



Cisco Catalyst 3850 Series and Cisco Catalyst 3650 Series Switches Best Practices Guide

First Published: November 30, 2015
Last Updated: December 14, 2015

Cisco Systems, Inc.
www.cisco.com

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

© 2015 Cisco Systems, Inc. All rights reserved.



Preface vii

Audience iii-vii

Conventions vii

Obtaining Documentation and Submitting a Service Request viii

Ease of Deployment 1-1

Purpose 1-1

Configuration Tool 1-2

Catalyst Switch Configuration Best Practices 1-2

LAN Access Switch Topology 1-4

Switch Address Plan 1-5

Initial Switch Configuration 2-7

Purpose 2-7

Prerequisites 2-7

Identify Configuration Values 2-8

Assign Initial Management Information 2-8

 Configure the Hostname for Switch Identification 2-9

 Configure Secure HTTPS and Secure Shell for Secure LAN Management 2-9

 Configure SNMP for Remote Management 2-10

 Configure Local Login and Password for Switch Access 2-10

 Configure Centralized User Authentication Through TACACS+ 2-10

 Assign an IP Address to the Switch 2-11

 Configure the Management IP Address on an Out-of-Band Interface 2-12

 Configure the Management IP Address on an In-Band Interface 2-14

 Create a Management VLAN in Hardware 2-15

 Verify Basic Switch Configuration 2-17

Show Running Configuration for Initial Management Information 2-17

Switch Stack Update 3-21

Purpose 3-21

Prerequisites 3-21

Identify Configuration Values 3-22

- LAN Access Switch Topology with Configured FTP Server 3-22
- Performing the Stack Update 3-23
 - Obtain the Switch Software Image 3-23
 - Check the Software Version on the Stack Members 3-23
 - Configure the Switch to Run in Install Mode 3-24
 - Download the Switch Image from Cisco.com to a FTP Server 3-25
 - Update the Switch Stack Image 3-27
 - Enable Switch Image Auto-Upgrade 3-27
 - Verify that Stack Members Are Running the Same Software Image 3-28

Global System Configuration 4-29

- Purpose 4-29
- Prerequisites 4-29
- Identify Configuration Values 4-29
- Assign Global Configuration Information 4-30
 - Configure High Availability on the Switch Stack 4-31
 - Configure VTP Transparent Mode 4-31
 - Enable Rapid Per-VLAN Spanning Tree 4-32
 - Configure BPDU Guard for Spanning-Tree PortFast Interfaces 4-32
 - Configure UDLD to Detect Link Failure 4-33
 - Configure an Access List to Limit Switch Access 4-33
 - Configure System Clock and Console Timestamps 4-34
 - Configure DHCP Snooping Security Features 4-34
 - Configure ARP Inspection 4-34
 - Configure EtherChannel Load Balancing 4-35
 - Create Access Layer VLANs 4-35
 - Create IPv6 First Hop Security Policies 4-35
 - Increase the TFTP Block Size 4-36
 - Enable New Members to Automatically Update to the Switch Stack Image 4-36
 - Verify Global Switch Configuration 4-37
- Show Running Configuration For Global Management Information 4-37

Uplink Interface Connectivity 5-41

- Purpose 5-41
- Prerequisites 5-41
- Restrictions 5-41
- Identify Configuration Values 5-42
- LAN Access Switch Topology with Uplinks to a Distribution Switch or Distribution Router 5-43
- Configure Uplink Interface Connectivity 5-44

