Cisco Edge 340 Series Software Configuration Guide, Release 1.0.5RB1

April 2, 2014

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.

Text Part Number: OL-29491-02

Cisco Edge 340 Series Software Configuration Guide, Release 1.0.5RB1

Preface

This document describes how to configure the Cisco Edge 340 Series in your network.

This guide does not describe how to install the Cisco Edge 340 Series. For information about how to install the Cisco Edge 340 Series, see the hardware installation guide pertaining to your device.

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 Edge 340 Series Installation Guide*
- *Release Notes for the Cisco Edge 340 Series*

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 340 Series Overview

Cisco Edge 340 Series Overview

Cisco Edge 340 Series is the next-generation device for vertical and enterprise-connected room deployments that provide rich media-enablement capabilities and vertical-specific application support. It integrates rich connectivity to enable all the essential components of a digital connected room experience with Ethernet LAN uplink, wireless access, rich media, and application computing. It is also an open application platform that allows you to customize it to enable vertical solutions.

Digital Media Player

The Cisco Edge 340 Series device functions as a next-generation digital media player for the following solutions:

- Digital media signage
- Sports and entertainment
- iServcies

In the digital media signage solution, the Cisco Edge 340 Series device acts as a Digital Media Player (DMP) to provide the functions of both video and audio player. Additionally, it also provides high computing capability and local storage for the content.

Application Support

The Cisco Edge 340 Series supports vertical applications and provides computing power, storage, and simple connectivity functions.

Home Automation Gateway

The Cisco Edge 340 Series functions as a home service gateway that is deployed at homes, sitting behind a residential gateway device, to provide home automation service through WiFi, to connect and control smart electric appliances.

Cisco Edge 340 Series Features and Application Support

The Cisco Edge 340 Series provides these features and application support:

- Video conference
- Video player
- Document viewer
- VLC player
- VPN client support
- SNMP support
- Screen capture

For detailed information about these features and applications, refer to *Release Notes for the Cisco Edge 340 Series* for your version.

Logging in to the System

To power on and log in to the Cisco Edge 340 Series system, follow these steps:

Step 1 Connect the power cord of the Cisco Edge 340 Series to an electrical outlet.

Step 2 Connect the monitor, keyboard, and mouse to the Cisco Edge 340 Series.

Step 3 Press the **Power** button to power on the Cisco Edge 340 Series. The following screen is displayed:

Figure 1-1 Log In Screen - User name

Step 4 Enter **user** in the Username field and click **Log In**. The following screen is displayed:

Figure 1-2 Log In Screen - User name

Step 5 Enter **User123!** in the Password field and click the **Log In** button to log in to the system.

Note Change the default password immediately after you have successfully logged in to the system.

Management and Configuration Support

The Cisco Edge 340 Series supports the following management and configuration methods:

- Local CLI—CLISH
- Web GUI

Local CLI—CLISH

You can use CLISH to configure the Cisco Edge 340 Series that is used for the local CLI configuration. The CLI uses only those commands that are specific to the Cisco Edge 340 Series. Although the syntax is similar to the Cisco IOS CLI, the commands are *incompatible* with Cisco IOS commands. For more information, see Chapter 2, "Configuring Local CLI - CLISH."

Web GUI

You can use the web GUI to configure the Cisco Edge 340 Series and monitor the status locally or remotely. For more information, see Chapter 3, "Configuring the Web GUI."

System Installation and Upgrade

The Cisco Edge 340 Series supports the following installation and upgrade types:

- USB Mode Installation and Upgrade
- Remote Upgrade

- BIOS Upgrade

USB Mode Installation and Upgrade

The Cisco Edge 340 Series software releases a self-extract installer. The file name is Cisco-Edge-*version*-i386-DVD.bin. It is an executive file that helps you to perform the installation automatically. When you execute the self-extract installer, the installation-related files are extracted to the hard drive of the Cisco Edge 340 Series, and a livecd is created in the internal USB. The system then boots from the internal USB (also known as the factory mode) and performs the installation automatically.

If the internal USB has already been created as a livecd, you can press the factory mode pinhole on the front panel of the Cisco Edge 340 Series to enter the factory mode and perform the installation procedure automatically.

Note Usually, the internal USB is created as a livecd in the factory. Executing the self-extract installer will overwrite the original livecd and create a new one.

Command Description

You can use the Cisco-Edge-*version*-i386-DVD.bin command with different parameters to implement installation or upgrade, print help, or create livecd only. In the command, *version* indicates the image version, which will be 1.0.5rb1 for this release. For the installation and upgrade of the releases higher than 1.0.5rb1, refer to the software configuration guide of corresponding releases.

Note When you use this method to install or upgrade the system, make sure there is 1.5G free space at least.

1. To select the internal USB as a livecd disk and then boot into factory mode to finish installation automatically, use the following command:

   ```
   Cisco-Edge-1.0.5rb1-i386-DVD.bin
   ```

2. To print help and then exit, use the following command:

   ```
   Cisco-Edge-1.0.5rb1-i386-DVD.bin  --help|-h
   ```

3. To create livecd only, without entering factory mode nor executing the system installation program, use the following command,:

   ```
   Cisco-Edge-1.0.5rb1-i386-DVD.bin <dev>
   ```

   <dev> is the full path of the target u-disk into which the livecd will be burned, for example, /dev/sdb1.

Remote Upgrade

You can perform a remote upgrade for the Cisco Edge 340 Series using the web GUI if you have the address to download the self-extract installer. When you choose to perform the remove upgrade, the system will automatically download the self-extract-installer from the URL that you provide and execute the self-extract-installer to finish the installation.

BIOS Upgrade

BIOS upgrade can only be performed by manually installing the package and executing the commands in the Linux environment. BIOS is a critical part of the system, and there is no software recovery method if it crashes. To ensure successful BIOS upgrade, make sure that the external power supply is always connected, and do *not* perform any power cycle action during the upgrade process.

Configuring Local CLI - CLISH

This chapter contains the following sections:

Configuration Guidelines

You can configure the Cisco Edge 340 Series in CLISH, which is used for the local CLI configuration. The CLI uses only those commands that are specific to the Cisco Edge 340 Series. Although the syntax is similar to the Cisco IOS CLI, these commands are *incompatible* with Cisco IOS commands.

You can use CLISH in two modes:

- User mode—When you log in to the Cisco Edge 340 Series as an ordinary user, you enter the user mode. To enter the privileged mode, enter the **enable** command and then enter the password of the root user.
- Global (privileged) mode—When you log in to the Cisco Edge 340 Series as root user, you enter the global mode directly and do not have to enter the **enable** command.

Use the CLI to configure these device settings:

- Basic device settings—Hostname, MAC address, bluetooth settings, password, Network Time Protocol (NTP) server, and device 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
- Service Set Identifier (SSID) security settings—Broadcast, authentication, and encryption

Follow these configuration guidelines when using CLISH:

- Enter **ssh** *username*@*ip-address* or **ssh root**@*ip-address* in the command prompt in your PC, and enter the password in the welcome screen. Enter the **mgtcmd** command to start the CLISH process.
- If you log in as an ordinary user, enter the **enable** command and the password of the root user to switch to the global mode.
- Start a Cisco Edge configuration with the **configure terminal** global command. End the Cisco Edge configuration file with the **exit** global command.

Note If you log in to the Cisco Edge 340 Series as ordinary user, and you want to enter CLISH as the root user, use the Linux command **su -**, where - means to switch ordinary user to root user, and use the environment variables of root. If more than 10 minutes passed by without any activity after you enter the privileged mode, you will exit the privileged mode automatically. Notice the prompt > and #; > means user mode, and # means privileged mode.

- 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 AP interface configuration mode

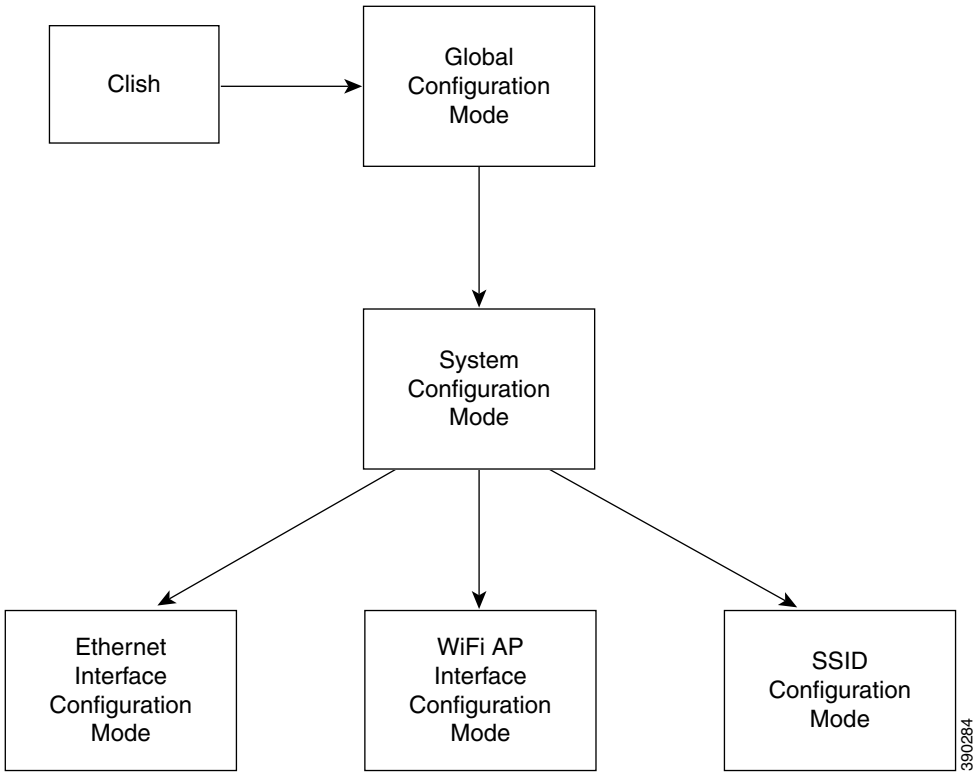
    Use the **interface** system configuration command to enter this mode. We recommend that before you configure any wireless settings, you use the **wireless-mode** WiFi configuration command to set the 802.11 wireless mode. Use the **exit** global configuration command to return to the system configuration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

Figure 2-1 shows the logic sequence of the CLISH functional structure.

Figure 2-1 Logic Sequence of the CLISH Functional Structure



Command Reference

This sections contains the commands of the following modes:

- User Configuration Mode Commands
- Global Configuration Mode Commands
- System Configuration Mode Commands
- Ethernet Interface Configuration Mode Commands
- WiFi AP Interface Configuration Mode Commands
- SSID Configuration Mode
- show Commands

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

User Configuration Mode Commands

This section contains user configuration mode commands. Table 2-1 describes the functions these commands perform.

Table 2-1 User Configuration Mode Commands

Command	Function
enable	Enters the global configuration mode.
exit	Exits from the CLI.
help	Shows the descriptions of the interactive help system.
ping	Diagnoses basic network connectivity, and verifies if the remote device is reachable.
show	Shows running system information.
traceroute	Prints the route packets trace to the network host.

enable

To enter the global configuration mode, use the **enable** command in the user configuration mode.

enable

Command Modes

User configuration

Usage Guidelines

Use the **enable** command and enter the password of the **root** user to switch to the global configuration mode.

exit

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

exit

Command Modes

User configuration
Global configuration
System configuration
Ethernet interface configuration
WiFi AP interface configuration
SSID configuration

Usage Guidelines

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

help

To display a brief description of the help system, use the **help** command in the user configuration mode.

help

Command Modes

User configuration

Global configuration

Usage Guidelines

The **help** command displays a list of available commands, along with a brief description of each. To display additional details for a specific command, enter the command name followed by the -? option.

ping

To diagnose basic network connectivity on a Cisco Edge 340 Series device, use the **ping** command in the user configuration mode or the global configuration mode.

ping {[**ip** | **ipv6** | **arp**] *hostname* | *ip_address*}

Syntax Description

ip	Sends Internet Control Message Protocol (ICMP) IPv4 messages to network hosts (default).
ipv6	Sends ICMP IPv6 messages to network hosts.
arp	Sends ARP requests to neighbor hosts.
hostname	Hostname to ping.
ip_address	IP address to ping.

Command Modes

User configuration

Global configuration

Usage Guidelines

The **ping** command sends an echo request packet to an address then waits for a reply. Ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning.

traceroute

To discover the routes that packets will pass through when traveling to their destination address, use the **traceroute** command in the user configuration mode or the global configuration mode.

traceroute [*protocol*] *destination* [[**resolve**] **source** *ip_address* | **interface** *interface_name*]

Syntax Description

protocol	(Optional) Protocol; either IP or IPv6. When not specified, the protocol argument is based on an examination of the destination format by the software. The default protocol is IP.
destination	The destination address or hostname of the route that you want to trace.
resolve	Resolves the hostname.
source *ip_address*	Specifies the source IP address.
interface *interface_name*	Specifies the source interface.

Command Modes

User configuration

Global configuration

Usage Guidelines

The **traceroute** command works by taking advantage of the error messages generated by devices when a datagram exceeds its hop limit value.

The **traceroute** command first sends probe datagrams with a hop limit of 1. Including a hop limit of 1 with a probe datagram causes the neighboring devices to discard the probe datagram and send back an error message. The **traceroute** command sends several probes with increasing hop limits and displays the round-trip time for each.

The **traceroute** command sends out one probe at a time. Each outgoing packet might result in one or more error messages. A `time-exceeded` error message indicates that an intermediate device has seen and discarded the probe. A `destination unreachable` error message indicates that the destination node has received and discarded the probe because the hop limit of the packet has reached a value of 0. If the timer goes off before a response comes in, the **traceroute** command prints an asterisk (*).

The **traceroute** command is terminated when the destination responds, when the hop limit is exceeded, or when the user interrupts the trace with the escape sequence. By default, to invoke the escape sequence, simultaneously press and release the **Ctrl**, **Shift**, and **6** keys, and then press the **X** key.

