Cisco Edge 300 Series Switch Software Configuration Guide, Release 1.6

March 20, 2015

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

CONTENTS

CHAPTER 6   **Configuring HTTP API**   **6-1**

Cisco Edge 300 Series Switch Software Configuration Guide, Release 1.6

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 *What's New in Cisco Product Documentation* at:
http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

Cisco Edge 300 Series Switch

- Cisco Edge 300 Series Switch Overview
- Central Management and Configuration

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, and camera
- Output devices such as a monitor, television, projector, speakers, and headphones

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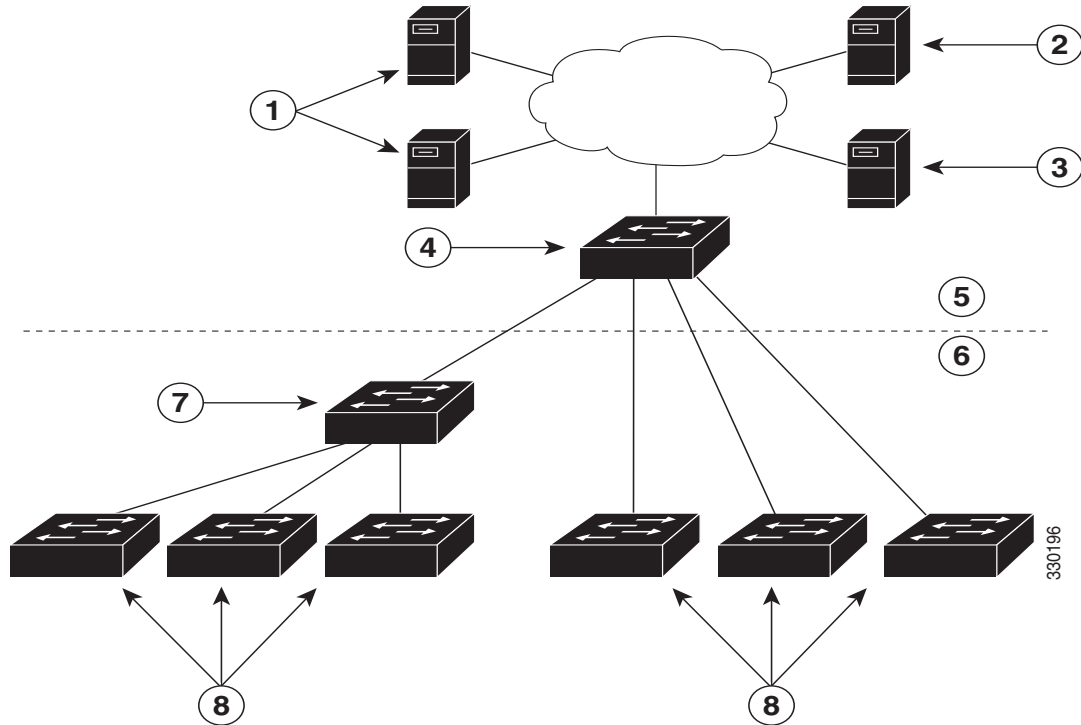
1	Cloud and application delivery servers	5	Aggregation layer
2	DHCP server	6	Access layer
3	TFTP server	7	Intermediate switch
4	Director	8	Client switches

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

- VLC player

- VPN support

- SNMP support

- VLAN support (You can configure at most 6 active VLANs on the Cisco Edge 300 switch.)

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. 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 also can support these functions in the network, or other devices in the network can 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 obtain 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 2-7.

✎ **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 2-9).

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 specifies an individual configuration that applies to a single client switch in a group. The groups include 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 2-25 and Chapter 4, "Configuring Local CLI - Clish").

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 2-35.

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.

Configuring the Smart Install Network

- Configuring the Director and DHCP Server
- Configuring the TFTP Server
- Installing and Using the GUI
- Switch Image and Configuration Upgrades
- CLI Configuration Mode in the Smart Install Server

Configuring the Director and DHCP Server

- DHCP and Smart Install
- Configuring the DHCP Server
- Using Static IP Addresses
- Configuring the Smart Install Director

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 2-25.

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.

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 2-7.
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.
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 the 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 2-7.

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 2-2. 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.

Selection Guidelines

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

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

Using the GUI

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 2-17).
- Add individual switches to the GUI or import lists of switches into the GUI (see the "Managing the Edge Switch List" section on page 2-18).
- 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 2-20.
- Create a Cisco Edge configuration file (see the "Managing Cisco Edge Configuration Files" section on page 2-25).

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

- Yum Package Manager—This software should be part of the Fedora preinstalled software package. If you do not install a Yum package manager during the Fedora installation, you can download it from http://yum.baseurl.org/.

✎
Note Make sure that the Yum repositories can be reachable. For example, if you are using Fedora 14, the default repositories of your system are deprecated.

Updating the Yum Repositories

If the default repositories of your system are deprecated, you need to update them manually.

✎
Note If you are using CentOS, see http://wiki.centos.org/AdditionalResources/Repositories for the repositories information.

Before installing the GUI, use the following steps to update the Yum repositories on Fedora:

Step 1 Update /etc/yum.repos.d/fedora.repo

```
[fedora]
name=Fedora $releasever - $basearch
failovermethod=priority
#baseurl=http://download.fedoraproject.org/pub/fedora/linux/releases/$releasever/Everythin
g/$basearch/os/
baseurl=http://archives.fedoraproject.org/pub/archive/fedora/linux/releases/$releasever/Ev
erything/$basearch/os/
#mirrorlist=https://mirrors.fedoraproject.org/metalink?repo=fedora-$releasever&arch=$basea
rch
enabled=1
metadata_expire=7d
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-fedora-$basearch

[fedora-debuginfo]
name=Fedora $releasever - $basearch - Debug
failovermethod=priority
#baseurl=http://download.fedoraproject.org/pub/fedora/linux/releases/$releasever/Everythin
g/$basearch/debug/
baseurl=http://archives.fedoraproject.org/pub/archive/fedora/linux/releases/$releasever/Ev
erything/$basearch/debug/
#mirrorlist=https://mirrors.fedoraproject.org/metalink?repo=fedora-debug-$releasever&arch=
$basearch
enabled=0
metadata_expire=7d
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-fedora-$basearch

[fedora-source]
name=Fedora $releasever - Source
failovermethod=priority
#baseurl=http://download.fedoraproject.org/pub/fedora/linux/releases/$releasever/Everythin
g/source/SRPMS/
baseurl=http://archives.fedoraproject.org/pub/archive/fedora/linux/releases/$releasever/Ev
erything/$basearch/SRPMS/
#mirrorlist=https://mirrors.fedoraproject.org/metalink?repo=fedora-source-$releasever&arch
=$basearch
enabled=0
metadata_expire=7d
```

```
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-fedora-$basearch
```

Step 2   Update /etc/yum.repos.d/fedora-updates.repo

```
[updates]
name=Fedora $releasever - $basearch - Updates
failovermethod=priority
#baseurl=http://download.fedoraproject.org/pub/fedora/linux/updates/$releasever/$basearch/
baseurl=http://archives.fedoraproject.org/pub/archive/fedora/linux/updates/$releasever/$ba
search/
#mirrorlist=https://mirrors.fedoraproject.org/metalink?repo=updates-released-f$releasever&
arch=$basearch
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-fedora-$basearch

[updates-debuginfo]
name=Fedora $releasever - $basearch - Updates - Debug
failovermethod=priority
#baseurl=http://download.fedoraproject.org/pub/fedora/linux/updates/$releasever/$basearch/
debug/
baseurl=http://archives.fedoraproject.org/pub/archive/fedora/linux/updates/$releasever/$ba
search/debug/
#mirrorlist=https://mirrors.fedoraproject.org/metalink?repo=updates-released-debug-f$relea
sever&arch=$basearch
enabled=0
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-fedora-$basearch

[updates-source]
name=Fedora $releasever - Updates Source
failovermethod=priority
#baseurl=http://download.fedoraproject.org/pub/fedora/linux/updates/$releasever/SRPMS/
baseurl=http://archives.fedoraproject.org/pub/archive/fedora/linux/updates/$releasever/SRP
MS/
#mirrorlist=https://mirrors.fedoraproject.org/metalink?repo=updates-released-source-f$rele
asever&arch=$basearch
enabled=0
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-fedora-$basearch
```

Step 3   Update /etc/yum.repos.d/fedora-updates-testing.repo

```
[updates-testing]
name=Fedora $releasever - $basearch - Test Updates
failovermethod=priority
#baseurl=http://download.fedoraproject.org/pub/fedora/linux/updates/testing/$releasever/$b
asearch/
baseurl=http://archives.fedoraproject.org/pub/archive/fedora/linux/updates/testing/$releas
ever/$basearch/
#mirrorlist=https://mirrors.fedoraproject.org/metalink?repo=updates-testing-f$releasever&a
rch=$basearch
enabled=0
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-fedora-$basearch

[updates-testing-debuginfo]
name=Fedora $releasever - $basearch - Test Updates Debug
failovermethod=priority
#baseurl=http://download.fedoraproject.org/pub/fedora/linux/updates/testing/$releasever/$b
asearch/debug/
baseurl=http://archives.fedoraproject.org/pub/archive/fedora/linux/updates/testing/$releas
ever/$basearch/debug/
```

```
#mirrorlist=https://mirrors.fedoraproject.org/metalink?repo=updates-testing-debug-f$releas
ever&arch=$basearch
enabled=0
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-fedora-$basearch

[updates-testing-source]
name=Fedora $releasever - Test Updates Source
failovermethod=priority
#baseurl=http://download.fedoraproject.org/pub/fedora/linux/updates/testing/$releasever/SR
PMS/
baseurl=http://archives.fedoraproject.org/pub/archive/fedora/linux/updates/testing/$releas
ever/SRPMS/
#mirrorlist=https://mirrors.fedoraproject.org/metalink?repo=updates-testing-source-f$relea
sever&arch=$basearch
enabled=0
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-fedora-$basearch
```

Step 4   Execute the **yum makecache** command in the terminal as root.

Installing the GUI, Associated Software Components, and Images

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   Download the latest release of the Cisco Edge 300 series Operation System from the official website. The file name of the package is edge300k9-1.3.0.tar

Step 2   Copy the package to the server that you want to set up the GUI on.

Step 3   Switch to the super user (root) by entering the **su** Linux command and enter your root password.

Step 4   Change the directory to the one that contains the release package, edge300k9-1.3.0.tar.

Step 5   Extract the package by entering **tar xvf edge300k9-13.0.tar** and obtain SMI_UI_release-1.3.tar.gz.

Step 6   Extract the SMI_UI_release-1.3.tar.gz by entering **tar zxvf SMI_UI_release-1.3.tar.gz**.

Step 7   Change your directory to SMI_GUI by entering the **cd SMI_GUI** Linux command.

Step 8   Make sure that the system is connected to the Internet. Run ./installUI.sh. The GUI is installed in the /var/www/html/smartinstall directory on the server.

Step 9   When you see "Do you want to reboot the system now to finish the installation", press **Enter** to reboot the system.

Step 10   Verify that you can open the GUI by opening a browser (make sure that Javascript is enabled) and then entering https://*ip-address*/smartinstall, in which *ip-address* is the IP address of the server.

After you run the installUI.sh script, the TFTP and HTTP server packages are automatically added from the Internet. You then can move the images that have a suffix of delivery.tar.gz in edge300k9-1.3.0.tar to the TFTP server by the following commands:

```
mv os-sunbird-1.3-delivery.tar.gz /opt/Tftproot/image/OS/
mv fm-os-sunbird-1.3-delivery.tar.gz /opt/Tftproot/image/FM_OS
```

```
mv fonts-sunbird-1.3-delivery.tar.gz /opt/Tftproot/image/Fonts
mv 3rd-app-sunbird-1.3-delivery.tar.gz /opt/Tftproot/image/Partner
```

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 **https://***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 2-13).

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 if the selected language is Simplified Chinese or traditional Chinese.

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,| 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 running the reset.sh file in the Smart Install root directory.

Managing Image Servers (Optional)

- 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 2-15.

- **Clone**—Adds an image server in fast mode if there is any existing image server added to the GUI. For more information, see the "Cloning, Modifying, and Deleting Image Servers" section on page 2-15.

- **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 2-16.

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 with the suffix "IBDconf". 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 2-21). 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   (Optional) 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 image server 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 2-20.

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 Add a Cisco Edge page. You can continue to add another Cisco Edge, or click **Back** to 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 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 2-21). 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 2-17), 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 2-17 and the "Adding Members to a Switch Group" section on page 2-20.

> **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.
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.

	Command	Purpose
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 a 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.

	Command	Purpose
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 the **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 exported on the NFS server.
Cisco Edge Path	Enter the path to be mounted on the Cisco Edge 300 switch.
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. If you have more than one interface on the GUI server, the GUI IP address field is displayed and you must choose an IP that is connected to the Smart Install network.

Step 6   Click the **Apply** or the **Apply and reboot** 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

Note   You must configure the Cisco Edge Group first and then configure the Cisco Edge because the Cisco Edge configuration has a higher priority than the Cisco Edge group configuration. The group-device association files are generated only when you click the **Apply** or **Apply and reboot** button in the group configuration page.

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 exported on the NFS server.
Cisco Edge Path	Enter the path to be mounted on the Cisco Edge.
Status	Choose ON or OFF.

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

Step 5   Click the **Apply** or **Apply and reboot** button.

Note   When you click the Apply button, the configuration file is saved to the TFTP server. 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, "Configuring Local CLI - Clish."

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 2-34). For information about CLI commands, see Chapter 4, "Configuring Local CLI - Clish."

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 2-34).

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 2-25.

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.

CLI Configuration Mode in the Smart Install Server

You can switch to CLI mode to create a Cisco Edge configuration file on the GUI.

The GUI can generate the configuration file. Do not edit the file directly unless you are an expert on the CLI configuration.

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.

Configuration Guidelines

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

Follow these configuration guidelines:

- Click the button on the web GUI to enter the CLI edit mode.

- 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.

This file is generated by the smart install server, and dispatches to different Edge switches, and every switch only executes the **system identifier default** configuration and its own **mac address system identifier** configuration.

```
configure terminal
system identifier default
done
system identifier 1111.1111.1211
   hostname switch333
   mac address-table aging-time 3825
   mac address-table static 1111.1111.1111 vlan 1 interface fe1 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 vlan 1 interface cpu 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
       short-slot on
       packet aggregation on
   exit
done
exit
```

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.

> **Note** Users have to apply the group configuration, and reboot the Cisco Edge 300 Series switches manually for the first time in order to monitor the switches. After that, the switches can get the IP of the GUI server, and report the status of their own to the GUI server.

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.

System

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.

Ethernet 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.

Configuring Local CLI - Clish

- Configuration Guidelines
- Relationship Between Local Configuration and Smart Install Configuration
- Switch Command Reference

Configuration Guidelines

You can configure the Cisco Edge 300 series switch in Clish, which is used for the local CLI configuration. 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

Follow these configuration guidelines:

- Enter **ssh root**@*ip-address* in the command prompt in your PC, and enter the password after the welcome screen is displayed. Enter the **clish** command to enter the Global Configuration mode.
- Start a Cisco Edge configuration with the **configure terminal** global command. End the Cisco Edge configuration file with the **exit** global command.
- Within a Cisco Edge configuration, start each individual switch configuration with the **system identifier local** system configuration command. End each individual switch configuration with the **done** system configuration command.

Note　Use the **system identifier local** command for a local CLI configuration.

- 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
```

Relationship Between Local Configuration and Smart Install Configuration

The local configuration and Smart Install (SMI) both have a configuration file on the Cisco Edge 300 series switch. The local configuration and SMI also both have scripts to execute configuration files on the Cisco Edge 300 series switch, and there is an execution flag that decides which script to run. By default, the flag is SMI.

If **show running-configuration** is configured on the Cisco Edge 300 series switch, it will display the running configuration, and also display the source file that the running configuration is derived from. The **next-reboot** command specifies the configuration file to run next after the reboot. For example, if the **next reboot local** command is configured, the configuration file will be changed to the local configuration.

In release 1.1 and earlier, the Cisco Edge 300 series switch checks the flag when the system reboots. If the flag points to a local configuration file, then the system changes the flag back to SMI for the next reboot to make sure that the SMI works.

In release 1.2 and later, the Cisco Edge 300 series switch treats local configuration in two different ways based on the network status:

– If the Cisco Edge 300 series switch is connected to a SMI network and it is configured to apply SMI configuration, SMI configuration will always be applied instead of local configuration.

– If the Cisco Edge 300 series switch is connected to a non-smart install environment, it will supports remain local configuration in nand flash for every reboot if smi-environment is not setup for this particular box, you can do local configuration on it by the methods described in this chapter and then enter the following two commands to make sure that the Cisco Edge 300 series switch reboots from local configuration startup-config file next time, otherwise, all the configuration will be stored in RAM and will get lost after the reboot.