Recommendations for Configuring the Uplink Interface to a Router or Switch	5-44
Configure QoS on the Uplink EtherChannel Interfaces	5-44
Configure the Uplink Interface as an EtherChannel and as a Trunk	5-45
Configure the Uplink Interface to Connect to Distribution VSS or VPC Switches	5-45
Configure the Uplink Interface to Connect to Distribution Routers (or Standalone Distribution Switches)	5-46
Configure Security Features on the Uplink EtherChannel Interfaces	5-48
Spanning-Tree Recommendations for Uplink Interfaces Connecting to Distribution Switches	5-48
Verify Uplink Interface Configurations	5-49
Show Running Configuration for Uplink Interface Connectivity	5-49
Access Interface Connectivity	6-51
Purpose	6-51
Prerequisites	6-51
Identify Configuration Values	6-51
LAN Access Switch Topology with Connections to End Devices	6-53
Configure Access Interface Connectivity	6-53
Recommendations for Configuring Access Interfaces	6-53
Configure the Interface for Access Mode	6-55
Configure VLAN Membership	6-55
Create an Interface Description	6-55
Configure Security Features on Access Interfaces	6-56
Configure QoS on the Access Interfaces	6-57
Verify Access Interface Configurations	6-58
Show Running Configuration for Access Interface Connectivity	6-61
Access Control on the Wired Network	7-65
Purpose	7-65
Prerequisites	7-65
Restrictions	7-65
Identify Configuration Values	7-66
LAN Access Switch Topology with IEEE 802.1x Secure Access Control	7-67
Provision IEEE 802.1x for Wired LAN	7-67
Recommendations for Configuring Security on a Wired LAN	7-67
Provision Common Wired Security Access	7-68
Provision in Monitor Mode	7-71
Provision in Low Impact Mode	7-72
Provision in High Impact Mode	7-73
Verify Secure Access Control on the Switch	7-74

Show Running Configuration for Provisioning Modes 7-74

Monitoring IEEE 802.1x Status and Statistics 7-77

Converged Wired and Wireless Access 8-81

Purpose 8-81

Prerequisites 8-81

Restrictions 8-82

Identify Configuration Values 8-82

LAN Access Switch Topology with Wireless Connectivity 8-83

Enable the Switch as a Wireless Controller 8-84

 Install Access Point Licenses on the Switch 8-84

 Verify AP-Count License Installation 8-85

 Configure a Wireless Management VLAN 8-86

 Configure Service Connectivity 8-86

 Enable Wireless Controller Functionality 8-87

 Change a Switch to Run in Mobility Controller Mode 8-87

 Enable the Access Point Connections 8-88

 Enable a Client VLAN 8-89

Provisioning a Small Branch WLAN 8-90

 Provision in Easy-RADIUS 8-90

 Disable Authentication to Enable Easy-RADIUS 8-90

 Configure QoS to Secure the WLAN 8-91

 Verify Client Connectivity in RADIUS 8-91

 Provision in Secure Mode 8-93

 Enable the AAA RADIUS Server 8-93

 Configure the WLAN with IEEE 802.1x Authentication 8-94

 Configure QoS Service Policies for an Open WLAN 8-94

 Obtain WLAN Client IP Addresses 8-95

 Manage Radio Frequency and Channel Settings 8-95

 Disable Low Data Rates 8-96

 Enable Clean Air 8-97

 Enable Dynamic Channel Assignment 8-97

 Associate WLAN Clients 8-98

 Verify WLAN Client Connectivity 8-98

 Verify the Converged Access Configuration on the Switch 8-99

Show Running Configuration for Wireless LAN Converged Access 8-99

System Health Monitoring 9-103

Purpose 9-103

Prerequisites	9-103
Show Running Status	9-103
Run a System Baseline for Core Resources	9-104
Obtain CPU and Core Processor Usage	9-104
Obtain Switch Memory Usage	9-106
Monitor File Systems Usage	9-106
Run a System Baseline for Environmental Resources	9-107
Other System Monitoring Considerations	9-108
Spanning Tree Monitoring	9-108

INDEX



Preface

Audience

This document is written for managing the Cisco Catalyst 3850 Series Switches and the Cisco 3650 Series switches and switch stacks in their network. A basic understanding of Ethernet networking is expected. Cisco Certified Network Associate level (CCNA) knowledge is helpful, but not required.

Conventions

This document uses the following conventions:

Convention	Indication
<i>italic</i> blue font	Example configuration values that are replaced with reader values.
bold font	Commands and keywords and user-entered CLI appear in bold font.
<i>italic</i> font	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic</i> font.
[]	<ul style="list-style-type: none">• Default responses to system prompts are in square brackets.• Elements in square brackets are optional.
{x y z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string, or the string will include the quotation marks.
<code>courier</code> font	Terminal sessions and information the system displays appear in <code>courier</code> font.
< >	Nonprinting characters such as passwords are in angle brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.



Note

Means *reader take note*. Notes contain helpful suggestions or references to material that is not covered in the manual.

**Tip**

The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

**Timesaver**

You can save time by performing the action described in the paragraph.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: <http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>.