Global Configuration Mode Commands

This section contains global configuration mode commands. Table 2-2 describes the functions these commands perform.

Table 2-2 Global Configuration Mode Commands

Command	Function
configure terminal	Starts the Cisco Edge configuration file, and enters the global configuration mode.
copy running-config startup-config	Saves the running configuration as the startup configuration file.
exit	Exits the global configuration mode.
export	Exports the running-config or startup-config to a destination path.
help	Shows the descriptions of the interactive help system.
import	Imports a configuration file to running-config or startup-config.
ping	Diagnoses the basic network connectivity, and verifies if the remote device is reachable.
reboot	Halts and performs a cold restart.
restore	Restores the default factory configuration.
show	Shows running system information.
traceroute	Prints the route packets trace to the network host.

configure terminal

To enter the global configuration mode, use the **configure terminal** in the global configuration mode.

configure terminal

Command Modes Global configuration

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

export

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

export startup-config to *destination*

Syntax Description

destination	Destination that you want to export the configuration file to. The destination can be either a USB or a local directory.

Command Modes

Global configuration

Usage Guidelines

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

import

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

import startup-config from *source*

Syntax Description

source	Location of the configuration file that you want to import. The source can be either a USB or a local directory.

Command Modes

Global configuration

Usage Guidelines

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

reboot

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

reboot

Command Modes Global configuration

restore

To restore default factory configuration, use the **restore** command in the global configuration mode.

restore factory-default

Command Modes Global configuration mode

show

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

show

Command Modes

User configuration

Global configuration

System Configuration Mode Commands

This section contains system configuration mode commands. Table 2-3 describes the functions these commands perform.

Table 2-3 System Configuration Mode Commands

Command	Function
auto-login	Enables or disables auto login to the system.
bluetooth	Enables or disables bluetooth on the device.
clock	Configures the time zone.
display	Configures the relation between HDMI and VGA when two monitors are connected.
do	Executes user EXEC or privileged EXEC commands from the global configuration mode or other configuration modes or submodes.
exit	Exits the system configuration mode.
hdmi	Configures HDMI resolution and rotation.
hostname	Configures the hostname of the device.
interface	Enters the Ethernet interface configuration mode to configure the Gigabit Ethernet interface, or enters the WiFi AP interface configuration mode to configure the wireless interface.
language support	Configures the language of the device.
log	Configures the log size.
monitor	Enables or disables HDMI or VGA.
ntp	Configures the NTP server that is used by the device.
proxy-server	Configures the proxy server.
ssh	Configures the SSH users.
ssid	Configures the SSID name and enters the SSID configuration mode to configure the security settings for the access point.
vga	Configures VGA resolution and rotation.
wifi-mode	Sets the WiFi mode.

auto-login

To configure the auto login of the system, use the **auto-login** command in the system configuration mode.

auto-login {**enable** | **disable**}

Syntax Description

enable	Enables auto login to the system.
disable	Disables auto login to the system.

Command Default

Auto login is disabled.

Command Modes

System configuration

bluetooth

To enable or disable bluetooth on the Cisco Edge 340 Series device, use the **bluetooth** command in the system configuration mode.

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

Command Default Bluetooth is on.

Command Modes System configuration

clock

To set the time zone for display purposes, use the **clock** command in the system configuration mode.

clock timezone *timezone*

Syntax Description

timezone	Continent or ocean. Valid values are **Africa**, **America**, **Antarctica**, **Arctic**, **Asia**, **Atlantic**, **Australia**, **Europe**, **Indian**, **Mideast**, and **Pacific**.

Command Modes

System configuration

display

To configure the relation between two monitors, use the **display** command in the system configuration mode.

display type {**hdmi** | **vga**} **relation** *type* {**hdmi** | **vga**}

Syntax Description

type	Selects monitor type, either **HDMI** or **VGA**.
relation *type*	Configures relation between the two monitors. Valid values are **same-as**, **right**, **left**, **below**, and **above**.

Command Modes

System configuration

do

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

do *command*

Syntax Description

command	User configuration or global configuration command to be executed.

Command Default

A user configuration or global configuration command is not executed from a configuration mode.

Command Modes

All configuration modes.

Usage Guidelines

Use this command to execute user configuration or global configuration commands (such as **show**, **copy**, and **export**) while configuring your routing device. After the command is executed, the system will return to the configuration mode that you were using.

hdmi

To configure high-definition multimedia (HDMI) resolution or rotation, use the **hdmi** command in the system configuration mode.

hdmi {**resolution** *resolution_value* | **rotation** *rotation_value*}

Syntax Description

resolution_value	Resolution that you want to set, in the form *xx@yy*.
rotation_value	Rotation that you want to set. Valid values are **normal**, **right**, **inverted**, and **left**.

Command Modes

System configuration

hostname

To configure the hostname of the Cisco Edge 340 Series device, use the **hostname** command in the system configuration mode.

hostname *name*

Syntax Description

name	Name that you assign to the device.

Command Modes

System configuration

Usage Guidelines

Changing the hostname requires a reboot.

interface

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

interface {**ethernet ge** | **wireless bvi1**}

Syntax Description

ethernet ge	Configures the Gigabit Ethernet interface.
wireless bvi1	Configures the wireless interface.

Command Modes

System configuration

Usage Guidelines

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

Related Commands

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

Table 2-4 on page 2-37 lists the Ethernet interface configuration mode commands.

Table 2-5 on page 2-46 lists the WiFi AP interface configuration mode commands.

language support

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

language support *language_value*

Syntax Description		
	language_value	Language for the device. Valid values are **zh_CH.utf8**, **en_US.utf8**, **ko_KR.utf8**, and **ja_JP.utf8**.

Command Default

The default is English (en_US.utf8).

Command Modes

System configuration

Usage Guidelines

Changing the language requires a reboot.

log

To set the log size, use the **log command** in the system configuration mode.

log size *value*

Syntax Description		
	size *value*	Sets the log size. Default unit is MB. The valid range is from 1 to 10000. Default is 10 MB.

Command Modes System configuration

monitor

To enable or disable the monitor type of HDMI or VGA, use the **monitor** command in the system configuration mode.

monitor type {**hdmi** | **vga**} {**on** | **off**}

Syntax Description

type	Sets the monitor type.
hdmi	Sets the monitor type to HDMI.
vga	Sets the monitor type to VGA.
on	Enables the monitor.
off	Disables the monitor.

Command Modes

System configuration

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

ntp

To configure the Network Time Protocol (NTP) server that is used by the Cisco Edge 340 Series device, use the **ntp** command in the system configuration mode.

ntp {**refresh** {**on** | **off**} | **server** *ip_address*}

Syntax Description

refresh	Configures auto sync of the NTP server.
on	Enables auto sync of the NTP server.
off	Disables auto sync of the NTP server.
server *ip_address*	Configures the IP address of the NTP server

Command Modes

System configuration

proxy-server

To configure the proxy server, use the **proxy-server** command in the system configuration mode.

proxy-server *server* [*type*] [**port** *port_number*]

Syntax Description

server	Hostname or IP address of the proxy server.
type	(optional) Type of proxy server. Valid values are **no_for**, **all**, **http**, **ftp**, and **https**.
port *port_number*	(optional) Specifies the proxy port number. The range is from 0 to 65535.

Command Modes

System configuration

ssh

To configure a Secure Shell (SSH) user, use the **ssh** command in the system configuration mode.

ssh {**add** *user* | **delete** *user*}

Syntax Description

add *user*	Adds an SSH user.
delete *user*	Deletes an SSH user.

Command Modes

System configuration

ssid

To set the Service Set Identifier (SSID) name and enter the SSID configuration mode to configure the security settings for the access point of the device, use the **ssid** command in the system configuration mode.

ssid *ssid*

Syntax Description

ssid	SSID name for the access point. The name can include all the ASCII characters except ' \ " ? = , and space.

Command Default

The default SSID name is CISCO_EDGE.

Command Modes

System configuration

Related Commands

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

Table 2-6 on page 2-77 lists the SSID configuration mode commands.

vga

To configure the Video Graphics Array (VGA) resolution or rotation, use the **vga** command in the system configuration mode.

vga {**resolution** *resolution* | **rotation** *rotation*}

Syntax Description

resolution	Resolution that you want to set, in the form *xx@yy*.
rotation	Rotation that you want to set. Valid values are **normal**, **right**, **inverted**, and **left**.

Command Modes

System configuration

wifi-mode

To set the WiFi mode of the Cisco Edge 340 Series device, use the **wifi-mode** command in the global configuration mode.

wifi-mode {ap | client | off}

Syntax Description

ap	Sets the WiFi mode to access point (AP) after reboot.
client	Sets the WiFi mode to client after reboot.
off	Sets the WiFi mode to off.

Command Modes

System configuration

Usage Guidelines

If you choose the AP mode, the Cisco Edge 340 Series device will work in the AP mode immediately, and only the commands that are specific to the AP mode are visible. If you choose the client mode, the Cisco Edge 340 series device will work in the client mode immediately, and only the commands that are specific to the client mode are visible.

Ethernet Interface Configuration Mode Commands

This section contains Ethernet interface configuration mode commands. Table 2-4 describes the functions these commands perform.

Table 2-4 Ethernet Interface Configuration Mode Commands

Command	Function
do	Executes user configuration or global configuration commands from the global configuration mode or other configuration modes.
duplex	Configures the duplex mode for the Gigabit Ethernet (GE) interface.
exit	Exits the Ethernet interface configuration mode.
ip address	Configures the IP address of an interface.
ip default-gateway	Configures the default gateway.
ip name-server	Configures the DNS server.
ipv6 address	Configures the IPv6 address of an interface.
ipv6 default-gateway	Configures the IPv6 default gateway.
ipv6 name-server	Configures the IPv6 DNS server.
speed	Configures the speed for the GE interface.

duplex

To configure the duplex mode for the Gigabit Ethernet (GE) interface, use the **duplex** command in the Ethernet interface 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.

ip address

To set the IP address for an interface, use the **ip address** command in the Ethernet interface configuration mode.

ip address {*dhcp* | *ip_address*}

Syntax Description

dhcp	IP address negotiated through the Dynamic Host Configuration Protocol (DHCP).
ip_address	IP address of the interface.

Command Default

The default is dhcp.

ipv6 address

To set the IPv6 address for an interface, use the **ipv6 address** command in the Ethernet interface configuration mode.

ipv6 address {*dhcp* | *ipv6_address*}

Syntax Description

dhcp	IPv6 address negotiated through DHCP.
ipv6_address	IPv6 address of the interface.

Command Default

The default is dhcp.

ip default-gateway

To specify the default gateway for the Cisco Edge 340 Series device, use the **ip default-gateway** command in the Ethernet interface configuration mode.

ip default-gateway *ip_address*

Syntax Description

ip_address	IP address of the default gateway.

ipv6 default-gateway

To specify the IPv6 default gateway for the Cisco Edge 340 Series device, use the **ipv6 default-gateway** command in the Ethernet interface configuration mode.

ipv6 default-gateway *ipv6_address*

Syntax Description

ip_address	IPv6 address of the default gateway.

ip name-server

To specify the Domain Name System (DNS) server, use the **ip name-server** command in the Ethernet interface configuration mode.

ip name-server *ip_address*

Syntax Description

ip_address	IP address of the DNS server.

ipv6 name-server

To specify the IPv6 DNS server, use the **ipv6 name-server** command in the Ethernet interface configuration mode.

ipv6 name-server *ipv6_address*

Syntax Description

ip_address	IPv6 address of the DNS server.

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 Mbps speed.
100	Configures 100 Mbps speed.
1000	Configures 1000 Mbps speed and full-duplex mode.

Command Default

The default is auto.

WiFi AP Interface Configuration Mode Commands

This section contains WiFi AP interface configuration mode commands. Table 2-5 describes the functions these commands perform.

Table 2-5 WiFi AP Interface Configuration Mode Commands

Command	Function
aggregation-msdu	Enables or disables aggregation MAC Service Data Unit (MSDU).
ap-isolation	Configures wireless separation for clients that are connected to the same SSID.
apsd	Configures Wi-Fi Multimedia (WMM) power save mode for an access point.
auto-block	Enables or disables auto block.
ba-decline	Enables or disables to decline a ba request.
beacon-interval	Configures the beacon interval for an access point.
bg-protection	Configures the CTS-to-self protection for an access point.
channel bandwidth	Configures the channel width when the access point functions in the 802.11n mode or the 802.11n mixed mode.
channel number	Configures the channel number (which sets the frequency) for an access point.
data-beacon-rate	Configures the Delivery Traffic Indication Message (DTIM) interval for an access point.
do	Executes user configuration or global configuration commands from the global configuration mode or other configuration modes.
exit	Exits the WiFi AP 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 the 802.11n mode or the 802.11n mixed mode.
frag-threshold	Configures the frag threshold.
guard-interval	Configures the period between packets when an access point functions in the 802.11n mode or the 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 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 the 802.11n mode.
packet aggregation	Configures Aggregate MAC Service Data Unit (A-MSDU) packet aggregation when an access point functions in the 802.11n mode or the 802.11n mixed mode.

Table 2-5 WiFi AP Interface Configuration Mode Commands (continued)

Command	Function
rdg	Configures the Reverse Direction Grant (RDG) when an access point functions in the 802.11n mode or the 802.11n mixed mode.
rts-threshold	Sets the RTS threshold.
short-slot	Configures the short-slot time when the access point functions in the 802.11g mode or the 802.11g mixed mode.
stbc	Configures the space time block coding (STBC).
transmit burst	Configures the transmit burst (Tx burst) for an access point.
transmit preamble	Configures the preamble for an access point.
transmit power	Configures the power at which an access point radio transmits its wireless signal.
wireless-mode	Configures the 802.11 wireless mode for an access point.
wmm	Configures Wi-Fi Multimedia (WMM) for an access point.

aggregation-msdu

To enable or disable MAC Service Data Unit (MSDU) aggregation, use the **aggregation-msdu** command in the WiFi AP interface configuration mode.

aggregation-msdu {on | off}

Syntax Description

on	Enables aggregation MSDU.
off	Disables aggregation MSDU.

