (WPA) authentication and associated encryption for the access point.
exit	Exits SSID configuration mode.

broadcast ssid

To enable or disable broadcast of the SSID name, use the **broadcast ssid** SSID configuration command.

broadcast ssid {**on** | **off**}

Syntax Description

on	Enables broadcast of the SSID name.
off	Disables broadcast of the SSID name.

Command Default

The SSID is broadcast.

Usage Guidelines

Disable broadcast of the SSID for enhanced security. Only wireless clients who know the SSID can connect to the access point.

Enable broadcast of the SSID for wider availability and easier access.

encryption mode (open, shared, or WEP configuration)

To configure open, shared, or Wired Equivalency Privacy (WEP) authentication and associated encryption for the access point, use the **encryption mode** SSID configuration command.

encryption mode {**open** | **shared**} **type** {**none** | **wep** {**key** {**1** | **2** | **3** | **4**} {**hex** *number* | **ascii** *phrase*}}}

Syntax Description

open	Configures open access without authentication.
shared	Configures authentication with a shared key.
none	Configures no encryption.
wep	Configures WEP encryption.
key 1 **key 2** **key 3** **key 4**	Configures the key number for WEP encryption. (You can use only one of the four keys.)
hex *number*	Configures either authentication with a hexadecimal key or authentication and encryption with a hexadecimal key: • When you select the **none** keyword, configures authentication with a hexadecimal key. • When you select the **wep** keyword, configures authentication and encryption with a hexadecimal key. For *number*, enter either 10 or 26 hexadecimal digits.
ascii *phrase*	Configures either authentication with a passphrase or authentication and encryption with a passphrase: • When you select the **none** keyword, configures authentication with a passphrase. • When you select the **wep** keyword, configures authentication and encryption with a passphrase. For *phrase*, enter either 5 or 13 alphanumerical characters. Dash (-) and underscore (_) characters are supported.

Command Default

The default is open access and no encryption.

Usage Guidelines

For shared access without encryption, the WEP hexadecimal number or passphrase is used only for authentication.

For shared access with WEP encryption, the WEP hexadecimal number or passphrase is used for both authentication and encryption.

Examples

This example configures shared authentication and WEP encryption, using key 3 and a passphrase of 3uifsfis-_0r5:

```
encryption mode shared type wep key 3 ascii 3uifsfis-_0r5
```

encryption mode (WPA configuration)

To configure Wi-Fi Protected Access (WPA) authentication and associated encryption for the access point, use the **encryption mode** SSID configuration command.

encryption mode {**wpapsk** | **wpa2psk** | **wpapskwpa2psk**} **type** {**tkip** | **aes** | **tkipaes**} **pass-phrase** *phrase*

Syntax Description

wpapsk	Configures WPA with preshared key (PSK) authentication.
wpa2psk	Configures WPA2 with PSK authentication.
wpapskwpa2psk	Configures combined WPA and WPA2 with PSK authentication.
tkip	Configures Temporal Key Integrity Protocol (TKIP) encryption.
aes	Configures Advanced Encryption Standard (AES) encryption.
tkipaes	Configures combined TKIP and AES encryption.
pass-phrase *phrase*	Configures a passphrase (password). For *phrase*, enter at least 8 and at most 63 alphanumerical characters. Dash (-) and underscore(_) characters are supported.

Command Default

The default is open access and no encryption.

Examples

This example configures combined WPA and WPA2 authentication with combined TKIP and AES encryption, using a passphrase of safE478_Ty33Yep-:

```
encryption mode wpapskwpa2psk type tkipaes pass-phrase safE478_Ty33Yep-
```

APPENDIX A

Third-Party Software Image Requirements

These are the requirements for third-party application images to run on the Cisco Edge 300 series switch:

- The image must be a single package in the form of a *delivery.tar.gz file.
- The image must contain a header file that is placed in a separate header directory. The name of the header file must describe the image.
- The name of the header file must also be the name of the image file. For example, if the header file for the third-party application is 3rd-app-edge300-0.2.5.0-delivery.header, the name of the third-party application image file must be 3rd-app-edge300-0.2.5.0-delivery.tar.gz.

