

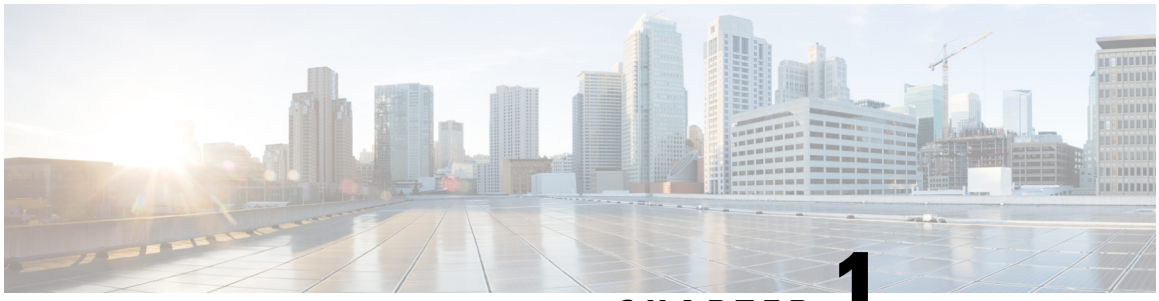
Cisco Embedded Services 3300 Series Configuration

First Published: 2018-08-15

Last Modified: 2023-10-23

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

© 2018–2023 Cisco Systems, Inc. All rights reserved.



CHAPTER 1

Cisco Embedded Service 3300 Series Switches Software Configuration Overview

This section contains:

- General Description, on page 1
- Finding Feature Information, on page 2
- SKU Information, on page 2
- Main Module, on page 3
- Expansion Module, on page 3
- SD Support, on page 4
- SFP Support, on page 4
- Secure Boot Architecture, on page 6

General Description

The Cisco ESS 3300 is an embedded Ethernet switch card that has a small form factor board size. The compact design simplifies integration and offers system integrators the ability to use the Cisco ESS 3300 in a wide variety of applications. The Cisco ESS 3300 consists of a Main Board and an optional Expansion Board. Both the Main Board and the Expansion Board are available with Cisco-designed cooling plates, and are also available without the cooling plates for system integrators who want to design their own custom thermal solutions.

The ESS-3300 is a ruggedized GigE Embedded platform for tactical, outdoor and mobile installations. Some of the key features are:

- Main Board – 2 Optical 10G + 8 GE ports (4 combo)
- Expansion Board – 16 GE ports (4 combo)
- Next Generation IE switch feature set
- Software: IOS-XE, Network Essentials and Network Advantage
- Native PoE software visibility
- Push Button, that supports the Zero-ize feature
- Two alarm inputs and One alarm output
- One SD interface
- One USB 2.0 Host interface for USB Flash Memory Device.
- One USB 2.0 Console Interface.

- One RS-232 Console Interface.

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

SKU Information

The following table lists the different SKUs available for the ESS3300.

Table 1: Cisco ESS 3300 SKUs

SKU	Description	Feature Software	Ports
ESS-3300-NCP-E	Main Board without a cooling plate.	Network Essentials	2 ports of 10 GE fiber, 8 ports of GE copper. 4 of the 8 GE copper ports can also be combo ports.
ESS-3300-CON-E	Main Board conduction cooled	Network Essentials	2 ports of 10 GE fiber, 8 ports of GE copper. 4 of the 8 GE copper ports can also be combo ports
ESS-3300-24T-NCP-E	Main Board with a 16p Expansion Board without a cooling plate	Network Essentials	2 ports of 10 GE fiber, 24 ports of GE copper 4 of 8 GE ports can be combo ports on mainboard 4 of 16 GE ports can be combo ports on expansion board
ESS-3300-24T-CON-E	Main Board with a 16p Expansion Board conduction cooled	Network Essentials	2 ports of 10 GE fiber, 24 ports of GE copper 4 of 8 GE ports can be combo ports on mainboard 4 of 16 GE ports can be combo ports on expansion board
ESS-3300-NCP-A	Main Board without a cooling plate.	Network Advantage	2 ports of 10 GE fiber, 8 ports of GE copper. 4 of the 8 GE copper ports can also be combo ports.

SKU	Description	Feature Software	Ports
ESS-3300-CON-A	Main Board conduction cooled	Network Advantage	2 ports of 10 GE fiber, 8 ports of GE copper. 4 of the 8 GE copper ports can also be combo ports
ESS-3300-24T-NCP-A	Main Board with a 16p Expansion Board without a cooling plate	Network Advantage	2 ports of 10 GE fiber, 24 ports of GE copper 4 of 8 GE ports can be combo ports on mainboard 4 of 16 GE ports can be combo ports on expansion board
ESS-3300-24T-CON-A	Main Board with a 16p Expansion Board conduction cooled	Network Advantage	2 ports of 10 GE fiber, 24 ports of GE copper 4 of 8 GE ports can be combo ports on mainboard 4 of 16 GE ports can be combo ports on expansion board

Main Module

- 2 - Optical 10G Ports on the main module
- 4 - 1G Combo Ports on the main module
  - Support 10/100/1000 Copper
  - Support 100/1000 SFP interfaces
- 4 - Dedicated 10/100/1000 Copper ports on the main module for total of 8 – 1G network ports

Note MACsec is not available for the two 10 / 1 GE uplink ports (regardless of the speed used) due to hardware constraints.

Expansion Module

- 4 - 1G Combo Ports on the main module
  - Support 10/100/1000 Copper
  - Support 100/1000 SFP interfaces
- 12 - Dedicated 10/100/1000 Copper ports on the main module for total of 16 network ports

Note 802.3af and 802.3at support is available if the integrator provides the PoE controllers on their finished product.

The ESS-3300 supports IOS-XE software control of PoE if the integrator adds the appropriate circuitry to their host chassis.

SD Support

SFP Support

Both 100BASE-X and 1000BASE-X SFP transceivers are supported by the eight combo ports, four on the Main Board and four on the Expansion Board.

Supported SFP+ Modules

The following table lists the supported SFP+ Modules.

SFP	Distance	Fiber	Commercial (0C to 70C)	Extended (-5C to 85C)	Industrial (-40C to 85C)	DOM
SFP-10G-SR-X	2 km	MMF		X		
SFP-10G-LR-X	10 km	SMF		X		
SFP-10G-SR	2 km	MMF	X			
SFP-10G-LR	10 km	SMF	X			
SFP-10G-ER	40 km	SMF	X			
SFP-10G-BXD-I	10 km	SMF			X	
SFP-10G-BXU-I	10 km	SMF			X	
SFP-10G-BX40D-I	40 km	SMF			X	
SFP-10G-BX40U-I	40 km	SMF			X	
SFP-H10G-CU1M	1 m	Passive Twinax	X			
SFP-H10G-ACU7M		Active Twinex	X			
SFP-H10G-ACU10M		Active Twinex	X			

Supported SFP Modules

The following table lists the Supported SFP Modules.

SFP	Distance	Fiber	Commercial (0C to 70C)	Extended (-5C to 85C)	Industrial (-40C to 85C)	DOM
GLC-SX-MM-RGD	220-550 m	MMF			X	

SFP	Distance	Fiber	Commercial (0C to 70C)	Extended (-5C to 85C)	Industrial (-40C to 85C)	DDM
GLC-LX-SM-RGD	550 m/10 km	MMF/SMF			X	
GLC-ZX-SM-RGD	70 km	SMF			X	X
SFP-GE-S	220-550 m	MMF		X		X
SFP-GE-L	550 m/10 km	MMF/SMF		X		X
SFP-GE-Z	70 km	SMF		X		X
GLC-BX-U	10 km	SMF	X			X
GLC-BX-D	10 km	SMF	X			X
GLC-SX-MM	220-550 m	MMF	X			
GLC-LH-SM	550 m/10 km	MMF/SMF	X			
GLC-ZX-SM	70 km	SMF	X			X
GLC-EX-SMD	40 km	SMF	X			X

Supported Fast Ethernet SFP Modules

The following table lists the Supported Fast Ethernet SFP Modules.

SFP	Distance	Fiber	Commercial (0C to 70C)	Extended (-5C to 85C)	Industrial (-40C to 85C)	DDM
GLC-FE-100FX-RGD	2 km	MMF			X	
GLC-FE-100LX-RGD	10 km	SMF			X	
GLC-FE-100FX	2 km	MMF	X			
GLC-FE-100LX	10 km	SMF	X			
GLC-FE-100EX	40 km	SMF	X			
GLC-FE-100ZX	80 km	SMF	X			
GLC-FE-100BX-U	10 km	SMF	X			
GLC-FE-100BX-D	10 km	SMF	X			

Secure Boot Architecture

The processor uses a multi-stage boot process that supports both a non-secure and a secure boot. For a secure boot, the system decrypts and authenticates the images while the 4096-bit RSA block authenticates the image. Upon reset, the CPU reads the device mode pins to determine the primary boot device to be used. Booting from these flash boot devices is supported.

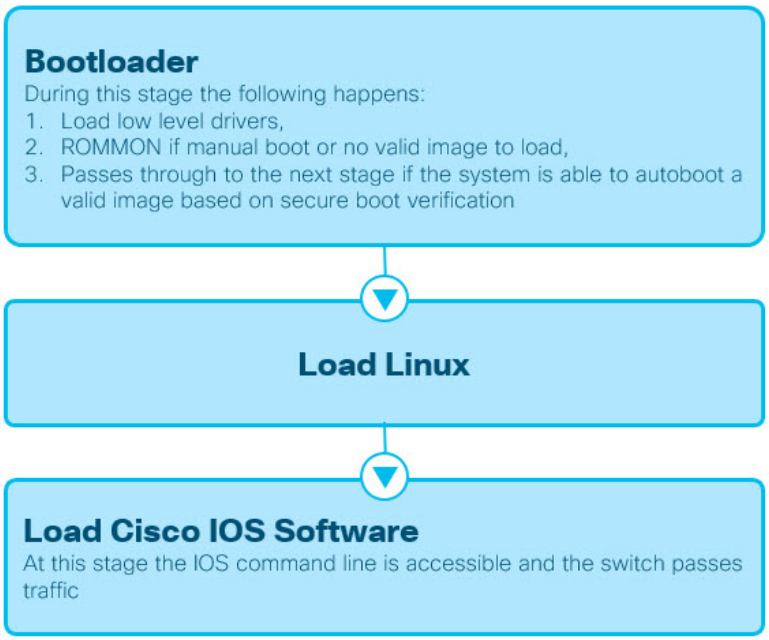
- SD Flash
- On-board Flash

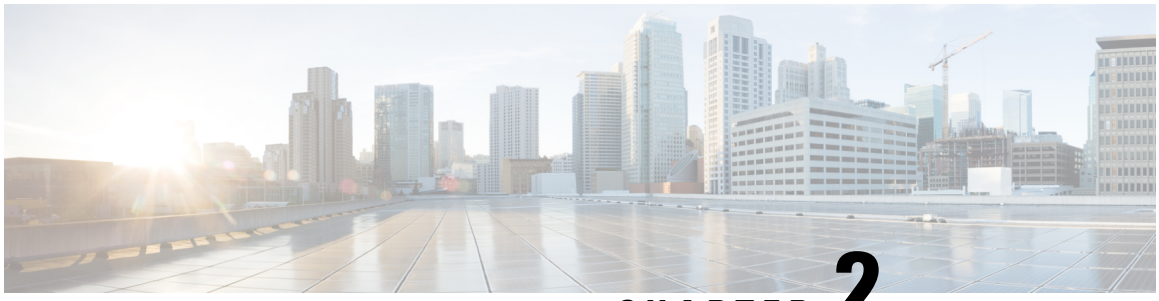
Note The prior generation, ESS 2020, runs Cisco IOS Classic while the ESS 3300 uses Cisco IOS XE.

Auto Boot Stages

See the following graphic for an illustration of the auto boot sequence.

Figure 1: Auto Boot Stages





CHAPTER 2

Installation and Boot

This section contains the following:

- Configuring the Switch with the CLI-Based Setup Program, on page 7
- Upgrading the Switch Software, on page 23
- Software Boot Modes, on page 25
- Licensing, on page 28
- Boot from the USB, on page 36
- Clearing the Startup Configuration, on page 37
- Emergency Recovery Installation, on page 38

Configuring the Switch with the CLI-Based Setup Program

This section provides a command-line interface (CLI)-based setup procedure for a switch. You must be connected to the switch through the console port to use the CLI. The ESS3300 auto detects whether the console port is RJ-45 or USB.

If using an RJ-45 console connection, configure with these parameters:

- 9600 baud
- 8 data bits
- 1 stop bit
- No parity
- None (flow control)

If you are connecting the switch USB-mini console port to a Windows-based PC for the first time, install a USB driver. If your laptop or PC warns you that you do not have the proper drivers to communicate with the router, you can obtain them from your computers manufacturer, or go here: https://www.silabs.com/products/development-tools/software/usb-to-uart-bridge-vcp-drivers

Start the terminal-emulation program on the PC or the terminal. The program, frequently a PC application such as HyperTerminal or ProcommPlus, makes communication possible between the switch and your PC or terminal.

Connect power to the device. The PC or terminal displays the bootloader sequence. Press **Enter** to display the setup prompt.

Entering the Initial Configuration Information

To set up the switch, you need to complete the setup program, which runs automatically after the switch is powered on. You must assign an IP address and other configuration information necessary for the switch to communicate with the local routers and the Internet. This information is also required if you plan to use WebUI to configure and manage the switch.

In Cisco IOS XE 17.10.1 and later, you can set a password encryption level so that user passwords are not stored in plain text. See System Security Configuration (Cisco IOS XE 17.10.1 and later), on page 10.

IP Settings

You need this information from your network administrator before you complete the setup program:

- Encryption level and Master key (Cisco IOS XE 17.10.1 and later)
- Switch IP address
- Subnet mask (IP netmask)
- Default gateway (router)
- Enable secret password
- Enable password

Initial Configuration (Cisco IOS XE 17.9.x and earlier)

Complete the following steps to create an initial configuration for the switch with the setup program:

1. Enter **Yes** at these two prompts:

```
Would you like to enter the initial configuration dialog? [yes/no]: yes
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system.
Would you like to enter basic management setup? [yes/no]: yes
```

2. Enter a hostname for the switch, and press **Return**.

   On a command switch, the hostname is limited to 28 characters; on a member switch, it is limited to 31 characters. Do not use *-n* , where n is a number, as the last character in a hostname for any switch.

```
Enter host name [Switch]: host_name
```

3. Enter an enable secret password, and press **Return**.

   The password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, allows spaces, but ignores leading spaces. The secret password is encrypted, and the enable password is in plain text.

```
Enter enable secret: secret_password
```

4. Enter an enable password, and press **Return**.

```
Enter enable password: enable_password
```

5. Enter a virtual terminal password, and press **Return**.

   The password can be from 1 to 25 alphanumeric characters, is case sensitive, allows spaces, but ignores leading spaces.

```
Enter virtual terminal password: terminal-password
```

6. (Optional) Configure Simple Network Management Protocol (SNMP) by responding to the prompts. You can also configure SNMP later through the CLI, Device Manager, or the Cisco Network Assistant application. To configure SNMP later, enter **no**.

```
Configure SNMP Network Management? [no]: no
```

7. Enter the interface name (physical interface or VLAN name) of the interface that connects to the management network, and press **Return**. For this release, always use **vlan1** as that interface.



Note The switch will transmit a DHCP discover message on the **vlan1** interface. If the switch is connected to the network before the CLI initial setup process is started, the interface may have been assigned a dynamic IP address. It is all right if you do not see an IP address on the **vlan1** interface. This process allows you set a static IP address for management, which will over write the dynamically assigned IP address.

```
Current interface summary
Any interface listed with OK? value "NO" does not have a valid configuration
Interface IP-Address OK? Method Status Protocol
Vlan1 unassigned NO unset up down
GigabitEthernet1/1 unassigned YES unset down down
GigabitEthernet1/2 unassigned YES unset down down
GigabitEthernet1/3 unassigned YES unset down down
GigabitEthernet1/4 unassigned YES unset down down
GigabitEthernet1/5 unassigned YES unset down down
GigabitEthernet1/6 unassigned YES unset down down
GigabitEthernet1/7 unassigned YES unset down down
GigabitEthernet1/8 unassigned YES unset down down
GigabitEthernet1/9 unassigned YES unset down down
GigabitEthernet1/10 unassigned YES unset down down
Enter interface name used to connect to the
management network from the above interface summary: vlan1
Enter interface name used to connect to the
management network from the above interface summary: vlan1
```

8. Configure the interface by entering the switch IP address and subnet mask and pressing Return. The IP address and subnet masks shown here are examples.

```
Configuring interface Vlan1:
Configure IP on this interface? [yes]:
IP address for this interface: 10.1.1.2
Subnet mask for this interface [255.255.255.0] :
Class A network is 10.0.0.0, 8 subnet bits; mask is /24
```

9. This summary appears:

```
The following configuration command script was created:
hostname ie3300
enable secret 9 $9$rkqtjJhIkZyANU$Ib4nfuxrpHBi.lixF.0Ir94k9XWYsW3nyF7Glmc6lkc
enable password cisco
line vty 0 15
```

```
password cisco
no snmp-server
!!
interface Vlan1
no shutdown
ip address 10.1.1.2 255.255.255.0
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface GigabitEthernet1/3
!
interface GigabitEthernet1/4
!
interface GigabitEthernet1/5
!
interface GigabitEthernet1/6
!
interface GigabitEthernet1/7
!
interface GigabitEthernet1/8
!
interface GigabitEthernet1/9
!
interface GigabitEthernet1/10
!
end
```

After you complete the setup program, the switch can run the default configuration that you created. If you want to change this configuration or want to perform other management tasks, use one of these tools:

- Command-line interface (CLI)

To use the CLI, enter commands at the Switch> prompt through the console port by using a terminal emulation program. For configuration information, see the switch Cisco Catalyst IE3x00 Rugged Switch software configuration guides.