Command Modes

WiFi AP interface configuration

ap-isolation

To configure wireless separation for clients that are connected to the same Service Set Identifier (SSID), use the **ap-isolation** command in the WiFi AP 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.

Command Default

Wireless separation is disabled.

Related Commands

WiFi AP interface configuration

apsd

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

Command Modes

WiFi AP interface configuration

Usage Guidelines

You can configure the **apsd** command only when the WMM is enabled.

Related Commands

Use the **wmm** command to enable WMM.

auto-block

To configure auto block, use the **auto-block** command in the WiFi AP interface configuration mode.

auto-block {on | off}

Syntax Description

on	Enables auto block.
off	Disables auto block.

Related Commands WiFi AP interface configuration

ba-decline

To enable or disable the task of declining a BA request, use the **ba-decline** command in the WiFi AP interface configuration mode.

ba-decline {**on** | **off**}

Syntax Description

on	Enables the task of declining a BA request.
off	Disables the task of declining a BA request.

Command Modes

WiFi AP interface configuration

beacon-interval

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

beacon-interval *interval*

Syntax Description

interval	Period that you want to configure the beacon interval with. The range is between 20 and 1000 milliseconds. The default is 100 milliseconds.

Command Default

The default period is 100 milliseconds.

Command Modes

WiFi AP interface configuration

Usage Guidelines

The default setting should work well for most networks.

Configure a long interval to:

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

Configure a short interval to:

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

bg-protection

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

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

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

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.

Command Modes

WiFi AP interface configuration

Usage Guidelines

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

channel bandwidth

To configure the channel width in a scenario there an access point functions in the 802.11n mode, use the **channel bandwidth** command in the WiFi AP interface configuration mode.

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

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

Syntax Description

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

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

Command Modes WiFi AP interface configuration

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 a channel number, which sets the frequency for an access point, use the **channel number** command in the WiFi AP interface configuration mode.

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

Syntax Description

auto	Configures automatic selection of a channel number.
number	Channel number. Value between 1 to 13, 149, 153, 157, 161, and 165. The default is 6.

Command Default

The default channel number is 6.

Command Modes

WiFi AP interface configuration

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 have to change the channel number, use the following numbers based on your location:

- China and Europe: 1 to 13
- America: 1 to 11

data-beacon-rate

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

data-beacon-rate *rate*

Syntax Description		
	rate	The range is between 1 and 255 milliseconds. The default is 1 millisecond.

Command Default

The default rate is 1 millisecond.

Command Modes

WiFi AP interface configuration

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 may delay multicast and broadcast traffic.

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

Related Commands

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

extension channel

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

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

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

Syntax Description

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

Command Default

The lower extension channel is configured.

Command Modes

WiFi AP interface configuration

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 to 4 range), use the upper extension channel.

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

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

frag-threshold

To configure the Frag threshold, use the **frag-threshold** command in the WiFi AP interface configuration mode.

frag-threshold *value*

Syntax Description

value	Configures the Frag threshold value. The range is from 256 to 2346.

Command Modes

WiFi AP interface configuration

guard-interval

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

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

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

Syntax Description

400	Configures a short guard interval of 400 nanoseconds (ns).
800	Configures a long guard interval of 800 ns.

Command Default

The default is 400 ns.

Command Modes

WiFi AP interface configuration

Usage Guidelines

Use a 400-ns interval to increase the throughput performance for 802.11n clients, but may result in 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 Internet Group Management Protocol (IGMP) snooping on a wireless interface, use the **igmp-snoop** command in the WiFi AP interface configuration mode.

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

Syntax Description

on	IGMP snooping is on.
off	IGMP snooping is off.

Command Default

IGMP snooping is off.

Command Modes

WiFi AP interface configuration

mcs

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

mcs *index_number*

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

Syntax Description

index_number	The range is from 0 to 15, and 33 (automatic selection).

Command Default The default is 33 (automatic rate configuration).

Command Modes WiFi AP interface configuration

Usage Guidelines This table shows the MCS index numbers with their potential data rates in Mbps based on MCS, guard interval, and channel width.

Index Number	Guard Interval of 800 nanoseconds		Guard Interval of 400 nanoseconds	
	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

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

multicast-mcs *index_number*

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

Syntax Description

index_number	The range is from 0 to 15.

Command Default The default is 2.

Usage Guidelines This table shows the MCS index numbers with their potential data rates in Mbps 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 the PHY mode on multicast frames when an access point functions in the 802.11n mode, use the **multicast-phy-mode** command in the WiFi AP interface configuration mode.

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

Syntax Description

0	Specifies that the mode is disabled.
1	Specifies Complementary Code Keying (CCK) (802.11b).
2	Specifies Orthogonal Frequency Division Multiplexing (OFDM) (802.11g). This is the default.
3	Specifies HTMIX (802.11b/g/n).

Command Default

The default is 2.

Command Modes

WiFi AP interface configuration

operating-mode

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

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

Note This command applies to the 802.11n mode.

Syntax Description

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

Command Default

The default is **mixed**.

Command Modes

WiFi AP interface configuration

Usage Guidelines

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

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

packet aggregation

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

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

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

Syntax Description

on	Enables packet aggregation.
off	Disables packet aggregation.

Command Default

Packet aggregation is off.

Command Modes

WiFi AP interface configuration

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.

rdg

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

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

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

Syntax Description

on	Enables RDG.
off	Disables RDG.

Command Default

RDG is disabled.

Command Modes

WiFi AP interface configuration

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 of 802.11n traffic.

rts-threshold

To configure the Request to Send (RTS) threshold, use the **rts-threshold** command in the WiFi AP interface configuration mode.

rts-threshold *value*

Syntax Description

value	Sets the RTS threshold. The range is from 1 to 2347.

Command Modes

WiFi AP interface configuration

short-slot

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

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

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

Syntax Description

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

Command Default

Short-slot time is enabled.

Command Modes

WiFi AP interface configuration

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.

stbc

To configure the space time block coding (STBC), use the **stbc** command in the WiFi AP interface configuration mode.

stbc {**on** | **off**}

Syntax Description

on	Enables STBC.
off	Disables STBC.

Related Commands WiFi AP interface configuration

transmit burst

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

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

Syntax Description

on	Enables Tx burst.
off	Disables Tx burst.

Command Default

Tx burst is enabled.

Command Modes

WiFi AP interface configuration

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 an access point, use the **transmit preamble** command in the WiFi AP 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.

Command Modes

WiFi AP interface configuration

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 an access point radio transmits its wireless signal, use the **transmit power** command in the WiFi AP interface configuration mode.

transmit power *percentage*

Syntax Description

percentage	Percentage of transmit power. The range is from 1 to 100.

Command Default

The default is 100 percent.

Command Modes

WiFi AP interface configuration

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 the clients are in a small room, lower the percentage.

wireless-mode

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

wireless-mode {**0** | **1** | **2** | **4** | **6** | **7** | **8** | **9** | **11**|}

Syntax Description

0	Configures the 802.11b/g mixed mode.
1	Configures the 802.11b mode.
2	Configures the 802.11a mode for 5GHz only.
4	Configures the 802.11g mode.
6	Configures the 802.11n mode for 2GHz only.
7	Configures the 802.11n/g mixed mode.
8	Configures the 802.11a/n mixed mode for 5GHz only.
9	Configures the 802.11b/g/n mixed mode.
11	Configures the 802.11n mode for 5GHz only.

Command Default

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

Command Modes

WiFi AP interface configuration

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 the devices in the wireless network only support 802.11b.

802.11a mode for 5GHz only—Select this mode if all the devices in the wireless network only support 802.11a in the 5GHz band.

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

802.11n mode for 2GHz only—Select this mode if all the devices in the wireless network only support 802.11n in the 2GHz band.

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.

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

wmm

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

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

Syntax Description

on	Enables WMM.
off	Disables WMM.

Command Default

WMM is disabled.

Command Modes

WiFi AP interface configuration

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

This section contains Service Set Identifier (SSID) configuration mode commands. Table 2-6 describes the functions these commands perform.

Table 2-6 SSID Configuration Commands

Command	Function
broadcast ssid	Enables or disables broadcast of the Service Set Identifier (SSID) name.
do	Executes THE user EXEC or privileged EXEC commands from global configuration mode or other configuration modes or submodes.
encryption mode (open, shared, or WEP configuration)	Configures open, shared, Wi-Fi Protected Access (WPA), WPA1WPA2, WPA2, WPA2PSK, WPAPSK, and WPAPSKWPA2PSK authentication and associated encryption for the access point.
encryption mode (WPA configuration)	
exit	Exits the 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.
wep-keyid	Configures the Wired Equivalent Privacy (WEP) encryption.

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.

Command Modes

SSID configuration

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 an 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.

Command Modes

SSID configuration

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 the passphrase 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 an 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 a maximum of 63 alphanumerical characters. Dash (-) and underscore(_) characters are supported.

Command Default

The default is open access and no encryption.

Command Modes

SSID configuration

Examples

This example shows how to configure combined WPA and WPA2 authentication with combined TKIP and AES encryption, using the passphrase 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 an access point, use the **encryption mode** command in the SSID configuration mode.

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

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

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.

Command Modes

SSID configuration

Examples

This example shows how to configure combined WPA and WPA2 authentication with combined TKIP and AES encryption, using the 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 *hostname* [**auth-port** *port_number*] [**key** *secret*]

Syntax Description

hostname	Hostname or IP address of the RADIUS server.
auth-port	Specifies the authentication port number of the RADIUS server.
port_number	Authentication port number of the RADIUS server. The range is from 0 to 65535. The default is 1812.
key	Specifies the password of the authentication service on the RADIUS server.
secret	Password of the authentication service on the RADIUS server.

Command Default

The default value for *port_number* is 1812.

The default value for *secret* is NULL.

Command Modes

SSID configuration

Examples

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

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

wep-keyid

To configure valid Wired Equivalent Privacy (WEP) encryption, use the **wep-keyid** in the SSID configuration mode.

wep-keyid *wep_key*

Syntax Description

wep_key	Valid WEP key. The range is from 1 to 4.

Command Default

The default value for *wep_key* is 1.

Command Modes

SSID configuration

Usage Guidelines

The WEP encryption supports four groups of password. You should use the **wep-keyid** command to configure which group of password takes effect. For example, the four groups of WEP password are **cisco1**, **cisco2**, **cisco3**, and **cisco4**. The command **wep-keyid 3** means the password **cisco3** will take effect.

show Commands

User Configuration Mode

Use the following **show** commands in the user configuration mode to display the configuration on a Cisco Edge 340 Series device:

- **show cpu**—Displays CPU information.
- **show mac**—Displays MAC address.
- **show memory**—Displays memory usage information.
- **show mount**—Displays mount information.
- **show os-build-time**—Displays release build time.
- **show os-version**—Displays release version.
- **show os-install-time**—Displays release installed time.
- **show storage**—Displays storage information.

Global Configuration Mode

Use the following **show** commands in the global configuration mode to display the configuration on a Cisco Edge 340 Series device:

- **show all-running-config**—Displays all information about the running configuration.
- **show all-startup-config**—Displays all information about the startup configuration.
- **show running-config**—Displays the configuration saved in the RAM.
- **show startup-config**—Displays the configuration saved in the database.
- **show bluetooth**—Displays bluetooth information.
- **show hdmi dev-name**—Displays the device name of the connected HDMI monitor.
- **show hdmi current-resolution**—Displays the current resolution of the connected HDMI monitor.
- **show hdmi support-resolution**—Displays the connected HDMI monitor support resolution.
- **show hostname**—Displays the hostname.
- **show ip interface**—Displays the status of interfaces configured for IP.
- **show log-size**—Displays the log size.
- **show monitor-full**—Displays all the current monitor information.
- **show ssid**—Displays the AP wireless ssid setting.
- **show wifi-mode**—Displays the WiFi mode.
- **show vga dev-name**—Displays the device name of the connected VGA monitor.
- **show vga current-resolution**—Displays the current resolution of the connected VGA monitor.
- **show vga support-resolution**—Displays the connected VGA monitor support resolution.

Configuring the Web GUI

The web-based GUI is used to configure a Cisco Edge 340 Series device and monitor the status of the Cisco Edge 340 Series locally or remotely.

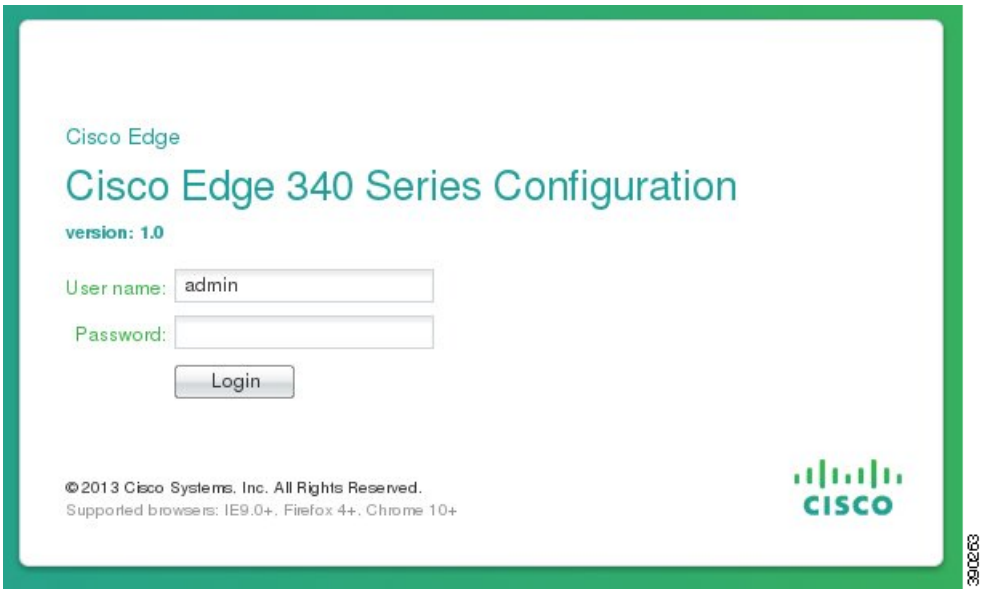
To configure a Cisco Edge 340 Series device using the web-based GUI, follow the steps described in these sections:

Logging In to the Web GUI

Access the web-based GUI at https://[*Cisco Edge 340's IP address*] and log in to the web portal locally or remotely by entering the username admin and password of the admin account. The default password of the admin account is **aDMIN123#**.