  This figure shows the directory structure on the TFTP server after the image package has been unzipped and placed in the /opt/Tftproot/image directory. The bold text parts must match:

```
/opt/Tftproot
|---Image
|    |---OS
|    |    |-- os-edge300-0.2.5.0-delivery.tar.gz
|    |    |-- header/os-edge300-0.2.5.0-delivery.header
|    |    |-- root-edge300-0.2.5.0.tar.gz
|    |    |-- bzImage-21official-beta0.1
|    |---CiscoApp
|    |    |-- cisco-app-edge300-0.2.5.0-delivery.tar.gz
|    |    |-- header/cisco-app-edge300-0.2.5.0-delivery.header
|    |    |-- cisco-app-edge300-0.2.5.0.tar.gz
|    |---Partner
|    |    |-- 3rd-app-edge300-0.2.5.0-delivery.tar.gz
|    |    |-- header/3rd-app-edge300-0.2.5.0-delivery.header
|    |    |-- 3rd-app-edge300-0.2.5.0.tar.gz
```

- The header file must specify these fields, and the IMAGE_TYPE, CPU_TYPE and VIDEO_OUT fields must contain the information that is shown after the equal (=) sign:

```
IMAGE_TYPE=3RD_APP
IMAGE_SIZE=
VERSION=
DDR=
SLC=
MLS=
CPU_CORE=
CPU_TYPE=CE4150
USB=
DOWN_PORTS=
UP_PORTS=
WIRELESS_AP=
BT=
ZIGBEE=
VIDEO_OUT=HDMI
```

This is an example of a header file:

```
IMAGE_TYPE=3RD_APP
IMAGE_VERSION=0.2.5.0
IMAGE_SIZE=1000K
DDR=1G
SLC=1G
MLC=1G
CPU_CORE=1
CPU_TYPE=CE4150
USB=2
DOWN_PORTS=4
UP_PORTS=1
WIRELESS_AP=0
BLUETOOTH=1
ZIGBEE=0
VIDEO_OUT=HDMI
IMAGE_NAME=3rd-app-edge300-0.2.5.0-delivery.tar.gz
```

APPENDIX B

Importing a Spreadsheet with Client Switch Information

The "Importing a List of Client Switches" section on page 2-16 explains how to import a file with client switch information into the GUI. This appendix provides an example with more detailed steps.

To import a spreadsheet into the GUI, follow these steps:

Step 1 Make sure that the first row of the spreadsheet is the title row and does not include any switch information. The switch information can start on the second row.

Step 2 Save the spreadsheet in the CSV format.

Note If a confirmation pop-up window appears, click **OK** or **Yes**.

Step 3 On the Manage Cisco Edges screen, click the 📁 icon and choose the saved spreadsheet.

Step 4 Click **Upload** to import the spreadsheet. The imported client switches appear in the table.

Note If the MAC address (MAC) are not unique, a warning message appears.

Note A MAC address must consist of six groups of two hexadecimal digits, separated by colons. If the format of a MAC address in the spreadsheet is not correct, a warning message appears.

APPENDIX C

Setting Up Image Servers for the Smart Install GUI

You can set up your own image servers for Smart Install instead of using the GUI server.

Note Use either the GUI server as the local image server (that is, the GUI server and the image server run on the same machine), or use a distributed image server. You *must not* use both the local server and the distributed server as image servers at the same time.

You can set up an image server on Windows or Redhat Linux (such as CentOS/Fedora). Smart Install does not currently support image servers running on Ubuntu. The Smart Install GUI supports the following two types of deployment scenarios:

- Setting Up an Image Server on Windows 2008
- Setting Up an Image Server on CentOS 6

Setting Up an Image Server on Windows 2008

To configure an image server on Windows 2008, follow these steps:

Step 1 Create a folder named Tftproot at the location that you prefer (for example, C:\Tftproot).

Step 2 Create the following subfolder structure under the Tftproot folder:

```
/Tftproot
|---image
|    |---CiscoApp
|    |---FM_OS
|    |---Fonts
|    |---OS
|    |---Partner
|---imglist
|---sb_conf
```

Step 3 Use the following steps to share the Tftproot folder:

a. Right-click the Tftproot folder and choose **Properties** from the menu.

b. Click the **Sharing** tab, and click the **Share...** button. The File Sharing dialog box opens.

c. Click the **Share** button, you will see a screen that displays “Your folder is shared.”

Note You can also share the folder with other users in the Administrators group. The password of the user *must not* contain a comma (,).

Step 4 Download TFTP software, for example, Tftpd32.

Step 5 In the TFTP software, set Current Directory to the path of Tftproot folder (for example, C:\Tftproot).

Step 6 Add the image server to the Smart Install GUI with the username “administrator” and the password that you set for it. For more information about adding an image server to the GUI, see the “Creating Image Servers” section on page 2-13.