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



Ease of Deployment

This document describes best practices for deploying your Cisco Catalyst 3850 Series and Cisco Catalyst 3650 Series switches.



Note

Unless otherwise noted, the term *switch* refers to a standalone Catalyst 3850 switch, a Catalyst 3650 switch, or a switch stack.

A Cisco switch deployment best practice is a preferred configuration method to employ on your Catalyst switches. It is a proven and tested way to improve network security, performance, and availability.

A best practice configuration includes an explanation of why you should perform a given task and a sample snapshot of a full running configuration that you can extrapolate for your specific scenario.



Tip

Use the configuration recommendations in this document as a template for your switch deployments.



Note

Many Cisco documents are available that define best practices for a variety of features and solutions. There will be some overlap between the information provided in this guide and other best practices and deployment guides. When relevant, this document references other existing documents so the reader can get a deeper understanding of an aspect of the 3850 operation. Otherwise, this document is self-contained, and provides complete best practice configuration.

Configuration Tool

The configuration examples in this document use the Cisco IOS CLI configuration tool, which is the most common tool used to configure a switch.

However, you do have the flexibility to use a different tool to perform switch configuration. Other configuration tools are the Express Setup, Device Manager, and Cisco Prime.

The examples provided in this document show the CLI commands that you should execute on your switch. You must replace the blue italicized example values with your own values.



set system location *Building 1, San Jose, CA*

LAN Access Switch Topology

The workflows described in this document assume that a switch is deployed as a LAN access switch. Unless noted otherwise, a switch that is in the LAN access layer is configured as a Layer 2 switch, with all Layer 3 services provided by the directly connected distribution switch or router.

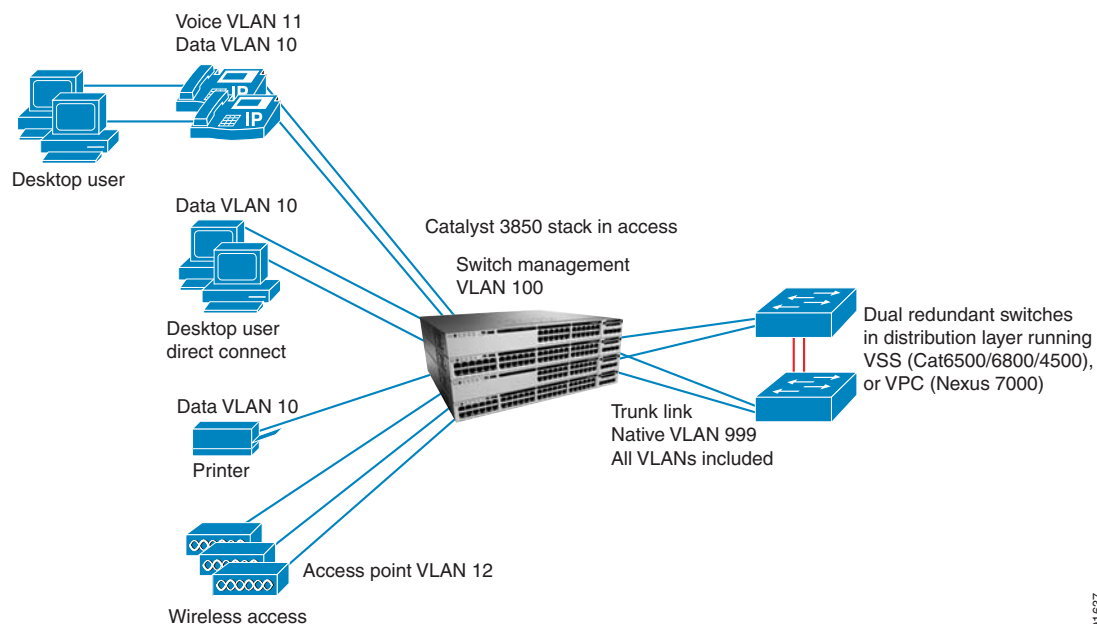
This document assumes that the switches are stacked together to form a switch stack (a common switching unit). We recommend that you use switch stacks because of built-in redundancy. We also recommend the use of using switch stacks when deploying switches in converged access mode (wireless mode) and connecting access points to different stack members.