```
> copy running-config startup-config(local)
> next-reboot local
```

Figure 4-1 shows the logic sequence for the local configuration and the SMI configuration.

Figure 4-1   *Logic Sequence for the Local Configuration and the SMI Configuration*
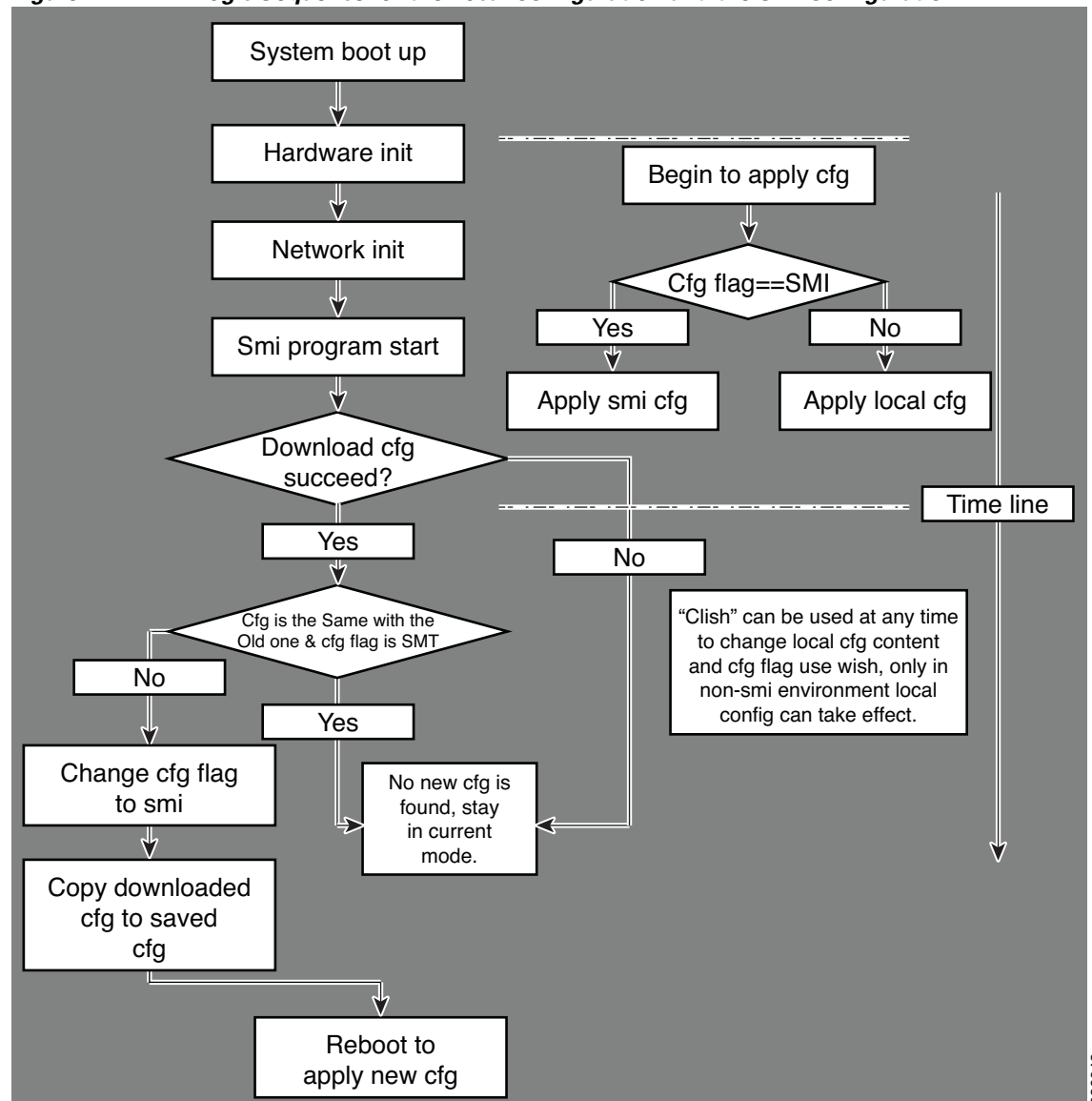
Switch Command Reference

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

- Enable Mode
- System Configuration Mode
- Ethernet Interface Configuration Mode
- WiFi Interface Configuration Mode
- SSID Configuration Mode
- Show Commands

Enable Mode

Table 4-1   Global Configuration Commands

Command	Function
configure terminal	Starts the Cisco Edge configuration file, and enters global configuration mode.
copy running-config startup-config	Saves the running configuration as the startup configuration file.
exit	Exits global configuration mode.
export-config	Exports a configuration file.
import-config	Imports a configuration file.
next-reboot	Selects next-reboot mode.
reboot	Halts and performs a cold restart.
remove	Removes local startup configuration.
show	Shows running system information.
wifi-mode	Sets the WiFi mode in the next reboot.

configure terminal

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

configure terminal

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

copy running-config startup-config

To save the running configuration as the startup configuration file, use the **copy running-config startup-config** command in the global configuration mode.

copy running-config startup-config

Command Modes   Global configuration mode

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.

export-config

To export a configuration file to the USB storage or a local directory, use the **export-config** command in the global configuration mode.

export-config type *type* **to** *destination*

Syntax Description	*type*	The export type used to export the configuration file:
		• overall—Copies the startup config, mode file, and the WiFi client network configuration files together.
		• wifi-network-only—Copies the startup config and WiFi client network configuration files together.
		• startup-config—Copies the mode file and startup config local configuration files together.
	destination	The destination that you want to export the configuration file. The destination can be either USB or a local directory.

Command Modes   Global configuration mode

Usage Guidelines   There are three types of configuration files on the Cisco Edge 300 series switch:

- Startup config—Local configurations of the Cisco Edge 300 series switch stored in /etc/startup-config.
- Mode file—The file used to mark whether the startup configuration is local or smart install, and whether the WiFi mode is AP or client.
- WiFi client network configuration—Stored in /etc/wpa_supplicant.

You can export a configuration file to either the USB storage or a local directory. If you choose to export a configuration file to the USB storage, the configuration is automatically detected, mounted, and exported to the external USB storage.

import-config

To import a configuration file from the USB storage or a local directory, use the **import-config** command in the global configuration mode.

> **import-config type** *type* **from** *source*

Syntax Description		
type	The import type that imports a configuration file from the source:	
	• overall—Copies the startup config, mode file, and the WiFi client network configuration files together.	
	• wifi-network-only—Copies the startup config and WiFi client network configuration files together.	
	• startup-config—Copies the mode file and startup config local configuration files together.	
source	The location of the configuration file that you want to import. The source can be either USB or a local directory.	

Command Modes   Global configuration mode.

Usage Guidelines   There are three types of configuration files on the Cisco Edge 300 series switch:

- Startup config—Local configurations of the Cisco Edge 300 series switch stored in /etc/startup-config.
- Mode file—The file used to mark whether the startup configuration is local or smart install, and whether the WiFi mode is AP or client.
- WiFi client network configuration—Stored in /etc/wpa_supplicant.

You can import a configuration file from either the USB storage or a local directory. If you choose to import a configuration file from the USB storage, the configuration is automatically detected, mounted, and imported from the external USB storage.

next-reboot

To select next-reboot mode, use the **next-reboot** command in the global configuration mode.

next-reboot

Command Modes   Global configuration mode

reboot

To halt and perform a cold restart, use the **reboot** command in the global configuration mode.

reboot

Command Modes   Global configuration mode

remove

To remove local startup configuration, use the **remove** command in the global configuration mode.

remove

Command Modes   Global configuration mode

show

To display running system information, use the **show** command in the global configuration mode.

show

Command Modes   Global configuration mode

wifi-mode

To set the WiFi mode of the Cisco Edge 300 series switch, use the **wifi-mode** command in the global configuration mode.

> **wifi-mode {ap | client}**

Syntax Description	ap	Sets the WiFi mode to AP after reboot.
	client	Sets the WiFi mode to client after reboot.

Usage Guidelines   This command will take effect after the reboot of the Cisco Edge 300 series switch. If you choose the AP mode, the Cisco Edge 300 will work in AP mode after reboot and only the commands that are specific to the AP mode are visible. If you choose the client mode, the Cisco Edge 300 will work in the client mode after reboot and only the commands that are specific to the client mode are visible.

wifi-mode client

To set the WiFi mode of Cisco Edge 300 series switch to client mode, use the **wifi-mode client** command in the global configuration mode.

> **wifi-mode client**

Usage Guidelines   This command will take effect after the reboot of Cisco Edge 300 series switch.

System Configuration Mode

Table 4-2   System Configuration Commands

Command	Function
agent3g	Enables or disables 3G service on the switch.
bluetooth	Enables or disables Bluetooth on the switch.
data-store	Configures the system data storage location.
desktop resolution	Configures the desktop parameter.
do	Executes user EXEC or privileged EXEC commands from global configuration mode or other configuration modes or submodes.
done	Defines the end of an individual switch configuration and returns to the global configuration mode.
exit	Exits the system configuration mode.
hostname	Configures the hostname of the switch.
hosts	Configures the IP address 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.
ip address	Configures the IP address of an interface.
ip default-gateway	Configures the default gateway.
ip name-server	Configures the DNS server.
language support	Configures the language of the switch.
locale	Configures the time zone of the switch.
login-window	Enables or disables the login window.
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.
mgrvlan	Configures the internal VLAN used by the system.
no	Removes the configuration for a command or sets the command to default.
ntp server	Configures the IP address of the NTP server that is used by the switch.
password	Sets the password.
snmp-server	Enables the Simple Network Management Protocol (SNMP) agent.
snmp-server community	Configures the community access string to permit access to the Simple Network Management Protocol (SNMP) protocol.
snmp-server contact	Configures the system contact (sysContact) string.
snmp-server group	Configures a new Simple Network Management Protocol (SNMP) group, or a table that maps SNMP users to SNMP views.
snmp-server location	Configures the system location string.

Table 4-2 ***System Configuration Commands (continued)***

Command	Function
snmp-server user	Configures a new user to an Simple Network Management Protocol (SNMP) group.
snmp-server view	Adds or updates a view entry.
snmp-server	Sets the SSID name, and enters SSID configuration mode to configure the security settings for the switch access point.
system identifier local	Enters system configuration mode to configure the local switch.
timezone	Configures the system timezone by city.
vlan	Adds a VLAN in system.
volume-ctl	Configures the volume of 3.5mm microphone or speaker.
wvlan	Configures the wireless VLAN used by the WIFI AP.

agent3g

To enable or disable 3G service on the switch, use the **agent3g** command in the system configuration mode.

agent3g {**on** | **off**}

Command Default   3G service is off.

bluetooth

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

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

Command Default   Bluetooth is off.

data-store

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

> **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 in the system configuration mode.

desktop resolution {**1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **help**}

Syntax Description

1	1280 x 960p85
2	720p
3	1024 x 768p60
4	1080p
5	720p50
6	1080p50
7	1080i
8	1080i50
9	auto-resolution
	Note If you set a resolution that is not supported, it will be automatically switched to the auto-resolution mode. We recommended that you connect the HDMI monitor before booting the system to enable this new feature.
help	Sets desktop resolution, input 1 to 9

Command Default   1024x768p60

Usage Guidelines   Changing the desktop resolution requires a reboot.

■ do

do

To execute user EXEC or privileged EXEC commands from global configuration mode or other configuration modes or submodes, use the **do** command in any configuration mode.

> **do** *command*

Syntax Description	*command* The user EXEC or privileged EXEC command to be executed.

Command Default   A user EXEC or privileged EXEC command is not executed from a configuration mode.

Command Modes   All configuration modes.

Usage Guidelines   Use this command to execute user EXEC or privileged EXEC commands (such as **show**, **clear**, and **debug** commands) while configuring your routing device. After the EXEC command is executed, the system will return to the configuration mode that you were using.

done

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

> **done**

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

hostname

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

hostname *name*

Syntax Description

name	Name that you assign to the switch.

Command Default   The default hostname is intel_ce_linux.

Usage Guidelines   Changing the hostname requires a reboot.

hosts

To configure the IP address of the switch, use the **hosts** command in the system configuration mode.

hosts *ip-address*

Syntax Description

ip-address	Identifies the IP address for the switch.

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** command in the system configuration mode.

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 4-52 lists the Ethernet interface configuration commands.

Table 4-4 on page 4-61 lists the WiFi interface configuration commands.

ip address

To set the IP address for an interface, use the **ip address** command.

ip address {*dhcp* | *ip_address*}

Syntax Description

dhcp	IP address negotiated through DHCP.
ip_address	IP address of the interface.

Command Default   The default is dhcp.

ip default-gateway

To specify the default gateway, use the **ip default-gateway** command.

ip default-gateway *ip_address*

Syntax Description	*ip_address*	IP address of default gateway.

ip name-server

To specify the DNS server, use the **ip name-server** command.

ip name-server *ip_address*

Syntax Description	*ip_address*	IP address of the DNS server.

language support

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

language support {**1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9**}

Syntax Description		
	1	English (US).
	2	Spanish (Europe).
	3	Spanish (Mexico).
	4	Simplified Chinese.
	5	Traditional Chinese (HK).
	6	Traditional Chinese (TW).
	7	Portuguese (PT).
	8	Portuguese (BR).
	9	Thai.

Command Default   The default is English (US).

Usage Guidelines   Changing the language requires a reboot.

locale

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

> **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
	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.

login-window

To enable or disable the login window, use the **login-window** command in the system configuration mode.

login-window *enable | disable*

Syntax Description

enable	Enables the login window.
disable	Disables the login window.

Command Default   The login window is enabled by default.

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** command in the system configuration mode.

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 VLANs and interfaces and set the default QoS mode, use the **mac address-table static** command in the system configuration mode.

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

Syntax Description

mac_address	Identifies the switch by its MAC address in the xxxx.xxxx.xxxx format.
vlan *vlan-id*	Specifies the vlan for the static MAC address.
interface *interface id*	(Optional) Identifies the interface or interfaces to which the static MAC address is applied. 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 for default QoS mode.
critical	(Optional) Configures the interface 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 shows how to assign the 1111.1111.1111 static MAC address to vlan 2 fe1 interfaces and sets the QoS mode to default:

```
mac address-table static 1111.1111.1111 vlan 2 interface fe1 default
```

mgrvlan

To configure the management VLAN of the switch, use the **mgrvlan** command in the system configuration mode.

mgrvlan *vlan-id*

Syntax Description

vlan-id	The VLAN ID you assigned to the switch as the management VLAN. Range is 1 to 4094.

Command Default   The default value for the *vlan-id* is 1.

■   **no**

no

To remove the configuration for a command or set the command to default, use the **no** command in the system configuration mode.

> **no**

Command Modes   System configuration

SSID configuration

ntp server

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

>**ntp server** *ip address*

Syntax Description

ip address	The IP address of the NTP server.

password

To set the root password and the student password, use **password** in the global configuration mode.

password

Command Modes   Global configuration mode

snmp-server

To enable the Simple Network Management Protocol (SNMP) agent, use the **snmp-server** command in the system configuration mode. To disable the service, use the **no** form of this command.

snmp-server

no snmp-server

Syntax Description   This command has no arguments or keywords.

Command Default   None.

snmp-server community

To configure the community access string to access the Simple Network Management Protocol (SNMP), use the **snmp-server community** in the system configuration command. To remove the specified community string, use the **no** form of this command.

snmp-server community *string* [**view** *view-name*] [**ro** | **rw**]

no snmp-server community *string*

Syntax Description

string	Community string that acts like a password and permits access to the SNMP protocol.
view	(Optional) Defines the objects available to the community.
view-name	Name of a previously defined view.
ro	(Optional) Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
rw	(Optional) Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects.

Command Default   By default, an SNMP community string permits read-only access to all objects.

snmp-server contact

To configure the system contact (sysContact) string, use the **snmp-server contact** in the system configuration mode. To remove the system contact information, use the **no** form of this command.

snmp-server contact *text*

no snmp-server contact

Syntax Description	*text*	String that describes the system contact information.

Command Default   No system contact string is set.

snmp-server group

To configure a new Simple Network Management Protocol (SNMP) group, or configure a table that maps SNMP users to SNMP views, use the **snmp-server group** in the system configuration mode. To remove a specified SNMP group, use the **no** form of this command.

snmp-server group *groupname* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *readview*] [**write** *writeview*]

no snmp-server group

Syntax Description		
groupname	The name of the group.
v1	Specifies the least secure of the possible security models.
v2c	Specifies the second least secure of the possible security models. It allows for the transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed.
v3	Specifies the most secure of the possible security models.
auth	Specifies authentication of a packet without encrypting it.
noauth	Specifies no authentication of a packet.
priv	Specifies authentication of a packet with encryption.
read	Specifies a read view.
readview	Name of the view that enables you only to view the contents of the agent. Range: 0 to 64 characters.
write	Specifies a write view.
writeview	Name of the view that enables you to enter data and configure the contents of the agent. Range: 0 to 64 characters.

Command Default   None

snmp-server location

To configure the SNMP server system location string, use the **snmp-server location** in the system configuration mode. To remove the location string, use the **no** form of this command .

snmp-server location *text*

no snmp-server location

Syntax Description

text	String that describes the system location information.

Defaults   No system location string is set.

snmp-server user

To configure a new user to an Simple Network Management Protocol (SNMP) group, use the **snmp-server user** in the system configuration mode. To remove a user from an SNMP group, use the **no** form of the command.

snmp-server user *username groupname* {**v1** | **v2c** | **v3**} **auth** {**md5** | **sha**} *auth-password* [**priv** {**des** | **aes**} *password*]

no snmp-server user

Syntax Description		
username	The name of the user connected to the agent on the host.
groupname	The name of the group associated to the user.
v1	Specifies the least secure of the possible security models.
v2c	Specifies the second least secure of the possible security models. It allows the transmission of informs and counter 64, which is twice what is normally allowed.
v3	Specifies the most secure of the possible security models.
auth	Initiates an authentication level setting session.
md5	Specifies the MD5 authentication level.
sha	Specifies the SHA authentication level.
auth-password	A string that enables the agent to receive packets from the host. Range: 8 to 64 characters.
priv	(Optional) Initiates a privacy authentication level setting session.
des	(Optional) Uses DES algorithm for encryption.
aes	(Optional) Uses AES algorithm for encryption.
password	(Optional) A string that enables the host to encrypt the contents of the message it sends to the agent. Range: 8 to 64 characters.

snmp-server view

To add or update a view entry, use the **snmp-server view** global configuration command. To remove the specified Simple Network Management Protocol server view entry, use the **no** form of this command.

snmp-server view *view-name oid-tree* {**included | excluded**}

no snmp-server view *view-name*

Syntax Description

view-name	Label for the view record that you are updating or creating. The name is used to reference the record.
oid-tree	Object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4.
included	Specifies the view as included.
excluded	Specifies the view as excluded.

Command Default   No view entry exists.

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** command in the system configuration mode.

ssid *ssid*

Syntax Description

ssid	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.

lists the SSID configuration commands.

system identifier local

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

system identifier local

Command Modes   Global configuration mode

timezone

To configure the time zone by city, use the **timezone** command in the system configuration mode.

> **timezone** *city*

Syntax Description

city	Specify the city string.

Command Default   The default timezone is UTC.

Note   Although timezone setting will take effect immediately, some applications or services may need to be restarted to reload the new timezone (for example, the rsyslog service). You are recommended to reboot the system after changing the timezone.

vlan

To add a VLAN in the system, use the **vlan** command in the system configuration mode.

vlan *vlan-id*

Syntax Description

vlan-id	VLAN ID assigned to the port. Range: 1 to 4094. Concurrent number should be less than 6.

Command Default   The default value for all ports is access mode vlan 1.

volume-ctl

To configure the volume of a 3.5 mm microphone or speaker, use the **volume-ctl** command in the system configuration mode.

volume-ctl *value*

Syntax Description	*value*	Volume value to be set to a 3.5 mm microphone or speaker. Range: 1 to 4094.

Command Default   The default value is 50.

wvlan

To configure the wireless VLAN of the switch, use the **wvlan** command in the system configuration mode.

wvlan *vlan-id*

Syntax Description

vlan-id	Wireless VLAN ID assigned to the switch.

Command Default   The default value for *vlan-id* is 1.

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.
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.
switchport mode	Configures the switchport mode of the switch.

disable

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

duplex {auto | half | full}

Syntax Description

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

Defaults   The default is automatic duplex mode sensing.

enable

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

enable {**fe1** | **fe2** | **fe3** | **fe4** | **bvi1**}

Syntax Description		
fe1	Enables the Fast Ethernet interface 1.
fe2	Enables the Fast Ethernet interface 2.
fe3	Enables the Fast Ethernet interface 3.
fe4	Enables the Fast Ethernet interface 4.
bvi1	Enables the wireless interface 1.

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** command in the Ethernet configuration mode.

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**.

priority

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

   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** command in the Ethernet interface configuration mode.

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** command in the Ethernet configuration mode.

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.

switchport mode

To configure the switchport mode of the switch, use the **switchport mode** command in the Ethernet configuration mode.

switchport mode trunk | access vlan *vlan-id*

Syntax Description	trunk	Sets the switch port mode to trunkmode with a specific VLAN.
		After you configured **switchport mode trunk,** the following three commands can be configured under the switchport mode trunk mode:
		• **native** *vlan_id*—Sets native VLAN ID.
		• **add** *vlan_id*—Adds a VLAN ID to the trunk port.
		• **remove** *vlan_id*—Removes VLAN ID from the trunk port VLAN list.
	access	Sets the switch port to access mode with a specific VLAN.
	vlan *vlan-id*	Specifies the VLAN ID.

Command Default   The default mode for switchport is access.

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.
enable	Enables the interface.
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** command in the WiFi interface configuration mode.

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

Syntax Description		
on	Enables wireless separation. Wireless clients that are connected to the same SSID are prevented from communicating with each other.	
off	Disables wireless separation. Wireless clients that are connected to the same SSID can 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** command in the WiFi interface configuration mode.

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** command in the WiFi interface configuration mode.

> **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** command in the WiFi interface configuration mode.

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** command in the WiFi interface configuration mode.

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** command in the WiFi interface configuration mode.

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** command in the WiFi interface configuration.

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** command in the WiFi interface configuration mode.

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 takes 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** command in the WiFi interface configuration mode.

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** command in the WiFi interface configuration mode.

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** command in the WiFi interface configuration mode.

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
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** command in the WiFi interface configuration mode.

> **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** command in the WiFi interface configuration mode.

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

Syntax Description	**0**	Specifies that the mode is disabled.
	1	Specifies CCK (802.11b).
	2	Specifies OFDM (802.11g).
	3	Specifies 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** command in the WiFi interface configuration mode.

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** command in the WiFi interface configuration mode.

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

Syntax Description

on	Enables packet aggregation.
off	Disables packet aggregation.

Command Default   Packet aggregation is off.

Usage Guidelines   Enable packet aggregation if network traffic consists primarily of data.

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

■ **radio**

radio

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

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

Syntax Description

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

Command Default   The wireless radio is disabled.

Usage Guidelines   If you do not intend to use the access point, turn off the radio. If you want to use the AP function, make sure to turn on 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** command in the WiFi interface configuration mode.

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** command in the WiFi interface configuration mode.

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** command in the WiFi interface configuration mode.

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** command in the WiFi interface configuration mode.

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** command in the WiFi interface configuration mode.

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** command in the WiFi interface configuration mode.

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** command in the WiFi interface configuration mode.

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.

■   **wmm**

SSID Configuration Mode

To enter SSID mode, perform the following steps:

```
configure terminal
system identifier local
ssid test
```

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, Wi-Fi Protected Access (WPA), WPA1WPA2, WPA2, WPA2PSK, WPAPSK, WPAPSKWPA2PSK authentication and associated encryption for the access point.
encryption mode (WPA configuration)	
exit	Exits SSID configuration mode.
no	Removes the configuration for a command or sets the command to default.
radius-server	Configures the name of a RADIUS server.

Note   Configuration for SSID will take effect after exiting the SSID configuring mode.

broadcast ssid

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

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** command in the SSID configuration mode.

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 shows how to configure 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** command in the SSID configuration mode.

> **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 shows how to configure 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-
```

encryption mode (802.1x)

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

Note The encryption mode (802.1x) should be used in combination with RADIUS server.

encryption mode {**wpa** | **wpa2** | **wpa1wpa2**} **type** {**tkip** | **aes** | **tkipaes**}

Syntax Description

wpa	Configures WPA with 802.1x authentication.
wpa2	Configures WPA2 with 802.1x authentication.
wpa1wpa2	Configures combined WPA and WPA2 with 802.1x authentication.
tkip	Configures Temporal Key Integrity Protocol (TKIP) encryption.
aes	Configures Advanced Encryption Standard (AES) encryption.
tkipaes	Configures combined TKIP and AES encryption.

Command Default The default mode is wpa2psk access, tkipaes encryption, and the password is Cisco123.

Examples This example shows how to configure combined WPA and WPA2 authentication with combined TKIP and AES encryption, using 802.1x authentication method:

```
encryption mode wpa1wpa2 type tkipaes
```

radius-server

To configure the related information of a radius-server, use the **radius-server** in the SSID configuration mode.

> **radius-server host** *hostname* [**auth-port** *port_number*] [**key** *secret*]

Syntax Description

hostname	The IP address of the radius server.
auth-port	Specifies the authentication port number of the radius server.
port_number	The authentication port number of the radius server.
key	Specifies the password of the authentication service on the radius server.
secret	The password of the authentication service on radius server.

Command Default

The default value for *port_number* is 1812.

The default value for *secret* is NULL.

Examples

This example shows how to configure the related information of a radius-server:

```
radius-server host 192.168.1.1 auth-port 1812 key pass1234
```

Show Commands

You can use the following **show** commands in the global configuration mode to display the configuration on the Cisco Edge 300 series switch:

- **show 3rd-party-software-version**: Displays the third-party software version.

- **show bluetooth**: Displays the bluetooth status.

- **show channel**: Displays the AP wireless channel setting.

- **show cisco-software-version**: Displays the Cisco software version.

- **show cpu**: Displays the CPU.

- **show desktop-resolution**: Displays the desktop resolution information.

- **show dhcp**: Displays the DHCP information.

- **show disk**: Displays the disk usage.

- **show dns**: Displays the DNS information.

- **show factory-mode-os-version**: Displays the Factoy-Mode OS version.

- **show hdmi-display-info**: Displays the current connected HDMI sink information.

- **show hostname**: Displays the hostname.

- **show interfaces**: Displays the interface status and configuration.

- **show ip**: Displays the IP information.

- **show mac**: Displays the MAC table information.

- **show memory**: Displays the memory usage.

- **show nfs**: Displays NFS mount status.

- **show os-version**: Displays the Normal-Mode OS version.

- **show port-statistics**: Displays the switch port statistics.

- **show port-status**: Displays the switch port status.

- **show qos**: Displays the current QoS configuration.

- **show running-config**: Displays the current operating configuration.

- **show snmp**: Displays the status of SNMP communications.

- **show snmp group**: Displays the names of groups on the router, the security model, the status of the different views, and the storage type of each group.

- **show snmp user**: Displays the information on each Simple Network Management Protocol (SNMP) username in the group username table.

- **show snmp view**: Displays the family name, storage type, status of a Simple Network Management Protocol (SNMP) configuration and associated MIB.

- **show ssid**: Displays the AP wireless ssid setting.

- **show startup-config**: Displays the contents of startup configuration.

- **show USB**: Displays the USB device information.

- **show vlan**: Displays the VLAN configuration.

- **show vstack config**: Displays the Smart Install VLAN configuration.

- **show wifi-client-status**: Displays the WiFi client status (for WiFi client mode only).

- **show wireless-clients**: Displays the AP wireless wireless-clients associated.

- **show wireless-clients-number**: Displays the associated wireless clients number.

- **show wireless-mode**: Displays the AP wireless wireless-mode setting.