Note Change the default password immediately after you have successfully logged in to the system.

Figure 3-1 Log in Page



Language Setting

After you log in, choose the language that you want to use with the web GUI. At the top of the GUI, choose a language from the drop-down list (Figure 3-2).

Figure 3-2 Language Setting of the Web GUI

System Configuration

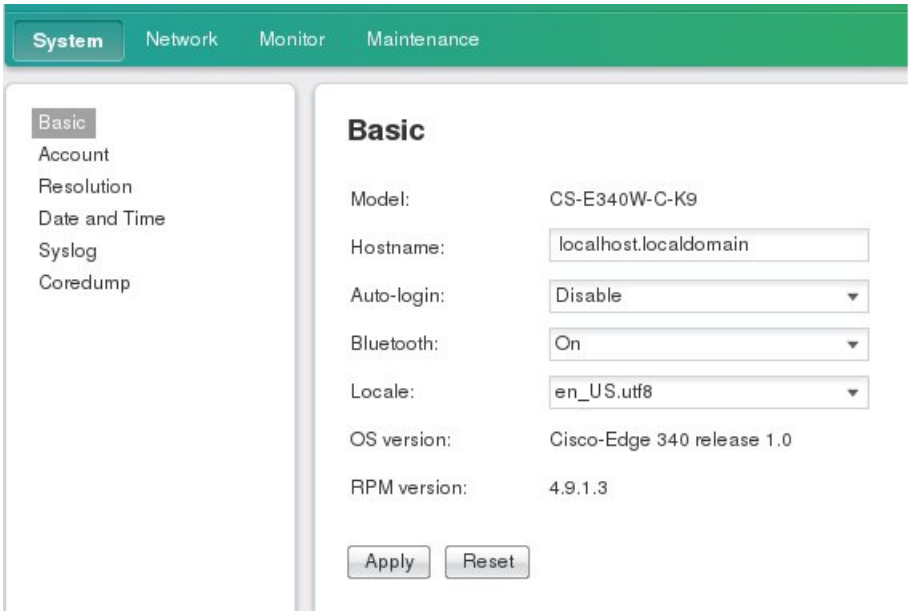
After you log in to the web GUI, the System configuration window is displayed. You can configure the Basic information, Account, Resolution, Date and Time, Syslog, and Coredump by clicking the corresponding link on the left pane.

Configuring Basic Information

Click **Basic** in the left pane to configure the host name, enable or disable auto login, choose a locale for the setting of system language and character set, and view the model, OS version, and RPM version (Figure 3-3). Click **Apply** to save the changes and **Reset** to restore the default values.

Note Change of locale needs reboot of the device to take effect. The locale options are defined in the following format: [language[_territory][.codeset][@modifier]]. Each option represents a language. For example, en_US.UTF-8 means U.S. English using the UTF-8 encoding.

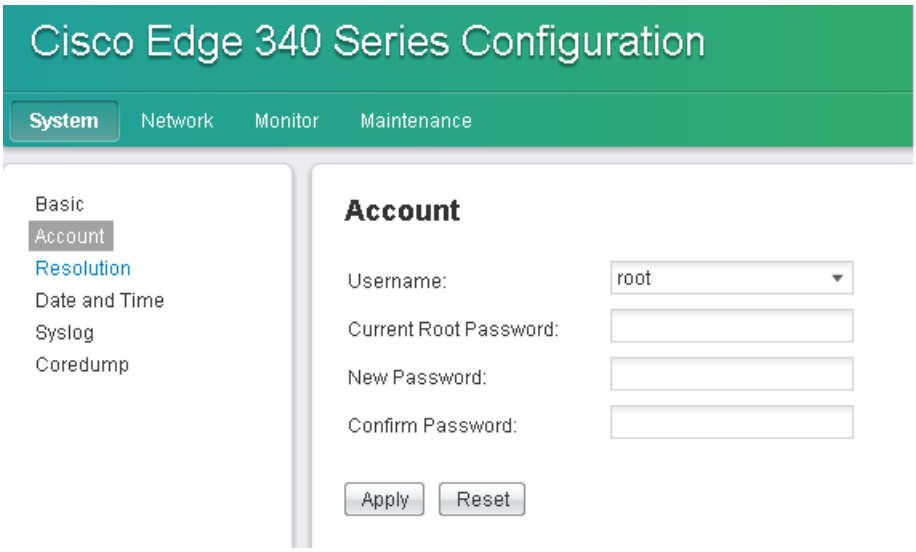
Figure 3-3 Basic Information



Configuring Account Information

Click **Account** in the left pane to change the password for a user, for example, the root user (Figure 3-4). Click **Apply** to save the changes and **Reset** to restore the default values.

Figure 3-4 Account Information

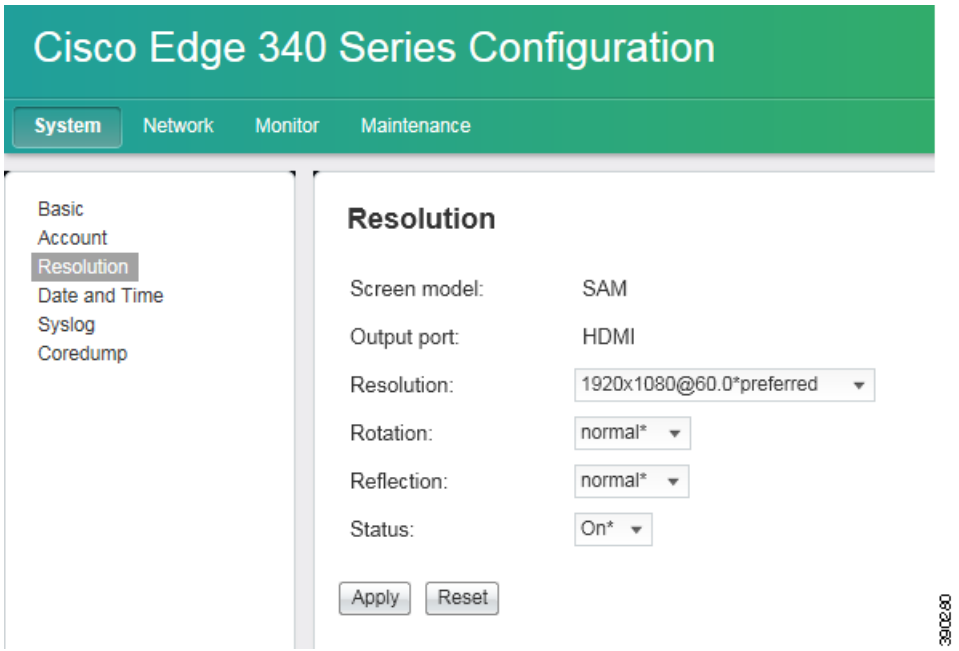


Note Follow these rules when you change the password:
Password should not be less than 8 characters;
The new password should contain characters from at least three of the following classes: lower case letters, upper case letters, digits, and special characters;
No character in the new password should be repeated more than three times consecutively;
The new password should be neither the same as the associated username, nor the reversed username.

Configuring Resolution

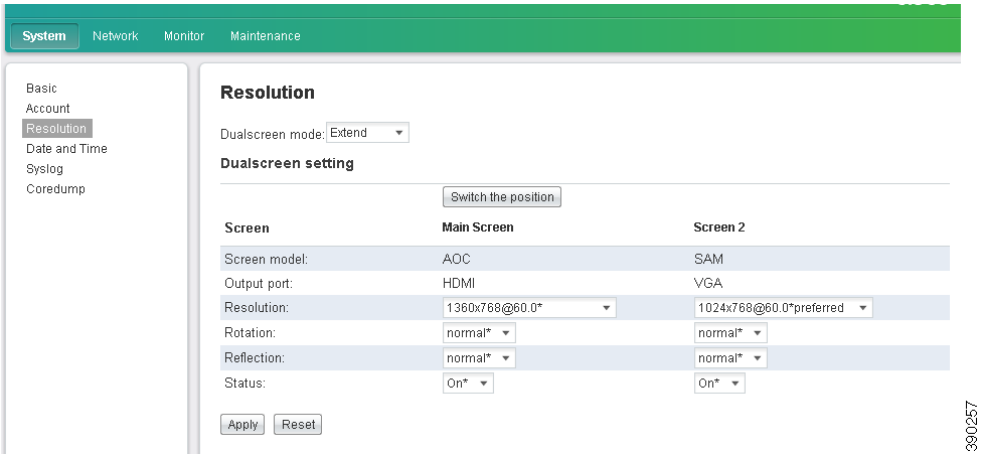
Click **Resolution** in the left pane to configure the Resolution, Rotation, Reflection, and Status of the connected monitor, and view the Screen model and Output port of the monitor (Figure 3-5).

Figure 3-5 Resolution Information



The Cisco Edge 340 Series supports the use of VGA and HDMI output ports at the same time. When two monitors are connected, you will see the Dualscreen mode configuration displayed (Figure 3-6).

Figure 3-6 Dualscreen Setting



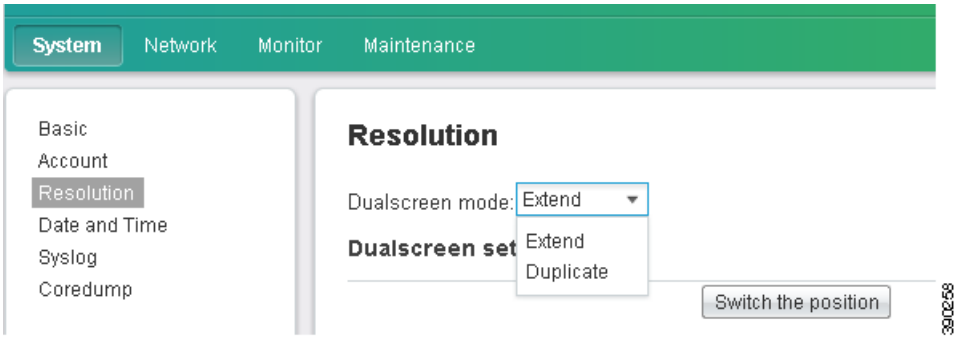
On the Dualscreen setting window, you can configure the Resolution, Rotation, Reflection, and Status for both the screens in one location, and view the Screen model and Output port for both screens. Note that the configuration of the two screens can be different.

There are two types of Dualscreen mode:

- Extend—The main screen displays the main view of the system, and screen 2 extends the main screen for more views.
- Duplicate—Both screens have the same view of the system.

You can choose dual screen mode type from the **Dualscreen** mode drop-down list (Figure 3-7). For the Extend type of Dualscreen mode, click **Switch the position** to exchange the main screen with screen 2.

Figure 3-7 Dualscreen Mode Type



Configuring Date and Time

Click **Date and Time** in the left pane to configure the date and time information of the Cisco Edge 340 Series device.

Step 1 Choose the mode of configuring date and time: **Automatically synchronize with NTP server** or **Manually set time**. Go to Step 4 if you choose **Manually set time**.

Step 2 If you choose Automatically synchronize with NTP server, the Date and Time fields are disabled; you cannot make changes to them.

Step 3 Enter the NTP server address in the **NTP server** field and go to Step 7.

Step 4 If you choose **Manually set time** for the mode in Step 1, the **NTP server** field is disabled; you cannot modify it.

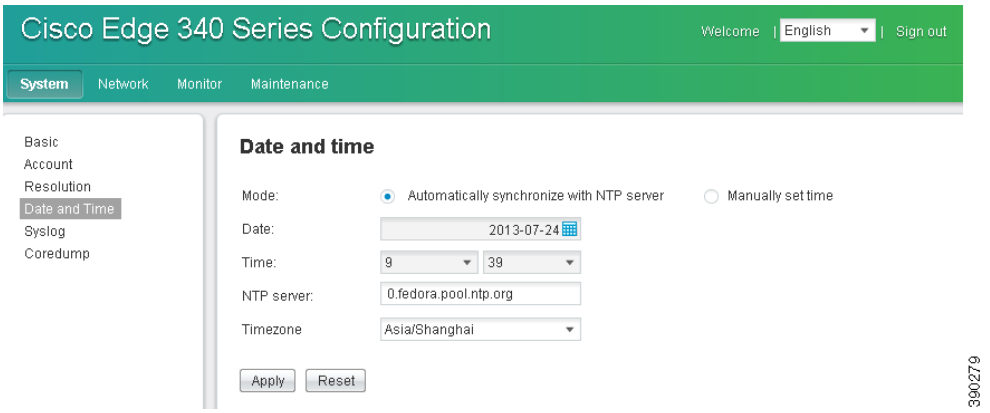
Step 5 Click the calendar icon to the right side of the **Date** field, choose month and year from the drop-down list, and click the corresponding date.

Step 6 In the **Time** field, choose hour in the left drop-down list and minute from the right drop-down list.

Step 7 From the **Time zone** drop-down list, choose a time zone.

Step 8 Click **Apply** to save the changes and **Reset** to restore the default values.

Figure 3-8 Date and Time Information



Configuring Syslog

Click **Syslog** in the left pane to configure the setting of syslog.

Step 1 Enter the path in which you want to store the syslog in the Path field. The system will automatically check if the path that you enter is valid.