A switch deployed at the LAN access layer provides high-bandwidth connections to devices through 10/100/1000 Ethernet, with both Gigabit and 10-Gigabit uplink connectivity options.

When a switch is deployed in access mode, it enables end devices, such as IP phones, wireless access points, and desktops to gain access to the network. The Power over Ethernet (PoE) switch models support PoE+ (30 W) and UPoE (60 W) to power IP phones, wireless access points, and IP cameras. The field-replaceable uplink module from the switch enables different uplink connectivity types.

Figure 1 shows an enterprise campus deployment, where the switch is connected to a distribution layer switch (such as a Catalyst 6500,6800,4500 or a Nexus 7000 switch).

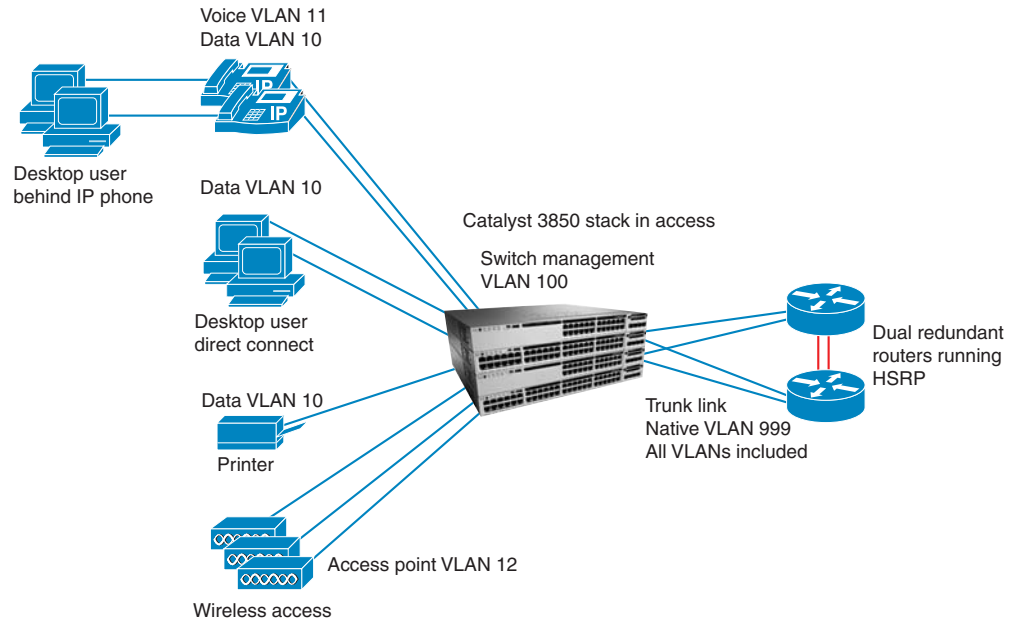
Figure 1 LAN Access Switch Topology with Distribution Switch



391637

Figure 2 shows a branch deployment, where the switch is connected to a router (ISR). Because the switch operates as a Layer 2 switch, not many differences occur in the configuration between the campus or branch deployment cases. Differences in the configuration are noted in the best practice procedures.