System Security Configuration (Cisco IOS XE 17.10.1 and later)

For enchanced security, sensitive information such as passwords needs to be encrypted. The configuration dialog includes a System Security Configuration Dialog that allows you to set the password encryption level. Encryption levels include type-6 and type-7 encryption. It is recommended that you enable both types.

- Type-6 uses Advanced Encryption Standard (AES) for encrypting the passwords. Type-6 password encryption and decryption is coupled with a master-key that you enter. You must remember the master key because it cannot be recovered.
- The master key is the password/key used to encrypt all other keys in the switch configuration with the use of an AES symmetric cipher. The master key is not stored in the switch configuration and cannot be seen or obtained in any way while connected to the switch. Once configured, the master key is used to encrypt any existing or new keys in the switch configuration. Keys are not encrypted until you issue the **password encryption aes** command.
- Type-7 passwords are an obfuscation of the original plain text password. It is based on Vigenere Cipher and prevents someone seeing the real passwords in a configuration.

You can use the setup program to set the password encryption level on both a new switch and a switch that is already configured. For a new switch, see Initial Configuration - Type-6 Encryption, on page 11 or Initial

Configuration - Type-7 Encryption, on page 14. To configure system security settings without running the initial setup, see Setting the Password Encryption Level, on page 17.

Initial Configuration - Type-6 Encryption

To create an initial configuration for the switch with the setup program with type-6 encryption, complete the following steps:

Before you begin

Access the CLI as described in Configuring the Switch with the CLI-Based Setup Program, on page 7.

Procedure

Step 1 Enter **Yes** at the following prompt:

```
        --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: yes
```

Step 2 At the prompt, enter the password encryption level that you want to apply:

```
  -----System Security Configuration Dialog-----

 Cisco recommends that for enchanced security users should encrypt sensitive info
 The configuration dialog will allow you to set encryption level
 It is recommended that both type-6 & type-7 encryption should be enabled by user
 For type-6 user will need to create and remember Master key as it cannot be recovered

 [0] for both type-6 & type-7 encryption to be applied on the box
 [1] for only type-7 encryption to be applied on the box
 [2] for no encryption to be applied on the box

 Enter your encryption selection [2]: 0
```

Note
In Cisco IOS XE 17.10.1, if you select both type 6 & type 7 encryption [0], only the username is automatically converted to type 6, and the enable password and the line vty password are automatically converted to type 7 instead of type 6.

Step 3 Enter the master key to be used to encrypt all other keys in the switch:

```
Enter the Master key min 8 chars  & max 127 chars, Master key should not begin with '!, #, ;' :
************
```

Step 4 Enter the master key again to confirm it:

```
Confirm the master key: ************

The following configuration command script was created:

key config-key password-encrypt
Testkey12345
!
password encryption aes
service password-encryption
!
!
end
```

Note
You should save the Master Key, because you will need it if this device is replaced.

Step 5 Enter **2** at the prompt to save the System Security Configuration:

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.
```

Step 6 Enter **yes** at the prompt to configure basic management settings:

```
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:
```

Step 7 Enter a hostname for the switch:

```
Enter host name [Switch]: Switch123
```

Step 8 Enter an enable secret password:

```
 The enable secret is a password used to protect
  access to privileged EXEC and configuration modes.
  This password, after entered, becomes encrypted in
  the configuration.
  ------------------------------------------------
  secret should be of minimum 10 characters and maximum 32 characters with
  at least 1 upper case, 1 lower case, 1 digit and
  should not contain [cisco]
  ------------------------------------------------
  Enter enable secret: **********
```

Step 9 Enter the enable secret password again to confirm it:

```
 Confirm enable secret: **********
```

Step 10 Enter an enable password:

```
 The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: ********
```

Step 11 Enter a virtual terminal password.

The password can be from 1 to 25 alphanumeric characters, is case sensitive, allows spaces, but ignores leading spaces.

```
  The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: ********
```

Step 12 Enter the interface name (physical interface or VLAN name) of the interface that connects to the management network. For this release, always use **vlan1** as that interface.

Note
The switch will transmit a DHCP discover message on the **vlan1** interface. If the switch is connected to the network before the CLI initial setup process is started, the interface may have been assigned a dynamic IP address. It is all right if you do not see an IP address on the **vlan1** interface. This process allows you set a static IP address for management, which will over write the dynamically assigned IP address.

```
Current interface summary

Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  10.16.1.120     YES DHCP   up                    up
GigabitEthernet1/1     unassigned      YES unset  up                    up
GigabitEthernet1/2     unassigned      YES unset  down                  down
GigabitEthernet1/3     unassigned      YES unset  up                    up
GigabitEthernet1/4     unassigned      YES unset  down                  down
GigabitEthernet1/5     unassigned      YES unset  down                  down
GigabitEthernet1/6     unassigned      YES unset  down                  down
GigabitEthernet1/7     unassigned      YES unset  up                    up
GigabitEthernet1/8     unassigned      YES unset  up                    up
GigabitEthernet1/9     unassigned      YES unset  down                  down
GigabitEthernet1/10    unassigned      YES unset  down                  down
AppGigabitEthernet1/1  unassigned      YES unset  up                    up

Enter interface name used to connect to the
management network from the above interface summary: vlan1

Configuring interface Vlan1:
    IP address for this interface [10.16.1.120]:
    Subnet mask for this interface [255.0.0.0] :
    Class A network is 10.0.0.0, 8 subnet bits; mask is /8

The following configuration command script was created:

hostname Switch123
enable secret 9 $9$4kYFyV4Hh9JVOk$Cwi3/tNTc7uHy7CBsBfOWo6u1q/Sg07in3NJ5e7Yy0U
enable password 0 password
service password-encryption
line vty 0 15
password 0 password
no snmp-server
!
!
interface Vlan1
no shutdown
ip address 10.16.1.120 255.0.0.0
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface GigabitEthernet1/3
!
interface GigabitEthernet1/4
```

Step 13 Enter **2** to save the configuration:

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]:  2
```

```
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.



Press RETURN to get started!
```

What to do next

After you complete the setup program, the switch can run the default configuration that you created. If you want to change this configuration or want to perform other management tasks, use one of these tools:

- Command-line interface (CLI)
- Web User Interface (WebUI)

To use the CLI, enter commands at the *Switch* > prompt through the console port by using a terminal emulation program or through the network by using Telnet. For configuration information, see the configuration guides for the Cisco IE3x00 switches.

To use WebUI, see the online help for WebUI.

Initial Configuration - Type-7 Encryption

To create an initial configuration for the switch with the setup program with only type-7 encryption, complete the following steps:

Before you begin

Access the CLI as described in Configuring the Switch with the CLI-Based Setup Program, on page 7.

Procedure

Step 1 Enter **Yes** at the following prompt:

```
        --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: yes
```

Step 2 At the prompt, enter **1** to apply only type-7 password encryption:

```
  -----System Security Configuration Dialog-----

 Cisco recommends that for enchanced security users should encrypt sensitive info
 The configuration dialog will allow you to set encryption level
 It is recommended that both type-6 & type-7 encryption should be enabled by user
 For type-6 user will need to create and remember Master key as it cannot be recovered

 [0] for both type-6 & type-7 encryption to be applied on the box
 [1] for only type-7 encryption to be applied on the box
 [2] for no encryption to be applied on the box

 Enter your encryption selection [2]: 1
```

Step 3 Enter **2** at the prompt to save the System Security Configuration:

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.
```

Step 4 Enter **yes** at the prompt to configure basic management settings:

```
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:
```

Step 5 Enter a hostname for the switch:

```
Enter host name [Switch]: Switch123
```

Step 6 Enter an enable secret password:

```
 The enable secret is a password used to protect
  access to privileged EXEC and configuration modes.
  This password, after entered, becomes encrypted in
  the configuration.
  ------------------------------------------------
  secret should be of minimum 10 characters and maximum 32 characters with
  at least 1 upper case, 1 lower case, 1 digit and
  should not contain [cisco]
  ------------------------------------------------
  Enter enable secret: **********
```

Step 7 Enter the enable secret password again to confirm it:

```
 Confirm enable secret: **********
```

Step 8 Enter an enable password:

```
 The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: ********
```

Step 9 Enter a virtual terminal password.

The password can be from 1 to 25 alphanumeric characters, is case sensitive, allows spaces, but ignores leading spaces.

```
  The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: ********
```

Step 10 Enter the interface name (physical interface or VLAN name) of the interface that connects to the management network. For this release, always use **vlan1** as that interface.

Note
The switch will transmit a DHCP discover message on the **vlan1** interface. If the switch is connected to the network before the CLI initial setup process is started, the interface may have been assigned a dynamic IP address. It is all right if you do not see an IP address on the **vlan1** interface. This process allows you set a static IP address for management, which will over write the dynamically assigned IP address.

```
Current interface summary

Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  10.16.1.120     YES DHCP   up                    up
GigabitEthernet1/1     unassigned      YES unset  up                    up
GigabitEthernet1/2     unassigned      YES unset  down                  down
GigabitEthernet1/3     unassigned      YES unset  up                    up
GigabitEthernet1/4     unassigned      YES unset  down                  down
GigabitEthernet1/5     unassigned      YES unset  down                  down
GigabitEthernet1/6     unassigned      YES unset  down                  down
GigabitEthernet1/7     unassigned      YES unset  up                    up
GigabitEthernet1/8     unassigned      YES unset  up                    up
GigabitEthernet1/9     unassigned      YES unset  down                  down
GigabitEthernet1/10    unassigned      YES unset  down                  down
AppGigabitEthernet1/1  unassigned      YES unset  up                    up

Enter interface name used to connect to the
management network from the above interface summary: vlan1

Configuring interface Vlan1:
    IP address for this interface [10.16.1.120]:
    Subnet mask for this interface [255.0.0.0] :
    Class A network is 10.0.0.0, 8 subnet bits; mask is /8

The following configuration command script was created:

hostname Switch123
enable secret 9 $9$4kYFyV4Hh9JVOk$Cwi3/tNTc7uHy7CBsBfOWo6u1q/Sg07in3NJ5e7Yy0U
enable password 0 password
service password-encryption
line vty 0 15
password 0 password
no snmp-server
!
!
interface Vlan1
no shutdown
ip address 10.16.1.120 255.0.0.0
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface GigabitEthernet1/3
!
interface GigabitEthernet1/4
```

Step 11 Enter **2** to save the configuration:

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]:  2
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.
```

```
Press RETURN to get started!
```

What to do next

After you complete the setup program, the switch can run the default configuration that you created. If you want to change this configuration or want to perform other management tasks, use one of these tools:

- Command-line interface (CLI)
- Web User Interface (WebUI)

To use the CLI, enter commands at the *Switch* > prompt through the console port by using a terminal emulation program or through the network by using Telnet. For configuration information, see the configuration guides for the Cisco IE3x00 switches.

To use WebUI, see the online help for WebUI.

Setting the Password Encryption Level

Follow this procedure to configure system security settings (type-6 and type-7 encryption) without running the initial setup.

Procedure

Step 1 Enter **No** at the following prompt:

```
         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:
Autoinstall trying DHCPv6 on Vlan1

Would you like to enter the initial configuration dialog? [yes/no]: no
```

Step 2 Enter the enable secret at the prompt:

```
  The enable secret is a password used to protect
  access to privileged EXEC and configuration modes.
  This password, after entered, becomes encrypted in
  the configuration.
  ------------------------------------------------
  secret should be of minimum 10 characters and maximum 32 characters with
  at least 1 upper case, 1 lower case, 1 digit and
  should not contain [cisco]
  ------------------------------------------------
  Enter enable secret: **********
  Confirm enable secret: **********

The following configuration command script was created:

enable secret 9 $9$YMkVvPLbxKn4bE$OAOX/akBBsukkRV1L.Tk7p2KaM0BXLQI.HbyGbXB8/g
!
end
```

Step 3 Enter **2** to save the configuration and go to the System Security Configuration:

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.
```

Step 4 At the prompt, enter the password encryption level that you want to apply:

```
  -----System Security Configuration Dialog-----

 Cisco recommends that for enchanced security users should encrypt sensitive info
 The configuration dialog will allow you to set encryption level
 It is recommended that both type-6 & type-7 encryption should be enabled by user
 For type-6 user will need to create and remember Master key as it cannot be recovered

 [0] for both type-6 & type-7 encryption to be applied on the box
 [1] for only type-7 encryption to be applied on the box
 [2] for no encryption to be applied on the box

 Enter your encryption selection [2]: 0
```

Step 5 Enter the master key to be used to encrypt all other keys in the switch:

```
Enter the Master key min 8 chars  & max 127 chars, Master key should not begin with '!, #, ;' :
************
```

Step 6 Enter the master key again to confirm it:

```
Confirm the master key: ************

The following configuration command script was created:

key config-key password-encrypt
Testkey12345
!
password encryption aes
service password-encryption
!
!
end
```

Note
You should save the Master Key, because you will need it if this device is replaced.

Step 7 Enter **2** at the prompt to save the System Security Configuration:

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.



Press RETURN to get started!
```

```
Switch>
```

CLI Setup Examples

Initial Configuration Example

```
         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: yes


  -----System Security Configuration Dialog-----

 Cisco recommends that for enchanced security users should encrypt sensitive info
 The configuration dialog will allow you to set encryption level
 It is recommended that both type-6 & type-7 encryption should be enabled by user
 For type-6 user will need to create and remember Master key as it cannot be recovered

 [0] for both type-6 & type-7 encryption to be applied on the box
 [1] for only type-7 encryption to be applied on the box
 [2] for no encryption to be applied on the box

 Enter your encryption selection [2]: 0

 Enter the Master key min 8 chars  & max 127 chars, Master key should not begin with '!,
#, ;' : ************

 Confirm the master key: ************

The following configuration command script was created:

key config-key password-encrypt
Testkey12345
!
password encryption aes
service password-encryption
!
!
end


[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.


At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system
```

```
Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:

  Enter host name [Switch]: Switch123

  The enable secret is a password used to protect
  access to privileged EXEC and configuration modes.
  This password, after entered, becomes encrypted in
  the configuration.
  ------------------------------------------------
  secret should be of minimum 10 characters and maximum 32 characters with
  at least 1 upper case, 1 lower case, 1 digit and
  should not contain [cisco]
  ------------------------------------------------
  Enter enable secret: **********
  Confirm enable secret: **********

  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: ********

  The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: ********

Current interface summary

Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  12.16.1.120     YES DHCP   up                    up
GigabitEthernet1/1     unassigned      YES unset  up                    up
GigabitEthernet1/2     unassigned      YES unset  down                  down
GigabitEthernet1/3     unassigned      YES unset  up                    up
GigabitEthernet1/4     unassigned      YES unset  down                  down
GigabitEthernet1/5     unassigned      YES unset  down                  down
GigabitEthernet1/6     unassigned      YES unset  down                  down
GigabitEthernet1/7     unassigned      YES unset  up                    up
GigabitEthernet1/8     unassigned      YES unset  up                    up
GigabitEthernet1/9     unassigned      YES unset  down                  down
GigabitEthernet1/10    unassigned      YES unset  down                  down
AppGigabitEthernet1/1  unassigned      YES unset  up                    up

Enter interface name used to connect to the
management network from the above interface summary: vlan1

Configuring interface Vlan1:
    IP address for this interface [12.16.1.120]:
    Subnet mask for this interface [255.0.0.0] :
    Class A network is 12.0.0.0, 8 subnet bits; mask is /8

The following configuration command script was created:

hostname Switch123
enable secret 9 $9$4kYFyV4Hh9JVOk$Cwi3/tNTc7uHy7CBsBfOWo6u1q/Sg07in3NJ5e7Yy0U
enable password 0 password
service password-encryption
line vty 0 15
password 0 password
no snmp-server
!
!
interface Vlan1
no shutdown
```

```
ip address 12.16.1.120 255.0.0.0
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface GigabitEthernet1/3
!
interface GigabitEthernet1/4


[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]:  2
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.



Press RETURN to get started!
```

System Security Configuration Example

```
         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:
Autoinstall trying DHCPv6 on Vlan1   yes


  -----System Security Configuration Dialog-----

 Cisco recommends that for enchanced security users should encrypt sensitive info
 The configuration dialog will allow you to set encryption level
 It is recommended that both type-6 & type-7 encryption should be enabled by user
 For type-6 user will need to create and remember Master key as it cannot be recovered

 [0] for both type-6 & type-7 encryption to be applied on the box
 [1] for only type-7 encryption to be applied on the box
 [2] for no encryption to be applied on the box

 Enter your encryption selection [2]: 0

 Enter the Master key min 8 chars  & max 127 chars, Master key should not begin with '!,
#, ;' : ************

 Confirm the master key: ************

The following configuration command script was created:

key config-key password-encrypt
Testkey12345
!
password encryption aes
service password-encryption
!
!
end
```

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.