Step 2 Choose the level of syslog from the **Level** drop-down list:

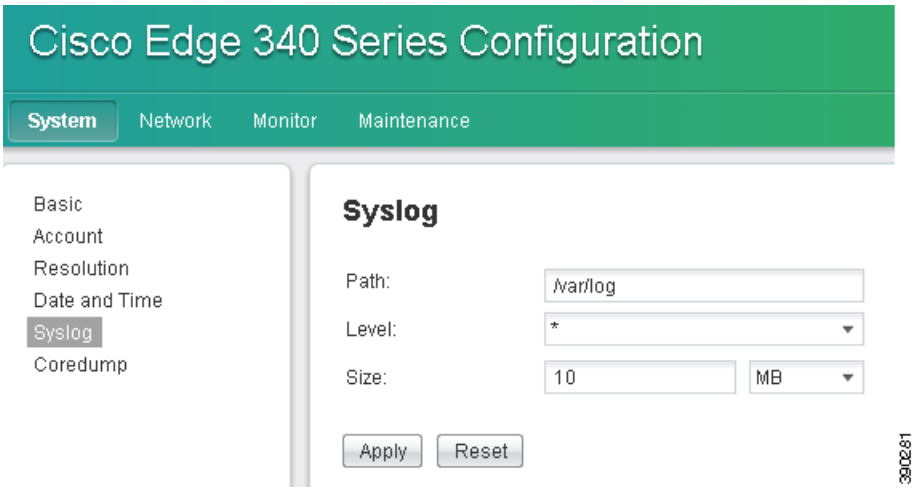
- Debug
- Info
- Notice
- Warning
- Error
- Critical
- Alert
- Emergency
- * (All of above)

Step 3 In the Size field, enter the size of the syslog in the left column and choose the unit of the log size from the right drop-down list.

Size has three units: KB, MB, and GB. The maximum log size is 50 MB, and the default size is 10 MB. If the value you provide exceeds 50 MB, the change fails and the original size is retained. You cannot use GB as the unit. If you choose KB or MB, the log size value cannot be 0.

Step 4 Click **Apply** to save the changes and **Reset** to restore the default values.

Figure 3-9 Syslog Information



Configuring Coredump

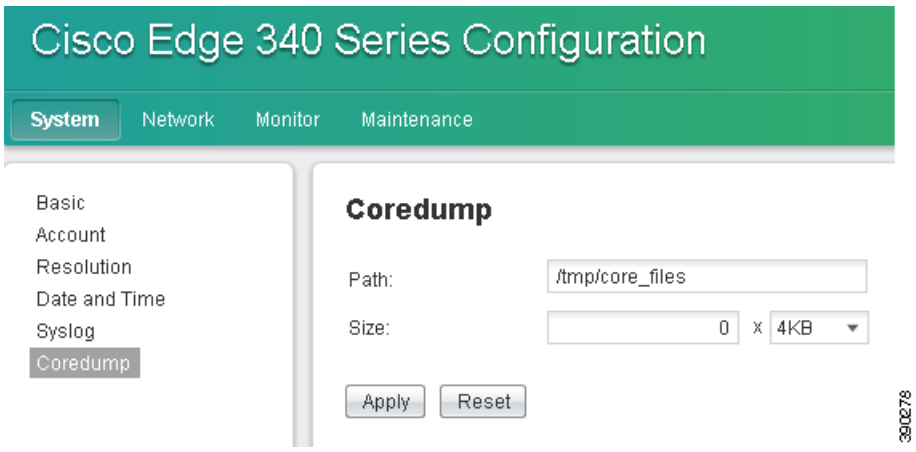
Click **Coredump** in the left pane to configure the setting of core dump.

Step 1 Enter the file name and the path in which you want to store the core dump in the Path field. The file can be created directly through the Path field.

Step 2 In the Size field, enter the size of the core dump in the left column and choose the unit of the core dump size from the right drop-down list.

Step 3 Click **Apply** to save the changes and **Reset** to restore the default values.

Figure 3-10 Coredump Information



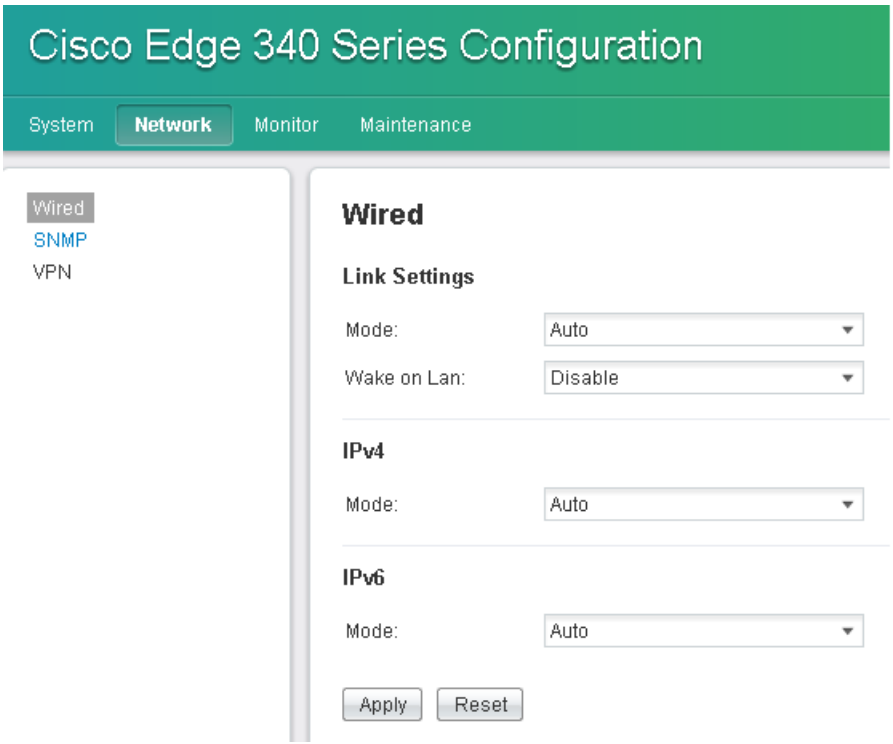
Network Configuration

You can configure wired, wireless, SNMP, and VPN settings using the Network tab.

Configuring Wired Settings

Under the Network tab, click **Wired** in the left pane to configure Link Settings, enable or disable Wake on Lan, and configure the IPv4 mode and the IPv6 mode. See Figure 3-11. Click **Apply** to save the changes and **Reset** to restore the default values.

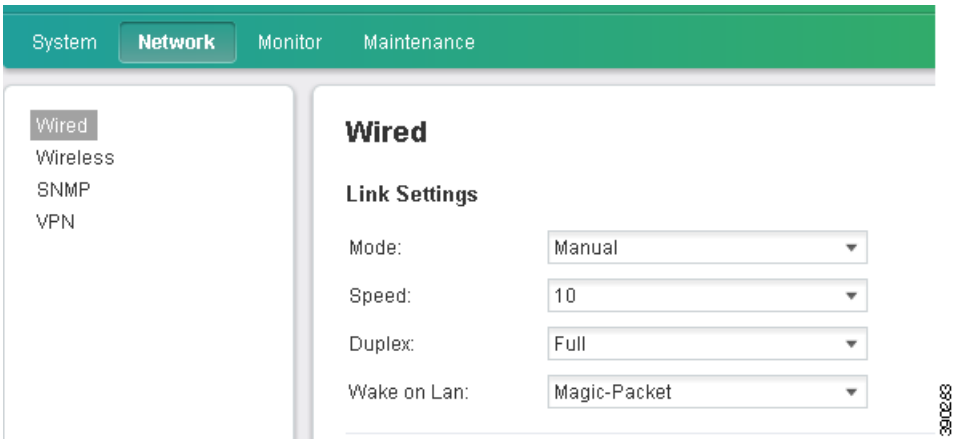
Figure 3-11 Wired Information



Configuring Wake on Lan

To enable the Wake on Lan function, select **Manual** from the **Mode** drop-down list, and **Magic-Packet** for the **Wake on Lan** drop-down list. Then you can configure the Speed and Duplex settings. See Figure 3-12.

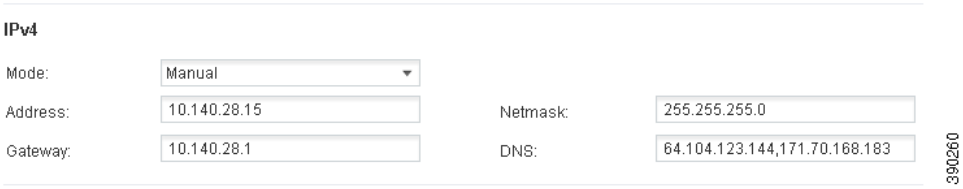
Figure 3-12 Wake on Lan Settings



Configuring IPv4 Settings

To view and configure IPv4 address, netmask, gateway, and DNS for IPv4, choose **Manual** from the **Mode** drop-down list. The IPv4 settings screen is displayed (Figure 3-13).

Figure 3-13 IPv4 Settings



Configuring IPv6 Settings

To view and configure IPv6 address, netmask, gateway, and DNS for IPv6, choose **Manual** from the **Mode** drop-down list. The IPv6 settings screen is displayed (Figure 3-14).

Figure 3-14 IPv6 Settings

Configuring Wireless Settings

The Cisco Edge 340 Series device supports the following wireless modes:

- Access Point (AP)—A device that allows wireless devices to connect to a wired network using Wi-Fi.
- Station—A wireless connection to connect to the other networks.
- Off—The wireless function is disabled.

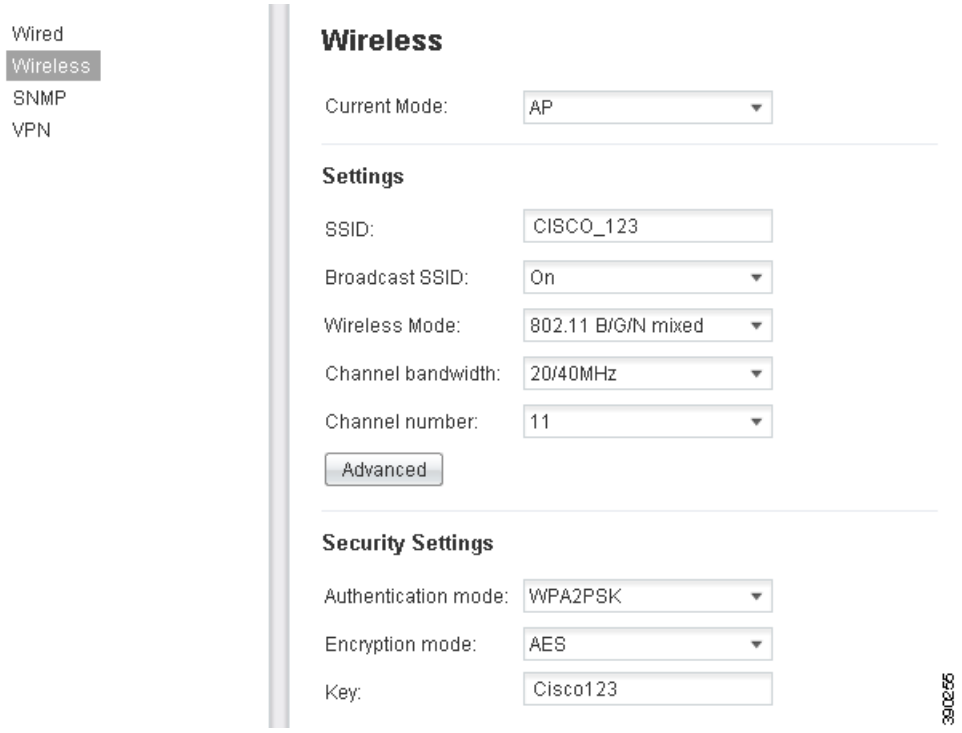
To select a desired wireless mode, click **Wireless** in the left pane and configure the settings for each mode.

Configuring AP Mode

If you select **AP** from the **Current Mode** drop-down list, you can configure the SSID name, broadcast SSID, wireless mode, channel bandwidth, channel number, and security settings for the AP mode. See Figure 3-15. Click **Apply** to save the changes and **Reset** to restore the default values.

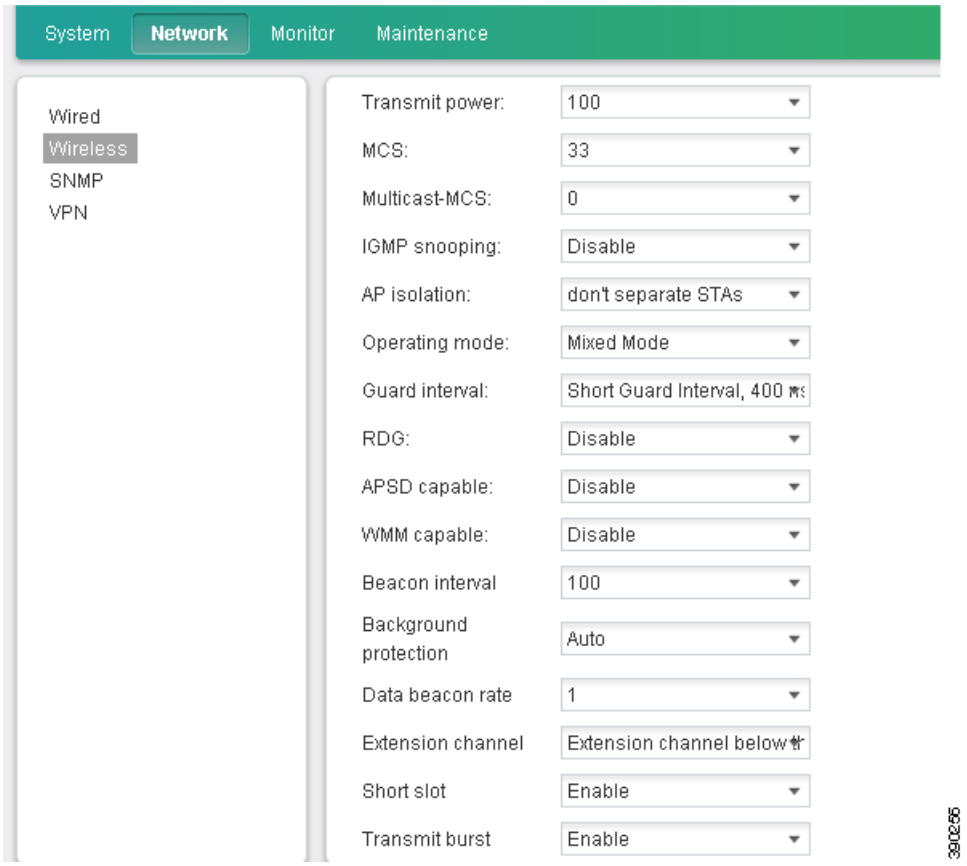
Note The country and region for Wi-Fi AP cannot be selected.