Figure 2 LAN Access Switch Topology with Distribution Router



391638

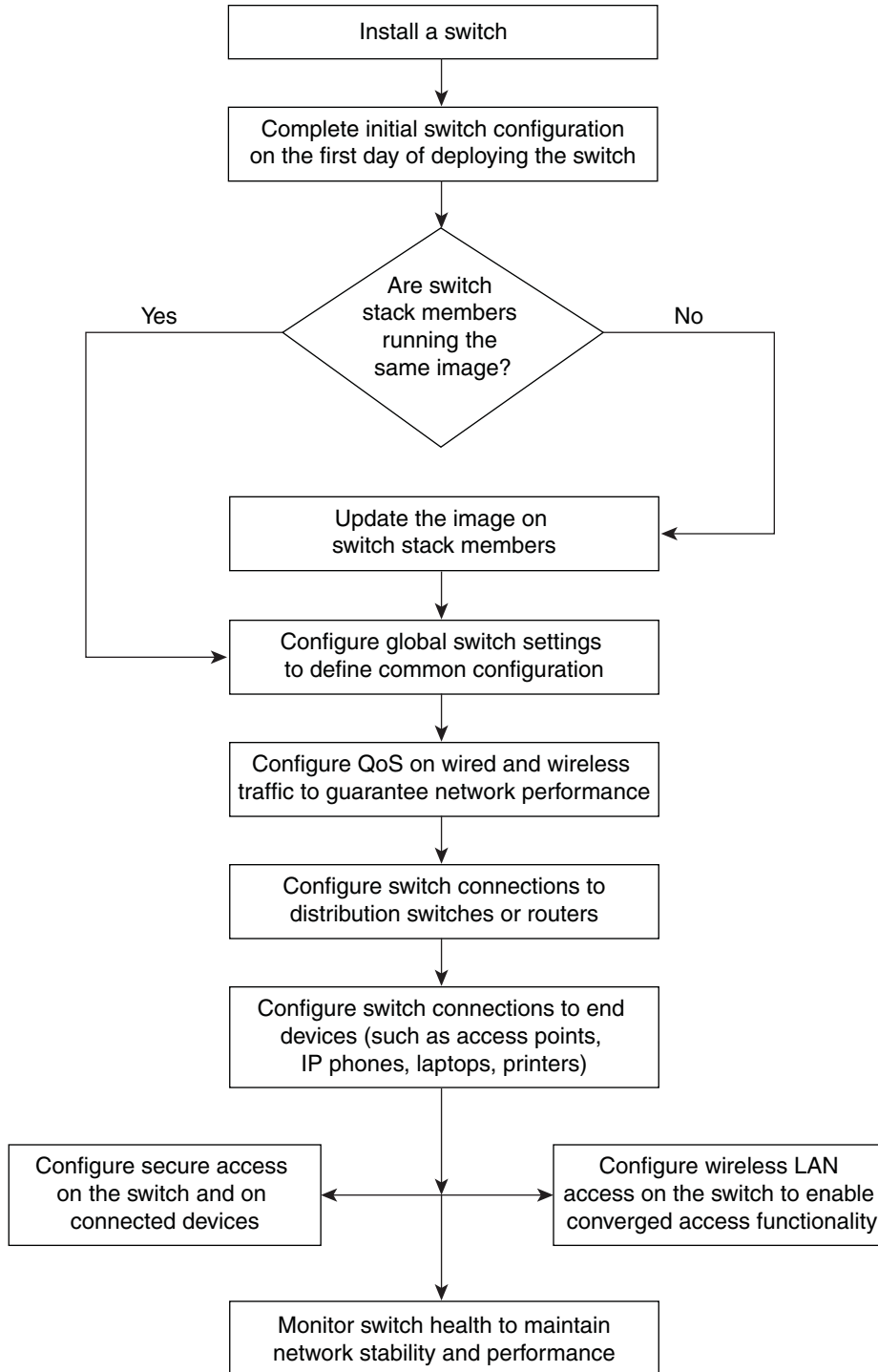
Cisco Catalyst Switch Configuration Workflow

This document focuses on configuring a switch network and is organized in a workflow pattern, beginning with the initial configuration of a switch after it is racked, mounted, connected, and powered on, and ending with monitoring system health.

Figure 3 shows the best-practice configurations described in this document.

See the *Switch Hardware Installation Guide* for information on how to install a switch.

Figure 3 *Cisco Catalyst Switch: Configuration Workflow*



953733

Switch Address Plan

The VLAN IDs and IP addresses designated for a switch and used throughout this document are not a component of practices; they are only specified for the configuration examples. Your deployment will have an IP address plan that suits your specific network.

In this document, all IP address ranges are /24 for the sake of simplicity. We recommend that VLAN IDs be reused across the access switches deployed.

For example, in the access layer, VLAN 10 is always used for data, and VLAN 11 is always used for voice. The IP subnets for those VLANs are different across the access switches, but the VLAN IDs are the same. This type of address plan makes it easier to operate the network because the same VLAN IDs are consistent.

Table 1 *IP Address Plan*

VLAN ID	IP Address	Server	Description
100	192.168.1.0/24	—	Switch in-band management VLAN.
10	192.168.10.0/24	Upstream device	Access data VLAN for end devices and subnet.
11	192.168.11.0/24	Upstream device	Access voice VLAN for IP phones and subnet.
12	192.168.12.0/24	Catalyst 3850 switch	Access point VLAN and subnet.
200	192.168.13.0/24	Upstream device	Wireless client VLAN and subnet.
—	192.168.254.0	—	IP address range for all central services. The services are not physically adjacent to the switch.