At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:

  Enter host name [Switch]: Switch123

  The enable secret is a password used to protect
  access to privileged EXEC and configuration modes.
  This password, after entered, becomes encrypted in
  the configuration.
  ------------------------------------------------
  secret should be of minimum 10 characters and maximum 32 characters with
  at least 1 upper case, 1 lower case, 1 digit and
  should not contain [cisco]
  ------------------------------------------------
  Enter enable secret: **********
  Confirm enable secret: **********

  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: ********

  The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: ********

Current interface summary

Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  12.16.1.120     YES DHCP   up                    up
GigabitEthernet1/1     unassigned      YES unset  up                    up
GigabitEthernet1/2     unassigned      YES unset  down                  down
GigabitEthernet1/3     unassigned      YES unset  up                    up
GigabitEthernet1/4     unassigned      YES unset  down                  down
GigabitEthernet1/5     unassigned      YES unset  down                  down
GigabitEthernet1/6     unassigned      YES unset  down                  down
GigabitEthernet1/7     unassigned      YES unset  up                    up
GigabitEthernet1/8     unassigned      YES unset  up                    up
GigabitEthernet1/9     unassigned      YES unset  down                  down
GigabitEthernet1/10    unassigned      YES unset  down                  down
AppGigabitEthernet1/1  unassigned      YES unset  up                    up

Enter interface name used to connect to the
```

```
management network from the above interface summary: vlan1

Configuring interface Vlan1:
    IP address for this interface [12.16.1.120]:
    Subnet mask for this interface [255.0.0.0] :
    Class A network is 12.0.0.0, 8 subnet bits; mask is /8

The following configuration command script was created:

hostname Switch123
enable secret 9 $9$4kYFyV4Hh9JVOk$Cwi3/tNTc7uHy7CBsBfOWo6u1q/Sg07in3NJ5e7Yy0U
enable password 0 password
service password-encryption
line vty 0 15
password 0 password
no snmp-server
!
!
interface Vlan1
no shutdown
ip address 12.16.1.120 255.0.0.0
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface GigabitEthernet1/3
!
interface GigabitEthernet1/4


[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]:  2
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.



Press RETURN to get started!
```

Upgrading the Switch Software

This section covers the various aspects of upgrading or downgrading the device software.

Finding the Software Version

The package files for the Cisco IOS XE software can be found on the system board flash device flash (flash:) or external SDFlash (sdflash:).

You can use the **show version** privileged EXEC command to see the software version that is running on your switch.

Note Although the **show version** output always shows the software image running on the switch, the model name shown at the end of this display is the factory configuration and does not change if you upgrade the software license.

You can also use the **dir** *filesystem:* privileged EXEC command to see the directory names of other software images that you might have stored in flash memory.

Software Images

The switch runs on Cisco IOS-XE, using an image named ess3x00-universalk9.<*release*>.SPA.bin.

Automatic Boot Loader Upgrade

When you upgrade from the existing release on your switch to a later or newer release for the first time, the boot loader may be automatically upgraded, based on the hardware version of the switch. If the boot loader is automatically upgraded, it will take effect on the next reload.

For subsequent Cisco IOS XE releases, if there is a new bootloader in that release, it may be automatically upgraded based on the hardware version of the switch when you boot up your switch with the new image for the first time.

Caution Do not power cycle your switch during the upgrade.

Scenario	Automatic Boot Loader Response

If you boot Cisco IOS XE the first time	Boot loader may be upgraded to version "7.1.5" for ESS-3300.
	`Checking Bootloader upgrade...`
	`…`
	`Bootloader upgrade successful`

Software Installation Commands

Summary of Software Installation Commands	
To install and activate the specified file, and to commit changes to be persistent across reloads—**install add file** *filename* [**activate commit**]	
add file tftp: *filename*	Copies the install file package from a remote location to the device and performs a compatibility check for the platform and image versions.
activate [**auto-abort-timer**]	Activates the file, and reloads the device. The **auto-abort-timer** keyword automatically rolls back image activation.
commit	Makes changes persistent over reloads.

Summary of Software Installation Commands	
remove	Deletes all unused and inactive software installation files.

Software Boot Modes

Your device supports two modes to boot the software packages. Installed mode and Bundle mode.

Installed Boot Mode

You can boot your device in installed mode by booting the software package provisioning file that resides in flash:

```
Switch: boot flash:packages.conf
```

Note The packages.conf file for particular release is created on following the install workflow described in the section, *Installing a Software Package*.

The provisioning file contains a list of software packages to boot, mount, and run. The ISO file system in each installed package is mounted to the root file system directly from flash.

Note The packages and provisioning file used to boot in installed mode must reside in flash. Booting in installed mode from usbflash0: or tftp: is not supported.

Installing a Software Package

You can install, activate, and commit a software package using a single command or using separate commands. This task shows how to use the **install add file activate commit** command for installing a software package.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**install add file tftp:** *filename* [**activate commit**] **Example:** `Device# install add file tftp://192.168.0.1//tftpboot/folder1/ess9300_iosxe.17.04.01.SPA.bin activate commit`	Copies the software install package from a remote location (via FTP, HTTP, HTTPs, TFTP) to the device, performs a compatibility check for the platform and image versions, activates the software package, and makes the package persistent across reloads.

	Command or Action	Purpose
	`Device# install add file flash:ess9300_iosxe.17.04.01.SPA.bin activate commit`	• This command extracts the individual components of the .bin file into sub-packages and packages.conf file. • The device reloads after executing this command.
Step 3	**exit** **Example:** `Device# exit`	Exits privileged EXEC mode and returns to user EXEC mode.

Managing the Update Package

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**install add file tftp:** *filename* **Example:** `Device# install add file tftp://172.16.0.1//tftpboot/folder1/ess9300_iosxe.17.04.01.SPA.bin`	Copies the software install package from a remote location (via FTP, HTTP, HTTPs, TFTP) to the device, and performs a compatibility check for the platform and image versions. • This command extracts the individual components of the .bin file into sub-packages and packages.conf file.
Step 3	**install activate** [**auto-abort-timer**] **Example:** `Device# install activate`	Activates the added software install package, and reloads the device. • When doing a full software install, do not provide a package filename. • The **auto-abort-timer** keyword, automatically rolls back the software image activation. The automatic timer is triggered after the new image is activated. If the timer expires prior to the issuing of the **install commit** command, then the install process is automatically terminated. The device reloads, and boots up with a previous version of the software image.
Step 4	**install abort** **Example:** `Device# install abort`	(Optional) Terminates the software install activation, and rolls back to the version that was running before current installation procedure. • You can use this command only when the image is in an activated state; and not when the image is in a committed state.

	Command or Action	Purpose
Step 5	**install commit** **Example:** `Device# install commit`	Makes the changes persistent over reload. • The **install commit** command completes the new image installation. Changes are persistent across reloads until the auto-abort timer expires.
Step 6	**install rollback to committed** **Example:** `Device# install rollback to committed`	(Optional) Rolls back the update to the last committed version.
Step 7	**install remove** {**file** *filesystem: filename* | **inactive**} **Example:** `Device# install remove inactive`	(Optional) Deletes all unused and inactive software installation files.
Step 8	**show install summary** **Example:** `Device# show install summary`	Displays information about the active package. • The output of this command varies according to the **install** commands that are configured.

Bundle Mode Upgrade

To upgrade the Cisco IOS XE software when the switch is running in bundle mode, follow these steps:

Procedure

Step 1 Download the bundle file to local storage media.

Step 2 Configure the **boot system** global configuration command to point to the bundle file.

Step 3 Reload the switch.

Example

Upgrading Cisco IOS XE Software Bundle Mode

This example shows the steps to upgrade the Cisco IOS XE software on a switch that is running in bundle mode. It shows using the **copy** command to copy the bundle file to flash:, configuring the boot system variable to point to the bundle file, saving a copy of the running configuration, and finally, reloading the switch.

```
Switch#copy scp: sdflash:
Address or name of remote host [10.106.224.22]?Enter
Source username [xxxxx]?Enter
Source filename []? sdflash/ess3x00-universalk9.17.04.01.SPA.bin
Destination filename [ess3x00-universalk9.17.04.01.SPA.bin]?Enter
This is a Cisco managed device to be used only for authorized purposes.
Your use is monitored for security, asset protection, and policy compliance.
```

```
Password:
 Sending file modes: C0644 344345038 ess3x00-universalk9.17.04.01.SPA.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
344345038 bytes copied in 637.684 secs (539993 bytes/sec)
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no boot system
Switch(config)#boot system sdflash:ess3x00-universalk9.17.04.01.SPA.bin
Switch(config)#end
Switch#write memory
*May 27 14:49:55.121: %SYS-5-CONFIG_I: Configured from console by console
Building configuration...
[OK]
Switch#
*May 27 14:50:01.341: %SYS-6-PRIVCFG_ENCRYPT_SUCCESS: Successfully encrypted private config
 file
Switch#sh boot
Current Boot Variables:
BOOT variable = sdflash:ess3x00-universalk9.17.04.01.SPA.bin;

Boot Variables on next reload:
BOOT variable = sdflash:ess3x00-universalk9.17.04.01.SPA.bin;
Config file = flash:/nvram_config
ENABLE_FLASH_PRIMARY_BOOT = no
MANUAL_BOOT variable = no
ENABLE_BREAK variable = yes

Switch#reload
Proceed with reload? [confirm]Enter

*May 27 14:50:08.989: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload
Command.
watchdog: watchdog0: watchdog did not stop!
reboot: Restarting system
```

Licensing

This section provides information about the licensing packages for features available on Cisco ESS3300 series switches.

License Levels - Usage Guidelines

- Base licenses (Network Essentials and Network-Advantage) are ordered and fulfilled only with a permanent license type.
- Add-on licenses (DNA Essentials and DNA Advantage) are ordered and fulfilled only with a term license type.
- An add-on license level is included when you choose a network license level. If you use DNA features, renew the license before term expiry, to continue using it, or deactivate the add-on license and then reload the switch to continue operating with the base license capabilities.
- Evaluation licenses cannot be ordered. They are not tracked via Cisco Smart Software Manager and expire after a 90-day period. Evaluation licenses can be used only once on the switch and cannot be regenerated. Warning system messages about an evaluation license expiry are generated only 275 days

after expiration and every week thereafter. An expired evaluation license cannot be reactivated after reload.

Note Network Essentials license is the default license. It is permanent. A connection to the Smart Licensing server is not required if the switch will be deployed with a Network Essentials license.

Note Entering the command **license smart reservation** after the initial configuration will prevent an erroneous message "Smart Licensing Status: UNREGISTERED/EVAL MODE" from appearing on your device.

ESS3300 Model Numbers and Licensing

The following table lists the supported hardware models and the default license levels they are delivered with.

	Default License Level	Description
ESS-3300-NCP-E	Network Essentials	Main Board without a cooling plate. 2 ports of 10 GE fiber, 8 ports of GE copper. 4 of the 8 GE copper ports can also be combo ports. Terminal Power: 16W
ESS-3300-NCP-A	Network Advantage	Main Board without a cooling plate. 2 ports of 10 GE fiber, 8 ports of GE copper. 4 of the 8 GE copper ports can also be combo ports. Terminal Power: 16W
ESS-3300-CON-E	Network Essentials	Main Board conduction cooled 2 ports of 10 GE fiber, 8 ports of GE copper. 4 of the 8 GE copper ports can also be combo ports Terminal Power: 16W
ESS-3300-CON-A	Network Advantage	Main Board conduction cooled 2 ports of 10 GE fiber, 8 ports of GE copper. 4 of the 8 GE copper ports can also be combo ports Terminal Power: 16W

	Default License Level	Description
ESS-3300-24T-NCP-E	Network Essentials	Main Board with a 16p Expansion Board without a cooling plate 2 ports of 10 GE fiber, 24 ports of GE copper 4 of 8 GE ports can be combo ports on mainboard 4 of 16 GE ports can be combo ports on expansion board Terminal Power: 24W
ESS-3300-24T-NCP-A	Network Advantage	Main Board with a 16p Expansion Board without a cooling plate 2 ports of 10 GE fiber, 24 ports of GE copper 4 of 8 GE ports can be combo ports on mainboard 4 of 16 GE ports can be combo ports on expansion board Terminal Power: 24W
ESS-3300-24T-CON-E	Network Essentials	Main Board with a 16p Expansion Board conduction cooled 2 ports of 10 GE fiber, 24 ports of GE copper 4 of 8 GE ports can be combo ports on mainboard 4 of 16 GE ports can be combo ports on expansion board Terminal Power: 24W
ESS-3300-24T-CON-A	Network Advantage	Main Board with a 16p Expansion Board conduction cooled 2 ports of 10 GE fiber, 24 ports of GE copper 4 of 8 GE ports can be combo ports on mainboard 4 of 16 GE ports can be combo ports on expansion board Terminal Power: 24W

Upgrading the License Level

The following commands show how to upgrade from Network Essentials to Network Advantage.

The following shows the switch running Network Essentials:

```
switch#show version
Cisco IOS XE Software, Version BLD_V174_1_THROTTLE_LATEST_20201207_031930_V17_4_0_193
Cisco IOS Software [Bengaluru], ESS3x00 Switch Software (ESS3x00-UNIVERSALK9-M), Experimental
 Version 17.4.20201207:040001
[S2C-build-v174_1_throttle-208-/nobackup/mcpre/BLD-BLD_V174_1_THROTTLE_LATEST_20201207_031930
```

```
 156]
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Mon 07-Dec-20 00:33 by mcpre


Cisco IOS-XE software, Copyright (c) 2005-2020 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: IOS-XE ROMMON
BOOTLDR: Version 7.0.6 [DEVELOPMENT SOFTWARE] crashkernel=64M
switch uptime is 7 weeks, 5 days, 5 hours, 7 minutes
Uptime for this control processor is 7 weeks, 5 days, 5 hours, 8 minutes
System returned to ROM by Reload Command
System image file is "flash:packages.conf"
Last reload reason: Reload Command


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.


Technology Package License Information:

------------------------------------------------------------------------------
Technology-package                                  Technology-package
Current                       Type                     Next reboot
------------------------------------------------------------------------------
network-essentials   Smart License                  network-essentials


Smart Licensing Status: Registration Not Applicable/Not Applicable

cisco ESS-3300-CON (ARM) processor (revision V01) with 890141K/6147K bytes of memory.
Processor board ID 32
1 Virtual Ethernet interface
24 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
3952748K bytes of physical memory.
523264K bytes of crashinfo at crashinfo:.
1684480K bytes of Flash at flash:.
3883008K bytes of sdflash at sdflash:.

Base Ethernet MAC Address          : 40:ce:24:b7:75:20
```

```
Motherboard Assembly Number        : 73-101439-03
Motherboard Serial Number          : FJZ22150D34
Model Revision Number              : V01
Motherboard Revision Number        : 3
Model Number                       : ESS-3300-CON
System Serial Number               : 32
Top Assembly Part Number           : 68-101690-01
Top Assembly Revision Number       : 17P
System FPGA version                : 0.88.0
SKU Brand Name                     : Cisco


Configuration register is 0x102

switch#
```

The following shows the licenses in use:

```
switch#show license summary
License Usage:
  License                Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  No licenses in use
switch#
```

The following shows a protocol not found in Network Essentials:

```
switch(config)#router ospf 10
Protocol not in this image
switch(config)#
```

Upgrade the switch to Network Advantage:

```
switch(config)#license boot level network-advantage
% use 'write' command to make license boot config take effect on next boot
switch(config)#end
switch(config)#write memory
Building configuration...
[OK]
switch#
```

Reload the switch:

```
switch#reload
Proceed with reload? [confirm]<Enter>

watchdog: watchdog0: watchdog did not stop!
reboot: Restarting system

Initializing disk drivers...
Initializing file systems...