■ **radius-server**

CHAPTER 5

Configuring the Web GUI

The web-based GUI is used to configure the Cisco Edge 300 series switch and monitor the status locally or remotely. The implementation of the web GUI configuration causes no conflict between the Smart Install configuration and local configuration.

In an Smart Install (SMI) environment, the web GUI only monitors the configuration status. The configurations are retrieved from the running-config file of SMI. In a non-SMI environment, you can configure and monitor the Cisco Edge 300 through the web GUI. The web GUI then generates a Clish configuration file for the local Clish to execute. The local Clish records the configurations that have been done and provides feedback to the web GUI.

To configure the Cisco Edge 300 series switch using the web-based GUI, follow these steps:

- Login, page 5-2
- Welcome, page 5-3
- Basic Configuration, page 5-3
- WiFi AP Configuration, page 5-8
- VLAN Configuration, page 5-9
- Ethernet Configuration, page 5-10
- Monitoring the Status, page 5-10

Login

You can access the web-based GUI at **https://**[*Cisco Edge 300's IP address*] and log in to the web portal locally or remotely by entering the password of **root**.

Figure 5-1   Login Page
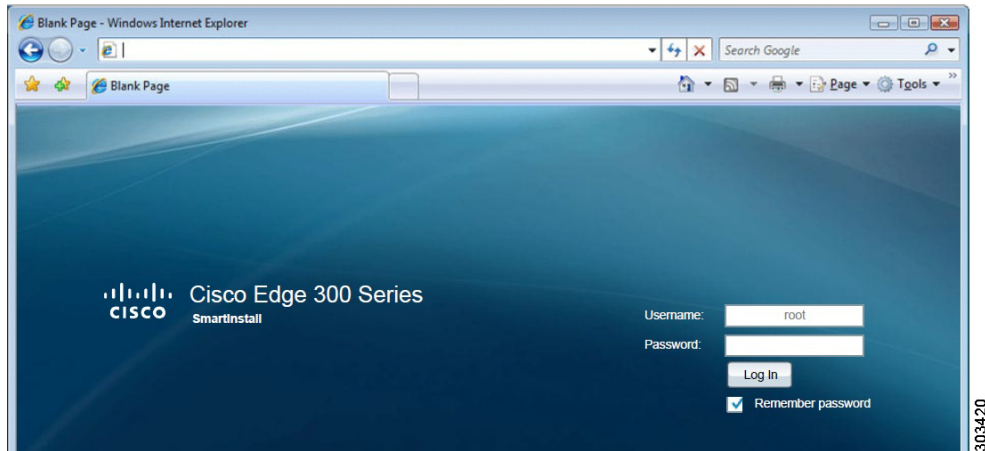
Choose the **Remember password** option so that the next time you visit the website, you can directly enter the relevant page.

Note   If you access the web GUI by Internet Explorer and enable the remember password function, make sure that the date and time on the Cisco Edge 300 series switch is correct. The stored cookies are used for future authentication. If the date and time of Cisco Edge 300 is not correct, the authentication fails and the remember password function does not take effect.

Welcome

After you log in to the web GUI, you will see the Welcome page.

Figure 5-2   *Welcome Page*
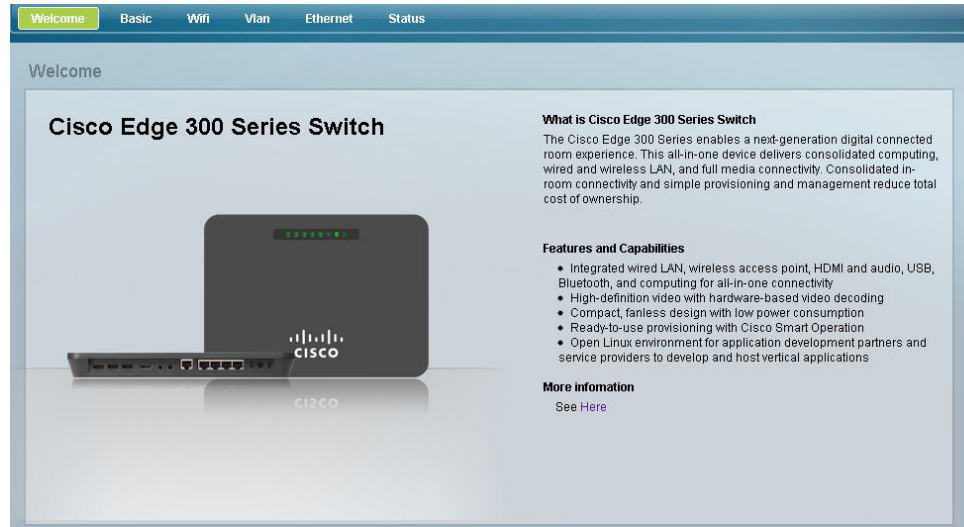
The Welcome page shows the brief introduction of the Cisco Edge 300 Series switches and their features and capabilities.

Basic Configuration

In the Basic tab, you can configure the basic information of Cisco Edge 300 series switch, import and export a configuration file, and configure IP addresses. The Basic tab consists of the following three sections:

- Basic Information
- Importing and Exporting a Configuration File
- IP Configuration

Basic Information

You can configure host name, login GUI, resolution, WiFi mode, bluetooth, language, timezone, NTP server, and log size in the basic information section.

Figure 5-3   Basic Information Configuration

When the Cisco Edge 300 series switch is in WiFi AP mode, click the **Switch to Client Mode** button to switch to WiFi client mode. If it is in the WiFi client mode, click the **Switch to AP mode** button to switch to the AP mode.

The language options in the language drop-down list are associated with the following values of the **language support** Clish command:

- 1=en_US.utf8, English (US)
- 3=es_MX.utf8, Spanish (Mexico)
- 4=zh_CN.utf8, Simplified Chinese
- 6=zh_TW.utf8, Traditional Chinese (TW)
- 7=pt_PT.utf, Portuguese (PT)
- 9=th_TH.utf8, Thai

When the modifications for resolution, hostname or language are applied, or a configuration file is imported, the switch needs to be rebooted. An indication in red will appear next to the item that you have changed, as shown in Figure 5-4.

Figure 5-4   Reboot Indication of Basic Information Changes

Although timezone settings will take effect immediately, some applications or services may need to be restarted to reload the new timezone (for example, the rsyslog service). You are recommended to reboot the system after changing the timezone.

When you click the **Apply** button on the bottom right of the Basic tab, a prompt window is displayed so that you can choose if you want to reboot the switch right now.

For other fields, clicking the **Apply** button applies the changes to the switch directly. A prompt message of "Changes apply successfully" is displayed to confirm the changes.

> **Note**   Clicking **Restore** resets all the fields on the Basic tab to factory default values.

Importing and Exporting a Configuration File

There are three types of configuration files on the Cisco Edge 300 series switch:

- Startup config—Local configurations of the Cisco Edge 300 series switch stored in /etc/startup-config.
- Mode file—The file used to mark whether the startup config is local or smartinstall, and whether the WiFi mode is ap or client.
- WiFi client network configuration—Stored in /etc/wpa_supplicant.

You can import or export a configuration file for the Cisco Edge 300 series switch in the Basic tab.

Figure 5-5   Import and Export

Importing a Configuration File

You can import a configuration file from either the USB storage or a local directory. If you choose to import a configuration file from the USB storage, the configuration is automatically detected, mounted, and imported from the external USB storage.

Note   An imported startup config or overall configuration needs a reboot to take effect. An imported wifi client network configuration will take effect immediately if the Cisco Edge 300 series switch is in wifi client mode.

To import a configuration file, follow these steps:

Step 1   Choose one of the following import types:

- overall—Copies all the three configuration files together.
- wifi-network-only—Copies the startup config and WiFi client network configuration.
- startup-config—Copies the mode file and startup config local together.

Step 2   Enter the path of the configuration file in the Import Path field.

Step 3   Click **Import** to import the configuration file.

Note   If you click the **Import** button while the Import Path is empty, a warning message is displayed.

Exporting a Configuration File

You can export a configuration file to either the USB storage or a local directory. If you choose to export a configuration file to the USB storage, the configuration is automatically detected, mounted, and exported to the external USB storage.

To export a configuration file, follow these steps:

Step 1   Choose one of the following export types:

- overall—Copies all the three configuration files together.
- wifi-network-only—Copies the startup config and WiFi client network configuration.

• startup-config—Copies the mode file and startup config local together.

Step 2   Enter the destination that you want to export the configuration file in the **Export Path** field.

Step 3   Click the **Export** button to export the configuration file.

> **Note**   If you click the **Export** button while the **Export Path** field is empty, a warning message is
> displayed.

IP Configuration

You can choose DHCP or static mode in the IP Configuration section of the Basic tab. By default, the
Cisco Edge300 series switch uses DHCP to obtain IP address.

Figure 5-6   IP Configuration

> **Note**   If you choose DHCP as the IPv4 connection type, the IPv4 address, IPv4 netmask, and IPv4 default
> gateway fields are disabled and greyed out. Only the DNS server can be configured for DHCP mode.

Configuring Static IP Address

To configure the static IP address, follow these steps:

Step 1   From the IPv4 connection type drop-down list, choose **Static**.

Step 2   Enter IPv4 address, IPv4 netmask, and IPv4 default gateway.

> **Note**   A warning message is displayed if the value entered is invalid.

Step 3   Enter DNS server information.

Step 4   Click **Apply** to apply the changes.

> **Note**   Clicking Restore resets all the fields in the Basic tab to factory default values.

Note If you change the IP address of Cisco Edge 300 series switch by using the web GUI, you need to enter the new IP address in the address box of the browser. Otherwise, the configuration and monitoring feature will be unavailable because the original IP address no longer exists.

WiFi AP Configuration

You can configure SSID name, radio, broadcast SSID, wireless mode, channel number, channel allocation, channel bandwidth, transmit power, MCS, Multicast-MCS, IGMP snoop, and security in the WiFi tab.

Note The Wifi AP configuration can only be visible when the Cisco Edge 300 series switch is in AP mode.

Figure 5-7 shows the WiFi tab.

Figure 5-7   WiFi AP Configuration

VLAN Configuration

You can click the gear icon on the right of the Vlan column to add or remove VLANs. You can also choose a port type of Gi1, fe1, fe2, fe3, and fe4 in the Mode field. When the port type is trunk, you can choose a native VLAN in the select list on the right of the table.

Figure 5-8 shows the Vlan tab.

Figure 5-8   Vlan Configuration

It is recommended that you keep **Use untagged cpu vlan in gi1** checked, otherwise, the system may lose network connection due to wrong configuration.

Note   When the Cisco Edge 300 series switch is in Wifi client mode, CPU and Wifi interface are invisible.

Ethernet Configuration

You can configure the status (for downlink), output-queue-strategy, pause (for downlink), priority, rate-limit, speed, duplex, enable, and disable in the Ethernet tab.

Figure 5-9   Ethernet Configuration
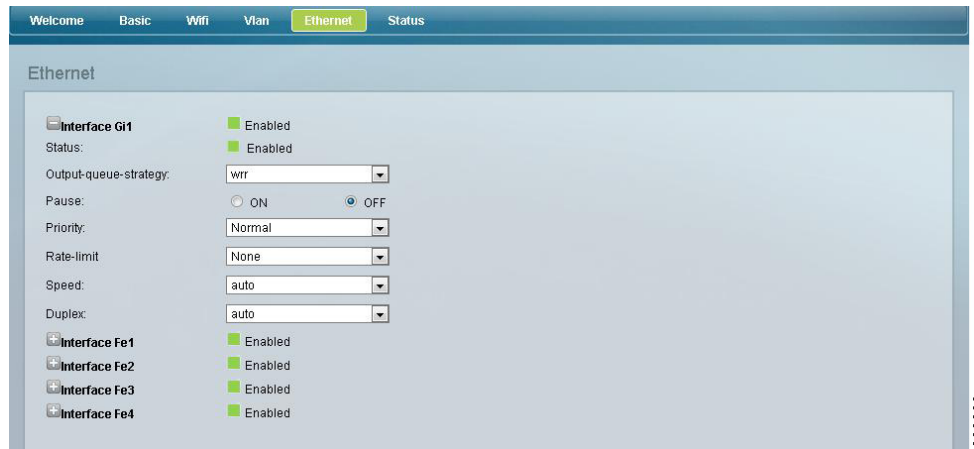
Monitoring the Status

You can monitor the status of system, version, network, WiFi, Ethernet port, other devices, logs, system status, and Ethernet/Wifi/Bluetooth/USB status in the Status tab. (See Figure 5-10, Figure 5-11, and Figure 5-12.)

Figure 5-10   Monitoring the Status–System, Version Information, and Network

Figure 5-11   *Monitoring the Status–Wifi, Ethernet Port, and Other Devices*

Figure 5-12   *Monitoring the Status–Logs*
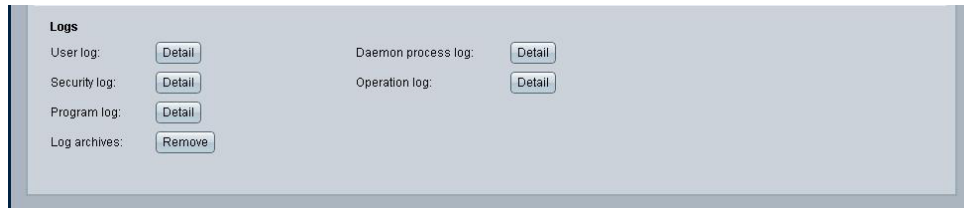
Configuring HTTP API

You can run an application either locally or remotely on the Cisco Edge 300 series switch to manage the switch by using HTTP API. Management of the switch consists of configuring the switch, monitoring the status, and installing and upgrading software.

The configuration of HTTP API for the Cisco Edge 300 series switch is supported from Release 1.5. This chapter explains each HTTP API including requests, replies, parameter restrictions, and error codes.

Note Curl is used as a sample tool to request APIs. 10.140.44.134 is used as a sample IP address of the Cisco Edge 300 series switch, and cisco123! is used as a sample admin password.

To configure the Cisco Edge 300 series switch by using HTTP API, see the following sections:

System API

Use the commands in this section to configure the system API.

Note   Curl is used as a sample tool to request APIs. 10.140.44.134 is used as a sample IP address of the Cisco Edge 300 series switch, and cisco123! is used as a sample admin password.

Set Hostname

Example: set hostname to cisco

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"hostname" : "cisco"}' https://10.140.44.134/api/1.0/sys/hostname
```

Reply

```
{"success":"true","updatedAt":"2012-11-06 17:39:47"}
```

Parameter restrictions

The length of hostname should be 1 to 64 and the valid parameter set is {a-zA-Z0-9-_}, or 004 error is reported.

Get Hostname

Example: get hostname

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/sys/hostname
```

Reply

```
{"hostname":"cisco","success":"true","getAt":"2012-11-06 17:44:37"}
```

Set Log Size

Example: set log size to 20 MB

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"size":"20"}'https://10.140.44.134/api/1.0/sys/log/size
```

Reply

```
{"success":"true","updatedAt":"2012-11-06 17:39:47"}
```

Parameter restrictions

The log size parameter should be an integer, in the range from 1 to 100, or 004 error is reported.

Get Log Size

Example: get log size

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/sys/log/size
```

Reply

```
{"size":"20","success":"true","getAt":"2011-04-21 04:33:55"}
```

Delete Logs

Example: delete all logs

Request

```
curl -k -X DELETE -H 'password: cisco123!' https://10.140.44.134/api/1.0/sys/log
```

Reply

```
{"success":"true","updatedAt":"2012-12-27 08:24:08"}
```

Set Account

Example: change the password of admin account from cisco123! to cisco123

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"account"
: "cisco123"}' https://10.140.44.134/api/1.0/sys/account
```

Reply

```
{"success":"true","updatedAt":"2012-11-06 17:48:06"}
```

Parameter restrictions

The password cannot be empty and the valid parameter set is {a-zA-Z0-9~!@#$%^&*+=-_}, otherwise 004 error is reported. The password should follow the busy box linux password requirement, otherwise 005 error is reported.

Get Account

003 error is reported if violated.

Set LoginGui

Example: set loginGui to enable

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"loginGui" : "enable"}' https://10.140.44.134/api/1.0/sys/loginGui
```

Reply

```
{"success":"true","updatedAt":"2012-11-06 17:39:47"}
```

Parameter restrictions

Valid strings for loginGui: enable and disable. Otherwise, 004 error is reported.

Get LoginGui

Example: get login gui

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/sys/loginGui
```

Reply

```
{"loginGui":"enable","success":"true","getAt":"2012-11-06 19:17:41"}
```

Set Resolution

Example: set resolution to 1080p

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"resolution" : "4"}' https://10.140.44.134/api/1.0/sys/resolution
```

Reply

```
{"success":"true","updatedAt":"2012-11-06 17:39:47"}
```

Parameter restrictions

The valid parameter set is number 1–9. Otherwise, 004 error is reported.

Get Resolution

Example: get resolution

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/sys/resolution
```

Reply

```
{"resolution":"9","success":"true","getAt":"2012-12-14 08:55:27"}
```

Get Hdmi Info

Example: get hdmi information

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/sys/hdmi
```

Reply

```
{"hdmi":" - Manufacturer ID: 0x294d\n - Product code : 0x9135\n - Sink name : HDMI TV\n -
Sink size (WxH) : 80 x 45\nCurrent working mode:\n 1920x1080p@59.94\nSupported modes:\n -
720x480p60 \n - 1024x768p60 \n - 1920x1080p60 \n - 1280x720p60 \n - 1920x1080p50 \n -
1280x720p50 \n - 1280x960p85 \n - 720x480p59.94 \n - 1024x768p59.94 \n - 1920x1080p59.94
\n - 1280x720p59.94 \n\n","success":"true","getAt":"2012-12-14 08:41:33"}
```

Set Bluetooth

Example: set bluetooth to on

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"bluetooth" : "on"}' https://10.140.44.134/api/1.0/sys/bluetooth
```

Reply

```
{"success":"true","updatedAt":"2012-11-06 17:39:47"}
```

Parameter restrictions

The valid parameter is on/off. Otherwise, 004 error is reported.

Get Bluetooth

Example: get bluetooth

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/sys/bluetooth
```

Reply

```
{"bluetooth":"on","success":"true","getAt":"2012-11-06 19:43:08"}
```

Set Language

Example: set language to 1

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"language" : "1"}' https://10.140.44.134/api/1.0/sys/language
```

Reply

```
{"success":"true","updatedAt":"2012-11-06 19:49:21"}
```

Parameter restrictions

The valid parameter set is number 1-9. Otherwise, 004 error is reported.

Get Language

Example: get language

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/sys/language
```

Reply

```
{"language":"1","success":"true","getAt":"2012-11-06 19:49:24"}
```

Set Locale

Example: set locale to ì8î

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"locale"
: "8"}' https://10.140.44.134/api/1.0/sys/locale
```

Reply

```
{"success":"true","updatedAt":"2012-11-06 19:49:21"}
```

Parameter restrictions

The valid parameter set is number 0-26. Otherwise, 004 error is reported.

Get Locale

Example: get locale

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/sys/locale
```

Reply

```
{"locale":"9","success":"true","getAt":"2012-11-06 20:13:31"}
```

Set ntpServer

Example: set NTP server to 202.120.2.101

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"ntpServer" : "ntp.sjtu.edu.cn"}' https://10.140.44.134/api/1.0/sys/ntpServer
```

Reply

```
{"success":"true","updatedAt":"2012-11-06 19:49:21"}
```

Parameter restrictions

The parameter should be a valid IPv4 address or a valid domain name.

Get ntpServer

Example: get ntPServer

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/sys/ntpServer
```

Reply

```
{"ntpServer":"ntp.sjtu.edu.cn","success":"true","getAt":"2012-12-27 08:04:34"}
```

Set Time

Example: set time

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"time" :
"2012-11-06 17:20:20"}' https://10.140.44.134/api/1.0/sys/time
```

Reply

```
{"success":"true","updatedAt":"2012-11-06 19:49:21"}
```

Parameter restrictions

The parameter should be in YYYY-MM-DD HH:MM:SS format. Otherwise, 004 error is reported.

Get Time

Example: get time

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/sys/time
```

Reply

```
{"time":"2012-11-07 15:22:15","success":"true","getAt":"2012-11-07 06:22:15"}
```

Set CPU

N/A. 003 error is reported if it is requested.

Get CPU

Example: get CPU

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/sys/cpu
```

Reply

```
{"cpu":"CPU:   9% usr   0% sys   0% nic  90% idle   0% io   0% irq   0%
sirq","success":"true","getAt":"2012-11-07 06:35:06"}
```

Set Memory

N/A. 003 error is reported if it is requested.

Get Memory

Example: get memory

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/sys/memory
```

Reply

```
{"memory":"Mem: 378112K used, 1310780K free, 0K shrd, 57188K buff, 155920K
cached","success":"true","getAt":"2012-11-07 08:08:07"}
```

Set Process

N/A. 003 error is reported if it is requested.

