Configuring Local CLI - Clish

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.

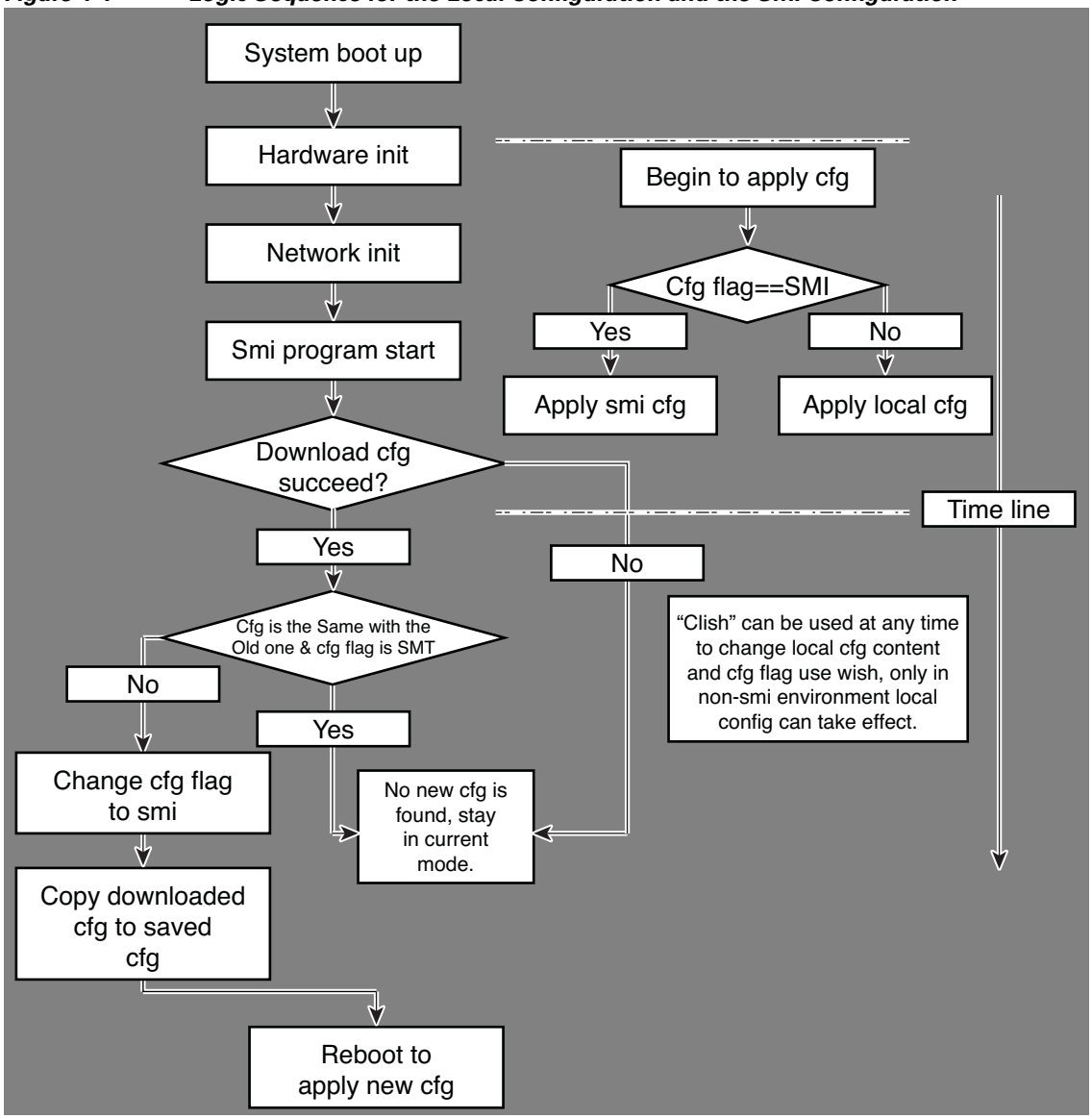
In release 1.2 and later, the Cisco Edge 300 series switch treats local configuration in two different ways based on the network status:

- 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

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

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

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.

Table 4-5 on page 4-86 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 aggregration if network traffic consists primarily of data.

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

radio

To turn the access point wireless radio on or off, use the **radio** 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.

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.