Setting Up an Image Server on CentOS 6

To configure an image server on CentOS 6, follow these steps:

Step 1 Enter the following commands in the terminal to create Tftproot folder and its subfolders:

```
mkdir -p /opt/Tftproot/sb_conf
mkdir -p /opt/Tftproot/imglist
mkdir -p /opt/Tftproot/image/CiscoApp
mkdir -p /opt/Tftproot/image/OS
mkdir -p /opt/Tftproot/image/FM_OS
mkdir -p /opt/Tftproot/image/Partner
mkdir -p /opt/Tftproot/image/Fonts
chown apache:apache /opt/Tftproot/*
chmod 777 /opt/Tftproot/ -R
```

Step 2 Enter the following commands to install the TFTP software:

```
yum -y install xinetd tftp tftp-server
/sbin/service xinetd start
sed -i "s/\(disable[\t]*= *\).*/\1no/" /etc/xinetd.d/tftp
sed -i "s/\(server_args[\t]*= *\).*/\1-s \/opt\/Tftproot -c/" /etc/xinetd.d/tftp
sed -i '$ a\/sbin/service xinetd start' /etc/rc.d/rc.local
sed -i "s/\(SELINUX=\).*/\1disabled/" /etc/selinux/config
sed -i '$ a\\/sbin\/chkconfig --level 2345 iptables off' /etc/rc.d/rc.local
/etc/init.d/iptables stop
```

Step 3 Enter the following commands to set up a samba account with a username that you prefer (for example, smbusr). The password *must not* contain a comma (,):

```
useradd smbusr
smbpasswd ña smbusr
enter the password:[Enter your password]
```

Step 4 Use vi/vim or nano to modify /etc/samba/smb.conf as follows:

```
[Tftproot]
    path = /opt/Tftproot
    valid users = smbusr
    read only = No
    guest ok = Yes
    force create mode = 777
```

Step 5 Enter the following command to restart the samba server:

```
service smb restart
```

Note By default, the samba service does not start automatically. For more information on configuring the automatic start of samba service after restart, see the "Configuring the Automatic Start of Samba Service After Booting Up" section on page C-3.

Step 6 Add the image server to the Smart Install GUI with the username "smbusr" and the password that you set for it. For more information about adding an image server to the GUI, see the "Creating Image Servers" section on page 2-13.

Configuring the Automatic Start of Samba Service After Booting Up

To configure the automatic start of the samba service after booting up on runlevel 3 and on runlevel 5, follow these steps:

Step 1 Enter the following command to list the samba (smb) service that automatically starts on all of the runlevels:

```
# chkconfig -list smb
smb 0:off 1:off 2:off 3:off 4:off 5:off 6:off
```

Step 2 Enter the following command to enable the samba server to automatically start when booting up on runlevel 3 and runlevel 5:

```
# chkconfig -level 35 smb on
```

Step 3 Verify the configuration changes by entering the following command:

```
# chkconfig -list smb
smb 0:off 1:off 2:off 3:on 4:off 5:on 6:off
```

APPENDIX D

Troubleshooting

General Troubleshooting

If there are problems with a Cisco Edge 300 series switch in the Smart Install network (for example, a failed upgrade), press and hold the switch Reset button. The switch starts up in factory-default mode, connects to the director, and downloads and installs the latest images.

If problems persist, follow these troubleshooting guidelines:

Step 1 Connect to the Cisco Edge 300 series switch (see the *Cisco Edge 300 Series Switch Installation Guide*):

a. Use the **ping** [*options*] **host** Linux command to ping the director to verify connectivity.

b. Use the **ls** [*options*] [*names*] Linux command on the Cisco Edge 300 series switch to make sure that:

   - The smistart.sh script exists in the scripts directory: /scripts/smistart.sh.
   - The smi.lease file exists in the tmp directory: /tmp/smi.lease.
   - The dhclient-enter-hooks script exists in a directory.

c. If the dhclient-enter-hooks exists but the smi.lease file does not exist in the tmp directory, verify that:

   - The DHCP client is running, that is, the **dhclient** Linux command is defined.
   - The DHCP server is running.
   - The switch can obtain the IP address of the DHCP server.

d. If the switch cannot obtain the IP address of the DHCP server, use the **ifconfig** [*interface*] **ifconfig** [*interface address_family parameters addresses*] Linux command to define the IP address of the DHCP server.

Step 2 On the Smart Install director:

- Make sure that the switch has not lost its director configuration.
- Make sure that the image list file and switch configuration file are configured on the director.
- Enter the **show ip dhcp snooping binding** [*ip-address*] [*mac-address*] user EXEC command to display the DHCP snooping bindings database and configuration information for the switch.

Step 3 On the TFTP server, make sure that:

- The image list file that is configured on the director exists on the TFTP server.
- The images that are defined in the image list file exist on the TFTP server.
- The director configuration file exists on the TFTP server.

- A new image that must replace an old image in an upgrade has a different version number than the old image, and the new image is defined in the image list file.
- The correct hardware parameters, including keywords and values, are defined in the image list file of a new image that must replace an old image in an upgrade.

Step 4 On the switch, use the **vi** [*options*] [*files*], **cat** [*options*] [*files*], or **more** [*options*] [*files*] Linux command to retrieve the syslog (smi_log) file from the tmp directory. Send the file to technical support.