Get Process

Example: get process

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/sys/proc
```

Reply

```
{"proc":"UID        PID  PPID  C STIME TTY          TIME CMD\nroot         1     0  0
10:57 ? 00:00:01 init      \nroot        2     0  0 10:57 ?        00:00:00
[kthreadd]\nroot 3     2  0 10:57 ?        00:00:00 [migration\/0]\nroot        4     2
0 10:57 ? 00:00:03 [ksoftirqd\/0]\nroot       5     2  0 10:57 ?        00:00:00
[events\/0]\nroot 6     2  0 10:57 ?        00:00:00 [khelper]\nroot        9     2  0
10:57 ?        00:00:00 [kstop\/0]\nroot      134     2  0 10:57 ?        00:00:00
[kblockd\/0]\nroot       136     2 0 10:57 ?        00:00:00 [kacpid]\nroot       137
2  0 10:57 ?        00:00:00 [kacpi_notify]\nroot      216     2  0 10:57 ?
00:00:00 [ata\/0]\nroot      217     2  0 10:57 ?        00:00:00 [ata_aux]\nroot
218     2  0 10:57 ?        00:00:00 [ksuspend_usbd]\nroot      224     2  0 10:57 ?
00:00:00 [khubd]\nroot      227     2  0 10:57 ?        00:00:00 [kseriod]\nroot      229
2  0 10:57 ?        00:00:00 [kgameportd]\nroot      232     2  0 10:57 ?        00:00:00
[kmmcd]\nroot       283     2  0 10:57 ?        00:00:00 [pdflush]\nroot       284     2
0 10:57 ?        00:00:00 [pdflush]\nroot      285     2  0 10:57 ?        00:00:00
[kswapd0]\nroot      326     2  0 10:57 ?        00:00:00 [aio\/0]\nroot       337     2
0 10:57 ?        00:00:00 [nfsiod]\nroot 342     2  0 10:57 ?        00:00:00
[cifsoplockd]\nroot       343     2  0 10:57 ? 00:00:00 [cifsdnotifyd]\nroot      527
2  0 10:57 ?        00:00:00 [scsi_eh_0]\nroot 529     2  0 10:57 ?        00:00:00
[scsi_eh_1]\nroot      533     2  0 10:57 ? 00:00:00 [mtdblockd]\nroot       579     2  0
```

```
10:57 ?        00:00:00 [kpsmoused]\nroot 588     2   0 10:57 ?        00:00:00
[hid_compat]\nroot         612     2   1 10:57 ? 00:06:35 [Glob_Spectra]\nroot        618
2   0 10:57 ?        00:02:18 [nandflush]\nroot 628     2   0 10:57 ?        00:00:00
[krfcommd]\nroot         631     2   0 10:57 ?        00:00:00 [rpciod\/0]\nroot         664
2   0 10:57 ?        00:00:00 [scsi_eh_2]\nroot         665     2 0 10:57 ?        00:00:00
[usb-storage]\nroot         672     2   0 10:57 ?        00:00:06 [kjournald]\nroot         935
1   0 10:57 ?        00:00:00 udevd -d\nroot         1750     2   0 10:57 ?        00:00:00
[SEC int]\nroot         1854     2   0 10:57 ?        00:00:35 [Clock_ISR]\nroot         1869
1   0 10:57 ?        00:00:00 \/bin\/cdp eth0 start\nroot 2142     1   0 10:57 ?
00:03:14 \/bin\/gdl_server blender_config 1\nroot         2211     2   0 10:57 ?
00:00:00 [VidDec_hal_pars]\nroot         2212     2   0 10:57 ?        00:00:00
[VidDec_hal_deco]\nroot         2218     2   0 10:57 ?        00:00:00 [VidPProc_ISR]\nroot
2219     2   0 10:57 ?        00:00:00 [VidPProc_IO]\nroot         2223     2   0 10:57 ?
00:00:24 [VidRend_IO]\nroot         2224     2   0 10:57 ?        00:00:00 [VidRend_IO]\nroot
2232     2   0 10:57 ?        00:01:18 [Audio_Rend_ISR]\nroot         2233     2   0 10:57 ?
00:00:27 [Audio_Timing]\nroot         2234     2   0 10:57 ?        00:00:08
[Audio_Pipe_Mgr]\nroot 2235     2   0 10:57 ?        00:00:00 [Audio_DSP0_ISR]\nroot
2236     2   0 10:57 ? 00:00:00 [Audio_DSP1_ISR]\nroot         2426     1   0 10:58 ?
00:00:00 \/bin\/konfd\nroot 2899     1   0 10:58 ?        00:00:00 php-fpm: master process
(\/usr\/local\/cisco\/php\/etc\/php-fpm.conf)\nroot         2900   2899   0 10:58 ?
00:00:02 php-fpm: pool root \nroot         2901   2899   0 10:58 ?        00:00:02 php-fpm:
pool root \nroot         2907     1   0 10:58 ?        00:00:00 nginx: master process
\/usr\/local\/cisco\/nginx\/sbin\/nginx\nroot         2908   2907   0 10:58 ?        00:00:14
nginx: worker process \nroot         2917     1   0 10:58 ?        00:00:00
\/usr\/local\/cisco\/\/sbin\/cupsd -C \/usr\/local\/cisco\/\/etc\/cups\/cupsd.conf\nroot
2920     1   0 10:58 ?        00:00:00 \/usr\/local\/cisco\/sbin\/xinetd\nroot         2930
1   0 10:58 ?        00:00:19 \/usr\/local\/cisco\/sbin\/snmpd\nroot         2934     1   0
10:58 ?        00:00:00 \/sbin\/sshd\nroot 2941     1   0 10:58 ?        00:00:16
\/usr\/local\/cisco\/sbin\/cron\nroot         2943     1   0 10:58 ?        00:00:00
\/usr\/local\/cisco\/bin\/mosaic_server 0 5050 10000\nroot         2944 1   0 10:58 ?
00:00:00 \/usr\/local\/cisco\/bin\/mosaic_server 1 5052 12000\nroot 2949     1   0 10:58 ?
00:00:00 audio_setup_outputs\nroot         2958     2   0 10:58 ? 00:00:00 [Audio_Input]\nroot
2959   2949   0 10:58 ?        00:00:00 [sh] <defunct>\nroot 2964     2   0 10:58 ?
00:00:01 [kjournald]\nroot         2966     1   0 10:58 ? 00:00:01
\/usr\/local\/cisco\/sbin\/rsyslogd -c5\n1000         2977     1   0 10:58 ? 00:00:08
dbus-daemon --system\n1001         2979     1   0 10:58 ?        00:00:00 hald
--daemon=yes\nroot         2980   2979   0 10:58 ?        00:00:00 hald-runner\nroot         2994
2980   0 10:58 ?        00:00:00 hald-addon-storage: polling \/dev\/ciscoapps (every 2
sec)\nroot 2997     1   0 10:58 ?        00:00:01 bluetoothd\nroot         3004     1   0 10:58
? 00:00:00 Agent_3g\nroot         3018     1   0 10:58 ?        00:00:00 wan_detector\nroot
3046 1   0 10:58 ?        00:00:05 slim\nroot         3089   3046   0 10:58 tty2     00:02:06
\/usr\/bin\/X -auth \/var\/run\/slim.auth\nroot         3134     1   0 10:58 ?        00:00:00
dhclient br0\nroot         3135     1   0 10:58 ?        00:00:19 \/bin\/sh
\/scripts\/status_check.sh\nroot 3209     1   0 10:59 ?        00:00:00 \/sbin\/smi\nroot
3243     2   0 10:59 ? 00:00:00 [kjournald]\nstudent     3380   3046   0 10:59 ?
00:00:00 \/bin\/sh \/etc\/xinitrc xfce4\nstudent     3392   3380   0 10:59 ?        00:00:00
\/bin\/sh \/scripts\/startxfce4\nstudent 3004   3392   0 10:59 ?        00:00:01
xfce4-session\nroot         3491     1   0 10:59 ? 00:00:00 init        \nstudent     3502     1
0 10:59 ?        00:00:00 dbus-launch --autolaunch 4b8ead68809b704d85084ca50000005c
--binary-syntax --close-stderr\nstudent     3504     1   0 10:59 ? 00:00:00
\/usr\/local\/cisco\/bin\/dbus-daemon --fork --print-pid 5 --print-address 7
--session\nstudent     3506     1   0 10:59 ?        00:00:00
\/usr\/local\/cisco\/lib\/xfce4\/xfconf\/xfconfd\nstudent     3554     1   0 10:59 ?
00:00:21 xfwm4\nstudent     3555 1   0 10:59 ?        00:00:00 xfsettingsd\nstudent     3565
1   0 10:59 ?        00:00:35 xfce4-panel\nstudent         3576     1   0 10:59 ?        00:00:00
Thunar --daemon\nstudent     3578 1   0 10:59 ?        00:00:03 xfdesktop\nstudent     3597
3004   0 10:59 ?        00:00:00 3G_Dongle\nstudent     3598   3004   0 10:59 ?        00:00:13
BlueToothUI\nstudent     3602   3565   0 10:59 ?        00:00:24
\/usr\/local\/cisco\/lib\/xfce4\/panel\/wrapper
\/usr\/local\/cisco\/lib\/xfce4\/panel\/plugins\/libsystray.so 6 16777251 systray
Notification Area Area where notification icons appear \nstudent     3621   3004   0 10:59 ?
00:00:03 wifi_status hide\nstudent     3632   3004   0 10:59 ?        00:00:12 wired_status
hide > \/dev\/null\nstudent 3635     1   0 10:59 ?        00:00:00
xfce4-settings-helper\nstudent     3679     1   0 10:59 ? 00:00:00
```

```
\/usr\/local\/cisco\/libexec\/gvfsd\nstudent   3692    1   0 10:59 ?          00:00:00
\/usr\/local\/cisco\/libexec\/gconfd-2\nstudent   3709    1   0 10:59 ?          00:00:00
\/usr\/local\/cisco\/libexec\/gvfs-hal-volume-monitor\nstudent   3717    1   0 10:59 ?
00:00:00 \/usr\/local\/cisco\/libexec\/\/gvfs-fuse-daemon
\/apps\/localconfig\/student\/.gvfs\nstudent   3730    1   0 10:59 ?          00:00:00
\/usr\/local\/cisco\/libexec\/gvfsd-trash --spawner :1.11
\/org\/gtk\/gvfs\/exec_spaw\/0\nstudent   0044    1   0 11:00 ?          00:00:00
\/usr\/local\/cisco\/lib\/scim-1.0\/scim-launcher -d -c simple -e all -f socket
--no-stay\nstudent   4068    1   0 11:00 ?          00:00:00
\/usr\/local\/cisco\/lib\/scim-1.0\/scim-helper-manager\nstudent   4069    1   0 11:00 ?
00:00:00 \/usr\/local\/cisco\/lib\/scim-1.0\/scim-panel-gtk --display :0.0 -c socket -d
--no-stay\nstudent   4071    1   0 11:00 ? 00:00:00
\/usr\/local\/cisco\/lib\/scim-1.0\/scim-launcher -d -c socket -e socket -f x11\nroot 6319
2980   0 16:40 ?          00:00:00 hald-addon-input: Listening on \/dev\/input\/event0
\/dev\/input\/event1 \/dev\/input\/event2\nroot    6510    2   0 16:41 ?          00:00:00
[Audio_Recovery]\nroot    6574    2   0 16:41 ?          00:00:00 [scsi_eh_4]\nroot
6575 2   0 16:41 ?          00:00:00 [usb-storage]\nroot    6680  2980  0 16:41 ?
00:00:00 hald-addon-storage: polling \/dev\/sdb (every 2 sec)\nroot    7088     2   0
16:41 ? 00:00:00 [kjournald]\nstudent   7938    1   0 11:04 ?          00:00:08
\/usr\/local\/cisco\/bin\/Terminal\nstudent   7997 7938  0 11:04 ?          00:00:00
gnome-pty-helper\nstudent   7998 7938 0 11:04 pts\/0   00:00:00 bash\nroot     10418
7998  0 11:40 pts\/0   00:00:00 -bash\nroot    15412  3135  0 17:23 ?          00:00:00
sleep 1\nroot    15432  2901  0 17:23 ? 00:00:00 sh -c cd
'\/usr\/local\/cisco\/nginx\/html\/api\/1.0\/sys' ; \/usr\/local\/cisco\/bin\/ps -ef
2>&1\nroot     15433 15432  0 17:23 ?          00:00:00 \/usr\/local\/cisco\/bin\/ps
-ef\n","success":"true","getAt":"2012-11-07 08:23:50"}
```

Set Storage

N/A. 003 error is reported if it is requested.

Get Storage

Example: get storage

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/sys/storage
```

Reply

```
{"storage":"Filesystem              Size    Used Available Use% Mounted
on\n\/dev\/root 1.6G     1.2G    343.1M  78% \/\ntmpfs                512.0M    428.0K
511.6M 0% \/tmp\ntmpfs                    4.0K       0     4.0K   0% \/media\ntmpfs
20.0M    228.0K   19.8M  1% \/var\n\/dev\/ciscoapps          1.8G   527.4M     1.2G
30% \/apps\n\/dev\/Glob_Spectraa1   96.6M    77.9M    13.8M  85%
\/tmp\/smi_spectraa1\ntmpfs                   32.0M    17.8M    14.2M  56%
\/tmp\/firefox_cached\n64.104.163.32:\/var\/www\/html\/api 25.6G    6.2G    18.1G  26%
\/usr\/local\/cisco\/nginx\/html\/api\n\/dev\/sdb1                7.3G    308.1M
6.7G   4% \/media\/sdb1\n","success":"true","getAt":"2012-11-07 08:35:55"}
```

Set Model

N/A. 003 error is reported if it is requested.

Get Model

Example: get model

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/sys/model
```

Reply

```
{"model":"CS-E300-AP-K9","success":"true","getAt":"2012-11-07 08:59:00"}
```

Set IP

Example: set IP address to 64.104.163.55 and netmask to 255.255.255.128

Request

```
curl -m 5 -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"type" : "static","ipv4":"64.104.163.55","netmask":"255.255.255.128"}'
https://64.104.163.47/api/1.0/sys/ip
```

Reply

```
{"success":"true","updatedAt":"2012-11-06 19:49:21"}
```

Parameter restrictions

The parameter type is static or DHCP. If static is specified in the type field, ipv4 and netmask must also be specified. IPv4 must be a valid IPv4 address. Netmask must be one of the following strings:

"255.0.0.0",

"255.128.0.0",

"255.192.0.0",

"255.224.0.0",

"255.240.0.0",

"255.248.0.0",

"255.252.0.0",

"255.254.0.0",

"255.255.0.0",

"255.255.128.0",

"255.255.192.0",

"255.255.224.0",

"255.255.240.0",

"255.255.248.0",

"255.255.252.0",

"255.255.254.0",

"255.255.255.0",

"255.255.255.128",

"255.255.255.192",

"255.255.255.224",

"255.255.255.240",

"255.255.255.248",

"255.255.255.252",

"255.255.255.254",

"255.255.255.255"

Note Since the IP address is changed after the execution, "-m 5" must be specified to make sure that the command will not be appending forever.

Get Ip Address

Example: get ip address

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/sys/ip
```

Reply

```
{"ip":"10.140.44.134","success":"true","getAt":"2012-11-08 08:48:53"}
```

Set Gateway

Example: set gateway

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"gateway":"64.104.163.1"}' https://10.140.44.134/api/1.0/sys/gateway
```

Reply

```
{"success":"true","updatedAt":"2011-04-21 05:46:07"}
```

Parameter restrictions

The gateway should be a valid IP address.

Get Gateway

Example: get gateway

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/sys/gateway
```

Reply

```
{"gateway":"64.104.163.1","success":"true","getAt":"2012-11-08 08:49:59"}
```

Set DNS

Example: set DNS to 8.8.8.8

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"dns":"8.8.8.8"}' https://10.140.44.134/api/1.0/sys/dns
```

Reply

```
{"success":"true","updatedAt":"2012-12-14 07:50:00"}
```

Parameter restrictions

DNS should be a valid IP address.

Get DNS

Example: get DNS

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/sys/dns
```

Reply

```
{"dns":"64.104.123.144 171.70.168.183 ","success":"true","getAt":"2012-11-08 08:50:37"}
```

Set Wifi Mode

Example: set WiFi mode

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"wifiMode":"client"}' https://10.140.44.134/api/1.0/sys/wifiMode
```

Reply

```
{"success":"true","updatedAt":"2012-12-14 08:11:16"}
```

Parameter restrictions

The WiFi mode should be AP or client.

Get Wifi Mode

Example: get WiFi mode

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/sys/wifiMode
```

Reply

```
{"wifiMode":"ap","success":"true","getAt":"2012-12-14 08:09:59"}
```

Set a Proxy of Chrome Browser

Example: set a proxy of chrome browser

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"proxy" :
{"host":"10.10.10.10","scheme":"http","port":"10","username":"cisco","password":"cisco"}}'
https://10.140.44.134/api/1.0/sys/proxy
```

Reply

```
{"success":"true","updatedAt":"2012-12-14 08:11:16"}
```

Parameter restrictions

host: IP address/hostname. If not specified, the proxy setting will be set to none.

scheme: http/https

port: Should be an integer within the range 0 and 65535.

username and password: Optional. Specify the account information of the proxy.

✎

Note   You must specify both username and password. If only the username is specified, both the username and password will be deleted.

Get the Proxy of Chrome Browser

Example: get the proxy of chrome browser

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.28.47/api/1.0/sys/proxy
```

Reply

```
{"proxy":"http://cisco:cisco@10.10.10.10:10","success":"true","getAt":"2011-04-21
04:04:03"}
```

Set System Information

Example: set hostname to ce300, NTP server to 202.120.2.101, and log size to 30 MB.

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"hostname":"ce300", "ntpServer" : "202.120.2.101",îlog_sizeî:î30î}'
https://10.140.44.134/api/1.0/sys
```

Reply

```
{"success":"true","updatedAt":"2012-11-06 19:49:21"}
```

Parameter restrictions

The parameter should be a valid IPv4 address.

Get System Information

Example: get all system information

Request:

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/sys
```