Figure 3-15 AP Mode Settings



Click the **Advanced** button at the end of the settings section in Figure 3-15, the AP Mode Advanced Settings screen is displayed (Figure 3-16).

Figure 3-16 AP Mode Advanced Settings



Note The antenna transmission setting is not provided on WEB GUI. Use the Transmit power drop-down list to set WLAN radio transmit power in percentage.

Click **Hide** at the bottom of the screen to get back to the simplified mode.

Configuring Station Mode

If you select **Station** from the **Current Mode** drop-down list, you can add, edit, remove, connect, and refresh wireless connections in the Station mode.

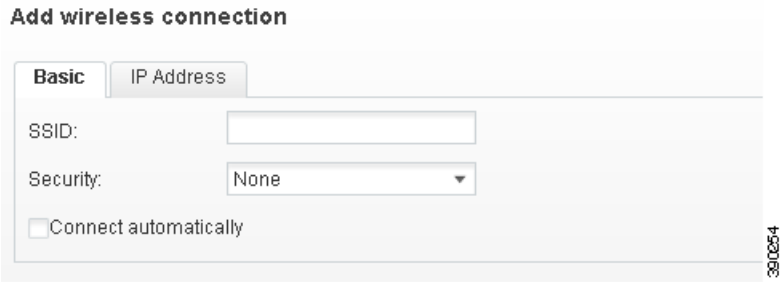
Add a Wireless Connection

To add a wireless connection, follow these steps:

Step 1 Click + in the Connections area.

Step 2 The Add wireless connection screen is displayed, as shown in Figure 3-17.

Figure 3-17 Add Wireless Connection



Step 3 Under the Basic tab, enter the name of the wireless connection in the SSID field and choose a security type from the Security drop-down list.

You can configure the following security types:

- None—If you choose **None** from the Security drop-down list, the security type of this wireless connection will be displayed as Open in the Connections area, as shown in Figure 3-18.

Figure 3-18 Security Type—None

- WEB 40/128-bit Key (Hex or ASCII)—You can configure SSID, Key, WEP index, and Authentication for the WEB 40/128-bit Key (Hex or ASCII) security type.
- WPA & WPA2 Personal—This type is typically used by personal users. You can configure a password for the WPA & WPA2 Personal security type.
- WPA & WPA2 Enterprise—This type is typically used by enterprise users. You can configure authentication, username, user certificate, CA certificate, private key, and private key password for the WPA & WPA2 Enterprise security type.

Step 4 (Optional) If you do not have a DHCP server, click the **IP Address** tab to enter IPv4 or IPv6 address information.

Step 5 If you select **Connect automatically**, the wireless connection will be the first choice for the next time to connect.

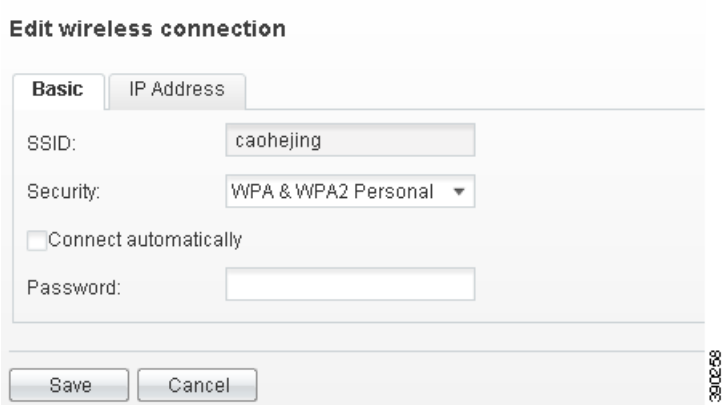
Step 6 Click **Save** to add the wireless connection.

Edit a Wireless Connection

To edit a wireless connection, follow these steps:

Step 1 Choose the wireless connection that you want to edit and click in the Connections area, the Edit wireless connection screen is displayed, as shown in Figure 3-19.

Figure 3-19 Edit Wireless Connection



Step 2 Edit the Security option or IP Address information as required, and click **Save**.

Note For detailed information about security options, see the "Add a Wireless Connection" section on page 3-12.

Note If a wireless network is connected successfully, it cannot be edited or removed unless it is disconnected.

Remove a Wireless Connection

To remove a wireless connection, follow these steps:

Step 1 Select the wireless connection that you want to remove from the Connections area.

Step 2 Click in the Connections area to remove the wireless connection.

Note If a wireless network is connected successfully, it cannot be edited or removed unless it is disconnected.

Connect a Wireless Network

To connect a wireless network, follow these steps:

Step 1 Select the wireless network that you want to connect from the Connections area.

Step 2 Click in the Connections area to connect the wireless network.

If you have entered incorrect settings information when you add or edit wireless connections, the message "`Connection failed, please correct settings and click save to reconnect`" is displayed in red. Correct the settings and click **Save** to connect the wireless network.

Refresh the Wireless Networks

To refresh the wireless networks, click in the Connections area.

Disable the Wireless Function

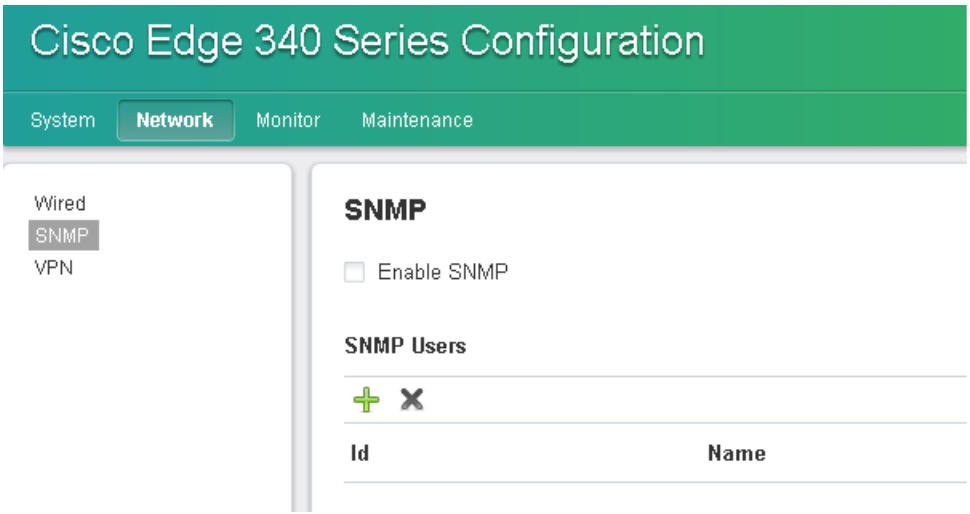
To disable the wireless function, choose **off** from the **Current Mode** drop-down list in the Wireless tab.

Configuring SNMP

To enable or disable SNMP, or add, remove, and view SNMP users, click **SNMP** in the left pane under the Network tab, as shown in Figure 3-20.

To enable SNMP, check the **Enable SNMP** check box.

Figure 3-20 Enabling SNMP



Add an SNMP User

To add an SNMP user, follow these steps:

Step 1 Click in the SNMP Users area.

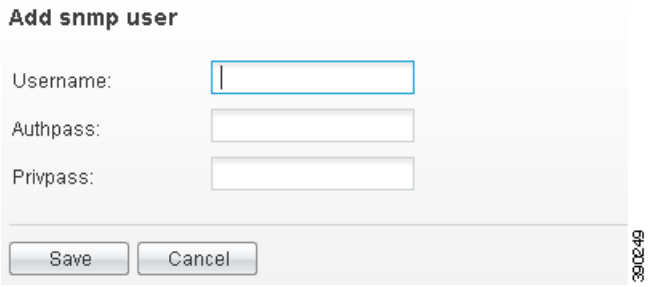
Step 2 The Add snmp user screen is displayed, as shown in Figure 3-21.

Step 3 Enter the username in the Username field. The username can only consist of letters, numbers, and _. The first character must be a letter. The length of the username should be between 4 and 33 numbers.

Step 4 Enter the passwords in the Authpass and Privpass fields. The password can only consist of letters, numbers, @, #, $, %, ^, &, +, =, and _. The length of the password should be between 8 and 32 numbers.

Step 5 Click **Save** to create the SNMP user.

Figure 3-21 Add SNMP User



Remove an SNMP User

To remove an SNMP user, follow these steps:

Step 1 Select the SNMP user that you want to remove in the SNMP Users area.

Step 2 Click in the SNMP Users area to remove the SNMP user.

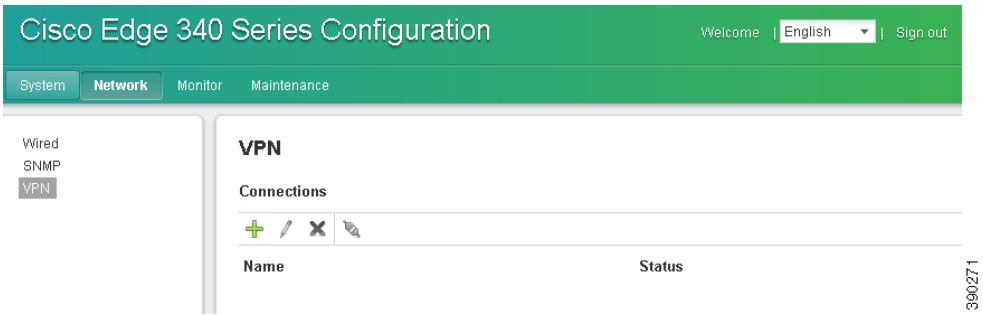
Configuring VPN

Cisco Edge 340 Series supports the following types of VPN connections:

- PPTP
- IPSEC/L2TP/PSK
- IPSEC/L2TP/RSA
- CISCO (supports PSK and Hybrid for auth mode)

To add, edit, and remove a VPN connection, or connect to a VPN, click **VPN** in the left pane under the Network tab, as shown in Figure 3-22.

Figure 3-22 VPN Information



Add a VPN connection of PPTP Type

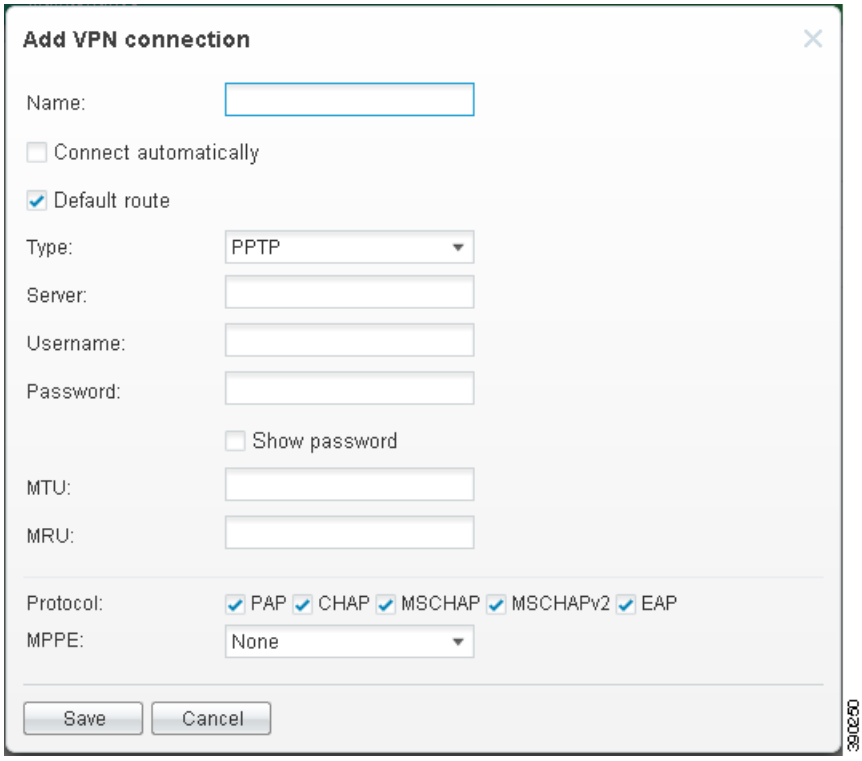
To add a VPN connection of PPTP type, follow these steps:

Step 1 Click **VPN** in the left pane under the Network tab.

Step 2 Click + in the right pane.

Step 3 The Add VPN connection window is displayed, as shown in Figure 3-23.

Figure 3-23 Add VPN Connection—PPTP



Step 4 In the Add VPN connection window, enter the name of the VPN connection that you want to add in the Name field.

Step 5 Check the **Connect automatically** check box if you want the Cisco Edge 340 Series device to automatically connect to this VPN.

Step 6 Choose **PPTF** for the type of the VPN connection from the Type drop-down list:

Step 7 Enter the VPN server address, username, and password in the Server, Username, and Password fields. Check the Show password check box if you want the password to be displayed in plain text.

Step 8 Enter the value of the Maximum Transmission Unit (MTU) and the Maximum Receive Unit (MRU).