Switch Stack Update

This workflow explains how to update all members of a switch stack with the same software image.

Before proceeding with global and advanced configurations on a switch stack, all stack members must be running the same Cisco IOS XE release to avoid mismatch issues. In addition, any new switch that needs to join the switch stack must also be running the same Cisco IOS XE release; otherwise, the switch stack will not converge and the new switch will remain in a standalone state.



Note

Updating a Catalyst 3850 or 3650 switch stack is different from updating a Catalyst 3750 switch stack. Simply changing the boot statement to the desired .bin file is not recommended for Catalyst 3850 and 3650 switch stacks. The update process for Catalyst 3850 and 3650 switch stacks includes a series of package files, which are extracted from the .bin file and loaded into flash.

Prerequisites

- Obtain a valid Cisco Connection Online (CCO) account with entitled credentials.
- The process to install the new IOS version will use either FTP or TFTP. This requires a FTP or TFTP server be available to host the 3850 IOS Software, and the server reachable over an IP network.
- Install and configure the TFTP or FTP before you begin.
- Verify that the TFTP block size is set at the maximum value of 8192, as described in the “Increase the TFTP Block Size” section.



Identify Configuration Values

We recommend that you identify certain switch configuration values in advance so that you are ready to proceed with this section without interruption. As you follow the configuration sequence, replace the values in column B with your values in column C.


Note

In the configuration examples, you must replace the blue italicized example values with your own values.

Table 1 *Switch Stack Update Configuration Values*

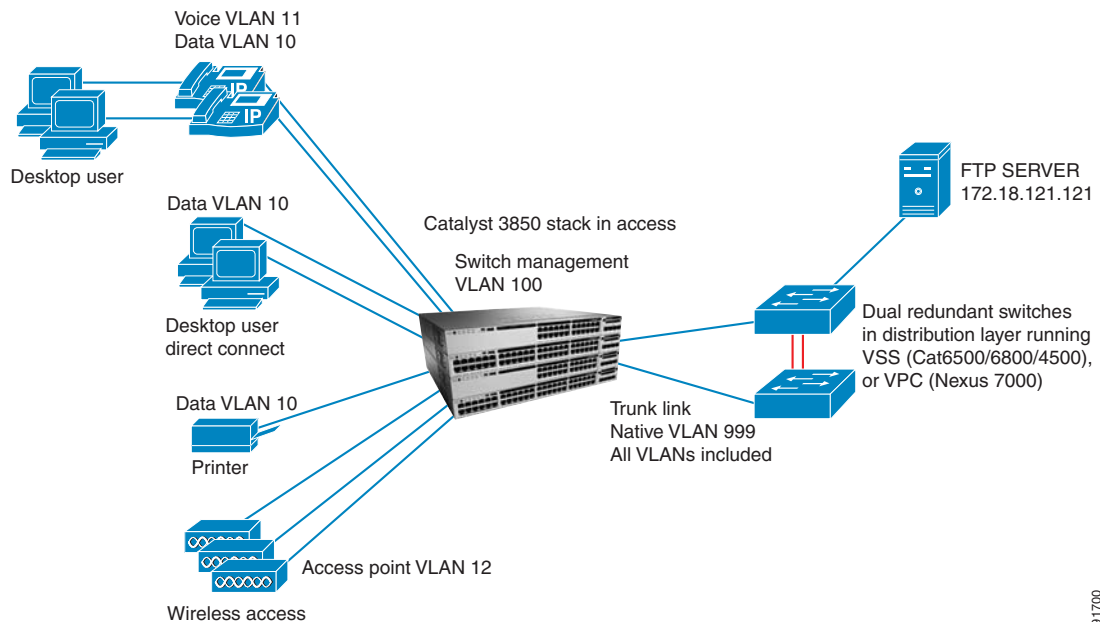
A. Value Name	B. Example Value Names	C. Your Value
hostname	<i>3850-access-Bld1Flr1</i>	
TFTP server	<i>192.168.254.12</i>	
Flash file	<i>cat3k_caa-universalk9.SSA.16.1.0.EFT3-1.bin</i>	


Note

Configuration examples begin in global configuration mode unless noted otherwise.