Reply

```
curl -k -X GET -H 'password: cisco123!'
https://10.140.44.134/api/1.0/sys{"hostname":"intel_ce_linux", "size":"30",
"ip":"10.140.44.134","gateway":"10.140.28.1","dns":"64.104.123.144
171.70.168.183","language":"1","model":"CS-E300-AP-K9","locale":"8","time":"2012-12-14
16:13:03","ntpServer":"10.81.254.202","loginGui":"disable","resolution":"9","wifiMode":"cl
ient","bluetooth":"on","memory":"Mem: 380776K used, 1308116K free, 0K shrd, 27764K buff,
170748K cached","storage":"Filesystem                Size    Used Available Use% Mounted
on\n\/dev\/root                   1.6G    1.2G   300.9M 81% \/\ntmpfs
512.0M 172.0K    511.8M   0% \/tmp\ntmpfs                  4.0K        0    4.0K
0% \/media\ntmpfs                 20.0M    88.0K   19.9M   0%
\/var\n\/dev\/ciscoapps 1.8G    539.6M    1.2G  30% \/apps\n\/dev\/Glob_Spectraa1
96.6M    84.4M     7.2M  92% \/tmp\/smi_spectraa1\ntmpfs                 32.0M
17.8M   14.2M 56% \/tmp\/firefox_cached\n10.140.28.35:\/var\/www\/html\/api
25.6G    7.2G 17.1G  30% \/usr\/local\/cisco\/nginx\/html\/api\n","cpu":"CPU:   0% usr
72% sys   0% nic  27% idle   0% io   0% irq   0% sirq","proc":"UID        PID  PPID  C
STIME TTY         TIME CMD\nroot        1    0  0 15:35 ?        00:00:01 init
\nroot        2    0  0 15:35 ? 00:00:00 [kthreadd]\nroot        3    2  0 15:35 ?
00:00:00 [migration\/0]\nroot 4    2  0 15:35 ?        00:00:00 [ksoftirqd\/0]\nroot
5    2  0 15:35 ? 00:00:00 [events\/0]\nroot        6    2  0 15:35 ?        00:00:00
[khelper]\nroot        9 2  0 15:35 ?        00:00:00 [kstop\/0]\nroot      134    2  0
15:35 ?        00:00:00 [kblockd\/0]\nroot      136    2  0 15:35 ?        00:00:00
[kacpid]\nroot      137    2  0 15:35 ?        00:00:00 [kacpi_notify]\nroot      216
2  0 15:35 ?        00:00:00 [ata\/0]\nroot      217    2  0 15:35 ?        00:00:00
[ata_aux]\nroot      218    2  0 15:35 ? 00:00:00 [ksuspend_usbd]\nroot      224    2
0 15:35 ?        00:00:00 [khubd]\nroot 227    2  0 15:35 ?        00:00:00
[kseriod]\nroot      229    2  0 15:35 ? 00:00:00 [kgameportd]\nroot      232    2  0
15:35 ?        00:00:00 [kmmcd]\nroot      283 2  0 15:35 ?        00:00:00
[pdflush]\nroot      284    2  0 15:35 ?        00:00:00 [pdflush]\nroot      285    2
0 15:35 ?        00:00:00 [kswapd0]\nroot      326    2  0 15:35 ?        00:00:00
[aio\/0]\nroot      337    2  0 15:35 ?        00:00:00 [nfsiod]\nroot 342    2  0
15:35 ?        00:00:00 [cifsoplockd]\nroot      343    2  0 15:35 ? 00:00:00
[cifsdnotifyd]\nroot      527    2  0 15:35 ?        00:00:00 [scsi_eh_0]\nroot 529
2  0 15:35 ?        00:00:00 [scsi_eh_1]\nroot      533    2  0 15:35 ? 00:00:00
[mtdblockd]\nroot      579    2  0 15:35 ?        00:00:00 [kpsmoused]\nroot 588    2
0 15:35 ?        00:00:00 [hid_compat]\nroot      612    2  6 15:35 ? 00:02:22
[Glob_Spectra]\nroot      618    2  0 15:35 ?        00:00:11 [nandflush]\nroot 628
2  0 15:35 ?        00:00:00 [krfcommd]\nroot      631    2  0 15:35 ?        00:00:00
[rpciod\/0]\nroot      688    2  0 15:35 ?        00:00:00 [scsi_eh_2]\nroot      689
2 0 15:35 ?        00:00:00 [usb-storage]\nroot      704    2  0 15:35 ?        00:00:00
[kjournald]\nroot      917    2  0 15:35 ?        00:00:00 udevd -d\nroot      2102
2  0 15:35 ?        00:00:00 [SEC int]\nroot      2134    1  0 15:35 ?        00:00:00
\/bin\/cdp eth0 start\nroot      2138    2  0 15:35 ?        00:00:04 [Clock_ISR]\nroot
2166    1  0 15:35 ?        00:00:21 \/bin\/gdl_server blender_config 1\nroot      2220
2  0 15:35 ? 00:00:00 [VidDec_hal_pars]\nroot      2221    2  0 15:35 ?        00:00:00
[VidDec_hal_deco]\nroot      2227    2  0 15:35 ?        00:00:00 [VidPProc_ISR]\nroot
2228    2  0 15:35 ?        00:00:00 [VidPProc_IO]\nroot      2232    2  0 15:35 ?
00:00:02 [VidRend_IO]\nroot      2233    2  0 15:35 ?        00:00:00 [VidRend_IO]\nroot
2237    2  0 15:35 ?        00:00:08 [Audio_Rend_ISR]\nroot      2238    2  0 15:35 ?
00:00:03 [Audio_Timing]\nroot      2239    2  0 15:35 ?        00:00:00
[Audio_Pipe_Mgr]\nroot 2240    2  0 15:35 ?        00:00:00 [Audio_DSP0_ISR]\nroot
2241    2  0 15:35 ? 00:00:00 [Audio_DSP1_ISR]\nroot      2446    1  0 15:36 ?
00:00:00 \/usr\/local\/cisco\/sbin\/snmpd -p \/var\/run\/snmpd.pid\nroot      2448    1
0 15:36 ?        00:00:00 \/bin\/konfd\nroot      2583    1  0 15:36 ?        00:00:00
```

```
php-fpm: master process (\/usr\/local\/cisco\/php\/etc\/php-fpm.conf)
\nroot      2584  2583  0 15:36 ? 00:00:00 php-fpm: pool root \nroot      2585  2583  0
15:36 ?        00:00:00 php-fpm: pool root \nroot      2592     1  0 15:36 ?
00:00:00 nginx: master process \/usr\/local\/cisco\/nginx\/sbin\/nginx\nroot      2602
1  0 15:36 ? 00:00:00 \/usr\/local\/cisco\/\/sbin\/cupsd -C
\/usr\/local\/cisco\/\/etc\/cups\/cupsd.conf\nroot      2606     1  0 15:36 ?
00:00:00 \/usr\/local\/cisco\/sbin\/xinetd\nroot      2611     1  0 15:36 ?
00:00:00 \/sbin\/sshd\nroot      2620     1  0 15:36 ? 00:00:11
\/usr\/local\/cisco\/sbin\/cron\nroot      2623     1  0 15:36 ?        00:00:00
\/usr\/local\/cisco\/bin\/mosaic_server 0 5050 10000\nroot      2624     1  0 15:36 ?
00:00:00 \/usr\/local\/cisco\/bin\/mosaic_server 1 5052 12000\nroot      2632     1  0
15:36 ? 00:00:00 audio_setup_outputs\nroot      2641     2  0 15:36 ?        00:00:00
[Audio_Input]\nroot      2643  2632  0 15:36 ?        00:00:00 [sh] <defunct>\nroot
2645 2  0 15:36 ?        00:00:00 [Audio_Recovery]\nroot      2647     2  0 15:36 ?
00:00:00 [kjournald]\nroot      2649     1  0 15:36 ?        00:00:00
\/usr\/local\/cisco\/sbin\/rsyslogd -c5\n1000      2660     1  0 15:36 ?        00:00:00
dbus-daemon --system\n1001      2662     1  0 15:36 ?        00:00:00 hald
--daemon=yes\nroot      2663  2662  0 15:36 ?        00:00:00 hald-runner\nroot      2668
2663  0 15:36 ?        00:00:00 hald-addon-input: Listening on \/dev\/input\/event2
\/dev\/input\/event1 \/dev\/input\/event0\nroot      2677  2663  0 15:36 ? 00:00:00
hald-addon-storage: polling \/dev\/ciscoapps (every 2 sec)\nroot      2680     1 0 15:36 ?
00:00:00 bluetoothd\nroot      2687     1  0 15:36 ?        00:00:00 Agent_3g\nroot
2715     1  0 15:36 ?        00:00:00 wan_detector\nroot      2743     1  0 15:36 ?
00:00:04 slim\nroot      2763  2743  1 15:36 tty2    00:00:22 \/usr\/bin\/X\nroot 2830
1  0 15:36 ?        00:00:00 dhclient br0\nroot      2831     1  0 15:36 ? 00:00:01
\/bin\/sh \/scripts\/status_check.sh\nstudent  2886  2743  0 15:36 ?        00:00:00
\/bin\/sh \/etc\/xinitrc xfce4\nstudent  2891  2886  0 15:36 ?        00:00:00 \/bin\/sh
\/scripts\/startxfce4\nstudent  2916  2891  0 15:36 ?        00:00:01 xfce4-session\nroot
2944     1  0 15:36 ?        00:00:00 \/sbin\/smi\nroot      2958     1  0 15:36 ?
00:00:00 \/bin\/heartbeat\nroot      2995     2  0 15:36 ?        00:00:00
[kjournald]\nstudent 3100     1  0 15:37 ?        00:00:00 dbus-launch --autolaunch
a822b50ba91705398f791a9200000055 --binary-syntax --close-stderr\nstudent   3120     1  0
15:37 ?        00:00:00 \/usr\/local\/cisco\/bin\/dbus-daemon --fork --print-pid 5
--print-address 7 --session\nstudent  3128     1  0 15:37 ?        00:00:00
\/usr\/local\/cisco\/lib\/xfce4\/xfconf\/xfconfd\nroot      3211 1  0 15:37 ?
00:00:00 init      \nstudent  3225     1  0 15:37 ?        00:00:00 xfsettingsd\nstudent
3244     1  0 15:37 ?        00:00:00 \/usr\/local\/cisco\/libexec\/gvfsd\nstudent  3255
1  0 15:37 ?        00:00:00 \/usr\/local\/cisco\/libexec\/\/gvfs-fuse-daemon
\/apps\/localconfig\/student\/.gvfs\nstudent  3259     1  0 15:37 ?        00:00:02
xfwm4\nstudent  3269     1  0 15:37 ?        00:00:02 xfce4-panel\nstudent  3278     1
0 15:37 ?        00:00:00 Thunar --daemon\nstudent  3287     1  0 15:37 ?        00:00:02
xfdesktop\nstudent  3309  2916  0 15:37 ?        00:00:00 3G_Dongle\nstudent  3311  2916
0 15:37 ?        00:00:01 BlueToothUI\nstudent  3329  2916  0 15:37 ?        00:00:01
wifi_status hide\nstudent  3337  2916  0 15:37 ?        00:00:03 wired_status hide >
\/dev\/null\nstudent 3338     1  0 15:37 ?        00:00:00 xfce4-settings-helper\nstudent
3363  3269  0 15:37 ? 00:00:01 \/usr\/local\/cisco\/lib\/xfce4\/panel\/wrapper
\/usr\/local\/cisco\/lib\/xfce4\/panel\/plugins\/libsystray.so 6 16777251 systray
Notification Area Area where notification icons appear \nstudent  3401     1  0 15:37 ?
00:00:00 \/usr\/local\/cisco\/libexec\/gvfs-hal-volume-monitor\nstudent   3411     1  0
15:37 ?        00:00:00 \/usr\/local\/cisco\/libexec\/gvfsd-trash --spawner :1.4
\/org\/gtk\/gvfs\/exec_spaw\/0\nstudent 3443     1  0 15:37 ?        00:00:00
\/usr\/local\/cisco\/libexec\/gconfd-2\nstudent  3942 1  0 15:38 ?        00:00:00
\/usr\/local\/cisco\/lib\/scim-1.0\/scim-launcher -d -c simple -e all -f socket
--no-stay\nstudent  4079     1  0 15:38 ?        00:00:00
\/usr\/local\/cisco\/lib\/scim-1.0\/scim-helper-manager\nstudent  4080     1  0 15:38 ?
00:00:00 \/usr\/local\/cisco\/lib\/scim-1.0\/scim-panel-gtk --display :0.0 -c socket -d
--no-stay\nstudent 4082     1  0 15:38 ?        00:00:00
\/usr\/local\/cisco\/lib\/scim-1.0\/scim-launcher -d -c socket -e socket -f x11\nstudent
4290     1  0 15:38 ?        00:00:03 \/usr\/local\/cisco\/bin\/Terminal\nstudent   4349
4290  0 15:38 ?        00:00:00 gnome-pty-helper\nstudent 4350  4290  0 15:38 pts\/0
00:00:00 bash\nroot      4428  4350  0 15:38 pts\/0    00:00:00 -bash\nroot      5492
2592  0 15:39 ?        00:00:01 nginx: worker process          \nroot 6203  2831  0
16:13 ?        00:00:00 sleep 1\nroot      6225  2585  0 16:13 ?        00:00:00 sh -c cd
'\/usr\/local\/cisco\/nginx\/html\/api\/1.0\/sys' ;
```

```
LC_ALL=zh_CN.utf-8;\/usr\/local\/cisco\/bin\/ps -ef 2>&1\nroot    6226 6225 0 16:13 ?
00:00:00 \/usr\/local\/cisco\/bin\/ps -ef\nroot    15865    2  0 15:50 ?         00:00:00
[RtmpTimerTask]\nroot    15866 2  0 15:50 ?         00:00:02 [RtmpMlmeTask]\nroot
15867    2  0 15:50 ?         00:00:00 [RtmpCmdQTask]\nstudent  23415  4290  0 15:58
pts\/1    00:00:00 bash\nroot    23433 23415  0 15:58 pts\/1    00:00:00 -bash\nroot
30190 23433  0 16:05 pts\/1    00:00:00 clish\n","success":"true","getAt":"2012-12-14
08:13:07"}
```

Set Custom Fonts

Example: set custom fonts

Request

- Fonts are located in a local directory:

```
curl -k -X PUT -H 'password: cisco' -H 'Content-Type: application/json' -d '{"fonts" :
"/usr/local/cisco/share/fonts/thai-ttf/Waree.ttf"}'
https://10.75.189.228/api/1.0/sys/fonts
```

- Fonts are obtained from an HTTP server:

```
curl -k -X PUT -H 'password: cisco' -H 'Content-Type: application/json' -d '{"fonts" :
"http://dl.1001fonts.com/rochester.zip"}' https://10.75.189.228/api/1.0/sys/fonts
```

Reply

```
{"success":"true","updatedAt":"2014-04-17 02:33:34"}
```

Parameter restrictions

The fonts can be obtained either from a local directory or from a remote site through HTTP, HTTPS, or FTP.

Get Fonts List

Example: get fonts list

Request

```
curl -k -X GET -H 'password: cisco' https://10.75.189.228/api/1.0/sys/fonts
```

Reply

```
{"fonts":"Fixed:style=Bold\nFixed:style=Bold
SemiCondensed\nFixed:style=SemiCondensed\nFixed:style=Oblique
SemiCondensed\nFixed:style=Oblique\nFixed:style=ko\nFixed:style=ja\nFixed:style=Regular\n"
,"success":"true","getAt":"2014-04-17 02:41:19"}
```

Remove Custom Fonts

Example: remove custom fonts

Request

```
curl -k -X DELETE -m 60 -H 'password: cisco' -H 'Content-Type: application/json' -d
'{"fonts" : "Waree.ttf"}' https://10.75.189.228/api/1.0/sys/fonts
```

Reply

```
{"success":"true","updatedAt":"2014-04-17 02:53:21"}
```

Parameter restrictions

Provide the custom installed fonts name.

Set Master Audio Volume

Example: set master volume to 77 and set mute to false

Request

```
curl -k -X PUT -H 'password: cisco' -H 'Content-Type: application/json' -d
'{"mute":"false", "volume":"77" }' https://64.104.169.83/api/1.0/sys/audio/default/Master
```

Reply

```
{"success":"true","updatedAt":"2012-12-14 07:50:00"}
```

Parameter restrictions

The volume range is 0–100. Valid values for mute are true and false.

Get Master Audio Volume

Example: get master audio volume information

Request

```
curl -k -X GET -H 'password: cisco' https://64.104.169.83/api/1.0/sys/audio/default/Master
```

Reply

```
{"mute":"true","volume":"50","success":"true","getAt":"2013-01-01 03:03:02"}
```

Set Capture Audio Volume

Example: set capture volume to 77 and set mute to false

Request

```
curl -k -X PUT -H 'password: cisco' -H 'Content-Type: application/json' -d
'{"mute":"false", "volume":"77" }' https://64.104.169.83/api/1.0/sys/audio/default/Capture
```

Reply

```
{"success":"true","updatedAt":"2012-12-14 07:50:00"}
```

Parameter restrictions

The volume range is 0–100. Valid values for mute are true and false.

Get Capture Audio Volume

Example: get capture audio volume information

Request

```
curl -k -X GET -H 'password: cisco'
https://64.104.169.83/api/1.0/sys/audio/default/Capture
```

Reply

```
{"mute":"true","volume":"50","success":"true","getAt":"2013-01-01 03:03:02"}
```

Set Time Zone

Example: set timezone to Asia/Shanghai

Request

```
curl -k -X PUT -H 'password: cisco' -H 'Content-Type: application/json' -d
'{"timezone":"Asia/Shanghai"}' https://64.104.169.102/api/1.0/sys/timezone
```

Reply

```
{"success":"true","updatedAt":"2012-12-14 07:50:00"}
```

Parameter restrictions

The valid strings for timezone are as following:

Africa/Sao_Tome, Africa/Johannesburg, Africa/Maputo, Africa/Lagos, Africa/Mogadishu, Africa/Dakar, Africa/Lubumbashi, Africa/Nouakchott, Africa/Timbuktu, Africa/Abidjan, Africa/Niamey, Africa/Tripoli, Africa/Bujumbura, Africa/Lusaka, Africa/Freetown, Africa/Kinshasa, Africa/Luanda, Africa/Ndjamena, Africa/Ceuta, Africa/Maseru, Africa/Khartoum, Africa/Dar_es_Salaam, Africa/Addis_Ababa, Africa/Algiers, Africa/Asmara, Africa/Libreville, Africa/Asmera, Africa/Djibouti, Africa/Malabo, Africa/Gaborone, Africa/Ouagadougou, Africa/Kigali, Africa/Porto-Novo, Africa/Windhoek, Africa/Monrovia, Africa/Cairo, Africa/Banjul, Africa/Conakry, Africa/Harare, Africa/Bangui, Africa/Tunis, Africa/Mbabane, Africa/Bissau, Africa/El_Aaiun, Africa/Brazzaville, Africa/Blantyre, Africa/Lome, Africa/Kampala, Africa/Nairobi, Africa/Accra, Africa/Bamako, Africa/Casablanca, Africa/Douala, America/Hermosillo, America/Rosario, America/Bahia, America/Martinique, America/Dominica, America/Atikokan, America/Recife, America/Aruba, America/Mendoza, America/Santarem, America/Montserrat, America/Jamaica, America/St_Johns, America/Knox_IN, America/Buenos_Aires, America/St_Kitts, America/Chicago, America/Guyana, America/Boise, America/North_Dakota/Center, America/North_Dakota/New_Salem, America/Miquelon, America/Lima, America/Regina, America/Inuvik, America/Pangnirtung, America/Winnipeg, America/Rankin_Inlet, America/Halifax, America/Nassau, America/Rio_Branco, America/Manaus, America/Cuiaba, America/Cancun, America/Blanc-Sablon, America/Moncton, America/Edmonton, America/Danmarkshavn, America/Jujuy, America/Ensenada, America/Tegucigalpa, America/Santiago, America/Cayenne, America/Merida, America/Belem, America/St_Lucia, America/Puerto_Rico, America/Glace_Bay, America/Coral_Harbour, America/Tijuana, America/Sao_Paulo, America/Mazatlan, America/La_Paz, America/Atka, America/Los_Angeles, America/Noronha, America/Tortola, America/Cayman, America/Porto_Velho, America/Caracas, America/Swift_Current, America/Mexico_City, America/Maceio, America/Cordoba, America/Rainy_River, America/Iqaluit, America/New_York, America/Montreal, America/Araguaina, America/Denver, America/Adak, America/Shiprock, America/Barbados, America/St_Vincent, America/Chihuahua, America/Guatemala, America/St_Thomas, America/Cambridge_Bay, America/Phoenix, America/Eirunepe, America/Belize, America/Guadeloupe, America/Antigua, America/Nome, America/Catamarca, America/Port_of_Spain, America/Indiana/Petersburg, America/Indiana/Vincennes, America/Indiana/Knox, America/Indiana/Marengo, America/Indiana/Winamac, America/Indiana/Vevay, America/Indiana/Indianapolis, America/Indiana/Tell_City, America/Paramaribo, America/Grand_Turk, America/Boa_Vista,

America/Panama, America/Thunder_Bay, America/Whitehorse, America/Godthab, America/Toronto, America/Goose_Bay, America/Guayaquil, America/Kentucky/Monticello, America/Kentucky/Louisville, America/Juneau, America/Campo_Grande, America/Anchorage, America/Argentina/Mendoza, America/Argentina/Buenos_Aires, America/Argentina/Rio_Gallegos, America/Argentina/La_Rioja, America/Argentina/Tucuman, America/Argentina/Jujuy, America/Argentina/Salta, America/Argentina/Cordoba, America/Argentina/San_Luis, America/Argentina/Ushuaia, America/Argentina/ComodRivadavia, America/Argentina/Catamarca, America/Argentina/San_Juan, America/Montevideo, America/Asuncion, America/Monterrey, America/Curacao, America/Menominee, America/Havana, America/Costa_Rica, America/Yakutat, America/Detroit, America/Managua, America/Louisville, America/Dawson_Creek, America/Dawson, America/Resolute, America/Nipigon, America/Yellowknife, America/Santo_Domingo, America/Fort_Wayne, America/Bogota, America/Indianapolis, America/Port-au-Prince, America/Grenada, America/Porto_Acre, America/Anguilla, America/St_Barthelemy, America/Fortaleza, America/Marigot, America/Scoresbysund, America/Virgin, America/El_Salvador, America/Thule, America/Vancouver, Antarctica/South_Pole, Antarctica/Mawson, Antarctica/Palmer, Antarctica/Rothera, Antarctica/DumontDUrville, Antarctica/Syowa, Antarctica/McMurdo, Antarctica/Davis, Antarctica/Vostok, Antarctica/Casey, Arctic/Longyearbyen, Asia/Brunei, Asia/Kuwait, Asia/Amman, Asia/Riyadh89, Asia/Aden, Asia/Thimphu, Asia/Jerusalem, Asia/Riyadh, Asia/Ujung_Pandang, Asia/Macao, Asia/Istanbul, Asia/Phnom_Penh, Asia/Shanghai, Asia/Bahrain, Asia/Taipei, Asia/Seoul, Asia/Bangkok, Asia/Ashgabat, Asia/Yerevan, Asia/Dhaka, Asia/Macau, Asia/Karachi, Asia/Tashkent, Asia/Dacca, Asia/Chongqing, Asia/Calcutta, Asia/Dubai, Asia/Chungking, Asia/Kashgar, Asia/Ashkhabad, Asia/Vientiane, Asia/Yakutsk, Asia/Beirut, Asia/Pontianak, Asia/Nicosia, Asia/Irkutsk, Asia/Tbilisi, Asia/Kuching, Asia/Tehran, Asia/Tokyo, Asia/Singapore, Asia/Bishkek, Asia/Dushanbe, Asia/Baku, Asia/Hong_Kong, Asia/Baghdad, Asia/Ulan_Bator, Asia/Damascus, Asia/Choibalsan, Asia/Jayapura, Asia/Yekaterinburg, Asia/Katmandu, Asia/Qyzylorda, Asia/Qatar, Asia/Kolkata, Asia/Kathmandu, Asia/Makassar, Asia/Ho_Chi_Minh, Asia/Thimbu, Asia/Oral, Asia/Sakhalin, Asia/Riyadh87, Asia/Magadan, Asia/Gaza, Asia/Anadyr, Asia/Krasnoyarsk, Asia/Aqtau, Asia/Riyadh88, Asia/Muscat, Asia/Urumqi, Asia/Omsk, Asia/Ulaanbaatar, Asia/Vladivostok, Asia/Kuala_Lumpur, Asia/Colombo, Asia/Samarkand, Asia/Kabul, Asia/Almaty, Asia/Harbin, Asia/Kamchatka, Asia/Aqtobe, Asia/Pyongyang, Asia/Novosibirsk, Asia/Manila, Asia/Jakarta, Asia/Rangoon, Asia/Tel_Aviv, Asia/Hovd, Asia/Dili, Asia/Saigon, Atlantic/Stanley, Atlantic/Madeira, Atlantic/St_Helena, Atlantic/Azores, Atlantic/Faroe, Atlantic/Jan_Mayen, Atlantic/South_Georgia, Atlantic/Faeroe, Atlantic/Reykjavik, Atlantic/Bermuda, Atlantic/Canary, Atlantic/Cape_Verde, Australia/Sydney, Australia/South, Australia/Currie, Australia/Perth, Australia/Yancowinna, Australia/North, Australia/West, Australia/Darwin, Australia/Lord_Howe, Australia/Lindeman, Australia/Victoria, Australia/NSW, Australia/ACT, Australia/Brisbane, Australia/Melbourne, Australia/Eucla, Australia/Hobart, Australia/Queensland, Australia/Adelaide, Australia/Tasmania, Australia/Canberra, Australia/LHI, Australia/Broken_Hill, Brazil/West, Brazil/Acre, Brazil/East, Brazil/DeNoronha, Canada/Pacific, Canada/Mountain, Canada/Atlantic, Canada/Central, Canada/Eastern, Canada/East-Saskatchewan, Canada/Saskatchewan, Canada/Newfoundland, Canada/Yukon, CET, Chile/EasterIsland, Chile/Continental, CST6CDT, Cuba, EET, Egypt, Eire, EST, EST5EDT, Etc/GMT+12, Etc/GMT+9, Etc/GMT, Etc/GMT-13, Etc/GMT0, Etc/GMT+11, Etc/GMT+5, Etc/GMT-0, Etc/GMT-2, Etc/GMT-10, Etc/GMT-11, Etc/GMT+2, Etc/UCT, Etc/GMT-1, Etc/GMT+3, Etc/GMT+0, Etc/UTC, Etc/GMT+10, Etc/GMT-7, Etc/Zulu, Etc/GMT-6, Etc/GMT+1, Etc/GMT-5, Etc/GMT-12, Etc/GMT+4, Etc/GMT-9, Etc/GMT+7, Etc/GMT+8, Etc/Universal, Etc/GMT-3, Etc/GMT-14, Etc/GMT-8, Etc/Greenwich, Etc/GMT+6, Etc/GMT-4, Europe/Bucharest, Europe/Riga, Europe/Kaliningrad, Europe/Monaco, Europe/San_Marino, Europe/Budapest, Europe/Gibraltar, Europe/Lisbon, Europe/Belgrade, Europe/Athens, Europe/Warsaw, Europe/Vatican, Europe/Chisinau, Europe/Istanbul, Europe/Madrid, Europe/Paris, Europe/Bratislava, Europe/Dublin, Europe/Helsinki, Europe/London, Europe/Zaporozhye, Europe/Volgograd, Europe/Tirane, Europe/Simferopol, Europe/Samara, Europe/Sarajevo, Europe/Mariehamn, Europe/Tallinn, Europe/Prague, Europe/Andorra, Europe/Ljubljana, Europe/Vienna, Europe/Kiev, Europe/Isle_of_Man, Europe/Oslo,

Europe/Nicosia, Europe/Skopje, Europe/Brussels, Europe/Rome, Europe/Belfast, Europe/Amsterdam, Europe/Sofia, Europe/Minsk, Europe/Zagreb, Europe/Luxembourg, Europe/Moscow, Europe/Tiraspol, Europe/Vaduz, Europe/Stockholm, Europe/Podgorica, Europe/Zurich, Europe/Copenhagen, Europe/Berlin, Europe/Jersey, Europe/Vilnius, Europe/Malta, Europe/Guernsey, Europe/Uzhgorod, Factory, GB, GB-Eire, GMT, GMT0, GMT-0, GMT+0, Greenwich, Hongkong, HST, Iceland, Indian/Cocos, Indian/Kerguelen, Indian/Christmas, Indian/Reunion, Indian/Antananarivo, Indian/Mauritius, Indian/Chagos, Indian/Maldives, Indian/Mayotte, Indian/Comoro, Indian/Mahe, Iran, Israel, Jamaica, Japan, Kwajalein, Libya, MET, Mexico/BajaNorte, Mexico/BajaSur, Mexico/General, Mideast/Riyadh89, Mideast/Riyadh87, Mideast/Riyadh88, MST, MST7MDT, Navajo, NZ, NZ-CHAT, Pacific/Majuro, Pacific/Guadalcanal, Pacific/Noumea, Pacific/Tongatapu, Pacific/Tarawa, Pacific/Palau, Pacific/Wallis, Pacific/Johnston, Pacific/Apia, Pacific/Kwajalein, Pacific/Kiritimati, Pacific/Norfolk, Pacific/Wake, Pacific/Easter, Pacific/Enderbury, Pacific/Fiji, Pacific/Ponape, Pacific/Gambier, Pacific/Pitcairn, Pacific/Truk, Pacific/Samoa, Pacific/Nauru, Pacific/Auckland, Pacific/Niue, Pacific/Fakaofo, Pacific/Rarotonga, Pacific/Chatham, Pacific/Tahiti, Pacific/Marquesas, Pacific/Funafuti, Pacific/Guam, Pacific/Saipan, Pacific/Honolulu, Pacific/Yap, Pacific/Pago_Pago, Pacific/Midway, Pacific/Kosrae, Pacific/Efate, Pacific/Galapagos, Pacific/Port_Moresby, Poland, Portugal, PRC, PST8PDT, ROC, ROK, Singapore, Turkey, UCT, Universal, US/Indiana-Starke, US/Pacific, US/Mountain, US/East-Indiana, US/Aleutian, US/Hawaii, US/Central, US/Eastern, US/Michigan, US/Samoa, US/Arizona, US/Alaska, UTC, WET, W-SU, Zulu,

Get Time Zone

Example: get timezone information

Request

```
curl -k -X GET -H 'password: cisco' https://64.104.169.102/api/1.0/sys/timezone
```

Reply

```
{"timezone":"Asia/Shanghai","success":"true","getAt":"2013-01-01 03:19:46"}
```

Ethernet API

Use the commands IN this section to configure Ethernet API.