Step 9 Choose the protocols that you want to use with this VPN connection.

Step 10 Choose the MPPE encryption type from the MPPE drop-down list:

- None
- MPPE
- MPPE40

- MPPE128

Step 11 Click **Save** to add the VPN connection.

Step 12 The VPN pane is updated to show the name and status of the new VPN connection

Add a VPN connection of IPSEC/L2TP/PSK Type

To add a VPN connection of IPSEC/L2TP/PSK type, follow these steps:

Step 1 Click **VPN** in the left pane under the Network tab.

Step 2 Click  in the right pane.

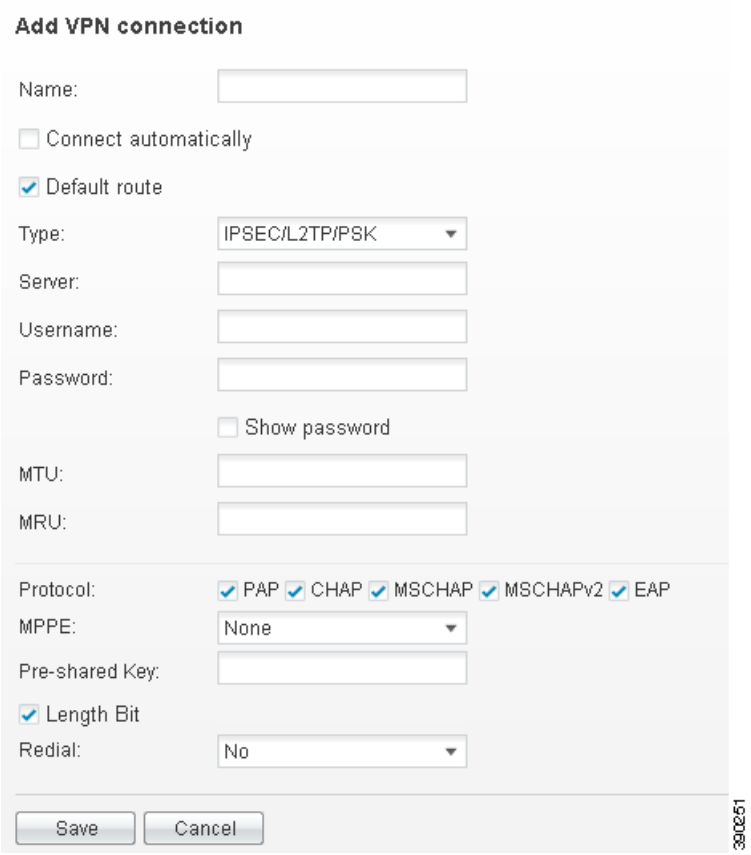
Step 3 The Add VPN connection window is displayed, as shown in Figure 3-24.

Step 4 In the Add VPN connection window, enter the name of the VPN connection that you want to add in the Name field.

Step 5 Check the Connect automatically check box if you want the Cisco Edge 340 Series device to automatically connect to this VPN.

Step 6 Choose **IPSEC/L2TP/PSK** for the type of the VPN connection from the Type drop-down list.

Figure 3-24 Add VPN Connection—IPSEC/L2TP/PSK



Step 7 Enter the VPN server address, username, and password in the Server, Username, and Password fields. Check the **Show password** check box if you want the password to be displayed in plain text.

Step 8 Enter the value of the MTU and the MRU.

Step 9 Choose the protocols that you want to use with this VPN connection.

Step 10 Choose the MPPE encryption type from the MPPE drop-down list:

Step 11 Enter the preshared key in the Pre-shared Key field.

Step 12 Choose Yes or No from the Redial drop-down list. If you choose Yes, you should enter values for the Timeout and Attempts fields (Figure 3-25).

Figure 3-25 Redial Information

- Timeout—The maximum time to connect the VPN server every time.
- Attempts—The maximum number of attempts made to connect the VPN server.

The value of Timeout multiplied by the value of Attempts is the time taken to connect the VPN server, which is 20 seconds, at most.

Step 13 Click **Save** to add the VPN connection.

Step 14 The VPN pane is updated to show the name and status of the new VPN connection.

Add a VPN connection of IPSEC/L2TP/RSA Type

To add a VPN connection of IPSEC/L2TP/RSA type, follow these steps:

Step 1 Click VPN in the left pane under the Network tab.

Step 2 Click  in the right pane.

Step 3 The Add VPN connection window is displayed (Figure 3-26).

Step 4 In the Add VPN connection window, enter the name of the VPN connection that you want to add in the Name field.

Step 5 Check the **Connect automatically** check box if you want the Cisco Edge 340 Series device to automatically connect to this VPN.

Step 6 Choose **IPSEC/L2TP/RSA** for the type of the VPN connection from the Type drop-down list.

Step 7 Enter the VPN server address, username, and password in the Server, Username, and Password fields. Check the **Show password** check box if you want the password to be displayed in plain text.

Step 8 Enter the value of the MTU and the MRU.

Step 9 Choose the protocols that you want to use with this VPN connection.

Step 10 Choose the MPPE encryption type from the MPPE drop-down list:

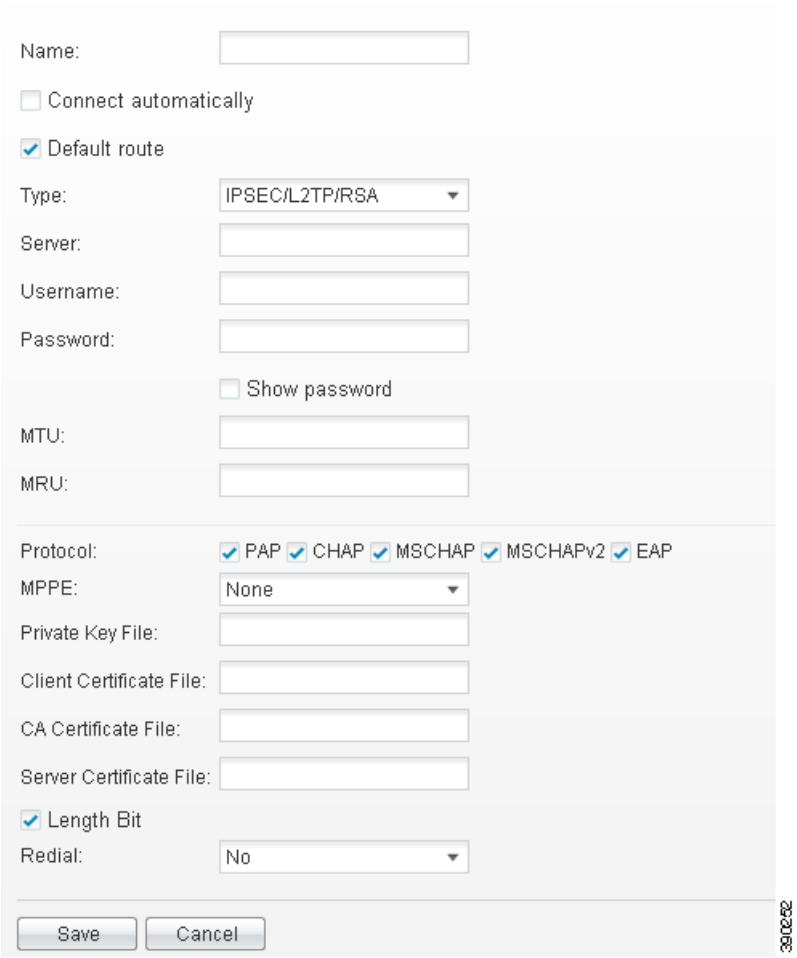
Step 11 Enter the paths of the private key file, client certificate file, CA certificate file, and server certificate file.

Step 12 Choose Yes or No from the Redial drop-down list. If you choose Yes, enter the relevant values in the Timeout and Attempts fields. The value of Timeout multiplied by the value of Attempts is the time taken to connect the VPN server, which is 20 seconds, at most.

Step 13 Click **Save** to add the VPN connection.

Step 14 The VPN pane is updated to show the name and status of the new VPN connection.

Figure 3-26 Add VPN Connection—IPSEC/L2TP/RSA



Add a VPN connection of CISCO Type

To add a VPN connection of CISCO type, follow these steps:

Step 1 Click **VPN** in the left pane under the Network tab.

Step 2 Click + in the right pane.

Step 3 The Add VPN connection window is displayed (Figure 3-27).

Step 4 In the Add VPN connection window, enter the name of the VPN connection that you want to add in the Name field.

Step 5 Check the **Connect automatically** check box if you want the Cisco Edge 340 Series device to automatically connect to this VPN.

Step 6 Choose **CISCO** for the type of the VPN connection from the Type drop-down list.

Step 7 Enter the VPN server address, username, and password in the Server, Username, and Password fields. Check the **Show password** check box if you want the password to be displayed in plain text.

Step 8 Enter the value of the MTU and the MRU.

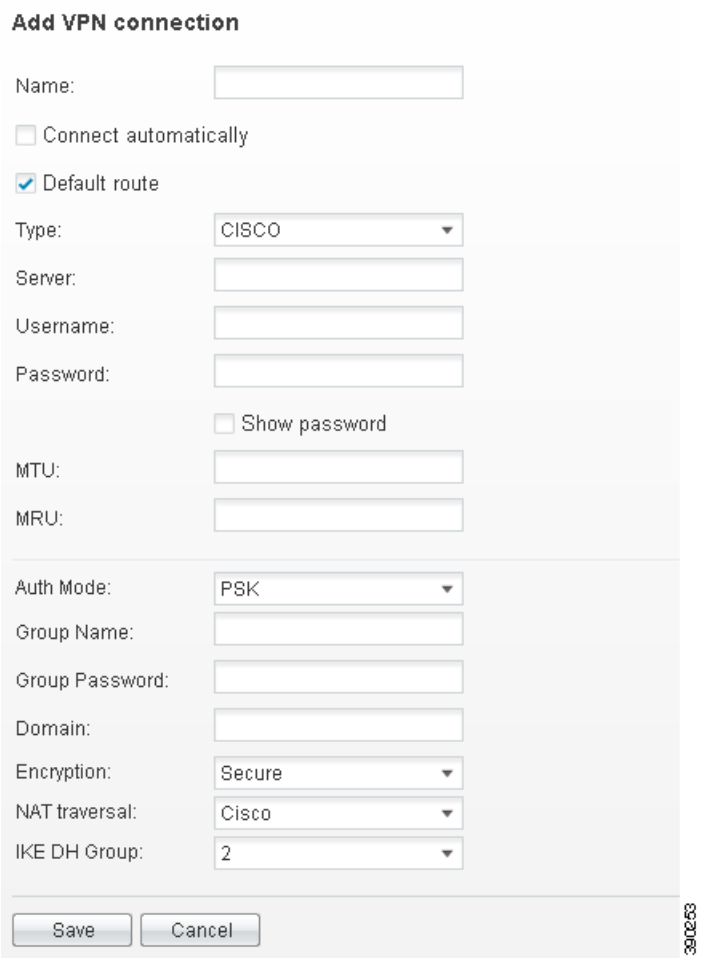
Step 9 Select PSK or Hybrid from the Auth Mode drop-down list.

Step 10 Enter the values in the Group Name, Group Password, Domain, Encryption, NAT traversal, and IKE DH Group fields. If you choose Hybrid as the auth mode, enter the path of CA certificate file.

Step 11 Click **Save** to add the VPN connection.

Step 12 The VPN pane is updated to show the name and status of the new VPN connection.

Figure 3-27 Add VPN Connection—CISCO



Edit a VPN Connection

To edit a VPN connection, follows these steps:

Step 1 From the Connections area, select the VPN connection that you want to edit, and click .

Step 2 Edit the configurations in the VPN connection screen.

Step 3 Click **Save**.

Remove a VPN Connection

To remove a VPN connection, select the VPN connection that you want to remove from the connection list in the Connections area, and click .

Connect a VPN Connection

To connect a VPN connection, select the VPN connection that you want to connect from the connection list in the Connections area, and click .

Monitor the Status of Platform and Network

You can monitor the status of the Cisco Edge 340 platform and the network using the Monitor tab. Figure 3-28 shows the Platform pane under the Monitor tab.