************************************************************
* Rom Monitor for ESS3300                                  *
* Copyright (c) 2017-2020 by Cisco Systems, Inc.           *
* All rights reserved.                                     *
************************************************************

* Version:  7.0.6
* Compiled: Sun 08-Nov-20 22:38 [DEVELOPMENT SOFTWARE]
* Boot Partition: qspi-upgrade-bootloader
* Reset Reason: Soft Reset
* REL and DEV keys installed

Loading "flash:packages.conf" to memory...
```

```
Loading "flash:/ess3x00-rp_iot.BLD_V174_1_THROTTLE_LATEST_20201207_031930_V17_4_0_193.SSA.pkg"
 to memory...
Verifying image
"flash:/ess3x00-rp_iot.BLD_V174_1_THROTTLE_LATEST_20201207_031930_V17_4_0_193.SSA.pkg"...
Image passed digital signature verification
Loading "flash:/ess3x00-rpboot.BLD_V174_1_THROTTLE_LATEST_20201207_031930_V17_4_0_193.SSA.pkg"
 to memory...
Verifying image
"flash:/ess3x00-rpboot.BLD_V174_1_THROTTLE_LATEST_20201207_031930_V17_4_0_193.SSA.pkg"...
Image passed digital signature verification

Booting ss-rommon...
Version:  7.0.6
Compiled: Sun 08-Nov-20 22:38 [DEVELOPMENT SOFTWARE]

Address Map    : Total: 7884608 bytes
 IOT Pkg Header: 0x00000000 size: 1396
 SS-Rommon     : 0x00000574 size: 628960
 Sup PL[01]    : 0x001836c4 size: 5568668
 Rtos[01]      : 0x0009a3ec size: 953668
 BL[1835014]   : 0x006d3500 size: 727616

Address Map    : Total: 56306701 bytes
 RP_Boot Header: 0x00000000 size: 1396
 Kernel        : 0x00000574 size: 32541248
 Dtb           : 0x01f08fb4 size: 45144
 InitRamFs     : 0x01f1400c size: 23718913

Checking for Bootloader upgrade...
Bootloader upgrade not required
SUP PL (profile: 1) configuration done successfully
RTOS (profile: 1) boot successful

Taking BP out of reset
Taking LC1 out of reset
Taking LC2 out of reset
Taking LC3 out of reset

              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           Cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706



Cisco IOS Software [Bengaluru], ESS3x00 Switch Software (ESS3x00-UNIVERSALK9-M), Experimental
 Version 17.4.20201207:040001
[S2C-build-v174_1_throttle-208-/nobackup/mcpre/BLD-BLD_V174_1_THROTTLE_LATEST_20201207_031930
 156]
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Mon 07-Dec-20 00:33 by mcpre


This software version supports only Smart Licensing as the software licensing mechanism.
```

```
PLEASE READ THE FOLLOWING TERMS CAREFULLY. INSTALLING THE LICENSE OR
LICENSE KEY PROVIDED FOR ANY CISCO SOFTWARE PRODUCT, PRODUCT FEATURE,
AND/OR SUBSEQUENTLY PROVIDED SOFTWARE FEATURES (COLLECTIVELY, THE
"SOFTWARE"), AND/OR USING SUCH SOFTWARE CONSTITUTES YOUR FULL
ACCEPTANCE OF THE FOLLOWING TERMS. YOU MUST NOT PROCEED FURTHER IF YOU
ARE NOT WILLING TO BE BOUND BY ALL THE TERMS SET FORTH HEREIN.

Your use of the Software is subject to the Cisco End User License Agreement
(EULA) and any relevant supplemental terms (SEULA) found at
http://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html.

You hereby acknowledge and agree that certain Software and/or features are
licensed for a particular term, that the license to such Software and/or
features is valid only for the applicable term and that such Software and/or
features may be shut down or otherwise terminated by Cisco after expiration
of the applicable license term (e.g., 90-day trial period). Cisco reserves
the right to terminate any such Software feature electronically or by any
other means available. While Cisco may provide alerts, it is your sole
responsibility to monitor your usage of any such term Software feature to
ensure that your systems and networks are prepared for a shutdown of the
Software feature.


All TCP AO KDF Tests Pass
cisco ESS-3300-CON (ARM) processor (revision V01) with 890141K/6147K bytes of memory.
Processor board ID 32
1 Virtual Ethernet interface
24 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
3952748K bytes of physical memory.
523264K bytes of crashinfo at crashinfo:.
1684480K bytes of Flash at flash:.
3883008K bytes of sdflash at sdflash:.

Base Ethernet MAC Address          : 40:ce:24:b7:75:20
Motherboard Assembly Number        : 73-101439-03
Motherboard Serial Number          : FJZ22150D34
Model Revision Number              : V01
Motherboard Revision Number        : 3
Model Number                       : ESS-3300-CON
System Serial Number               : 32
Top Assembly Part Number           : 68-101690-01
Top Assembly Revision Number       : 17P
System FPGA version                : 0.88.0
SKU Brand Name                     : Cisco


Press RETURN to get started!


switch>
```

Once the above step is completed, the switch will have the EVAL license. The customer needs to purchase the Network Advantage license so that it reflects in the corresponding smart account. For Smart licensing, the license from the smart account is consumed once the device establishes communication to the CSSM server. For the SLR model below, these are the steps to apply the license in the switch from smart account.

```
switch#license smart reservation request all
```

Using the Reservation code generated from the above command, a Reservation Authorization code should be generated from the smart account and used in the following command:

```
switch#license smart reservation install <Reservation Auth code>
```

Verify the change by showing the license summary:

```
switch#show license summary
License Usage:
  License                 Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  network-advantage       (ESS3300_Network_Advantage)       1 IN USE

switch#
```

The following shows that the protocol displayed earlier is now available in Network Advantage:

```
switch(config)#router ospf 10
switch(config-router)#
```

The following commands show the license usage:

```
switch#show license tech support
Smart Licensing Tech Support info

Smart Licensing Status
======================

Smart Licensing is ENABLED

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: cslu
  Cslu address: <empty>
  Proxy:
    Address: <empty>
    Port: <empty>
    Username: <empty>
    Password: <empty>
  Server Identity Check: False

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
```

```
switch#show license usage
License Authorization:
  Status: Not Applicable

network-advantage (ESS3300_Network_Advantage):
  Description: network-advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-advantage
  Feature Description: network-advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual

switch#
```

The following displays the switch inventory:

```
switch#show inventory
NAME: "Chassis", DESCR: "Cisco ESS-3300-CON"
PID: ESS-3300-CON      , VID: V01  , SN: 32

NAME: "Supervisor", DESCR: "ESS3x00-M 2 uplink SFP's, 8x1GE Copper PoE ports Conduction
cooled"
PID: ESS-3300-CON      , VID: V01  , SN: 32

NAME: "TenGigabitEthernet1/2", DESCR: "SFP-10GBase-SR"
PID: SFP-10G-SR          , VID: V03  , SN: FNS21300STA

NAME: "GigabitEthernet1/3", DESCR: "1000BaseSX SFP"
PID: GLC-SX-MMD          , VID: V02  , SN: OPM24030S4U

NAME: "GigabitEthernet1/4", DESCR: "100BaseLX-FE SFP"
PID: GLC-FE-100LX-RGD    , VID: V02  , SN: ACW23390FY4

NAME: "GigabitEthernet1/5", DESCR: "10/100/1000BaseTX SFP"
PID: GLC-TE              , VID: V01  , SN: AVC233122E1

NAME: "Expansion Module", DESCR: "ESS3x00-Ex Expansion Module 16x1GE Copper PoE Conduction
 cooled"
PID: ESS-3300-16T-CON  , VID: V01  , SN: 16

switch#
```

Boot from the USB

The switch can be booted from configuration files located on the pluggable USB. Customized startup configuration files can be booted from IOS or from ROMMON.

Booting from ROMMON

The following configuration steps need to be taken in order to boot from the USB.

From the ROMMON prompt, execute **set CONFIG_FILE=usbflash0:** <*filename*>

For example:

```
rommon 2 > set CONFIG_FILE=usbflash0:my_startupcfg
```

```
rommon 3 > sync
rommon 4 > set
PS1=rommon ! >
MCU_UPGRADE=SKIP
THRPUT=
LICENSE_BOOT_LEVEL=
RET_2_RTS=
MCP_STARTUP_TRACEFLAGS=00000000:00000000
BSI=0
RANDOM_NUM=1275114933
BOOT=flash:Jun5_1.SSA,12
RET_2_RCALTS=951454376
CONFIG_FILE=usbflash0:my_startupcfg
```

Continue booting the IOS image as usual from the ROMMON prompt.

Booting from the USB Feature Summary

- Once the CONFIG_FILE is set to a non-default value, the **nvram:startup-config** command is aliased to this new location.
- Any change made to the config file in usbflash will be reflected in nvram:startup-config as well.
- The EXEC command **erase nvram:startup-config** erases the contents of NVRAM, and deletes the file referenced by CONFIG_FILE variable.
- When the configuration is saved using the **copy system:running-config nvram:startup-config** command, the device saves a complete version of the configuration file to the location specified by the CONFIG_FILE environment variable, and a distilled version to NVRAM. A distilled version is one that does not contain access list information.

Clearing the Startup Configuration

You can clear the configuration information from the startup configuration. If you reboot the device with no startup configuration, the device enters the Setup command facility so that you can configure the device from scratch. To clear the contents of your startup configuration, complete the task in this section:



Important The IOS command parser may show a **factory-reset all** command. For embedded platforms this command is **NOT** supported as it leads to an ambiguity of which factory does it reference. A partner or integrator may install value add features that could be wiped out and not restored when such a command is executed. The system is obviously not in the state when it left the patrner or integrator's factory. If the desire is to perform a deep wipe of the on-board flash file system, the user should use the zeroization function and be completely familiar with the recovery features of the platform.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**erase nvram** **Example:** `Device# erase nvram`	Clears the contents of your startup configuration. **Note** For all platforms except the Class A Flash file system platforms, this command erases NVRAM. The startup configuration file cannot be restored once it has been deleted. On Class A Flash file system platforms, when you use the **erase startup-config** EXEC command, the device erases or deletes the configuration pointed to by the CONFIG_FILE environment variable. If this variable points to NVRAM, the device erases NVRAM. If the CONFIG_FILE environment variable specifies a flash memory device and configuration filename, the device deletes the configuration file. That is, the device marks the file as "deleted," rather than erasing it. This feature allows you to recover a deleted file.

Emergency Recovery Installation

The following procedure supports the Cisco ESS3300 and the Cisco ESS9300.

Note There is different terminology used when referring to the push button depending on the product. The IE3x00 switches call this the Express Setup switch. Other products may refer to this as the Factory Default Switch. In either case, the functionality is the same.

If the other recovery methods fail, the switch has a trap door method that you can use in order to recover the system. You must have a terminal that is connected to port Gi1/3 of the switch that runs a TFTP server. Download a valid image file from CCO and store it in the root of the TFTP server.

It is likely that the switch is stuck at the **switch**: prompt. However, if you are in a boot loop, you can use the push button functionality in order to break the cycle: hold the button for approximately 5 seconds, and the switch breaks the cycle and stops at the **switch**: prompt.

Complete these steps in order to perform an emergency recovery:

Step 1: Boot the emergency install image.

```
switch: boot emgy0:<image-name>.SPA.bin
Booting golden bootloader...
Initializing disk drivers...
Initializing file systems...
**********************************************************
* Rom Monitor for ESS3300                                *
* Copyright (c) 2017-2018 by Cisco Systems, Inc.         *
* All rights reserved.                                   *
**********************************************************
* Version:  1.1.1
* Compiled: Sun 01-Jul-18 22:17 [RELEASE SOFTWARE]
* Boot Partition: qspi-golden-bootloader
```

```
* Reset Reason: Soft Reset
Loading "emgy0:ess3x00-universalk9.17.04.01.SPA.bin" to memory...
Verifying image "emgy0:ess3x00-universalk9.17.04.01.SPA.bin"...
Image passed digital signature verification
Checking for Bootloader upgrade...
Bootloader upgrade not required
SUP PL (profile: 1) configuration done successfully
<...>
Press RETURN to get started!
Switch>
```

Step 2: Configure an IP address on the switch. Additional details on IP configuration can be found here

```
switch(config-if)# ip address <ip-address> <subnet-mask>
```

Step 3: Ping the terminal that contains the TFTP server in order to test the connectivity:

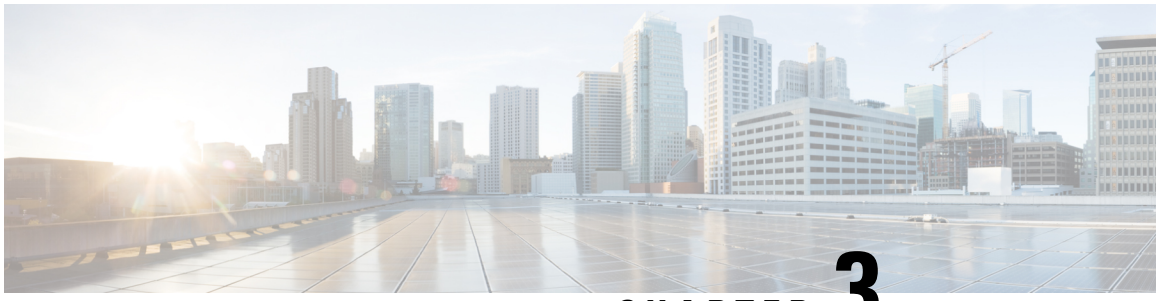
```
switch> ping 192.0.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 192.0.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Step 4: Copy the image via tftp

```
switch> copy tftp://location/directory/bundle_name flash:

<...>
```

Step 5: Restart the system.



CHAPTER 3

Configuring the Switch Using the Web User Interface

This section contains the following:

- Introduction to Day 0 WebUI Configuration, on page 41
- Classic Day 0 Wizard, on page 41

Introduction to Day 0 WebUI Configuration

After you complete the hardware installation, you need to setup the switch with configuration required to enable traffic to pass through the network. On your first day with your new device, you can perform a number of tasks to ensure that your device is online, reachable and easily configured.

The Web User Interface (Web UI) is an embedded GUI-based device-management tool that provides the ability to provision the device, to simplify device deployment and manageability, and to enhance the user experience. You can use WebUI to build configurations, monitor, and troubleshoot the device without having CLI expertise.

Classic Day 0 Wizard

Use this wizard to configure the device with basic and advanced settings. Once complete, you can access the device through the WebUI using the management interface IP address.

Connecting to the Switch

Before you begin

Set up the DHCP Client Identifier on the client to get the IP address from the switch, and to be able to authenticate with Day 0 login credentials.

Setting up the DHCP Client Identifier on the client for Windows

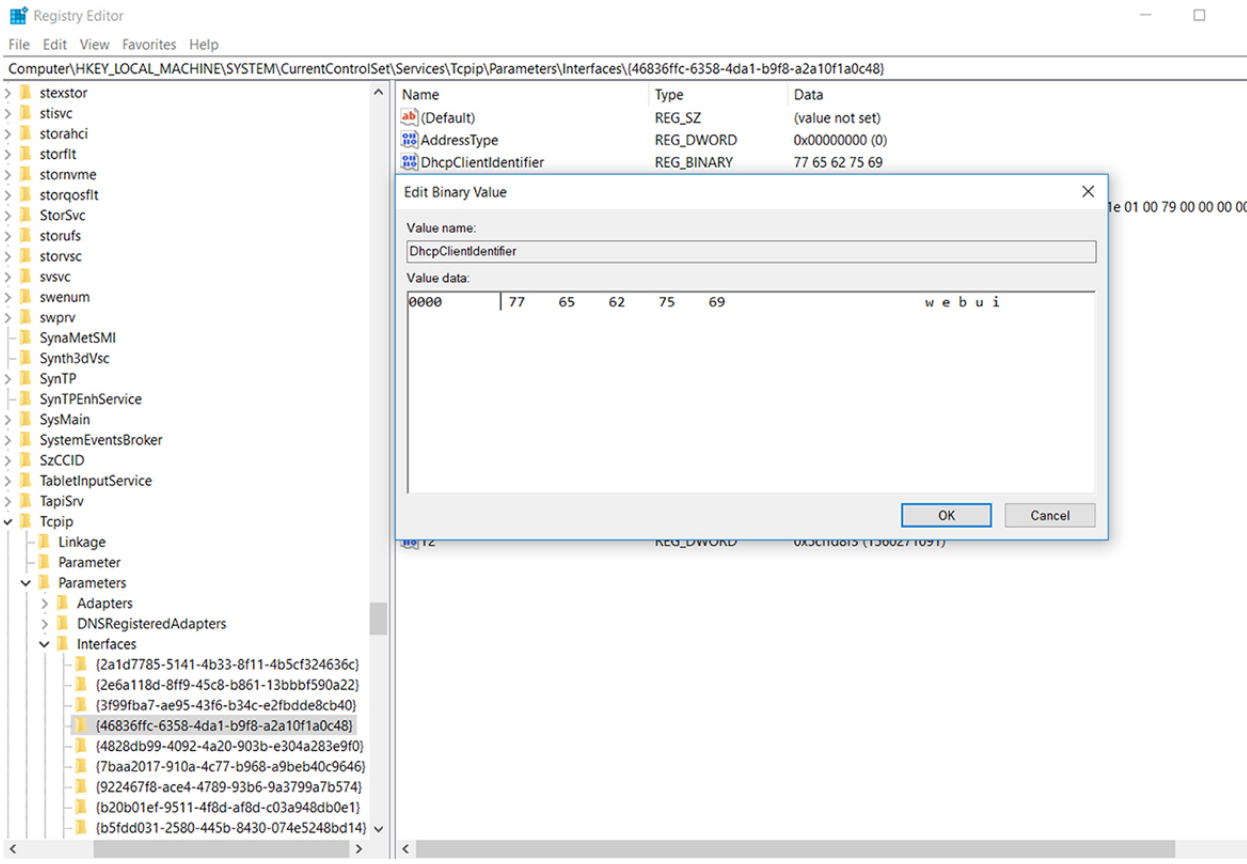
1. Type **`regedit`** in the Windows search box on the taskbar and press *enter*.
2. If prompted by User Account Control, click **Yes** to open the Registry Editor.