Note   Curl is used as a sample tool to request APIs. 10.140.44.134 is used as a sample IP address of the Cisco Edge 300 series switch, and cisco123! is used as a sample admin password.

Set Gi1 Status

N/A. 003 error is reported if it is requested.

Get Gi1 Status

Example: get gi1 status

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/gi1/status
```

Reply

```
{"status":"enable","success":"true","getAt":"2012-11-08 08:47:44"}
```

Set Gi1 MAC

N/A. 003 error is reported if it is requested.

Get Gi1 MAC

Example: get gi1 mac

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/gi1/mac
```

Reply

```
{"mac":"1C:AA:07:97:A3:C0","success":"true","getAt":"2012-11-08 08:51:19"}
```

Set Gi1 output-queue-strategy

Example: set gi1 output-queue-strategy to wrr

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"oqs" :
"wrr"}' https://10.140.44.134/api/1.0/eth/gi1/oqs
```

Reply

```
{"success":"true","updatedAt":"2012-11-08 08:54:26"}
```

Parameter restrictions

wrr and strict are the valid strings for oqs. Otherwise, 004 error is reported.

Get Gi1 output-queue-strategy

Example: get gi1 output-queue-strategy

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/gi1/oqs
```

Reply

```
{"oqs":"wrr","success":"true","getAt":"2012-11-08 09:07:08"}
```

Set Gi1 Pause

Example: set gi1 pause to on

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"pause" :
"on"}' https://10.140.44.134/api/1.0/eth/gi1/pause
```

Reply

```
{"success":"true","updatedAt":"2012-11-08 08:54:26"}
```

Parameter restrictions

on and off are the valid strings for oqs. Otherwise, 004 error is reported.

Get Gi1 Pause

Example: get gi1 pause

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/gi1/pause
```

Reply

```
{"pause":"on","success":"true","getAt":"2012-11-08 09:29:55"}
```

Set Gi1 Priority

Example: set gi1 pause to on

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"priority" : "normal"}' https://10.140.44.134/api/1.0/eth/gi1/priority
```

Reply

```
{"success":"true","updatedAt":"2012-11-08 09:37:31"}
```

Parameter restrictions

normal and high are the valid strings for oqs. Otherwise, 004 error is reported.

Get Gi1 Priority

Example: get gi1 priority

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/gi1/priority
```

Reply

```
{"priority":"normal","success":"true","getAt":"2012-11-08 09:39:52"}
```

Set Gi1 Rate Limit

Example: set gi1 rate limit to ìunknown-unicastî

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"rateLim"
: "set unknown-unicast 100"}' https://10.140.44.134/api/1.0/eth/gi1/rateLim
```

Reply

```
{"success":"true","updatedAt":"2012-11-08 09:37:31"}
```

Parameter restrictions

Only none and set broadcast/unknown-unicast/both [1-100] are valid parameters.

Get Gi1 Rate Limit

Example: get gi1 rate limit

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/gi1/rateLim
```

Reply

```
{"rateLim":"set unknown-unicast 100","success":"true","getAt":"2012-11-09 03:21:16"}
```

Set Gi1 Speed

Example: set gi1 rate limit to ìunknown-unicastî

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"speed" :
"auto"}' https://10.140.44.134/api/1.0/eth/gi1/speed
```

Reply

```
{"success":"true","updatedAt":"2012-11-08 09:37:31"}
```

Parameter restrictions

Only auto, 10, 100, and 1000 are valid parameters.

Get Gi1 Speed

Example: get gi1 rate limit

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/gi1/speed
```

Reply

```
{"speed":"auto","success":"true","getAt":"2012-11-14 07:03:00"}
```

Set Gi1 Duplex

Example: set gi1 duplex to ìautoî

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"duplex"
: "auto"}' https://10.140.44.134/api/1.0/eth/gi1/duplex
```

Reply

```
{"success":"true","updatedAt":"2012-11-08 09:37:31"}
```

Parameter restrictions

Only auto, full, and half are valid parameters.

Get Gi1 Duplex

Example: get gi1 rate limit

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/gi1/duplex
```

Reply

```
{"duplex":"auto","success":"true","getAt":"2012-11-15 01:18:14"}
```

Set Gi1 Information

Example: set gi1 rate limit to ìunknown-unicastî, to pause to off

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"rateLim"
: "set unknown-unicast 100", "pause":"off"}' https://10.140.44.134/api/1.0/eth/gi1
```

Reply

```
{"success":"true","updatedAt":"2012-11-08 09:37:31"}
```

Parameter restrictions

Only none and set broadcast/unknown-unicast/both [1-100] are valid parameters.

Get Gi1 Information

Example: get gi1 information

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/gi1
```

Reply

```
{"status":"enable","dns":"64.104.123.144
171.70.168.183","mac":"1C:AA:07:97:A3:C0","oqs":"strict","pause":"on","priority":"normal",
"rateLim":"set unknown-unicast 100","speed":"100","success":"true","getAt":"2012-11-09
08:53:52"}
```

Set Fe1 Status

Example: set fe1 status to disable

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"status"
: "disable"}' https://10.140.44.134/api/1.0/eth/fe1/status
```

Reply

```
{"success":"true","updatedAt":"2012-11-08 08:54:26"}
```

Parameter restrictions

enable and disable are the valid strings for status. Otherwise, 004 error is reported.

Get Fe1 Status

Example: get fe1 status

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe1/status
```

Reply

```
{"status":"disable","success":"true","getAt":"2012-11-21 06:33:40"}
```

Set Fe1 output-queue-strategy

Example: set gi1 output-queue-strategy to wrr

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"oqs" :
"wrr"}' https://10.140.44.134/api/1.0/eth/fe1/oqs
```

Reply

```
{"success":"true","updatedAt":"2012-11-21 06:35:35"}
```

Parameter restrictions

wrr and strict are the valid strings for oqs. Otherwise, 004 error is reported.

Get Fe1 output-queue-strategy

Example: get fe1 output-queue-strategy

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe1/oqs
```

Reply

```
{"oqs":"wrr","success":"true","getAt":"2012-11-08 09:07:08"}
```

Set Fe1 Priority

Example: set fe1 pause to ìonî

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"priority" : "normal"}' https://10.140.44.134/api/1.0/eth/fe1/priority
```

Reply

```
{"success":"true","updatedAt":"2012-11-21 06:42:18"}
```

Parameter restrictions

normal and high are the valid strings for oqs. Otherwise, 004 error is reported.

Get Fe1 Priority

Example: get gi1 priority

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe1/priority
```

Reply

```
{"priority":"normal","success":"true","getAt":"2012-11-08 09:39:52"}
```

Set Fe1 Rate Limit

Example: set fe1 rate limit to ìunknown-unicastî

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"rateLim"
: "set unknown-unicast 100"}' https://10.140.44.134/api/1.0/eth/fe1/rateLim
```

Reply

```
{"success":"true","updatedAt":"2012-11-21 06:43:28"}
```

Parameter restrictions

Only none and set broadcast/unknown-unicast/both [1-100] are valid parameters.

Get Fe1 Rate Limit

Example: get fe1 rate limit

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe1/rateLim
```

Reply

```
{"rateLim":"set unknown-unicast 100","success":"true","getAt":"2012-11-09 03:21:16"}
```

Set Fe1 Speed

Example: set fe1 rate limit to ìunknown-unicastî

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"speed" :
"auto"}' https://10.140.44.134/api/1.0/eth/fe1/speed
```

Reply

```
{"success":"true","updatedAt":"2012-11-08 09:37:31"}
```

Parameter restrictions

Only auto, 10, and 100 are valid parameters.

Get Fe1 Speed

Example: get fe1 rate limit

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe1/speed
```

Reply

```
{"speed":"auto","success":"true","getAt":"2012-11-14 07:03:00"}
```

Set Fe1 Duplex

Example: set fe1 duplex to ìautoî

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"duplex"
: "auto"}' https://10.140.44.134/api/1.0/eth/fe1/duplex
```

Reply

```
{"success":"true","updatedAt":"2012-11-08 09:37:31"}
```

Parameter restrictions

Only auto, full and half are valid parameters.

Get Fe1 Duplex

Example: get fe1 rate limit

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe1/duplex
```

Reply

```
{"duplex":"auto","success":"true","getAt":"2012-11-15 01:18:14"}
```

Set Fe1 Information

Example: set fe1 rate limit to unknown-unicast, to pause to off

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"rateLim"
: "set unknown-unicast 100","duplex":"auto"}' https://10.140.44.134/api/1.0/eth/fe1
```

Reply

```
{"success":"true","updatedAt":"2012-11-08 09:37:31"}
```

Parameter restrictions

Only none and set broadcast/unknown-unicast/both [1-100] are valid parameters.

Get Fe1 Information

Example: get fe1 information

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe1
```

Reply

```
{"status":"disable","oqs":"wrr","priority":"normal","rateLim":"set unknown-unicast
100","speed":"auto","duplex":"auto","success":"true","getAt":"2012-11-21 06:47:52"}
```

Set Fe2 Status

Example: set fe2 status to ìdisableî

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"status"
: "disable"}' https://10.140.44.134/api/1.0/eth/fe2/status
```

Reply

```
{"success":"true","updatedAt":"2012-11-08 08:54:26"}
```

Parameter restrictions

enable and disable are the valid strings for status. Otherwise, 004 error is reported.

Get Fe2 Status

Example: get fe2 status

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe2/status
```

Reply

```
{"status":"disable","success":"true","getAt":"2012-11-21 06:33:40"}
```

Set Fe2 output-queue-strategy

Example: set gi1 output-queue-strategy to wrr

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"oqs" :
"wrr"}' https://10.140.44.134/api/1.0/eth/fe2/oqs
```

Reply

```
{"success":"true","updatedAt":"2012-11-21 06:35:35"}
```

Parameter restrictions

wrr and strict are the valid strings for oqs. Otherwise, 004 error is reported.

Get Fe2 output-queue-strategy

Example: get fe2 output-queue-strategy

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe2/oqs
```

Reply

```
{"oqs":"wrr","success":"true","getAt":"2012-11-08 09:07:08"}
```

Set Fe2 Priority

Example: set fe2 pause to ìonî

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"priority" : "normal"}' https://10.140.44.134/api/1.0/eth/fe2/priority
```

Reply

```
{"success":"true","updatedAt":"2012-11-21 06:42:18"}
```

Parameter restrictions

normal and high are the valid strings for oqs. Otherwise, 004 error is reported.

Get Fe2 Priority

Example: get gi1 priority

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe2/priority
```

Reply

```
{"priority":"normal","success":"true","getAt":"2012-11-08 09:39:52"}
```

Set Fe2 Rate Limit

Example: set fe2 rate limit to ìunknown-unicastî

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"rateLim"
: "set unknown-unicast 100"}' https://10.140.44.134/api/1.0/eth/fe2/rateLim
```

Reply

```
{"success":"true","updatedAt":"2012-11-21 06:43:28"}
```

Parameter restrictions

Only none and set broadcast/unknown-unicast/both [1-100] are valid parameters.

Get Fe2 Rate Limit

Example: get fe2 rate limit

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe2/rateLim
```

Reply

```
{"rateLim":"set unknown-unicast 100","success":"true","getAt":"2012-11-09 03:21:16"}
```

Set Fe2 Speed

Example: set fe2 rate limit to ìunknown-unicastî

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"speed" :
"auto"}' https://10.140.44.134/api/1.0/eth/fe2/speed
```

Reply

```
{"success":"true","updatedAt":"2012-11-08 09:37:31"}
```

Parameter restrictions

Only auto, 10, and 100 are valid parameters.

Get Fe2 Speed

Example: get fe2 rate limit

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe2/speed
```

Reply

```
{"speed":"auto","success":"true","getAt":"2012-11-14 07:03:00"}
```

Set Fe2 Duplex

Example: set fe2 duplex to ìautoî

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"duplex"
: "auto"}' https://10.140.44.134/api/1.0/eth/fe2/duplex
```

Reply

```
{"success":"true","updatedAt":"2012-11-08 09:37:31"}
```

Parameter restrictions

Only auto, full and half are valid parameters.

Get Fe2 Duplex

Example: get fe2 rate limit

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe2/duplex
```

Reply

```
{"duplex":"auto","success":"true","getAt":"2012-11-15 01:18:14"}
```

Set Fe2 Information

Example: set fe2 rate limit to unknown-unicast, to pause to off

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"rateLim"
: "set unknown-unicast 100","duplex":"auto"}' https://10.140.44.134/api/1.0/eth/fe2
```

Reply

```
{"success":"true","updatedAt":"2012-11-08 09:37:31"}
```

Parameter restrictions

Only none and set broadcast/unknown-unicast/both [1-100] are valid parameters.

Get Fe2 Information

Example: get fe2 information

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe2
```

Reply

```
{"status":"disable","oqs":"wrr","priority":"normal","rateLim":"set unknown-unicast
100","speed":"auto","duplex":"auto","success":"true","getAt":"2012-11-21 06:47:52"}
```

Set Fe3 Status

Example: set fe3 status to disable

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"status"
: "disable"}' https://10.140.44.134/api/1.0/eth/fe3/status
```

Reply

```
{"success":"true","updatedAt":"2012-11-08 08:54:26"}
```

Parameter restrictions

enable and disable are the valid strings for status. Otherwise, 004 error is reported.

Get fe3 status

Example: get fe3 status

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe3/status
```

Reply

```
{"status":"disable","success":"true","getAt":"2012-11-21 06:33:40"}
```

Set Fe3 output-queue-strategy

Example: set gi1 output-queue-strategy to wrr

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"oqs" :
"wrr"}' https://10.140.44.134/api/1.0/eth/fe3/oqs
```

Reply

```
{"success":"true","updatedAt":"2012-11-21 06:35:35"}
```

Parameter restrictions

wrr and strict are the valid strings for oqs. Otherwise, 004 error is reported.

Get Fe3 output-queue-strategy

Example: get fe3 output-queue-strategy

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe3/oqs
```

Reply

```
{"oqs":"wrr","success":"true","getAt":"2012-11-08 09:07:08"}
```

Set Fe3 priority

Example: set fe3 pause to ìonî

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"priority" : "normal"}' https://10.140.44.134/api/1.0/eth/fe3/priority
```

Reply

```
{"success":"true","updatedAt":"2012-11-21 06:42:18"}
```

Parameter restrictions

normal and high are the valid strings for oqs. Otherwise, 004 error is reported.

Get fe3 priority

Example: get gi1 priority

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe3/priority
```

Reply

```
{"priority":"normal","success":"true","getAt":"2012-11-08 09:39:52"}
```

Set Fe3 Rate Limit

Example: set fe3 rate limit to unknown-unicast

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"rateLim"
: "set unknown-unicast 100"}' https://10.140.44.134/api/1.0/eth/fe3/rateLim
```

Reply

```
{"success":"true","updatedAt":"2012-11-21 06:43:28"}
```

Parameter restrictions

Only none and set broadcast/unknown-unicast/both [1-100] are valid parameters.

Get Fe3 Rate Limit

Example: get fe3 rate limit

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe3/rateLim
```

Reply

```
{"rateLim":"set unknown-unicast 100","success":"true","getAt":"2012-11-09 03:21:16"}
```

Set Fe3 Speed

Example: set fe3 rate limit to ìunknown-unicastî

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"speed" :
"auto"}' https://10.140.44.134/api/1.0/eth/fe3/speed
```

Reply

```
{"success":"true","updatedAt":"2012-11-08 09:37:31"}
```

Parameter restrictions

Only auto, 10, and 100 are valid parameters.

Get Fe3 Speed

Example: get fe3 rate limit

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe3/speed
```

Reply

```
{"speed":"auto","success":"true","getAt":"2012-11-14 07:03:00"}
```

Set Fe3 Duplex

Example: set fe3 duplex to auto

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"duplex"
: "auto"}' https://10.140.44.134/api/1.0/eth/fe3/duplex
```

Reply

```
{"success":"true","updatedAt":"2012-11-08 09:37:31"}
```

Parameter restrictions

Only auto, full, and half are valid parameters.

Get Fe3 Duplex

Example: get fe3 rate limit

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe3/duplex
```

Reply

```
{"duplex":"auto","success":"true","getAt":"2012-11-15 01:18:14"}
```

Set Fe3 Information

Example: set fe3 rate limit to unknown-unicast, pause, or off

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"rateLim"
: "set unknown-unicast 100","duplex":"auto"}' https://10.140.44.134/api/1.0/eth/fe3
```

Reply

```
{"success":"true","updatedAt":"2012-11-08 09:37:31"}
```

Parameter restrictions

Only none and set broadcast/unknown-unicast/both [1-100] are valid parameters.

Get Fe3 Information

Example: get fe3 information

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe3
```

Reply

```
{"status":"disable","oqs":"wrr","priority":"normal","rateLim":"set unknown-unicast
100","speed":"auto","duplex":"auto","success":"true","getAt":"2012-11-21 06:47:52"}
```

Set Fe3 Status

Example: set fe3 status to disable

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"status"
: "disable"}' https://10.140.44.134/api/1.0/eth/fe3/status
```

Reply

```
{"success":"true","updatedAt":"2012-11-08 08:54:26"}
```

Parameter restrictions

enable and disable are the valid strings for status. Otherwise, 004 error is reported.

Get Fe3 Status

Example: get fe3 status

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe3/status
```

Reply

```
{"status":"disable","success":"true","getAt":"2012-11-21 06:33:40"}
```

Set Fe3 output-queue-strategy

Example: set gi1 output-queue-strategy to wrr

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"oqs" :
"wrr"}' https://10.140.44.134/api/1.0/eth/fe3/oqs
```

Reply

```
{"success":"true","updatedAt":"2012-11-21 06:35:35"}
```

Parameter restrictions

wrr and strict are the valid strings for oqs. Otherwise, 004 error is reported.

Get Fe3 output-queue-strategy

Example: get fe3 output-queue-strategy

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe3/oqs
```

Reply

```
{"oqs":"wrr","success":"true","getAt":"2012-11-08 09:07:08"}
```

Set Fe3 Priority

Example: set fe3 pause to on

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"priority" : "normal"}' https://10.140.44.134/api/1.0/eth/fe3/priority
```

Reply

```
{"success":"true","updatedAt":"2012-11-21 06:42:18"}
```

Parameter restrictions

normal and high are the valid strings for oqs. Otherwise, 004 error is reported.

Get Fe3 Priority

Example: get gi1 priority

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe3/priority
```

Reply

```
{"priority":"normal","success":"true","getAt":"2012-11-08 09:39:52"}
```

Set Fe3 Rate Limit

Example: set fe3 rate limit to unknown-unicast

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"rateLim"
: "set unknown-unicast 100"}' https://10.140.44.134/api/1.0/eth/fe3/rateLim
```

Reply

```
{"success":"true","updatedAt":"2012-11-21 06:43:28"}
```

Parameter restrictions

Only none and set broadcast/unknown-unicast/both [1-100] are valid parameters.

Get Fe3 Rate Limit

Example: get fe3 rate limit

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe3/rateLim
```

Reply

```
{"rateLim":"set unknown-unicast 100","success":"true","getAt":"2012-11-09 03:21:16"}
```

Set Fe3 Speed

Example: set fe3 rate limit to unknown-unicast

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"speed" :
"auto"}' https://10.140.44.134/api/1.0/eth/fe3/speed
```

Reply

```
{"success":"true","updatedAt":"2012-11-08 09:37:31"}
```

Parameter restrictions

Only auto, 10, 100, and 1000 are valid parameters.

Get Fe3 Speed

Example: get fe3 rate limit

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe3/speed
```