LAN Access Switch Topology with Configured TFTP Server

Figure 1 *LAN Access Switch Topology with Configured TFTP Server*



391700


Performing the Stack Update

- [Obtain the Switch Software Image](#)
- [Check the Software Version on the Stack Members](#)
- [Configure the Switch to Run in Install Mode](#)
- [Installing IOS image from local TFTP/FTP server](#)
- [Update the Switch Stack Image](#)
-

**Note**

The following tasks are to be performed in a sequence that is listed here.

Obtain the Switch Software Image

We recommend that you review the appropriate switch release notes before installation to ensure compatibility with your network topology. Each platform on Cisco.com has a Cisco-suggested release based on software quality, stability, and longevity, which is designated by the  symbol, as displayed in [Appendix 2, “Cisco Catalyst 3850-48P-S Switch”](#)

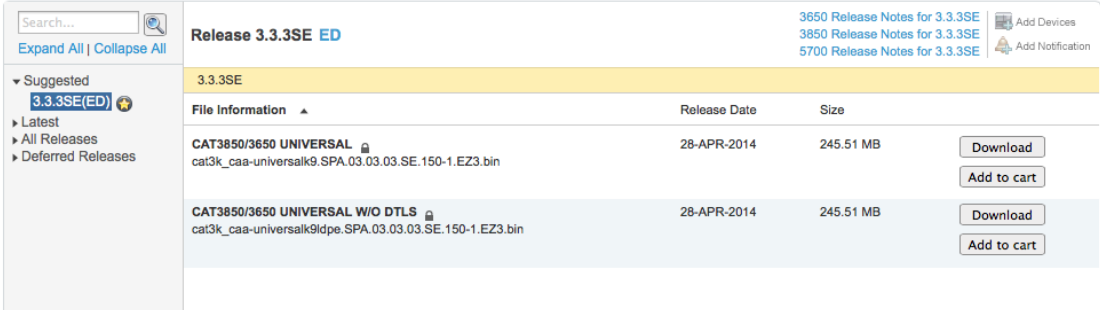
Step 1 Download the desired .bin file from Cisco.com to the switch flash storage.

**Note**

The purpose of this example is only to show you how the Cisco-suggested release symbol is designated, and not to give you recommended release versions because those change over time.

Figure 2 *Cisco Catalyst 3850-48P-S Switch*

Cisco Catalyst 3850-48P-S Switch



File Information	Release Date	Size	
CAT3850/3650 UNIVERSAL cat3k_caa-universalk9.SPA.03.03.03.SE.150-1.EZ3.bin	28-APR-2014	245.51 MB	Download Add to cart
CAT3850/3650 UNIVERSAL W/O DTLS cat3k_caa-universalk9ldpe.SPA.03.03.03.SE.150-1.EZ3.bin	28-APR-2014	245.51 MB	Download Add to cart

Check the Software Version on the Stack Members

Step 2 Verify the running software version.

Configure the Switch to Run in Install Mode

Your switches should run in install mode while in production. This mode is not a requirement, but the update procedure is different if your switches are running in a mode other than install mode.

Switch	Ports	Model	SW Version	SW Image	Mode
* BUNDLE	1 32	WS-C3850-24P	Denali 16.1.1	CAT3K_CAA-UNIVERSALK9	----
BUNDLE	2 32	WS-C3850-24P	Denali 16.1.1	CAT3K_CAA-UNIVERSALK9	
BUNDLE	3 32	WS-C3850-24P	Denali 16.1.1	CAT3K_CAA-UNIVERSALK9	

**Note**

To learn the differences for the install and bundle installation modes, see the [“Working with the Cisco IOS File System, Configuration File, and Software Bundle Files”](#) chapter of the *Cisco IOS File System, Configuration Files, and Bundle Files Appendix, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*

- Step 3** If your switch stack is running in bundle mode, use the **request platform software package expand switch file to flash** command to convert it to install mode.

```
request platform software package expand switch 1 file
flash:cat3k_caa-universalk9.BLD_V161_0_THROTTLE_LATEST_20151116_230450.SSA.b
to flash:
```

- Step 4** After the .bin file has successfully extracted to flash, change the boot statement and boot to the packages.conf file.

```
no boot system
boot system switch all flash:packages.conf
exit
write memory
reload
```

**Note**

Since the format of the packages.conf file has changed in Cisco IOS XE Release Denali 16.1, overwrite the old packages.conf with the new packages.conf file. Perform the above step for each switch in your stack. If you have a 3 member stack, it will need to be done on flash:, flash-2:, and flash-3.