3. Navigate to

   Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces and locate the **Ethernet Interface** Global Unique Identifier (GUID).

4. Add a new REG_BINARY **DhcpClientIdentifier** with Data **77 65 62 75 69** for **`webui`**. You need to manually type in the value.

   Figure 2: Setting up DHCP Client Identifier on Windows

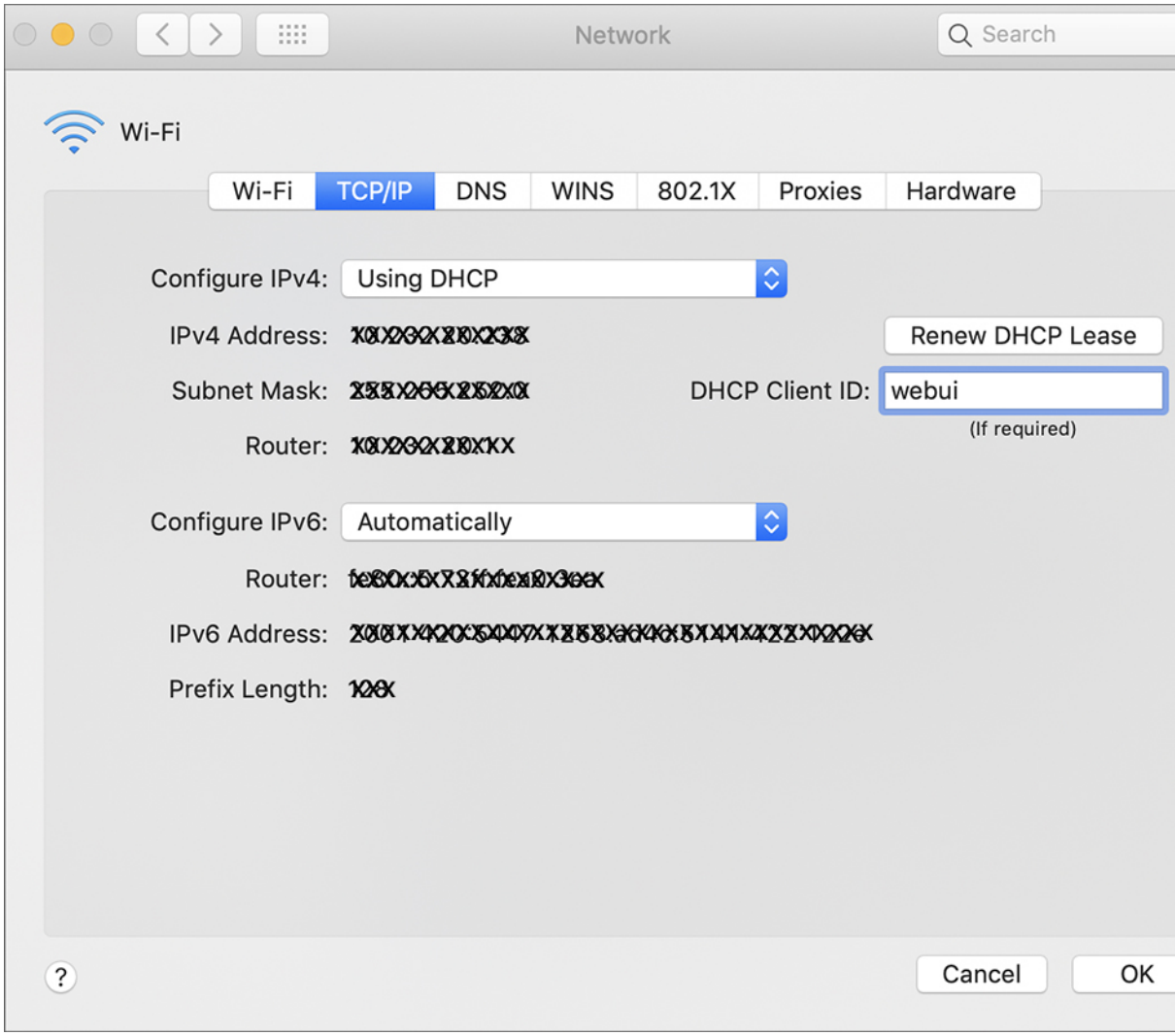


5. Restart the PC for the configuration to take effect.

Setting up the DHCP Client Identifier on the client for MAC

1. Go to **System Preferences >Network >Advanced >TCP >DHCP Client ID:** and enter **`webui`**.

Figure 3: Setting up DHCP Client Identifier on MAC



2. Click **OK** to save the changes.

The bootup script runs the configuration wizard, which prompts you for basic configuration input: (**Would you like to enter the initial configuration dialog? [yes/no]:**). To configure Day 0 settings using the web UI, do not enter a response. Perform the following tasks instead:

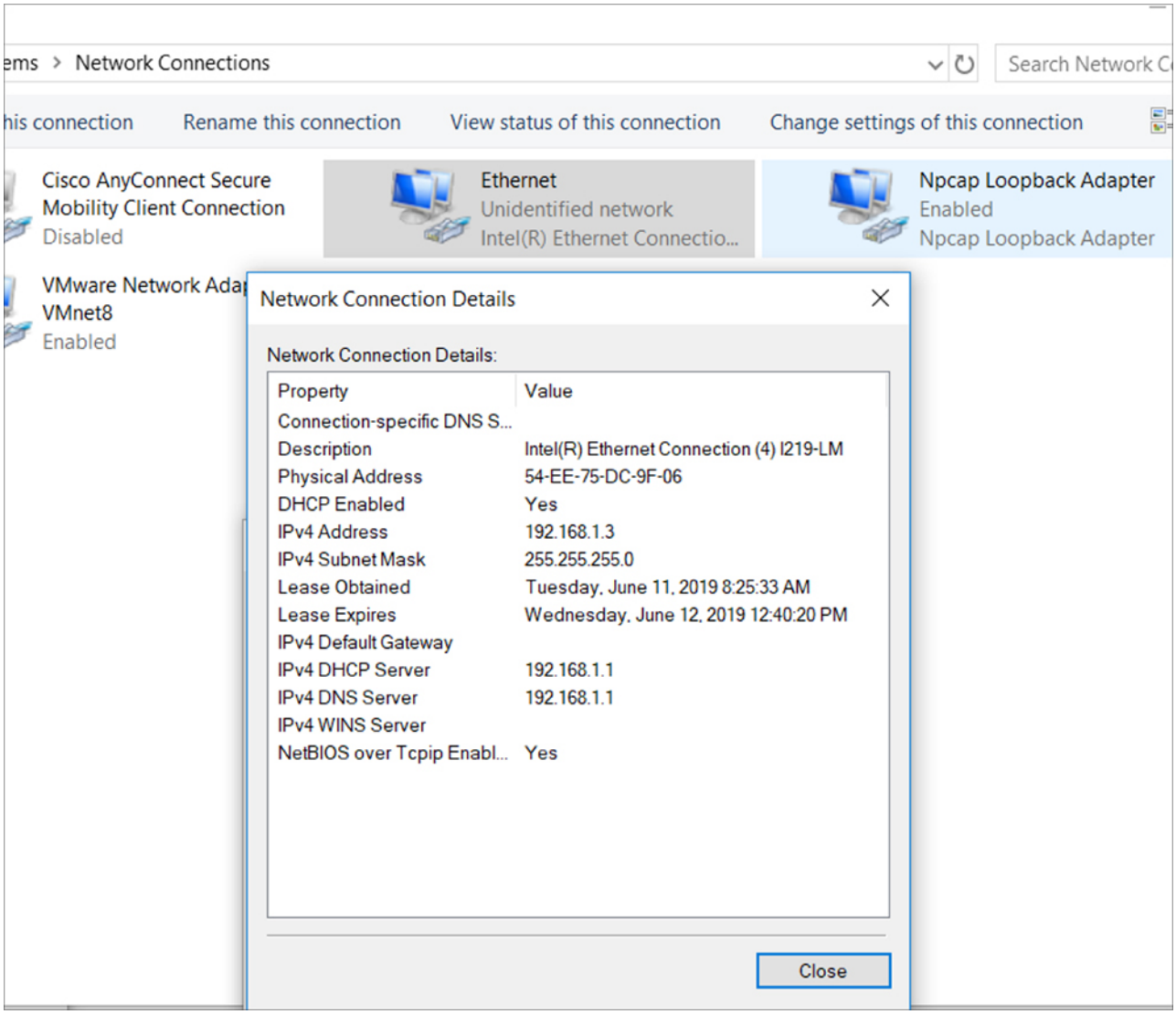
Procedure

Step 1 Make sure that no devices are connected to the switch.

Step 2 Connect one end of an ethernet cable to one of the downlink (non-management) ports on the active supervisor and the other end of the ethernet cable to the host (PC/MAC).

Step 3 Set up your PC/MAC as a DHCP client, to obtain the IP address of the switch automatically. You should get an IP address within the 192.168.1.x/24 range.

Figure 4: Obtaining the IP Address



It may take up to three mins. You must complete the Day 0 setup through the web UI before using the device terminal.

Step 4 Launch a web browser on the PC and enter the device IP address (`https://192.168.1.1`) in the address bar.

Step 5 Enter the Day 0 **username** `webui` and **password** `cisco`.

What to do next

Create a user account.

Creating User Accounts

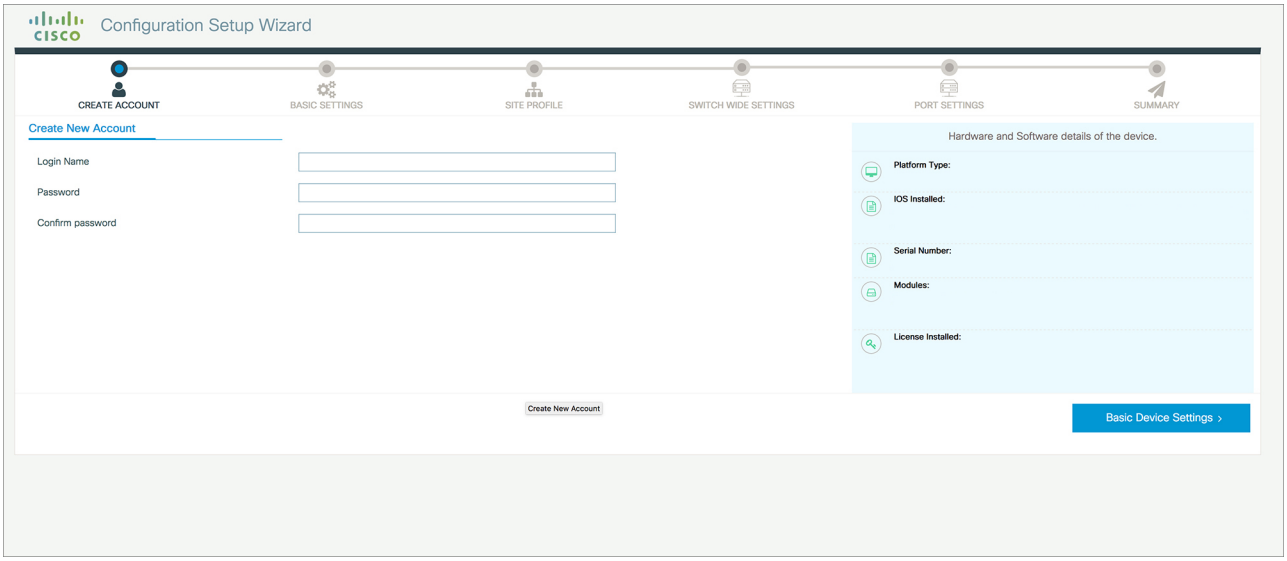
Setting a username and password is the first task you will perform on your device. Typically, as a network administrator, you will want to control access to your device and prevent unauthorized users from seeing your network configuration or manipulating your settings.

Procedure

Step 1 Log on using the default username and password provided with the device.

Step 2 Set a password of up to 25 alphanumeric characters. The username password combination you set gives you privilege 15 access. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces.

Figure 5: Create Account



Choosing Setup Options

Select **Wired Network** to configure your device based on a site profile, and continue to configure switch wide settings. Otherwise, continue to the next step and configure only basic settings for your device.

Configuring Basic Device Settings

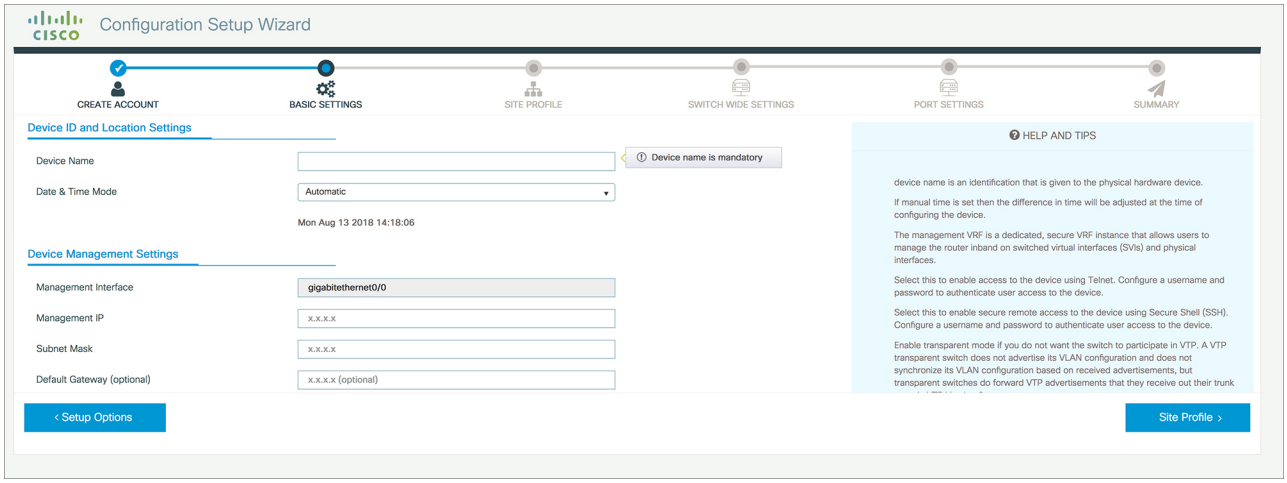
On the **Basic Device Settings** page configure the following information:

Procedure

Step 1 In the **Device ID and Location Settings** section, type a unique name to identify your device in the network.

Step 2 Choose the date and time settings for your device. To synchronize your device with a valid outside timing mechanism, such as an NTP clock source, choose Automatic, or choose Manual to set it yourself.

Figure 6: Basic Settings - Device ID and Location Settings



Step 3 In the **Device Management Settings** section, assign an **`IP address`** to the management interface. Ensure that the IP address you assign is part of the subnet mask you enter.

Step 4 Optionally, enter an **`IP address`** to specify the default gateway.

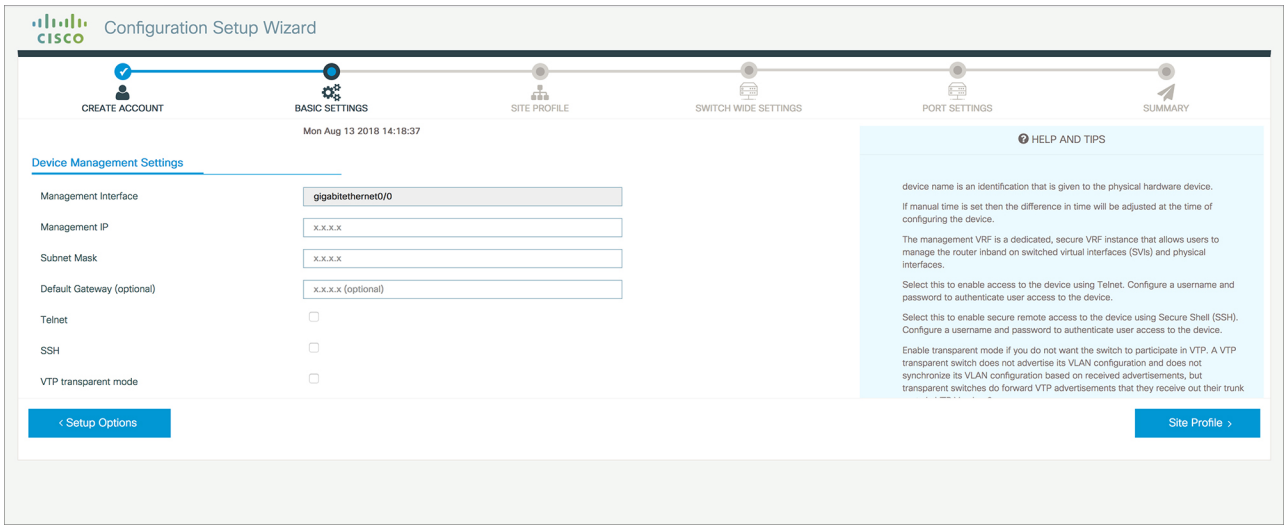
Step 5 To enable access to the device using telnet, check the **Telnet** check box.