Reply

```
{"speed":"auto","success":"true","getAt":"2012-11-14 07:03:00"}
```

Set Fe3 Duplex

Example: set fe3 duplex to auto

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"duplex"
: "auto"}' https://10.140.44.134/api/1.0/eth/fe3/duplex
```

Reply

```
{"success":"true","updatedAt":"2012-11-08 09:37:31"}
```

Parameter restrictions

Only auto, full, and half are valid parameters.

Get Fe3 Duplex

Example: get fe3 rate limit

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe3/duplex
```

Reply

```
{"duplex":"auto","success":"true","getAt":"2012-11-15 01:18:14"}
```

Set Fe3 Information

Example: set fe3 rate limit to unknown-unicast, to pause to off

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"rateLim"
: "set unknown-unicast 100","duplex":"auto"}' https://10.140.44.134/api/1.0/eth/fe3
```

Reply

```
{"success":"true","updatedAt":"2012-11-08 09:37:31"}
```

Parameter restrictions

Only none and set broadcast/unknown-unicast/both [1-100] are valid parameters.

Get Fe3 Information

Example: get fe3 information

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe3
```

Reply

```
{"status":"disable","oqs":"wrr","priority":"normal","rateLim":"set unknown-unicast
100","speed":"auto","duplex":"auto","success":"true","getAt":"2012-11-21 06:47:52"}
```

Set Fe4 Status

Example: set fe4 status to disable

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"status"
: "disable"}' https://10.140.44.134/api/1.0/eth/fe4/status
```

Reply

```
{"success":"true","updatedAt":"2012-11-08 08:54:26"}
```

Parameter restrictions

enable and disable are the valid strings for status. Otherwise, 004 error is reported.

Get Fe4 Status

Example: get fe4 status

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe4/status
```

Reply

```
{"status":"disable","success":"true","getAt":"2012-11-21 06:33:40"}
```

Set Fe4 output-queue-strategy

Example: set gi1 output-queue-strategy to wrr

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"oqs" :
"wrr"}' https://10.140.44.134/api/1.0/eth/fe4/oqs
```

Reply

```
{"success":"true","updatedAt":"2012-11-21 06:35:35"}
```

Parameter restrictions

wrr and strict are the valid strings for oqs. Otherwise, 004 error is reported.

Get Fe4 output-queue-strategy

Example: get fe4 output-queue-strategy

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe4/oqs
```

Reply

```
{"oqs":"wrr","success":"true","getAt":"2012-11-08 09:07:08"}
```

Set Fe4 priority

Example: set fe4 pause to on

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"priority" : "normal"}' https://10.140.44.134/api/1.0/eth/fe4/priority
```

Reply

```
{"success":"true","updatedAt":"2012-11-21 06:42:18"}
```

Parameter restrictions

normal and high are the valid strings for oqs. Otherwise, 004 error is reported.

Get Fe4 Priority

Example: get fe4 priority

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe4/priority
```

Reply

```
{"priority":"normal","success":"true","getAt":"2012-11-08 09:39:52"}
```

Set Fe4 Rate Limit

Example: set fe4 rate limit to unknown-unicast

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"rateLim"
: "set unknown-unicast 100"}' https://10.140.44.134/api/1.0/eth/fe4/rateLim
```

Reply

```
{"success":"true","updatedAt":"2012-11-21 06:43:28"}
```

Parameter restrictions

Only none and set broadcast/unknown-unicast/both [1-100] are valid parameters.

Get Fe4 Rate Limit

Example: get fe4 rate limit

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe4/rateLim
```

Reply

```
{"rateLim":"set unknown-unicast 100","success":"true","getAt":"2012-11-09 03:21:16"}
```

Set Fe4 Speed

Example: set fe4 rate limit to unknown-unicast

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"speed" :
"auto"}' https://10.140.44.134/api/1.0/eth/fe4/speed
```

Reply

```
{"success":"true","updatedAt":"2012-11-08 09:37:31"}
```

Parameter restrictions

Only auto, 10, and 100 are valid parameters.

Get Fe4 Speed

Example: get fe4 rate limit

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe4/speed
```

Reply

```
{"speed":"auto","success":"true","getAt":"2012-11-14 07:03:00"}
```

Set Fe4 Duplex

Example: set fe4 duplex to auto

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"duplex"
: "auto"}' https://10.140.44.134/api/1.0/eth/fe4/duplex
```

Reply

```
{"success":"true","updatedAt":"2012-11-08 09:37:31"}
```

Parameter restrictions

Only auto, full, and half are valid parameters.

Get Fe4 Duplex

Example: get fe4 rate limit

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe4/duplex
```

Reply

```
{"duplex":"auto","success":"true","getAt":"2012-11-15 01:18:14"}
```

Set Fe4 Information

Example: set fe4 rate limit to unknown-unicast, to pause to off

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"rateLim"
: "set unknown-unicast 100","duplex":"auto"}' https://10.140.44.134/api/1.0/eth/fe4
```

Reply

```
{"success":"true","updatedAt":"2012-11-08 09:37:31"}
```

Parameter restrictions

Only none and set broadcast/unknown-unicast/both [1-100] are valid parameters.

Get Fe4 Information

Example: get fe4 information

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe4
```

Reply

```
{"status":"disable","oqs":"wrr","priority":"normal","rateLim":"set unknown-unicast
100","speed":"auto","duplex":"auto","success":"true","getAt":"2012-11-21 06:47:52"}
```

Set Fe4 Status

Example: set fe4 status to disable

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"status"
: "disable"}' https://10.140.44.134/api/1.0/eth/fe4/status
```

Reply

```
{"success":"true","updatedAt":"2012-11-08 08:54:26"}
```

Parameter restrictions

enable and disable are the valid strings for status. Otherwise, 004 error is reported.

Get Fe4 Status

Example: get fe4 status

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe4/status
```

Reply

```
{"status":"disable","success":"true","getAt":"2012-11-21 06:33:40"}
```

Set Fe4 output-queue-strategy

Example: set gi1 output-queue-strategy to wrr

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"oqs" :
"wrr"}' https://10.140.44.134/api/1.0/eth/fe4/oqs
```

Reply

```
{"success":"true","updatedAt":"2012-11-21 06:35:35"}
```

Parameter restrictions

wrr and strict are the valid strings for oqs. Otherwise, 004 error is reported.

Get Fe4 output-queue-strategy

Example: get fe4 output-queue-strategy

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe4/oqs
```

Reply

```
{"oqs":"wrr","success":"true","getAt":"2012-11-08 09:07:08"}
```

Set Fe4 Priority

Example: set fe4 pause to on

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"priority" : "normal"}' https://10.140.44.134/api/1.0/eth/fe4/priority
```

Reply

```
{"success":"true","updatedAt":"2012-11-21 06:42:18"}
```

Parameter restrictions

normal and high are the valid strings for oqs. Otherwise, 004 error is reported.

Get Fe4 Priority

Example: get gi1 priority

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe4/priority
```

Reply

```
{"priority":"normal","success":"true","getAt":"2012-11-08 09:39:52"}
```

Set Fe4 Rate Limit

Example: set fe4 rate limit to unknown-unicast

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"rateLim"
: "set unknown-unicast 100"}' https://10.140.44.134/api/1.0/eth/fe4/rateLim
```

Reply

```
{"success":"true","updatedAt":"2012-11-21 06:43:28"}
```

Parameter restrictions

Only none and set broadcast/unknown-unicast/both [1-100] are valid parameters.

Get Fe4 Rate Limit

Example: get fe4 rate limit

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe4/rateLim
```

Reply

```
{"rateLim":"set unknown-unicast 100","success":"true","getAt":"2012-11-09 03:21:16"}
```

Set Fe4 Speed

Example: set fe4 rate limit to unknown-unicast

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"speed" :
"auto"}' https://10.140.44.134/api/1.0/eth/fe4/speed
```

Reply

```
{"success":"true","updatedAt":"2012-11-08 09:37:31"}
```

Parameter restrictions

Only auto, 10, 100, and 1000 are valid parameters.

Get Fe4 Speed

Example: get fe4 rate limit

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe4/speed
```

Reply

```
{"speed":"auto","success":"true","getAt":"2012-11-14 07:03:00"}
```

Set Fe4 Duplex

Example: set fe4 duplex to auto

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"duplex"
: "auto"}' https://10.140.44.134/api/1.0/eth/fe4/duplex
```

Reply

```
{"success":"true","updatedAt":"2012-11-08 09:37:31"}
```

Parameter restrictions

Only auto, full, and half are valid parameters.

Get Fe4 Duplex

Example: get fe4 rate limit

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe4/duplex
```

Reply

```
{"duplex":"auto","success":"true","getAt":"2012-11-15 01:18:14"}
```

Set Fe4 Information

Example: set fe4 rate limit to unknown-unicast, to pause to off

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"rateLim"
: "set unknown-unicast 100","duplex":"auto"}' https://10.140.44.134/api/1.0/eth/fe4
```

Reply

```
{"success":"true","updatedAt":"2012-11-08 09:37:31"}
```

Parameter restrictions

Only none and set broadcast/unknown-unicast/both [1-100] are valid parameters.

Get Fe4 Information

Example: get fe4 information

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/eth/fe4
```

Reply

```
{"status":"disable","oqs":"wrr","priority":"normal","rateLim":"set unknown-unicast
100","speed":"auto","duplex":"auto","success":"true","getAt":"2012-11-21 06:47:52"}
```

Issue a Command

> ✎
> **Note**   Curl is used as a sample tool to request APIs. 10.140.44.134 is used as a sample IP address of the Cisco Edge 300 series switch, and cisco123! is used as a sample admin password.

Reboot Cisco Edge 300

Example: reboot Cisco Edge 300

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/cmd/reboot
```

Reply

```
{"reboot":"true","success":"true","getAt":"2012-11-12 05:10:43"}
```

Image Version Information

> ✎
> **Note**   Curl is used as a sample tool to request APIs. 10.140.44.134 is used as a sample IP address of the Cisco Edge 300 series switch, and cisco123! is used as a sample admin password.

Get OS Version Information

Example: get os version information

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/image/os
```

Reply

```
{"os":"1.3.9.1","success":"true","getAt":"2012-11-12 05:51:56"}
```

Get 3rd App Version Information

Example: get 3rd app version information

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/image/3rdapp
```

Reply

```
{"3rdapp":"1.3.9.1","success":"true","getAt":"2012-11-12 05:56:39"}
```

Get OS and 3rd App Version in One Go

Example: get os and 3rdapp version information in one go

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/image
```

Reply

```
{"os":"1.3.9.1","3rdapp":"1.3.9.1","success":"true","getAt":"2012-11-12 08:18:58"}
```

AP Information

Note   Curl is used as a sample tool to request APIs. 10.140.44.134 is used as a sample IP address of the Cisco Edge 300 series switch, and cisco123! is used as a sample admin password.

Set AP SSID

Example: set SSID to cisco

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"ssid" :
"cisco"}' https://10.140.44.134/api/1.0/wifi/ap/ssid
```

Reply

```
{"success":"true","updatedAt":"2012-11-12 06:25:47"}
```

Parameter restrictions

The length of AP SSID should be between 1 to 32 characters and the valid parameter set is {a-zA-Z0-9-_} or 004 error is reported.

Get AP SSID

Example: get SSID

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/wifi/ap/ssid
```

Reply

```
{"ssid":"abc","success":"true","getAt":"2012-11-12 06:22:54"}
```

Set AP Radio

Example: set AP radio to off

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"radio" : "off"}' https://10.140.44.134/api/1.0/wifi/ap/radio
```

Reply

```
{"success":"true","updatedAt":"2012-11-12 06:34:20"}
```

Parameter restrictions

Only on and off are valid parameters or 004 error is reported.

Get Radio Status

Example: get radio status

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/wifi/ap/radio
```

Reply

```
{"radio":"on","success":"true","getAt":"2012-11-12 06:33:20"}
```

Set Wireless Mode

Example: set wireless mode to 9

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"wirelessMode" : "7"}' https://10.140.44.134/api/1.0/wifi/ap/wirelessMode
```

Reply

```
{"success":"true","updatedAt":"2012-11-12 07:25:00"}
```

Parameter restrictions

Only 0, 1, 4, 6, 7, and 9 are valid parameters or 004 error is reported.

Get Wireless Mode

Example: get wireless mode

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/wifi/ap/wirelessMode
```

Reply

```
{"wirelessMode":"9","success":"true","getAt":"2012-11-12 07:23:22"}
```

Set Channel Number

Example: set channel number to 9

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"channelNumber" : "9"}' https://10.140.44.134/api/1.0/wifi/ap/channelNumber
```

Reply

```
{"success":"true","updatedAt":"2012-11-12 07:32:04"}
```

Parameter restrictions

Only 0–14 integers are valid parameters or 004 error is reported.

Get Channel Number

Example: get channel number

Request

```
curl -k -X GET -H 'password: cisco123!'
https://10.140.44.134/api/1.0/wifi/ap/channelNumber
```

Reply

```
{"channelNumber":"6","success":"true","getAt":"2012-11-12 07:29:41"}
```

Set Channel Allocation

Example: set channel allocation to china

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"channelAllocation" : "4"}' https://10.140.44.134/api/1.0/wifi/ap/channelAllocation
```

Reply

```
{"success":"true","updatedAt":"2012-11-12 07:32:04"}
```

Parameter restrictions

Only 1–4 integers are valid parameters or 004 error is reported.

Get Channel Allocation

Example: get channel allocation

Request

```
curl -k -X GET -H 'password: cisco123!'
https://10.140.44.134/api/1.0/wifi/ap/channelAllocation
```

Reply

```
{"channelNumber":"6","success":"true","getAt":"2012-11-12 07:29:41"}
```

Set Channel Bandwidth

Example: set channel bandwidth to 20

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"channelBandwidth" : "20"}' https://10.140.44.134/api/1.0/wifi/ap/channelBandwidth
```

Reply

```
{"success":"true","updatedAt":"2012-11-12 07:32:04"}
```

Parameter restrictions

Only 20 and 20/40 are valid parameters or 004 error is reported.

Get Channel Bandwidth

Example: get channel bandwidth

Request

```
curl -k -X GET -H 'password: cisco123!'
https://10.140.44.134/api/1.0/wifi/ap/channelBandwidth
```

Reply

```
{"channelNumber":"6","success":"true","getAt":"2012-11-12 07:29:41"}
```

Set Transmit Power

Example: set transmit power to 50

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"transmitPower" : "50"}' https://10.140.44.134/api/1.0/wifi/ap/transmitPower
```

Reply

```
{"success":"true","updatedAt":"2012-11-12 07:49:35"}
```

Parameter restrictions

Only 1–100 integers are valid parameters or 004 error is reported.

Get Transmit Power

Example: get transmit power

Request

```
curl -k -X GET -H 'password: cisco123!'
https://10.140.44.134/api/1.0/wifi/ap/transmitPower
```

Reply

```
{"transmitPower":"100","success":"true","getAt":"2012-11-12 07:48:15"}
```

Set MCS

Example: set mcs to 15

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"mcs" :
"15"}' https://10.140.44.134/api/1.0/wifi/ap/mcs
```

Reply

```
{"success":"true","updatedAt":"2012-11-12 07:49:35"}
```

Parameter restrictions

Only 0–15 and 33 integers are valid parameters or 004 error is reported.

Get MCS

Example: get mcs

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/wifi/ap/mcs
```

Reply

```
{"mcs":"33","success":"true","getAt":"2012-11-12 07:57:08"}
```

Set IGMP Snoop

Example: set igmp snoop to on

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"igmpSnoop" : "on"}' https://10.140.44.134/api/1.0/wifi/ap/igmpSnoop
```

Reply

```
{"success":"true","updatedAt":"2012-11-12 08:08:05"}
```

Parameter restrictions

Only on and off are valid parameters or 004 error is reported.

Get IGMP Snoop

Example: get igmp snoop

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/wifi/ap/igmpSnoop
```

Reply

```
{"igmpSnoop":"off","success":"true","getAt":"2012-11-12 08:06:44"}
```

Set Encription

Example 1: set encryption mode to open and type to none

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"mode" :
"open","type":"none"}' https://10.140.44.134/api/1.0/wifi/ap/encryption
```

Reply

```
{"success":"true","updatedAt":"2012-11-12 08:08:05"}
```

Example 2: set encryption mode to open, type to wep, key number to 1, key type to ASCII, key value to cisco

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"mode" :
"open","type":"wep","keyNum":"1","keyType":"ascii","key":"cisco"}'
https://10.140.44.134/api/1.0/wifi/ap/encryption
```

Reply

```
{"success":"true","updatedAt":"2012-11-12 08:08:05"}
```

Parameter restrictions

The following are the commands on Cisco Edge 300:

```
encryption mode open type none
encryption mode open type wep key [1-4] [ascii|hex] [key]
```

When the mode is open, only none and wep are valid types.

When you use the none type, you must not specify any other parameters.

When you use the wep type, you must specify the key number, key type, and key.

Key number: 1–4

Key type: ASCII or hex

When the key type is ASCII, {a-zA-Z0-9-_} is the valid character set, and the length must be 5 or 13.

When the key type is hex, {a-f0-9} is the valid character set, and the length must be 10 or 26.

Example 3: set encryption mode to shared, type to wep, key number to 1, key type to ASCII, key value to cisco

Request
```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"mode" :
"shared","type":"wep","keyNum":"1","keyType":"ascii","key":"cisco"}'
https://10.140.44.134/api/1.0/wifi/ap/encryption
```

Reply
```
{"success":"true","updatedAt":"2012-11-12 08:08:05"}
```

Parameter restrictions

The following is the command on Cisco Edge 300:
```
encryption mode shared type wep key  [1-4] [ascii|hex] [key]
```

When you use the shared mode, you must specify other 4 parameters:

Key type: must be wep

Key number: 1–4

Key type: ASCII or hex

When the key type is ASCII, {a-zA-Z0-9-_} is the valid character set, and the length must be 5 or 13.

When the key type is hex, {a-f0-9} is the valid character set, and the length must be 10 or 26.

Example 4: set encryption mode to wpa and key type to aes

Request
```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"mode":"wpa", "type":"aes"}' https://10.140.44.134/api/1.0/wifi/ap/encryption
Reply{"success":"true","updatedAt":"2012-11-12 08:08:05"}
```

Parameter restrictions

The following is the command on Cisco Edge 300:
```
encryption mode wpa type [tkip|aes|tkipaes]
```

When you use wpa mode, you must specify type as following:

type: must be tkip, aes, or tkipaes

Example 5: set encryption mode to wpa and key type to aes

Request
```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"mode":"wpa", "type":"aes"}' https://10.140.44.134/api/1.0/wifi/ap/encryption
```

Reply
```
{"success":"true","updatedAt":"2012-11-12 08:08:05"}
```

Parameter restrictions

The following is the command on Cisco Edge 300:

```
encryption mode [wpa|wpa2|wpa1wpa2] type [tkip|aes|tkipaes]
```

When you use wpa, wpa2, or wpa1wpa2 mode, you must specify type as following:

type: must be tkip, aes, or tkipaes

Example 6: set encryption mode to wpapsk and key type to tkipaes

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"mode":"wpapsk", "type":"tkipaes", "passPhrase":"cisco12345"}'
https://10.140.44.134/api/1.0/wifi/ap/encryption
```

Reply

```
{"success":"true","updatedAt":"2012-11-12 08:08:05"}
```

Parameter restrictions

The following is the command on Cisco Edge 300:

```
encryption mode [wpapsk|wpa2psk|wpapskwpa2psk] type [tkip|aes|tkipaes] pass-phrase [key]
```

When you use wpapsk, wpa2psk, or wpapskwpa2psk mode, you must specify type as following:

type: must be tkip, aes, or tkipaes,

pass phase: The valid character set for passphase is {0-9a-zA-Z_-}, and the length is between 8 and 63.

Set Radius Server

Example 1: set RADIUS server host to 1.1.1.1, auth-port to 444, and key to cisco123

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"host":"1.1.1.1", "auth-port":"444", "key":"cisco123"}'
https://10.140.44.134/api/1.0/wifi/ap/radius
```

Reply

```
{"success":"true","updatedAt":"2012-11-12 08:08:05"}
```

Parameter restrictions

host: mandatory parameter. You must enter a valid IPv4 address.

auth-port: optional parameter. You must enter a number range between 0 and 65535.

key: optional parameter. The valid character set is {0-9 a-z A-Z _-`~!@#$%^*()+:,<>./[]{}&}

Get Radius Server

Example: get RADIUS server

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/wifi/ap/radius
```

Reply

```
{"host_1":"1.1.1.1","auth-port_1":"444","key_1":"cisco123","host_2":"2.2.2.2","key_2":"2.2
.2.2","host_3":"3.3.3.3","auth-port_3":"1234","key_3":"cisco","success":"true","getAt":"20
12-11-14 06:35:30"}
```

Set AP Information

Example: set AP SSID to cisco and RADIUS server to "{"host":"1.1.1.1", "auth-port":"555", "key":"cisco123"}"

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"ssid":"cisco","radius":{"host":"1.1.1.1", "auth-port":"555", "key":"cisco123"}}'
https://10.140.44.134/api/1.0/wifi/ap/
```

Reply

```
{"success":"true","updatedAt":"2012-11-19 02:46:54"}
```

Get AP Information

Example: get AP information

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.134/api/1.0/wifi/ap
```

Reply

```
{"channelAllocation":"3","igmpSnoop":"off","radio":"off","wirelessMode":"7","channelBandwi
dth":"20","mcs":"15","radius":{"host_1":"1.1.1.1","auth-port_1":"555","key_1":"cisco123"},
"channelNumber":"9","multicastMcs":"15","ssid":"cisco","encryption":{"mode":"wpa2psk","key
Type":"tkipaes","key":"Cisco123"},"transmitPower":"50","success":"true","getAt":"2012-11-1
9 02:56:25"}
```

Wifi Client Information

Note Curl is used as a sample tool to request APIs. 10.140.44.134 is used as a sample IP address of the Cisco Edge 300 series switch, and cisco123! is used as a sample admin password.

Note Assume that the WiFi client IP address is 10.140.44.148.

Get ID of a Network

Example: get a new network ID

Request

```
curl -k -X GET -H 'password: cisco123!'
https://10.140.44.148/api/1.0/wifi/client/new_network_id
```

Reply

```
{"new_network_id":"3","success":"true","getAt":"2011-04-21 04:26:46"}
```

Get SSID of a Network

Example: get SSID of network 0

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.148/api/1.0/wifi/client/0/ssid
```

Reply

```
{"ssid":"blizzard","success":"true","getAt":"2011-04-21 04:09:14"}
```

Parameter restrictions

The length of parameter should be less than 33 characters or 004 error is reported.