Troubleshooting Software Upgrades

After a software download, the switch reboots to upgrade the software. If the software download fails, the switch does not reboot, and an error message is saved in the syslog file. If a monitor is attached to the switch, the error message also appears on the monitor.

If the software download succeeds but the downloaded image or configuration file is defective, reassociate the switches in the group to working image and configuration files. Instruct the end users to upgrade the switch again by restarting the switch or pressing the Reset button.

If a software upgrade fails, for example, because of a power failure or loss of network connectivity, the switch remains in factory default mode, and an error message is saved in the syslog file. If a monitor is attached to the switch, the error message also appears on the monitor. To recover from the failed software upgrade, the end user needs to restart the switch or press the Reset button.

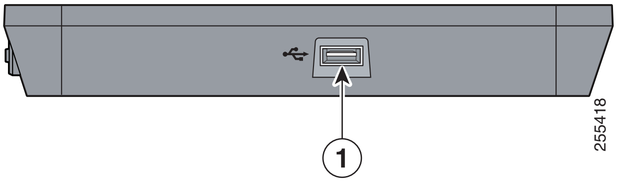
Manually Upgrading the Software Using the USB Port

Caution Before upgrading from software release 1.0 to release 1.1, remove the Factory Mode OS Version and Fonts selections from the GUI and apply the changes. See the "Managing Cisco Edge Configuration Files" section on page 2-23.

If the Cisco Edge 300 is unable to connect to the Smart Install director, you can use the Cisco Edge USB Smart Install tool to upgrade or restore the system firmware using a USB flash drive.

Use the USB port on the side of the Cisco Edge 300 to perform the USB Smart Install upgrade.

Figure 1 Cisco Edge 300 Series Switch



1	USB port

Formatting a USB Smart Install Flash Drive

Step 1 Format the USB flash drive with at least 1 GB of storage capability to the ext3 file system:

```
mkfs.ext3 /dev/sdb1
```

Step 2 Mount the USB flash drive and unpackage the smi-usb image into it:

```
sudo tar -zpxvf smi-usb-sunbird-1.1.0-delivery.tar.gz -C /media/sdb1
```

Using the USB Smart Install on Cisco Edge OS Version 1.1.0 and Later

Step 1 Detach all of the USB flash devices from the Cisco Edge 300 switch. Unplug the Ethernet cable from the Gigabit Ethernet (uplink) port.

Step 2 Start the Cisco Edge 300 switch and enter the user desktop.

Step 3 Plug in the USB Smart Install flash drive at the side USB port.

Step 4 Double-click the SmartInstall icon on the desktop.

Step 5 Enter the root password in the pop-up window and click **OK**.

Note Ask the system administrator if you do not know the password.

The main window displays the firmware version currently running on the Cisco Edge 300 switch and the firmware image version to be upgraded from the USB flash drive.

Step 6 Do one of the following:

- Select Normal Upgrade to upgrade the system.
- Select Force Upgrade to restore the system to the version provided by the USB flash drive.

Step 7 Click **OK** in the Warning window.

Note If you do not click OK, the system reboots in 10 seconds.

During the upgrade, the power LED blinks green. After 20 to 40 minutes, the system reboots normally with the new firmware installed.

Note An amber power LED indicates upgrade failure.

Step 8 Detach the USB Smart Install flash drive. Plug the Ethernet cable into the Gigabit Ethernet (uplink) port.

Using the USB Smart Install on Cisco Edge OS Version 1.0.0

Step 1 Detach all the USB flash devices from the Cisco Edge 300 switch. Unplug the Ethernet cable from the Gigabit Ethernet (uplink) port.

Step 2 Start the Cisco Edge 300 switch and enter the user desktop.

Step 3 Plug in the USB flash drive at the side USB port.

Step 4 When the USB flash drive icon appears on the desktop, double-click the icon to view the contents of the USB flash drive.

Step 5 Find the SmartInstall icon and double-click it.

Step 6 Enter the root password in the pop-up window and click **OK**.

Note Ask the system administrator if you do not know the password.

The main window displays the firmware version currently running on the Cisco Edge 300 switch and the firmware image version to be upgraded from USB flash drive.

Step 7 Do one of the following:

- Select Normal Upgrade to upgrade the system.
- Select Force Upgrade to restore the system to the version provided by USB flash drive.

Step 8 Click **OK** in the Warning window.

Note If you do not click OK, the system reboots in 10 seconds.

During the upgrade, the power LED blinks green. After 20 to 40 minutes, the system reboots normally with the new firmware installed.

Note An amber power LED indicates upgrade failure.

Step 9 Detach the USB Smart Install flash drive. Plug the Ethernet cable into the Gigabit Ethernet (uplink) port.

Note If the SmartInstall window displays “PIC version too old,” your Cisco Edge 300 hardware version is too old to support the USB SmartInstall tool.