Step 6 To enable secure remote access to the device using Secure Shell (SSH), check the **SSH** check box.

Step 7 Check the **VTP transparent mode** check box to disable the device from participating in VTP.

If you did not select **Wired Network**, in the earlier step, continue to the next screen to verify your configuration on the **Day 0 Config Summary** screen, and click **Finish**. To automatically configure your device based on a site profile, click **Setup Options**, and select **Wired Network**.

Figure 7: Basic Settings - Device Management Settings



Configuring Your Device Based on a Site Profile

To ease your configuration tasks and save time, choose a site profile based on where your device may be installed and managed in your network. Based on the site profile you choose, your device is automatically configured according to Cisco best practices. You can easily modify this default configuration, from the corresponding detailed configuration screens.

Choosing a site profile as part of Quick Setup allows you to configure your device based on the business needs of your enterprise. For example, you could use your device as an access switch, to connect client nodes and endpoints on your network, or as a distribution switch, to route packets between subnets and VLANs.

Table 2: Default Configuration Loaded with Each Site Profile (Access Switches)

Setting	Single Access Switch (Single Uplink)	Single Access Switch (Single Port Channel Uplink)	Single Access Switch (Redundant Port Channel Uplink)
Hostname	The hostname or device name you provided as part of Quick Setup	The hostname or device name you provided as part of Quick Setup	The hostname or device name you provided as part of Quick Setup
Spanning Tree Mode	RPVST+	RPVST+	RPVST+
VTP	Mode Transparent	Mode Transparent	Mode Transparent
UDLD	Enabled	Enabled	Enabled
Error Disable Recovery	Recovery mode set to Auto	Recovery mode set to Auto	Recovery mode set to Auto
Port Channel Load Balance	Source Destination IP	Source Destination IP	Source Destination IP
SSH	Version 2	Version 2	Version 2
SCP	Enabled	Enabled	Enabled
VTY Access to Switch	Enabled	Enabled	Enabled
Service Timestamp	Enabled	Enabled	Enabled
VLAN	The following VLANs are created: • Default VLAN • Data VLAN • Voice VLAN • Management VLAN	The following VLANs are created: • Default VLAN • Data VLAN • Voice VLAN • Management VLAN	The following VLANs are created: • Default VLAN • Data VLAN • Voice VLAN • Management VLAN

Setting	Single Access Switch (Single Uplink)	Single Access Switch (Single Port Channel Uplink)	Single Access Switch (Redundant Port Channel Uplink)
Management Interface	Layer 3 settings configured on the management port, based on Quick Setup	Layer 3 settings configured on the management port, based on Quick Setup	Layer 3 settings configured on the management port, based on Quick Setup
IPv6 Host Policy	IPv6 host policy created	IPv6 host policy created	IPv6 host policy created
QoS Policy for Downlink Ports	Auto QoS Policy for Access defined	Auto QoS Policy for Access defined	Auto QoS Policy for Access defined
QoS Policy for Uplink Ports	QoS Policy for Distribution created	QoS Policy for Distribution created	QoS Policy for Distribution created
Uplink Interfaces	Selected uplink interfaces configured as trunk ports, set to allow all VLANs	Selected ports configured as Port-channel in trunk mode, set to allow all VLANs.	Selected ports configured as Port-channel in trunk mode, set to allow all VLANs.
Downlink Interfaces	Downlink ports configured in Access mode	Downlink ports configured in Access mode	Downlink ports configured in Access mode
Port-channel	Not configured	Port-channel to distribution created	Port-channel to distribution created

Figure 8: Site Profile - Access Switches

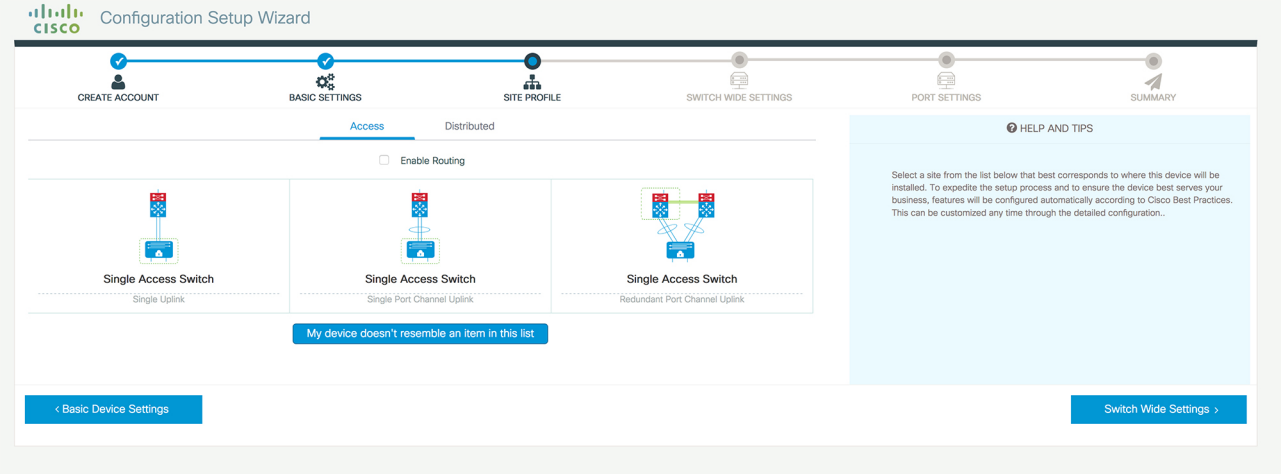


Figure 9: Site Profile - Access Switches (with Routed Access)

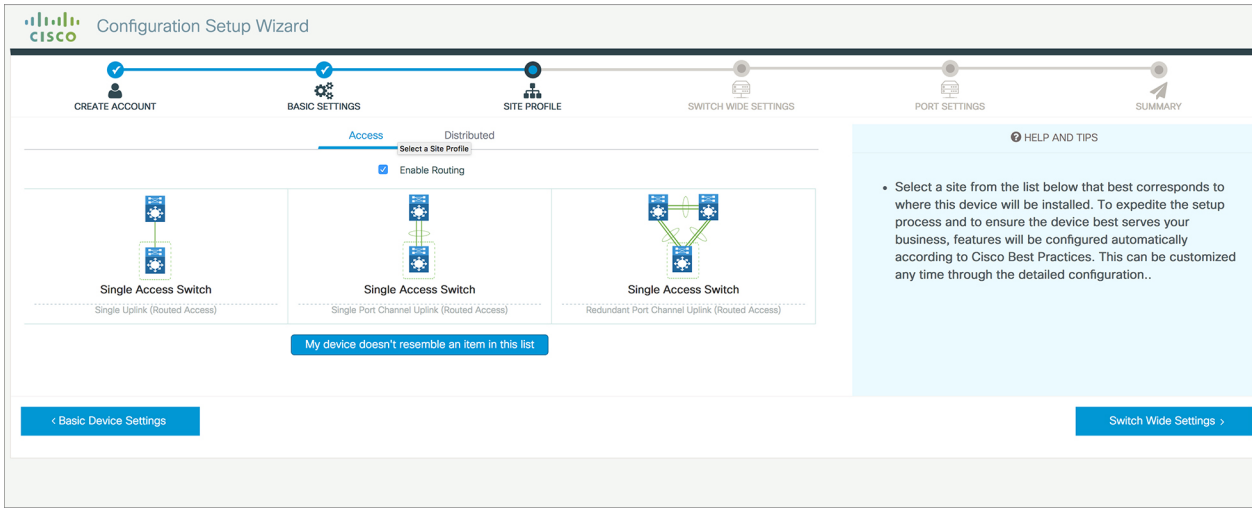


Table 3: Default Configuration Loaded with Each Site Profile (Distribution Switches)

Setting	Single Distribution Switch (Single Downlink)	Single Distribution Switch (Single Port Channel Downlink)	Redundant Distribution Switch (Port Channel Peer and Downlink)
Hostname	The hostname or device name you provided as part of Quick Setup	The hostname or device name you provided as part of Quick Setup	The hostname or device name you provided as part of Quick Setup
Spanning Tree Mode	RPVST+	RPVST+	RPVST+
VTP	Mode Transparent	Mode Transparent	Mode Transparent
UDLD	Enabled	Enabled	Enabled
Error Disable Recovery	Recovery mode set to Auto	Recovery mode set to Auto	Recovery mode set to Auto
SSH	Version 2	Version 2	Version 2
SCP	Enabled	Enabled	Enabled
VTY Access to Switch	Enabled	Enabled	Enabled
Service Timestamp	Enabled	Enabled	Enabled

Setting	Single Distribution Switch (Single Downlink)	Single Distribution Switch (Single Port Channel Downlink)	Redundant Distribution Switch (Port Channel Peer and Downlink)
VLAN	The following VLANs are created: • Default VLAN • Data VLAN • Voice VLAN • Management VLAN	The following VLANs are created: • Default VLAN • Data VLAN • Voice VLAN • Management VLAN	The following VLANs are created: • Default VLAN • Data VLAN • Voice VLAN • Management VLAN
Management Interface	Layer 3 settings configured on the management port, based on Quick Setup	Layer 3 settings configured on the management port, based on Quick Setup	Layer 3 settings configured on the management port, based on Quick Setup
QoS Policy	QoS Policy for Distribution defined	QoS Policy for Distribution defined	QoS Policy for Distribution defined
Uplink Interfaces	Selected uplink ports connect to other distribution or core switches	Selected uplink ports connect to other distribution or core switches	Selected uplink ports connect to other distribution or core switches
Downlink Interfaces	Downlink connections to access switches configured in Trunk mode	Downlink connections to access switches configured in Trunk mode	Downlink connections to access switches configured in Trunk mode
Port-channel	Port-channel to core created	Port-channel to core or access created	Port-channel to core or distribution created

Figure 10: Site Profile - Distribution Switches

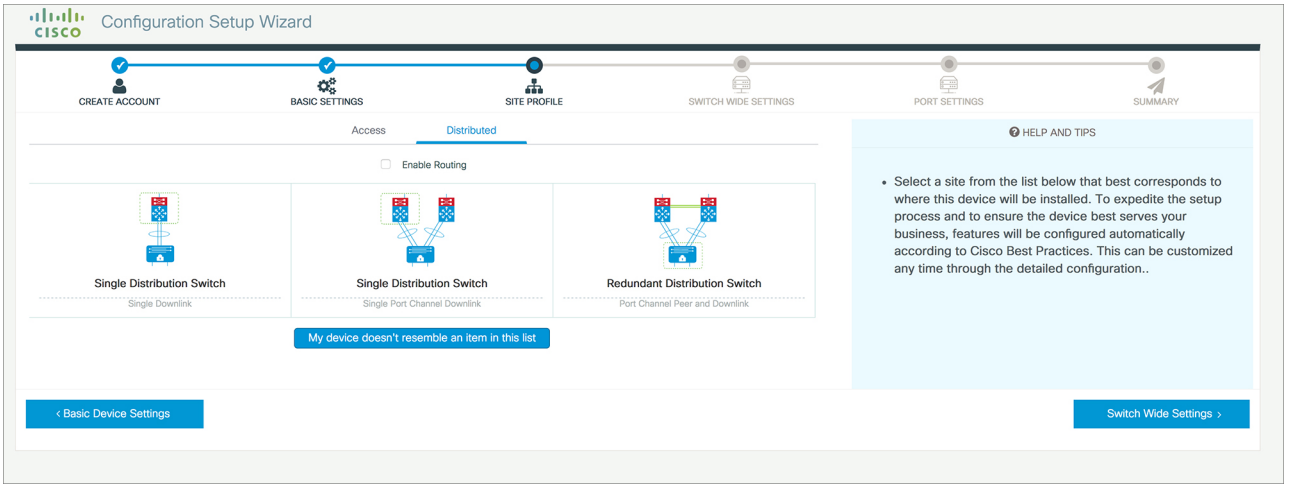


Figure 11: Site Profile - Distribution Switches (with Routed Access)

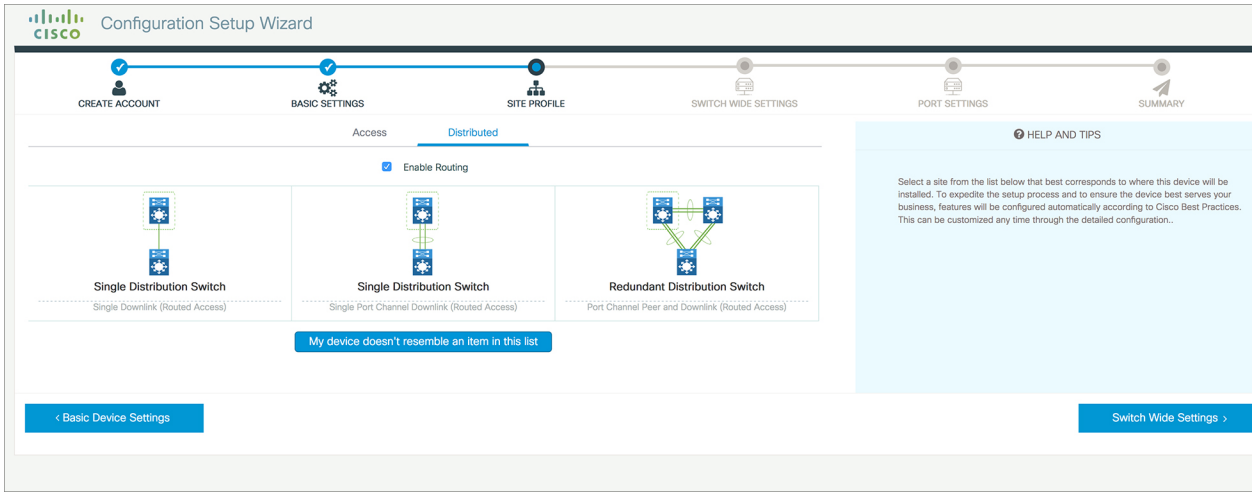
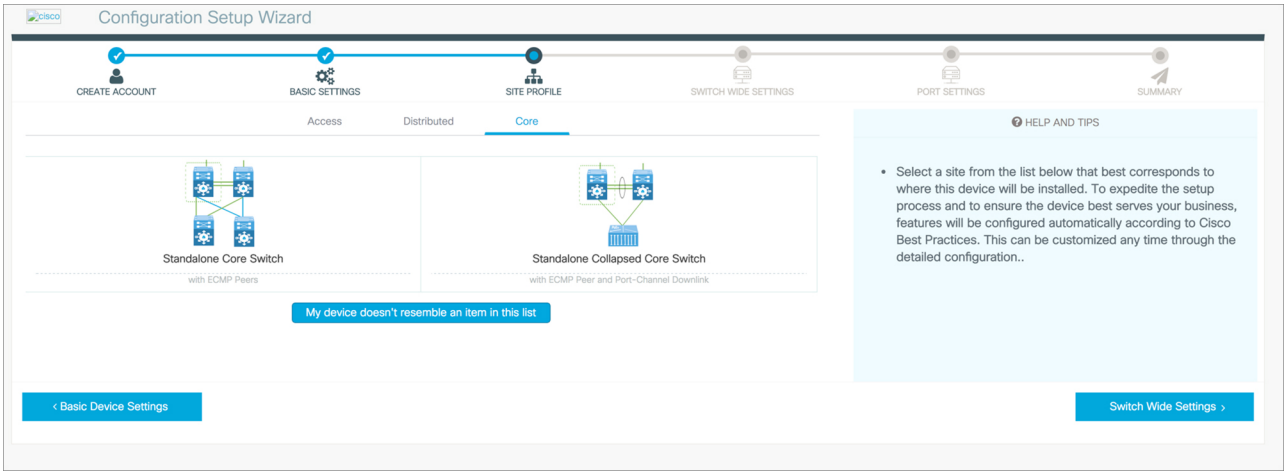


Table 4: Default Configuration Loaded with Each Site Profile (Core Switches)

Setting	Standalone Core Switch (with ECMP Peers)	Standalone Collapsed Core Switch (with ECMP Peer and Port Channel Downlink)
Hostname	The hostname or device name you provided as part of Quick Setup	The hostname or device name you provided as part of Quick Setup
UDLD	Enabled	Enabled
Error Disable Recovery	Recovery mode set to Auto	Recovery mode set to Auto
Port Channel Load Balance	Source Destination IP	Source Destination IP
SSH	Version 2	Version 2
SCP	Enabled	Enabled
VTY Access to Switch	Enabled	Enabled
Mitigate Address Spoofing	Unicast RPF (uRPF) in strict mode	Unicast RPF (uRPF) in strict mode
Service Timestamp	Enabled	Enabled
Management Interface	Layer 3 settings configured on the management port, based on Quick Setup	Layer 3 settings configured on the management port, based on Quick Setup
QoS Policy	QoS Policy for Distribution/Core defined	QoS Policy for Distribution/Core defined
Uplink Interfaces	Selected uplink ports connect to MAN/WAN device	Selected uplink ports connect to MAN/WAN device

Setting	Standalone Core Switch (with ECMP Peers)	Standalone Collapsed Core Switch (with ECMP Peer and Port Channel Downlink)
Downlink Interfaces	Downlink connections to access switches	Downlink connections to distribution switches
Cross-connect Interfaces	Selected ports connect to other core switches	Selected ports connect to other core switches

Figure 12: Site Profile - Core Switches



Configuring VLAN Settings

Procedure

Step 1 In the **VLAN Configuration** section, you can configure both data and voice VLANs. Type a name for your data VLAN.