Set SSID of a Network

Example: set an SSID of network 0 to Cisco Edge 300

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d '{"ssid" :
"blizzard_2"}' https://10.140.44.148/api/1.0/wifi/client/0/ssid
```

Reply

```
{"ssid":"blizzard","success":"true","getAt":"2011-04-21 05:07:50"}
```

Get an SSID Scan Status of a Network

Example: check SSID scan status of network 0

Request

```
curl -k -X GET -H 'password: cisco123!'
https://10.140.44.148/api/1.0/wifi/client/0/scan_ssid
```

Reply

```
{"scan_ssid":"0","success":"true","getAt":"2011-04-21 04:20:36"}
```

Set SSID Scan of a Network

Example: set an SSID scan of network 1

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"scan_ssid":"1"}' https://10.140.44.148/api/1.0/wifi/client/0/scan_ssid
```

Reply

```
{"success":"true","updatedAt":"2011-04-21 06:13:49"}
```

Parameter restrictions

Only 0 and 1 are valid parameters or 004 error is reported.

Get Key Management Type of a Network

Example: get key management type of network 0

Request

```
curl -k -X GET -H 'password: cisco123!'
https://10.140.44.148/api/1.0/wifi/client/0/key_mgmt
```

Reply

```
{"key_mgmt":"WPA-EAP","success":"true","getAt":"2011-04-21 04:22:47"}
```

Set Key Management Type of a Network

Example: set key management type of a network to WPA-EAP

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"key_mgmt":"WPA-EAP"}' https://10.140.44.148/api/1.0/wifi/client/0/key_mgmt
```

Reply

```
{"success":"true","updatedAt":"2011-04-21 06:13:49"}
```

Parameter restrictions

Only WPA-PSK, WPA-EAP, and None are valid parameters or 004 error is reported.

Get Pairwise Type of a Network

Example: get pairwise type of network

Request

```
curl -k -X GET -H 'password: cisco123!'
https://10.140.44.148/api/1.0/wifi/client/0/pairwise
```

Reply

```
{"pairwise":"CCMP","success":"true","getAt":"2011-04-21 04:27:17"}
```

Set Pairwise Type of a Network

Example: set pairwise type of a network to CCMP

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"pairwise":"CCMP"}' https://10.140.44.148/api/1.0/wifi/client/0/pairwise
```

Reply

```
{"success":"true","updatedAt":"2011-04-21 06:13:49"}
```

Parameter restrictions

Only CCMP and TKIP are valid parameters or 004 error is reported.

Get Group of a Network

Example: get group of network 0

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.148/api/1.0/wifi/client/0/group
```

Reply

```
{"group":"CCMP TKIP WEP104 WEP40","success":"true","getAt":"2011-04-21 04:29:11"}
```

Set Group of a Network

Example: set group of a network to CCMP TKIP WEP104 WEP40

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"group":"CCMP"}' https://10.140.44.148/api/1.0/wifi/client/0/group
```

Reply

```
{"success":"true","updatedAt":"2011-04-21 06:13:49"}
```

Parameter restrictions

Only CCMP, TKIP, WEP104, and WEP40 are valid parameters or 004 error is reported.

Get PSK of a Network

Example: get psk of network 0

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.148/api/1.0/wifi/client/0/psk
```

Reply

```
{"psk":"*","success":"true","getAt":"2011-04-21 04:33:16"}
```

> ✎
>
> **Note**   If PSK is not set, the return value is FAIL. If it is set, the return value is *.

Set PSK of a Network

Example: set psk of a network to cisco

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"psk":"cisco"}' https://10.140.44.148/api/1.0/wifi/client/0/psk
```

Reply

```
{"success":"true","updatedAt":"2011-04-21 06:13:49"}
```

Parameter restrictions

The PSK parameter must be a string includes 0-9,a-z,A-Z _- and the length should be 8–63.

Get wep_key0 of a Network

Example: get wep_key0 of network 0

Request

```
curl -k -X GET -H 'password: cisco123!'
https://10.140.44.148/api/1.0/wifi/client/0/wep_key0
```

Reply

```
{"wep_key0":"*","success":"true","getAt":"2011-04-21 04:37:46"}
```

> ✎
>
> **Note**   The wep_key0 is in cipher text to protect private information of customer.

Set wep_key0 of a Network

Example 1: set wep_key0 of network 0 to cisco

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"wep_key0":"cisco"}' https://10.140.44.148/api/1.0/wifi/client/0/wep_key0
```

Reply

```
{"success":"true","updatedAt":"2011-04-21 06:13:49"}
```

Example 2: set wep_key0 of network 0 to 01234567890

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"wep_key0":"0x123456789a"}' https://10.140.44.148/api/1.0/wifi/client/0/wep_key0
```

Reply

```
{"success":"true","updatedAt":"2011-04-21 04:11:51"}
```

Parameter restrictions

Parameter length should be 5 or 13 in ASCII or 10 or 26 in hex digit. If the parameter is in hex digit, it must have a prefix of 0x (The prefix length is not counted). Or 004 error is reported.

Get wep_key1 of a Network

Example: get wep_key1 of network 0

Request

```
curl -k -X GET -H 'password: cisco123!'
https://10.140.44.148/api/1.0/wifi/client/0/wep_key1
```

Reply

```
{"wep_key1":"*","success":"true","getAt":"2011-04-21 04:37:46"}
```

Note   The wep_key1 is in cipher text to protect private information of customer.

Set wep_key1 of a Network

Example 1: set wep_key1 of network 0 to cisco

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"wep_key1":"cisco"}' https://10.140.44.148/api/1.0/wifi/client/0/wep_key1
```

Reply

```
{"success":"true","updatedAt":"2011-04-21 06:13:49"}
```

Example 2: set wep_key1 of network 0 to 01234567890

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"wep_key1":"0x123456789a"}' https://10.140.44.148/api/1.0/wifi/client/0/wep_key1
```

Reply

```
{"success":"true","updatedAt":"2011-04-21 04:11:51"}
```

Parameter restrictions

Parameter length should be 5 or 13 in ASCII or 10 or 26 in hex digit. If the parameter is in hex digit, it must have a prefix of 0x (The prefix length is not counted). Or 004 error is reported.

Get wep_key2 of a Network

Example: get wep_key2 of network 0

Request

```
curl -k -X GET -H 'password: cisco123!'
https://10.140.44.148/api/1.0/wifi/client/0/wep_key2
```

Reply

```
{"wep_key2":"*","success":"true","getAt":"2011-04-21 04:37:46"}
```

✎

Note   The wep_key2 is in cipher text to protect private information of customer.

Set wep_key2 of a Network

Example 1: set wep_key2 of network 0 to cisco

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"wep_key2":"cisco"}' https://10.140.44.148/api/1.0/wifi/client/0/wep_key2
```

Reply

```
{"success":"true","updatedAt":"2011-04-21 06:13:49"}
```

Example 2: set wep_key2 of network 0 to 01234567890

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"wep_key2":"0x123456789a"}' https://10.140.44.148/api/1.0/wifi/client/0/wep_key2
```

Reply

```
{"success":"true","updatedAt":"2011-04-21 04:11:51"}
```

Parameter restrictions

Parameter length should be 5 or 13 in ASCII or 10 or 26 in hex digit. If the parameter is in hex digit, it must have a prefix of 0x (The prefix length is not counted). Or 004 error is reported.

Get wep_key3 of a Network

Example: get wep_key3 of network 0

Request

```
curl -k -X GET -H 'password: cisco123!'
https://10.140.44.148/api/1.0/wifi/client/0/wep_key3
```

Reply

```
{"wep_key3":"*","success":"true","getAt":"2011-04-21 04:37:46"}
```

✎

Note   The wep_key3 is in cipher text to protect the private information of customer.

Set wep_key3 of a Network

Example 1: set wep_key3 of network 0 to cisco

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"wep_key3":"cisco"}' https://10.140.44.148/api/1.0/wifi/client/0/wep_key3
```

Reply

```
{"success":"true","updatedAt":"2011-04-21 06:13:49"}
```

Example 2: set wep_key3 of network 0 to 01234567890

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"wep_key3":"0x123456789a"}' https://10.140.44.148/api/1.0/wifi/client/0/wep_key3
```

Reply

```
{"success":"true","updatedAt":"2011-04-21 04:11:51"}
```

Parameter restrictions

Parameter length should be 5 or 13 in ASCII or 10 or 26 in hex digit. If the parameter is in hex digit, it must have a prefix of 0x (The prefix length is not counted). Or 004 error is reported.

Get EAP Type of a Network

Example: get EAP type of network 0

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.148/api/1.0/wifi/client/0/eap
```

Reply

```
{"eap":"PEAP","success":"true","getAt":"2011-04-21 04:38:13"}
```

Set EAP Type of a Network

Example: set EAP type of network 0 to PEAP

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"eap":"PEAP"}' https://10.140.44.148/api/1.0/wifi/client/0/eap
```

Reply

```
{"success":"true","updatedAt":"2011-04-21 06:13:49"}
```

Parameter restrictions

Only MSCHAPV2, TLS, PEAP, TTLS, FAST, and LEAP are valid parameters or 004 error is reported.

Get EAP Identity String of a Network

Example: get EAP identity string of network 0

Request

```
curl -k -X GET -H 'password: cisco123!'
https://10.140.44.148/api/1.0/wifi/client/0/identity
```

Reply

```
{"identity":"ce300","success":"true","getAt":"2011-04-21 04:43:04"}
```

Set EAP Identity String of a Network

Example: set EAP identity string of network 0 to ce300

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"identity":"ce300"}' https://10.140.44.148/api/1.0/wifi/client/0/identity
```

Reply

```
{"success":"true","updatedAt":"2011-04-21 06:13:49"}
```

Get Password of a Network

Example: get EAP password of network 0

Request

```
curl -k -X GET -H 'password: cisco123!'
https://10.140.44.148/api/1.0/wifi/client/0/password
```

Reply

```
{"password":"*","success":"true","getAt":"2011-04-21 04:49:46"}
```

✎

Note   The password is encrypted, which is shown as *.

Set Password of a Network

Example: set password of network 0 to ce300

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"password":"ce300"}' https://10.140.44.148/api/1.0/wifi/client/0/password
```

Reply

```
{"success":"true","updatedAt":"2011-04-21 06:13:49"}
```

Set the Status of a Network

Example: set the status of network 0 to enable

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"status":"enable"}' https://10.140.44.148/api/1.0/wifi/client/0/stauts
```

Reply

```
{"success":"true","updatedAt":"2011-04-21 06:13:49"}
```

Parameter restrictions

Only enable and disable are valid parameters or 004 error is reported.

Remove a Network

Example: remove network 0

Request

```
curl -k -X DELETE -m 10 -H 'password: cisco123!' -H 'Content-Type: application/json'
https://10.140.44.148/api/1.0/wifi/client/0
```

Reply

```
{"success":"true","updatedAt":"2011-04-21 06:13:49"}
```

Note The parameter –m sets the maximum time in seconds that the whole operation is allowed to take, which in this example is 10 seconds. If there is only one network on ce300, the remove operation will disconnect it from network. Therefore, if –m is not set, the request is holding.

Save the Network Configuration

Example: save the network configuration

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.148/api/1.0/wifi/client/saving
```

Reply

```
{"saving":"OK","success":"true","getAt":"2011-04-21 04:20:33"}
```

Show Connection Status

Example: show connection status

Request

```
curl -k -X GET -H 'password: cisco123!' https://10.140.44.148/api/1.0/wifi/client/
```

Reply

```
{"conn_status":"bssid=a4:56:30:5d:e1:d0\nssid=blizzard\nid=0\nmode=station\npairwise_ciphe
r=CCMP\ngroup_cipher=CCMP\nkey_mgmt=WPA2\/IEEE
802.1X\/EAP\nwpa_state=COMPLETED\nip_address=10.140.44.148\naddress=1c:aa:07:97:a3:c8\nSup
plicant PAE state=AUTHENTICATED\nsuppPortStatus=Authorized\nEAP
state=SUCCESS\nselectedMethod=25 (EAP-PEAP)\nEAP TLS cipher=AES256-SHA\nEAP-PEAPv1 Phase2
method=GTC\n","success":"true","getAt":"2011-04-21 04:56:29"}
```

Reload the Saved Configuration

Example: reload the saved configuration

Request

```
curl -k -X GET -H 'password: cisco123!'
https://10.140.44.148/api/1.0/wifi/client/reconfiguration
```

Reply

```
{"reconfiguration":"OK","success":"true","getAt":"2011-04-21 04:58:15"}
```

Export Configuration File

Example: export wifi-network-only configuration file to /tmp

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"type":"wifi-network-only","destination":"/tmp"}'
https://10.140.44.148/api/1.0/configuration/export
```

Reply

```
{"success":"true","updatedAt":"2011-04-21 05:12:11"}
```

Parameter restrictions

The type field can be wifi-network-only, overall, and startup-config. The destination field can be any string that contains 0-9 A-Z a-z.

Import Configuration File

Example: import wifi-network-only configuration file from /tmp

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"type":"wifi-network-only","source":"/abc"}'
https://10.140.44.148/api/1.0/configuration/import
```

Reply

```
{"success":"true","updatedAt":"2011-04-21 06:49:02"}
```

Parameter restrictions

The type field can be wifi-network-only, overall, and startup-config. The source field can be any string containing 0-9 A-Z a-z.

RS232 Configuration

✎
Note   Curl is used as a sample tool to request APIs. 10.140.44.134 is used as a sample IP address of the Cisco Edge 300 series switch, and cisco123! is used as a sample admin password.

Configure RS232

Example: configure RS-232 with the device name of /dev/ttyS0, baud rate of 9600, data rates of 8, stop bits of 1, parity of none, hex command of 123456

Request

```
curl -k -X PUT -H 'password: cisco123!' -H 'Content-Type: application/json' -d
'{"device":"/dev/ttyS0","data_rate":"9600","data_bits":"8","stop_bits":"1","parity_bits":"
n","command":"123456"}' https://64.104.163.36/api/1.0/rs232/configuration
```

Reply

```
{"success":"true","updatedAt":"2011-04-21 07:11:28"}
```

Parameter restrictions

The device parameter should be a string started with /dev/.

The data_rate parameter should be a string in the set {50, 75, 110, 134, 150, 200, 300, 600, 1200, 1800, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400, 460800, 500000, 576000}.

The data_bits parameter should be 7 or 8.

The stop_bits parameter should be 1 or 2.

The parity_bits parameter should be n, o, and e.

Upgrade

✎
Note   Curl is used as a sample tool to request APIs. 10.140.44.134 is used as a sample IP address of the Cisco Edge 300 series switch, and cisco123! is used as a sample admin password.

Upgrade an Image

Example: upgrade an image using smi_local

Request

```
curl -k -X PUT -H 'password: cisco' -H 'Content-Type: application/json' -d
'{"protocol":"nfs","url":"64.104.169.66:/home/","path":"/1.5rb1/","version":"1.5rb1","upgr
ade-fm":"on","upgrade-os":"off","upgrade-apps":"off","force-upgrade":"on","clear-config":"
off"}' https://64.104.169.70/api/1.0/upgrade/images
```

Reply

```
{"success":"true","updatedAt":"2011-04-21 07:11:28"}
```

Parameter restrictions

- version—The package version, which supports 1.5rb1 or above.

- protocol—The protocol to get a delivery image (http/https/ftp/udisk/nfs/cifs).

- url—The parent folder URL of the delivery image. The '/' at the end of the URL is necessary.

- path—For nfs/cifs/udisk, if the image is not in the top directory, it can be used to specified the sub-directory path.

- upgrade-fm—Valid value is on or off. Specify whether to upgrade factory or not.

- upgrade-os—Valid value is on or off. Specify whether to upgrade OS or not.

- upgrade-apps—Valid value is on or off. Specify whether to upgrade Cisco apps or not.

- force-upgrade—Valid value is on or off. Specify whether to compare versions between image and current system.

- username—User name for HTTP, FTP, or CIFS.

- password—Password for HTTP, FTP, or CIFS.

- clear-config—Valid value is on or off, while on means to clear config of smi_local; otherwise it should be off.

Pre-condition

Have super-user privileges when you perform the upgrade operation.

Error Codes

Table 6-1   Error Codes and Desctiptions

Error Code	Description
001	Invalid password
002	Content type error
003	The HTTP method used is not supported for this resource
004	Illegal parameter
005	Error is found when the commands are executed
006	Invalid resource
101	Json: maximum stack depth exceeded
102	Json: underflow or the modes mismatch
103	Json: unexpected control character found

Table 6-1   Error Codes and Desctiptions

Error Code	Description
104	Json: syntax error, malformed JSON
105	Json: malformed UTF-8 characters, possibly incorrectly encoded
106	Json: unknown error

APPENDIX **A**

Installing Third-Party Applications from the SMI Server

The Cisco Edge 300 series switch supports the installation of third-party applications from the Smart Install (SMI) server.

The original Cisco Edge 300 series switch package released by Cisco contains a default third-party application package, which includes Open Office and Chrome browser. You can modify the third-party application contents and repackage it, so that you can install partner applications into Cisco Edge 300 from the SMI server.

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
```

Installing a Third-Party Application Package

To generate the SMI third-party application package, following these steps.

Step 1 Use the following contents to create a header file under ${RELEASE_DEST} for the third-party application, with the file name **3rd.header**:

> ✎
>
> **Note** ${RELEASE_DEST} could be any place that you have write permission on the Linux machine.

```
IMAGE_TYPE=3RD_APP
IMAGE_VERSION=RELEASEVERSION
IMAGE_SIZE=RELEASESIZEK
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=image/Partner/3rd-app-sunbird-RELEASEVERSION.tar.gz
```

Step 2   Use the command **tar -zcvf 3rd-app.tar.gz** to create a 3rd-app.tar.gz file under ${RELEASE_DEST} from Cisco-provided SDK. This file contains the applications to be installed.

You also need two scripts, pre_install.sh and startup.sh, which are optional files with execution permission.

a.   When SMI downloads a third-party application, it executes pre_install.sh first, by which the tasks drafted in the script, such as configuring application environment and deleting old files, can be done before package extraction.

b.   SMI extracts the package to the target path.

c.   SMI executes post_install.sh to wrap the package off. You add commands that can clean up temporary files or create desktop icon in this script.

You need a pre_install.sh script for each third-party application package, and a startup.sh script for each application folder in it. The package structure of a third-party application looks like:

```
- 3rd-app.tar.gz
   - pre_install.sh
   - {YOUR_APP_FOLDER}
      - startup.sh
      - ......
   -......
```

Step 3   Use the following script to generate a 3rd-app-sunbird-${RELEASE_VERSION}.tar.gz file.

```
cd ${RELEASE_DEST}
RELEASE_VERSION=1.5.1 #<-- please change the version as you wish, 1.5.1 Here is an
example.
APP_SIZE=`du -k 3rd-app.tar.gz | awk '{print $1}'`
mv 3rd-app.tar.gz 3rd-app-sunbird-${RELEASE_VERSION}.tar.gz
#Generate 3rd-app md5 checksum
mkdir header
openssl dgst -md5 3rd-app-sunbird-${RELEASE_VERSION}.tar.gz > header/md5.txt
#Generate a header file according to template, version and size info.
APP_RELEASE_HEADER=3rd-app-sunbird-${RELEASE_VERSION}-delivery.header
cp 3rd.header header/3rd-app-sunbird-${RELEASE_VERSION}-delivery.header
cd header
sed -i "s@RELEASEVERSION@${RELEASE_VERSION}@g" ${APP_RELEASE_HEADER}
sed -i "s@RELEASESIZE@${APP_SIZE}@g" ${APP_RELEASE_HEADER}
cd ../
#Generate needed 3rd-app-sunbird-${RELEASE_VERSION}.tar.gz file
tar czvf 3rd-app-sunbird-${RELEASE_VERSION}-delivery.tar.gz
3rd-app-sunbird-${RELEASE_VERSION}.tar.gz header/${APP_RELEASE_HEADER} header/md5.txt
rm -rf header 3rd-app-sunbird-${RELEASE_VERSION}.tar.gz
```

Step 4   Put the 3rd-app-sunbird-${RELEASE_VERSION}.tar.gz file into the tftproot directory of the SMI server and install it. For detailed steps of the installation, see Chapter 2, "Configuring the Smart Install Network." The destination directory is /opt/Tftproot/image/Partner of the TFTP server.

APPENDIX B

Importing a Spreadsheet with Client Switch Information

The "Importing a List of Client Switches" section on page 2-18 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.

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 2-14.

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 -a 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 2-14.

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
```

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.

✎

Note   The Cisco Edge 300 series switch records all necessary information in the logging system with the syslog feature of Linux to an internal USB disk, and uploads the log to Smart Install server when its size is bigger than the threshold size.

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 1.5 to release 1.6, 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 2-25.

⚠

Caution   If the device was originally installed with software release 1.5 and higher, do not downgrade the software release to 1.4 or lower via USB manual upgrading. Otherwise, the device may be seriously damaged.

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 D-1   Cisco Edge 300 Series Switch
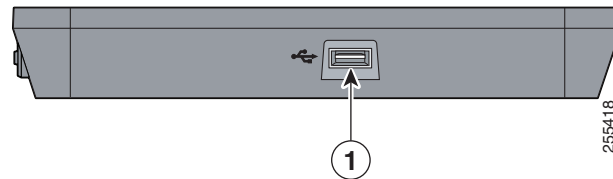
1	USB port

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.

> **Note**   When you are going to upgrade the system from release 1.x to release 1.6RB1_1 or release 1.6RB2, you can use only the Force Upgrade option.

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.

Force Upgrading the Software in Factory Mode

To force upgrade the software in factory mode, perform the following steps:

Step 1   Detach all the USB flash drivers on the Cisco Edge 300 Series switches if there are any.

Step 2   Plug in the USB flash drive at the USB port side of the Cisco Edge 300 Series switch.

Step 3   Make sure that the USB port you plug in is the only port at the side panel, not the front panel with a lot of ports.

Step 4   Press the Reset button for 4 seconds to enter factory mode.

Step 5   Wait for the system to reboot from the USB flash drive to upgrade.

Step 6   During the upgrade, the power LED will be green and be flashing. Wait about 10 minutes, the system will reboot with a new firmware installed. If the color of the power LED turns yellow, it indicates the upgrade failure.

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.