Figure 3-28 Platform Information

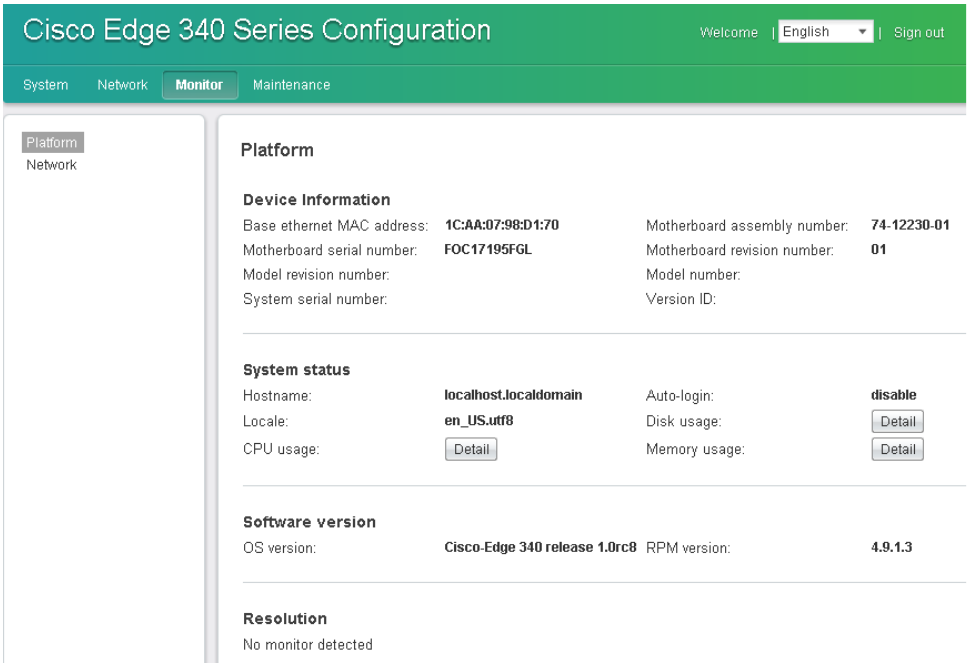
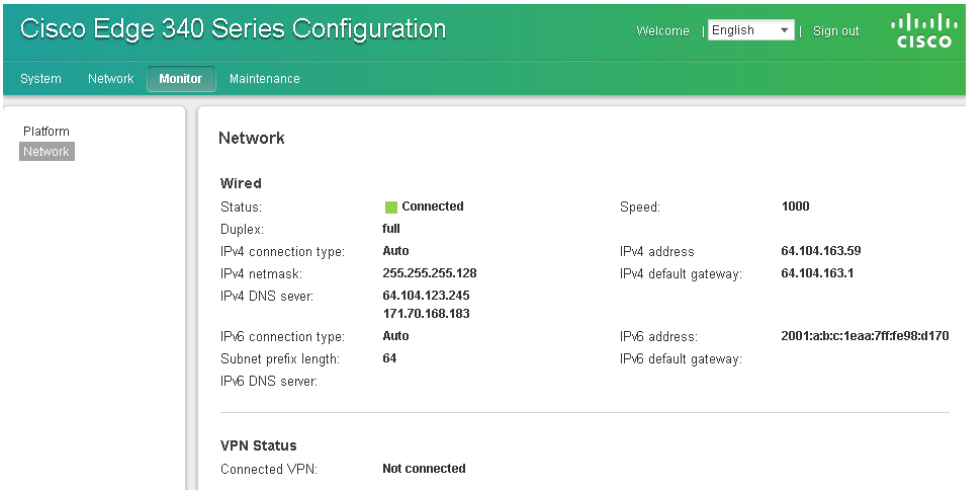


Figure 3-29 shows the Network pane under the Monitor tab.

Figure 3-29 Network Information



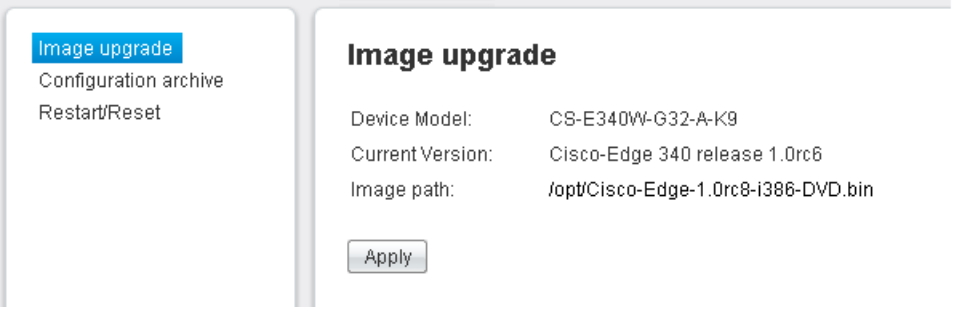
Maintenance

You can perform image upgrade, archive of the configuration, and restart or reset the Cisco Edge 340 Series device in the Maintenance tab.

Image Upgrade

Using the Image upgrade pane, you can view information pertaining to the device model and current version, and check if there is an available upgrade image file (.bin) in the /opt directory. If yes, click **Apply** to upgrade the system, as shown in Figure 3-30.

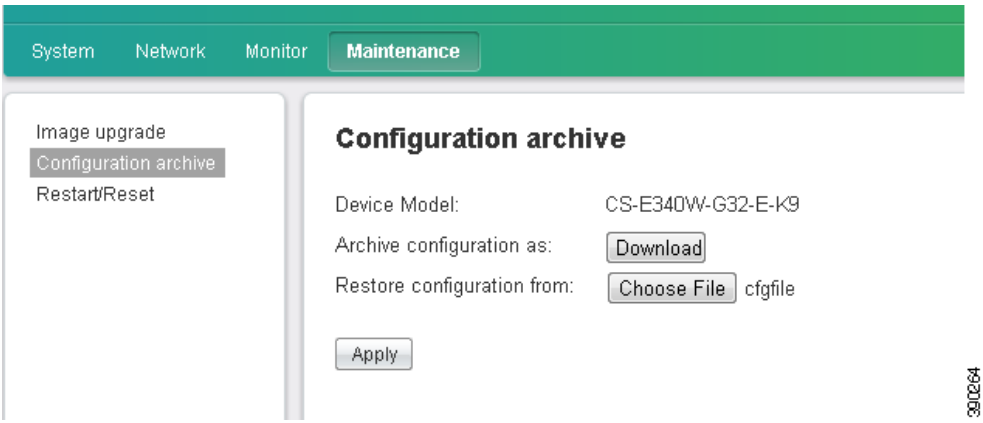
Figure 3-30 Image Upgrade Information



Configuration Archive

Using the Configuration archive pane, you can download the configuration file to either a USB storage or a local directory by clicking **Download**, as shown in Figure 3-31.

Figure 3-31 Configuration Archive Information



To copy the configuration file from one Cisco Edge 340 Series device to another Cisco Edge 340 Series device, follow these steps:

Step 1 Click **Download** to download the configuration file from the original Cisco Edge 340 Series device.

Step 2 Save the configuration file to another Cisco Edge 340 Series device by copying the configuration file locally or remotely.

Step 3 Open the web GUI from the second Cisco Edge 340 Series device, and click **Configuration archive** in the left pane under the Maintenance tab.

Step 4 Click **Choose File** to select the configuration file that you have saved in Step 2. The file name is displayed next to the Choose File button.

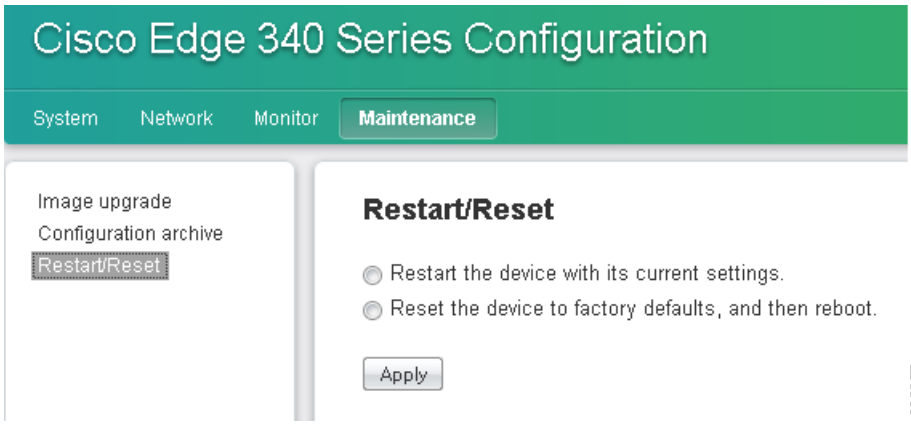
Step 5 Click **Apply.**

Step 6 The Cisco Edge 340 Series device reboots.

Restart or Reset

Using the Restart/Reset pane, you can restart the Cisco Edge 340 Series device with its current settings, or reset the Cisco Edge 340 Series device to factory defaults, and then reboot.

Figure 3-32 Restart/Reset Information



Troubleshooting

This appendix provides information about troubleshooting the Cisco Edge 340 Series device with the following issues:

Boot and Login

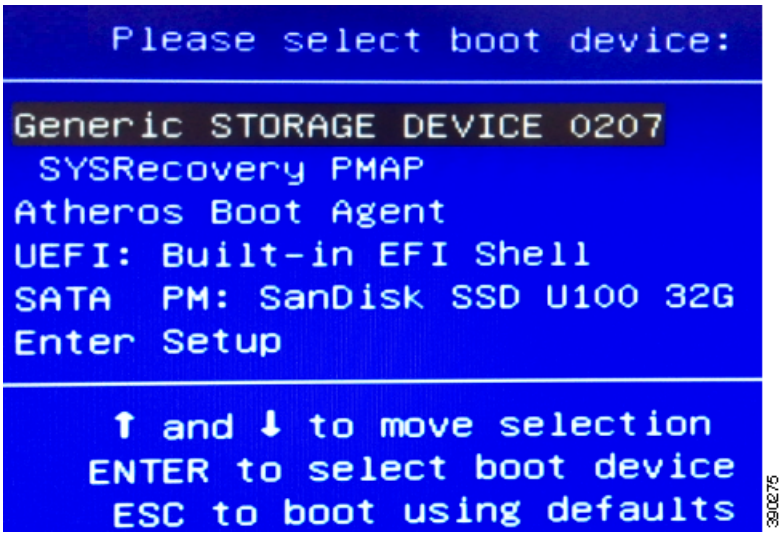
This section provides troubleshooting information about boot and login issues.

Forget Root Password

If you forget the root password of a Cisco Edge 340 Series device, follow these steps:

Step 1 Restart the Cisco Edge 340 Series device and press **F12** to enter the privileged mode as shown in Figure A-1.

Figure A-1 Select Boot Device



Step 2 Select **SYSRecovery PMAP** to enter the Troubleshooting screen.

Step 3 Choose language and keyboard type, and choose **NO** for the network disable item, and click **Continue** to enter the Rescue Mode.

Step 4 Select **Shell** to enter the root shell, and run the command **chroot /mnt/sysimage/** command to start the system.

Step 5 Enter the **passwd** command to reset your root password, as shown in the following example:

```
Starting shell...
bash-4.2# chroot /mnt/
install/ sysimage/
bash-4.2# chroot /mnt/sysimage/
sh-4.2# passwd
Changing password for user root.
New password:
BAD PASSWORD: it is based on a dictionary word
Retype new password:
passwd: all authentication tokens updated successfully.
sh-4.2#
```

System Starts Slowly

If the system takes more than one or two minutes to start, follow these steps:

Step 1 Plug in the console cable of the Cisco Edge 340 Series device.

Step 2 Check the log printed on the terminal to verify if the problem is caused by the insufficient power support from external devices.

Step 3 If yes, disconnect the external devices and restart the system. Alternatively, power off the Cisco Edge 340 Series device and restart it.

Step 4 If the problem is not caused by external devices, record the system log and contact a Cisco support representative.

System Locked After Using Wrong Password Five Times

If type the wrong password more than five times when you log in, the system is locked for 15 seconds. After 15 seconds have lapsed, the screen is unlocked and you can retype the password.

Reset and Upgrade

This section provides troubleshooting information about reset and upgrade issues.

Having Trouble Updating the System

If you have trouble updating the system of a Cisco Edge 340 Series device, perform one of the following actions:

- If you can log in to the system, execute the ***.bin** file to update the system automatically.
- If you cannot log in to the system, press **F12** when you start the Cisco Edge 340 Series device, and enter the privileged mode and choose **SYSRecovery PMAP** as the boot device, as shown in Figure A-1.
- Create a USB recovery disk with the ***.bin /dev/sdb1** command. Press **F12** when you start the Cisco Edge 340 Series device, and enter the privileged mode and choose your USB device as the boot device.

Restore Factory Settings Action Fails in Web GUI

If you fail to restore the factory settings in the Web GUI, try again by clicking **Restart/Reset** in the left pane under the Maintenance tab.

Display Issues

This section provides troubleshooting information about display issues.

No Signal Output

If you do not find signal output after connecting a monitor, and the network status of the Cisco Edge 340 Series device is Disconnected, follow these steps:

Step 1 Check if power is flowing to the monitor.

Step 2 Check if the VGA or HDMI connector is correctly connected.

Step 3 If both the power and connection are fine, use the console port to trouble shoot. Log in to the system with root permission. Enter the **DISPLAY:=0.0 xrandr** command to check if the monitor is detected by the Cisco Edge 340 Series device.

Note If the issue is not resolved, reimage the device.

Screen Blurred After Resolution is Changed

If you find the screen is blurred after changing the resolution, take one of the following actions:

- Check the connection of the Cisco Edge 340 Series device and the monitor, and restart the system.
- Change the current resolution to a new value in the web GUI.

Network Issues

This section provides troubleshooting information about network issues.

Connection Status Not Refreshed in the WiFi Station Mode

In the WiFi station mode, if you find that the connection status is not refreshed to be connected after connecting to an AP, click the **Refresh** button in the web GUI. If the issue still exists, click the **Wireless** option on the left navigation pane to refresh the screen.

Wake On LAN Not Effective

If the Wake on LAN is not effective, take one of the following actions:

- Verify that the Wake on LAN function is enabled on the Cisco Edge 340 Series device.
- Verify that the remote devices and the Cisco Edge 340 Series device are in the same broadcast domain.

DNS Not Parsed

Cisco Edge 340 Series supports up to three DNS servers. If the top three DNS servers cannot be parsed, other DNS servers can not be used although they are valid.

If the DNS cannot be parsed, edit the **resolve.config** file by entering the **#vi /etc/resolve.config** command to replace the top three DNS servers with the other valid servers.

Third-Party Device Cannot be Connected

If a third-party device that is in the station mode cannot connect to the Cisco Edge 340 Series device that is in the AP mode, take one of the following actions:

- Verify if the encryption and authentication mechanism between the third-party device and Cisco Edge 340 Series are matched.
- Verify if the network card in the third-party device supports 5G. The network cannot be connected unless this item is matched.

Power Issues

This section provides troubleshooting information about power issues.

Power Shortage of Peripheral Equipment

If the peripheral equipment is suffering from a power shortage and the Cisco Edge 340 Series device is powered by Power Over Ethernet (PoE), verify if the device is powered by PoE 802.3AF. If yes, change it to the 802.3AT mode, because the power supported by 802.3AT is more stable than the power supported by 802.3AF.

USB Ports on the Rear Panel Not Working

If only the two USB ports on the front panel are working, and the USB ports on the rear panel have no power, verify if the Cisco Edge 340 Series device is powered by PoE. To enable the USB ports on the rear panel, use external power supply.