Step 2 To configure a data VLAN, ensure that the **Data VLAN** check box is checked, type a name for your VLAN, and assign a VLAN ID to it. If you are creating several VLANs, indicate only a VLAN range.

Step 3 To configure a voice VLAN, ensure that the **Voice VLAN** check box is checked, type a name for your VLAN, and assign a VLAN ID to it. If you are creating several VLANs, indicate a VLAN range.

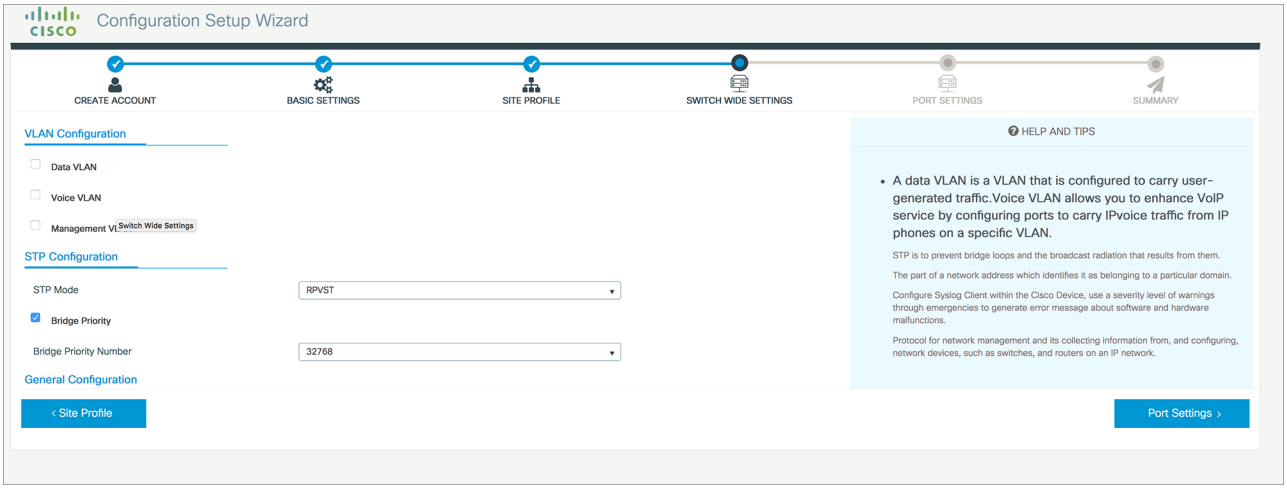
Configure STP Settings

Procedure

Step 1 RPVST is the default STP mode configured on your device. You can change it to PVST from the **STP Mode** drop-down list.

Step 2 To change a bridge priority number from the default value 32748, change **Bridge Priority** to Yes and choose a priority number from the drop-down list.

Figure 13: VLAN and STP Settings



Configuring DHCP, NTP, DNS and SNMP Settings

Procedure

Step 1 In the **Domain Details** section, enter a domain name that the software uses to complete unqualified hostnames.

Step 2 Type an IP address to identify the DNS server. This server is used for name and address resolution on your device.

Step 3 In the **Server Details** section, type the IP address of the DNS server that you want to make available to DHCP clients.

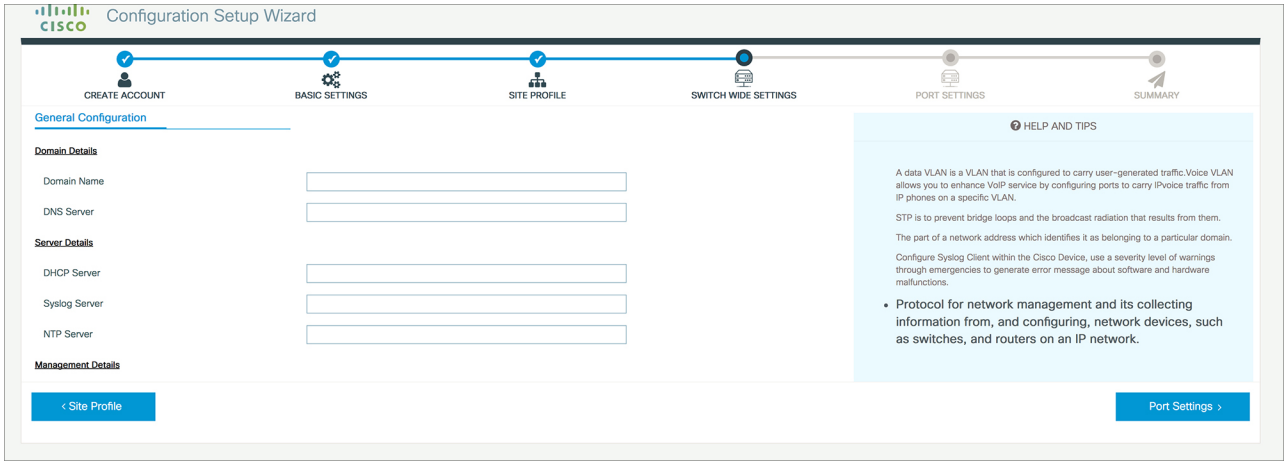
Step 4 In the **Syslog Server** field, type the IP address of the server to which you want to send syslog messages.

Step 5 To ensure that your device is configured with the right time, date and timezone, enter the IP address of the NTP server with which you want to synchronize the device time.

Step 6 In the **Management Details** section, type an IP address to identify the SNMP server. SNMPv1, SNMPv2, and SNMPv3 are supported on your device.

Step 7 Specify the **SNMP community** string to permit access to the SNMP protocol.

Figure 14: DHCP, NTP, DNS and SNMP Settings



What to do next

Configure port settings.

Configuring Port Settings

Procedure

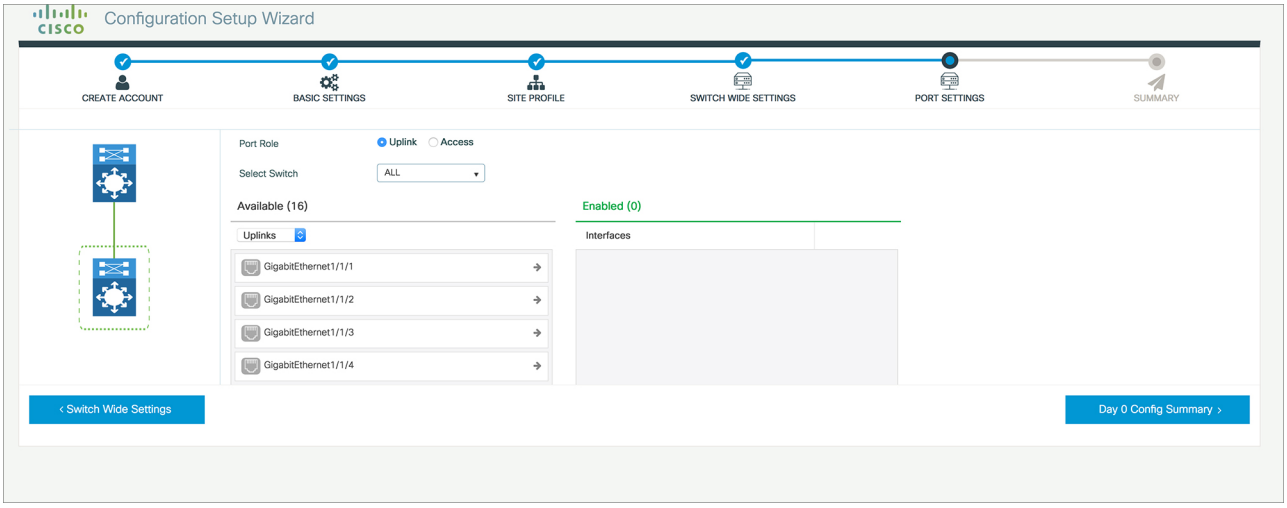
Step 1 Based on the site profile chosen in the earlier step which is displayed in the left-pane, select the **Port Role** from among the following options:

- Uplink – For connecting to devices towards the core of the network.
- Downlink – For connecting to devices further down in the network topology.
- Access – For connecting guest devices that are VLAN-unaware.

Step 2 Choose an option from the **Select Switch** drop-down list.

Step 3 Make selections from the **Available** list of interfaces based on how you want to enable them and move them to the **Enabled** list.

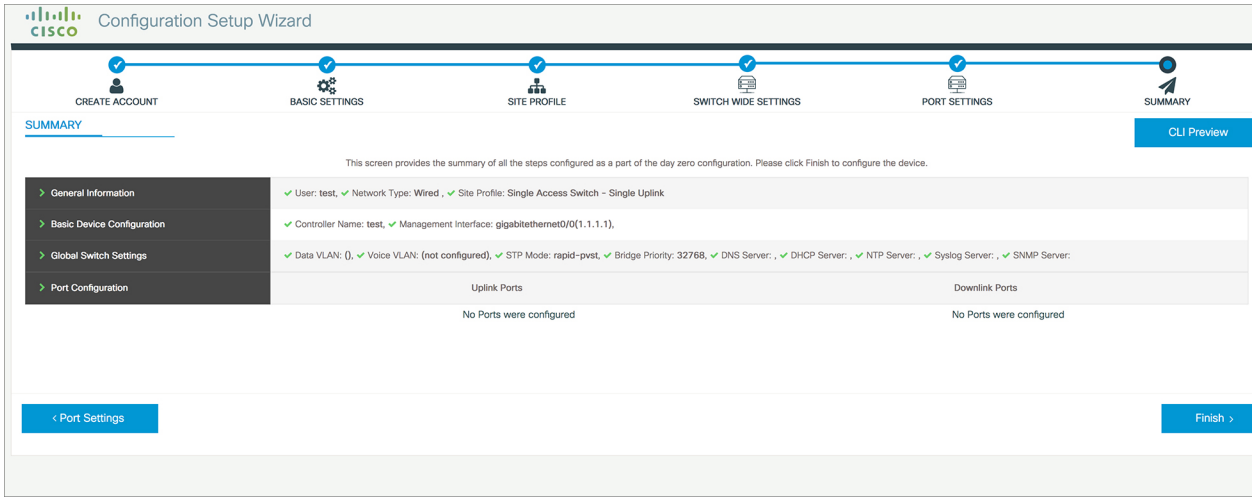
Figure 15: Port Settings



What to do next

- Click **Day 0 Config Summary** to verify your setup.
- Click **Finish**.

Figure 16: Day 0 Config Summary



Configuring VTY Lines

For connecting to the device through Telnet or SSH, the Virtual Terminal Lines or Virtual TeleType (VTY) is used. The number of VTY lines is the maximum number of simultaneous access to the device remotely. If the device is not configured with sufficient number of VTY lines, users might face issues with connecting to

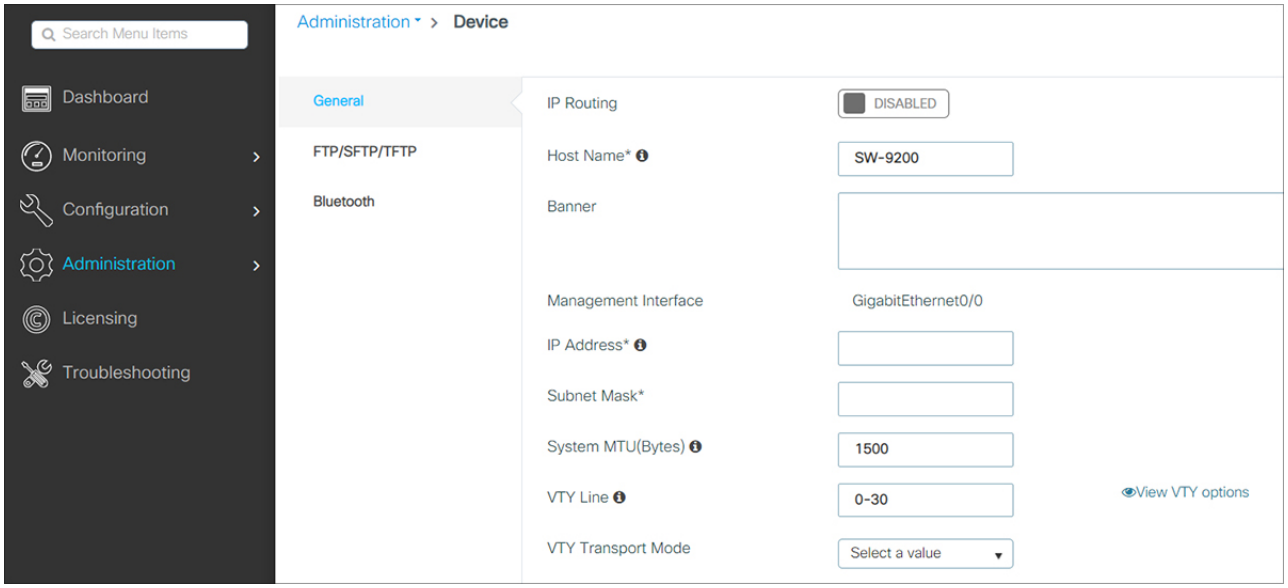
the WebUI. You must change the default value for VTY Line, 0-15 (or 0-4 in some models), to 0-30 to allow up to thirty simultaneous sessions.

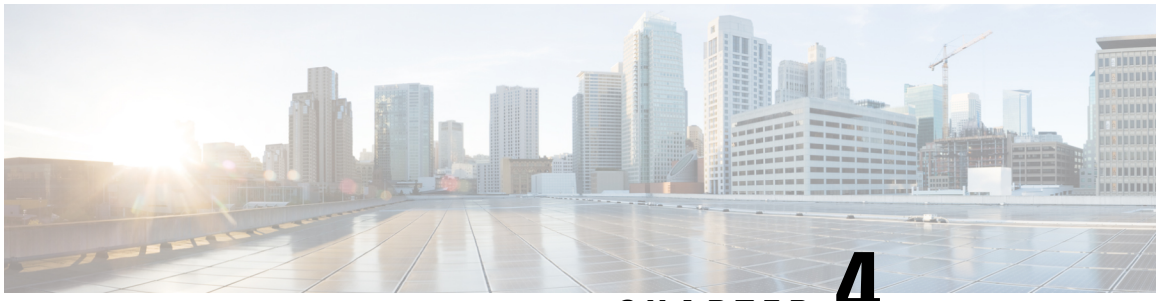
Procedure

Step 1 From the WebUI, navigate through **Administration > Device** and select the **General** page.

Step 2 In the **VTY Line** field, enter `0-30`.

Figure 17: Configuring VTY Line





CHAPTER 4

Implementation Options

This section contains the following:

- Power over Ethernet, on page 57
- Working with the External USB3.0, on page 61
- SFP Command Line, on page 62
- Zeroization, on page 62

Power over Ethernet

Power over Ethernet (PoE) is typically used to power up Access points, IP Cameras and IP Phones connected to the device's Ethernet ports.

The ESS3300 supports Power over Ethernet (PoE and PoE+) on up to 24 ports with visibility and management from Cisco IOS-XE Software. From Cisco IOS XE Release 17.17.1, UPoE+ is also supported.

From Cisco IOS XE Release 17.17.1, the maximum power per port is enhanced to 90W, from the earlier support of 30W. The system PoE budget has been enhanced to 2160W, from the earlier support of 720W.

Important The ESS3300 uses a SPI bus based device from Microsemi / Microchip PD69208M as the PoE controller. Failure of the integrator to use this controller will result in IOS-XE not recognizing the device.

Note The Powered Device (PD) will be detected if it is IEEE-compliance or a Cisco standard device. Support for CDP and LLDP is available for power negotiation, and must be enabled on the ESS3300.

Note CDP and/or LLDP must be enabled on the ESS3300, and the PD must support CDP and/or LLDP for the device to be able to negotiate power levels between 15 and 30 watts.

From 17.17.1 onwards, you can use CDP to negotiate upto 60W (Cisco UPOE) and LLDP to negotiate upto 90W (IEEE 802.3BT).

Note In ESS-3300 PoE devices, when a Powered Device (PD) is connected, if the switch or port lacks the power to bring up the PD, the port provides whatever power is available in the device. If the PD can operate with the given power, the port indicates the class for which the power is allocated. If the supplied power is insufficient to power up the PD, the port switches to power denial.

Note If the port is configured with a static value in the CLI, such as **power inline static max**, and the connected PD requires more power than configured, the port becomes error-disabled.

Device Detection and Power Allocation

The switch will detect a Cisco Pre-standard or an IEEE-compliant PD when the PoE is enabled and the connected device is not being powered by an AC adapter.

After device detection, the switch determines the power requirements based on power classification class. Depending on the available power in the power budget, the switch determines if a port can be powered. The switch initially allocates this power when it detects and powers the device. Power negotiation using CDP/LLDP protocols happens thereafter. On reload the PoE ports are powered down.(i.e they are powered down at rommon stage).

Power Management

Limit the PoE budget to prevent excess power consumption that may exceed the capacity of the power source.

To limit the PoE budget, configure the overall PoE budget using the **power inline wattage max** <watts-for-PSU> command in global configuration mode.

Note The switch needs a minimum wattage of power to run efficiently. The power budget for PoE is calculated as the total power of the PSU minus the minimum wattage. For example, if the PSU can provide 170W of power and needs a minimum of 20W of power to run the switch, then the maximum PoE budget that can be configured is 150W.

Command Line Interface

This section describes the CLI to use for configuring and displaying PoE.

Before you configure Power over Ethernet (PoE), note the following:

- **show inventory** and **show diag** commands will not display details of the vendor/system integrator's PoE controller.
- **show run** command will not reflect the current PoE configuration.
- On connecting a PD, power negotiation happens almost instantly. However, it takes 3-5 minutes to reflect accurate statistics using **show power inline**
- The default software mode is PoE and not PoE+ to prevent overdraw.

- There is limited support for LLDP-MED and LLDP-MDI.



Note Implementation of PoE is a partner option. The integrator is responsible for proper implementation into the finished product, therefore, it may or may not be available.

To configure auto or static or off:

```
power inline auto | static | never
```

Configuration example:

```
switch#config terminal
switch#interface g0/1/<1,2,3,4>
switch(config-if)#power inline {auto|static|never}
```

To enable CDP:

```
switch#config terminal
switch(config)#cdp run
switch(config#exit
```

To enable LLDP:

```
switch#config terminal
switch(config)#lldp run
switch(config#exit
```

To Verify your configuration:

```
switch#show power inline
Available:2160.0(w)  Used:88.3(w)  Remaining:2071.7(w)

Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Gi1/3     auto   on         7.0     Ieee PD             2     90.0
Gi1/4     auto   off        0.0     n/a                 n/a   90.0
Gi1/5     auto   off        0.0     n/a                 n/a   90.0
Gi1/6     auto   off        0.0     n/a                 n/a   90.0
Gi1/7     auto   off        0.0     n/a                 n/a   90.0
Gi1/8     auto   off        0.0     n/a                 n/a   90.0
Gi1/9     auto   on         30.0    WS-C3560CX-8PT-S    4     90.0
Gi1/10    auto   off        0.0     n/a                 n/a   90.0
Gi2/1     auto   off        0.0     n/a                 n/a   90.0
Gi2/2     auto   on         45.0    Ieee PD             5     90.0
Gi2/3     auto   off        0.0     n/a                 n/a   90.0
Gi2/4     auto   off        0.0     n/a                 n/a   90.0
Gi2/5     auto   off        0.0     n/a                 n/a   90.0
Gi2/6     auto   off        0.0     n/a                 n/a   90.0
Gi2/7     auto   off        0.0     n/a                 n/a   90.0
Gi2/8     auto   on         6.3     IP Phone 7960       2     90.0
Gi2/9     auto   off        0.0     n/a                 n/a   90.0
Gi2/10    auto   off        0.0     n/a                 n/a   90.0
Gi2/11    auto   off        0.0     n/a                 n/a   90.0
Gi2/12    auto   off        0.0     n/a                 n/a   90.0
Gi2/13    auto   off        0.0     n/a                 n/a   90.0
Gi2/14    auto   off        0.0     n/a                 n/a   90.0
Gi2/15    auto   off        0.0     n/a                 n/a   90.0
Gi2/16    auto   off        0.0     n/a                 n/a   90.0
```

```
--------- ------ ---------- ---------- ---------- ------ -----
Totals:          4    on    88.3
```

To show power on a particular interface:

```
switch#show power inline {interface-id}
```

Displays PoE status for a switch for the specified interface.

```
show power inline interface-id detail
```

To show power consumption:

```
Switch#show power inline police
Available:2160.0(w)  Used:88.3(w)  Remaining:2071.7(w)

Interface Admin  Oper       Admin      Oper       Cutoff Oper
          State  State      Police     Police     Power  Power
--------- ------ ---------- ---------- ---------- ------ -----
Gi1/3     auto   on         none       n/a        n/a    3.5
Gi1/4     auto   off        none       n/a        n/a    n/a
Gi1/5     auto   off        none       n/a        n/a    n/a
Gi1/6     auto   off        none       n/a        n/a    n/a
Gi1/7     auto   off        none       n/a        n/a    n/a
Gi1/8     auto   off        none       n/a        n/a    n/a
Gi1/9     auto   on         none       n/a        n/a    19.4
Gi1/10    auto   off        none       n/a        n/a    n/a
Gi2/1     auto   off        none       n/a        n/a    n/a
Gi2/2     auto   on         none       n/a        n/a    9.1
Gi2/3     auto   off        none       n/a        n/a    n/a
Gi2/4     auto   off        none       n/a        n/a    n/a
Gi2/5     auto   off        none       n/a        n/a    n/a
Gi2/6     auto   off        none       n/a        n/a    n/a
Gi2/7     auto   off        none       n/a        n/a    n/a
Gi2/8     auto   on         none       n/a        n/a    2.0
Gi2/9     auto   off        none       n/a        n/a    n/a
Gi2/10    auto   off        none       n/a        n/a    n/a
Gi2/11    auto   off        none       n/a        n/a    n/a
Gi2/12    auto   off        none       n/a        n/a    n/a
Gi2/13    auto   off        none       n/a        n/a    n/a
Gi2/14    auto   off        none       n/a        n/a    n/a
Gi2/15    auto   off        none       n/a        n/a    n/a
Gi2/16    auto   off        none       n/a        n/a    n/a
--------- ------ ---------- ---------- ---------- ------ -----
Totals:                                                  34.0
```

The list of commands for debugging PoE follows:

Command	Description
Debug ilpower controller	Display PoE controller debug messages
Debug ilpower event	Display PoE event debug messages
Debug ilpower port	Display PoE port manager debug messages
Debug ilpower powerman	Display PoE power management debug messages
Debug ilpower cdp	Display PoE CDP debug messages
Debug ilpower registries	Display PoE registries debug messages

Command	Description
Debug ilpower scp	Display PoE scp debug messages

Working with the External USB3.0

The ESS3300 provides access to a single USB 3.0 Type A device.

External USB3.0

The following details are important when working with an external USB device:

- The USB is for storage only and can be gracefully mounted/unmounted using IOS CLI.
- The USB is accessible in ROMMON, IOS, and IOx applications.
- USB device must have single partition, and in ext2, Fat16, or Fat32 format only.
- The user can copy files between usbflash0: to/from flash:/bootflash:, msata:
- In both ROMMON and IOS, use **dir usbflash0:** to view USB:

Caution No hot-plug support in rommon mode. On insertion of USB, reboot (rommon1>reset) to view usb.

Caution Cisco USBs are strongly recommended and are the only ones supported. Many generic USBs may not work. Some branded USBs which comply with protocol standards such as Kingston USB3.0 may work.

USB CLI Commands:

To access the USB file system through ROMMON, use the following command:

```
ROMMON>dir usbflash0:
```

To access the USB file system through IOS, use the following command:

```
switch#dir usbflash0:
```

To plug in and unplug the USB device gracefully, disable it first:

```
switch conf t
switch(config)#platform usb disable
switch#show platform usb status
USB disabled
```

To gracefully activate a mounted USB in IOS:

```
switch#no platform usb disable
switch#show platform usb status
USB enabled
```

The USB port could be considered a potential security risk. You may wish to disable it if it is not in use. To gracefully remove a USB when in IOS mode:

```
switch conf t
switch(config)#platform usb disable
Jun 4 05:44:52.339: %IOSD_INFRA-6-IFS_DEVICE_OIR: Device usbflash0 removed
switch#show platform usb status
USB disabled
```

To re-enable USB port:

```
switch(config)#no platform usb disable
*Jun 4 05:45:20.890: %IOSD_INFRA-6-IFS_DEVICE_OIR: Device usbflash0 added
switch#show platform usb status
USB enabled
```

SFP Command Line

To configure the WAN port as an RJ45 or an SFP:

```
switch#config terminal
switch(config)#config terminal
switch(config)#interface g0/0/{0|1}
switch(config-if)#media type ?
auto-select  Use whichever connector is attached
  rj45         Use RJ45 connector
  sfp          Use SFP connector
```

To configure auto-failover:

```
switch(config-if)#media-type {rj45|sfp} ?
  auto-failover  Automatic Fail over
  <cr>           <cr>
```

To validate your changes, use the following commands.

If SFP is detected:

```
switch#show inventory
```

To see if your configuration has taken effect:

```
switch#show run int g0/0/{0|1}
```

To reload the gigabit ethernet module:

```
switch#hwmodule subslot 0/0 reload force
```

Zeroization

On the ESS-3300, the Push Button is used exclusively for triggering the Zeroization process which zeroize and erase switch configuration files or entire flash file system depending on the option provided under “service declassify”.

The Zeroization process starts as soon as the Push Button is pressed. The CLI command, “service declassify”, is used to set the desired action in response to the Push Button press. To prevent accidental erasure of the system configuration/image, the default setting is set to “no service declassify”.

eMMC is a managed NAND. This means that our embedded switch or router system does not interact with the flash memory directly. The flash controller presents a block-style interface to our system, and it handles the flash management (analogous to the Flash Translation Layer). Our embedded switch or router system cannot access the raw flash directly.

The JEDEC standard has commands that are supposed to remove data from the raw flash. In Cisco's implementation, the "Erase" and "Sanitize" commands are used. The eMMC standard JESD84-B51 defines "Sanitize" as follows:

The Sanitize operation is a feature … that is used to remove data from the device according to Secure Removal Type. The use of the Sanitize operation requires the device to physically remove data from the unmapped user address space.

After the sanitize operation is completed, no data should exist in the unmapped host address space.



Important **service declassify erase-nvram** is NOT guaranteed to securely and completely erase the data from the underlying file system. The data may be recoverable by forensic analysis techniques. Consider using **service declassify erase-all** to securely delete all data on the device



Important Zeroization does NOT erase removable media such as SD Card and USB Storage. This media must be removed from the system and erased or destroyed using procedures that are outside the scope of this document.

Important Notice about Zeroization

Zeroize does a very thorough wipe of all non-protected parts of the eMMC flash using the best technology designed by the flash manufacturer today and can do so using the push of a button without the need for a console, ssh, or management session of any kind. It is the integrator's and end user's responsibility to determine the suitability regardless of the CLI keyword used to enable the feature.



Note **While Cisco IOS and Cisco IOS-XE use the command line text of "declassify" in the command line interface (CLI) to enable the zeroize feature, in no way does this represent any specific endorsement or acknowledgment of a Government approved flash erasure methodology.**

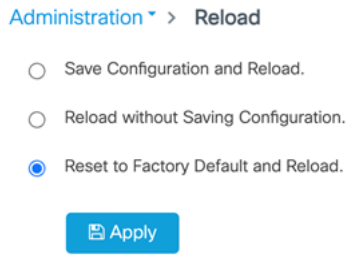
Declassification procedures are unique to each Government organization. Cisco solely provides the technical detail of the erasure operation here, not the policy distinction or any specific recommendation per classification.

Please refer to your respective Government Agency policies, procedures, and recommendations for the handling of sensitive data to see if this procedure meets with those requirements.

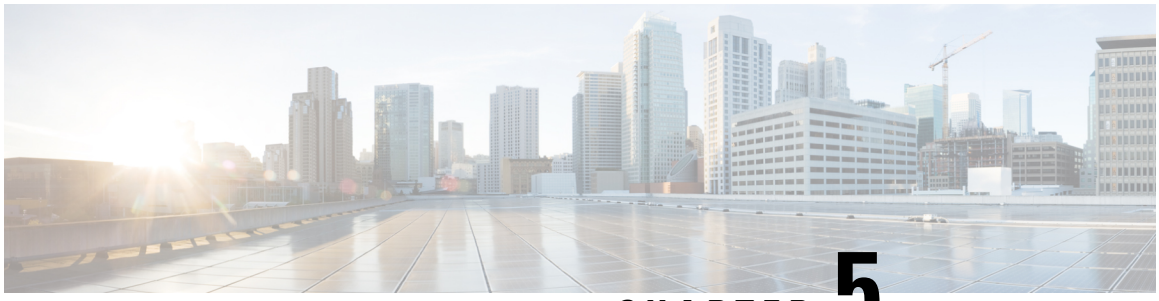
WARNING!

The CLI **service declassify erase-all** is literally a **software self-destruct mechanism** intended for defense and intelligence environments that attempts to wipe clean, all of the writable non-volatile storage on the device to clear the device configuration, other stored configurations and all security credentials including any additional license keys.

Please do not use this feature in lieu of doing a **write erase** from the CLI or from the Administration page, Reload option of the WebUI. Invoke the reload with the **Reset to Factory Default and Reload** option and click **Apply**. See the following figure.



If **service declassify erase-all** is invoked, after restoring the IOS-XE image and device configuration, you must re-license the device using the standard Cisco Smart Licensing procedures which ultimately require a Cisco Smart Account and access to the internet or a satellite license server.



CHAPTER 5

Additional Information and Configuration Guides

This section contains links to the following:

- Where to find Additional Information, on page 65
- Additional Configuration Guides, on page 65
- Communications, services, and additional information, on page 67

Where to find Additional Information

The ESS3300 offers a rich IOS-XE feature set. This marketing data sheet provides a complete list of all of the features.

Previous chapters in this guide provided an introduction the the ESS3300, as well as some of the basic configuration and feature differences for this product. The IOS-XE Operating System runs on numerous switching devices, and as such, has a wealth of additional configuration information.

The following is a sample of additional resources to use:

- Cisco IOS XE
- ESS3300 Product Support Information
- Cisco Catalyst Rugged Series Industrial Ethernet Switches

Additional Configuration Guides

The following sections list configuration guides that have content which applies to a number of different IoT switches.

Redundancy Protocol Configuration Guide

The Redundancy Protocol Configuration Guide contains the following sections:

- High-Availability Seamless Redundancy (HSR)
- Configuring Hot Standby Router Protocol (HSRP)
- Media Redundancy Protocol (MRP)
- Configuring Parallel Redundancy Protocol (PRP)

- Configuring Resilient Ethernet Protocol (REP)
- Configuring Resilient Ethernet Protocol (REP) Fast
- Virtual Router Redundancy Protocol (VRRP) V3 Protocol Support

PROFINET Configuration Guide

The PROFINET Configuration Guide contains the following sections:

- Configuring PROFINET
- Adding Small Form-Factor (SFP) Modules to the SIMATIC STEP7 or TIA Portal Automation applications

Security Configuration Guide

The Security Configuration Guide contains the following sections:

- Configuring IPv6 First Hop Security
- Cisco TrustSec Virtual Routing and Forwarding (VRF)-Aware Security Group Tag (SGT)
- Configuring Layer 2 Network Address Translation (NAT)
- Configuring the Secure Cloud Analytics Connector
- Cisco Umbrella Integration
- MACsec and the MACsec Key Agreement (MKA) Protocol
- Configuring Web-Based Authentication

System Management Configuration Guide

The System Management Configuration Guide contains the following sections:

- Configuring Precision Time Protocol (PTP)
- Configuring Flash Memory (SD) Swap Drive

Layer 2 Configuration Guide

The Layer 2 Configuration Guide contains the following sections:

- Configuring Layer 2 Protocol Tunneling
- Configuring Switch Port Analyzer (SPAN) and Remote SPAN (RSPAN)
- Configuring IEEE 802.1Q Tunneling
- Configuring Virtual LAN (VLAN) Mapping

IP Multicast Routing Configuration Guide

The IP Multicast Routing Configuration Guide contains the following sections:

- Configuring Basic Multicast Routing

- Configuring Multicast Source Discovery Protocol (MSDP)
- Configuring Protocol-Independent Multicast (PIM)
- Configuring Source-Specific Multicast (SSM)
- Implementing IPv6 Multicast

Network Management Configuration Guide

The Network Management Configuration Guide contains the following sections:

- Configuring Simple Network Management Protocol (SNMP)
- Configuring Switch Port Analyzer (SPAN) and Remote SPAN (RSPAN)
- Configuring Embedded Packet Capture (EPC)
- Flexible NetFlow Export of Cisco TrustSec Fields

QoS Configuration Guide

The entire QoS Configuration Guide is dedicated to configuring Quality of Service.

IP Routing Configuration Guide

The IP Routing Configuration Guide contains the following sections:

- Configuring Bidirectional Forwarding Detection
- Configuring IPv4 Policy-Based Routing
- Configuring IPv6 Unicast Routing
- Configuring Routing Information Protocol (RIP)
- Configuring Virtual Routing and Forwarding (VRF)-lite

CIP and MODBUS Configuration Guide

The CIP and MODBUS Configuration Guide contains the following sections:

- Common Industrial Protocol (CIP)
- Modicon Communication Bus (MODBUS)

Communications, services, and additional information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.

- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.