**Note**

Make sure the tftp server is reachable. To improve performance, increase the tftp block size to 8192. Use the **ip tftp blocksize bytes** command in global configuration mode.

Step 5 Confirm that the switch stack is now running in install mode.

```
Switch# show version
Cisco IOS Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version
Denali 16.1.1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Thu 12-Nov-15 16:23 by mcpre

Switch Ports Model          SW Version  SW Image          Mode
-----
*  1 32   WS-C3850-24P   Denali 16.1.1  CAT3K_CAA-UNIVERSALK9 BUNDLE
   2 32   WS-C3850-24P   Denali 16.1.1  CAT3K_CAA-UNIVERSALK9 BUNDLE
   3 32   WS-C3850-24P   Denali 16.1.1  CAT3K_CAA-UNIVERSALK9 BUNDLE
```

Installing IOS image from local TFTP/FTP server

You can use any file transfer method that you are familiar with, but we recommend TFTP or FTP.

Step 6 Confirm the block size config using the following command:

```
# show run | inc block
ip tftp blocksize 8192
```

We recommend that you use a TFTP block size of 8192 (maximum allowed value) before attempting to use TFTP or FTP to transfer a file to the switch. Refer to the “Increase the TFTP Block Size” section in the “[Global System Configuration](#)” workflow for details.

Step 7 Make sure that there is connectivity to the TFTP server.

In this example, a TFTP server is used that is accessible through the in-band network.

```
ping 192.168.254.12
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.254.12, timeout is 2 seconds: !!!!
```

Step 8 After verifying connectivity, make sure that there is enough room in flash on all the switch stack members.

Step 9 If you determine that files must be purged from flash, run the **request platform clean switch** command to erase unneeded files within flash on all the stack members.

We recommend using the **request platform clean switch** command instead of individually deleting files. The command provides a list of the files to purge so that you understand what files are deleted when you confirm deletion.



Note

Use switch all option to clean up all switches in your stack.



Note

The **request platform clean switch** command also deletes the .bin file that is used to install the new Cisco IOS software. After the .bin is extracted, you no longer need it.

```

Device# request platform software package clean switch all file flash:
Running command on switch 1
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
done.
Running command on switch 2
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
done.
The following files will be deleted:
[1]:
/flash/cat3k_caa-rpbase.BLD_V161_0_THROTTLE_LATEST_20151116_230450.SSA.pkg
/flash/cat3k_caa-srdriver.BLD_V161_0_THROTTLE_LATEST_20151116_230450.SSA.pkg
/flash/cat3k_caa-universalk9.BLD_V161_0_THROTTLE_LATEST_20151116_230450.SSA.bin
/flash/cat3k_caa-wcm.BLD_V161_0_THROTTLE_LATEST_20151116_230450.SSA.pkg
/flash/cat3k_caa-webui.BLD_V161_0_THROTTLE_LATEST_20151116_230450.SSA.pkg
/flash/packages.conf
/flash/packages.conf.00-
/flash/packages.conf.01-
/flash/packages.conf.02-
[2]:

/flash/cat3k_caa-rpbase.BLD_V161_0_THROTTLE_LATEST_20151116_230450.SSA.pkg
/flash/cat3k_caa-srdriver.BLD_V161_0_THROTTLE_LATEST_20151116_230450.SSA.pkg
/flash/cat3k_caa-universalk9.BLD_V161_0_THROTTLE_LATEST_20151116_230450.SSA.bin
/flash/cat3k_caa-wcm.BLD_V161_0_THROTTLE_LATEST_20151116_230450.SSA.pkg
/flash/cat3k_caa-webui.BLD_V161_0_THROTTLE_LATEST_20151116_230450.SSA.pkg
/flash/packages.conf
/flash/packages.conf.00-
/flash/packages.conf.01-
/flash/packages.conf.02-
Do you want to proceed? [y/n]y
[1]:
Deleting file flash:cat3k_caa-rpbase.BLD_V161_0_THROTTLE_LATEST_20151116_230450.SSA.pkg
...
done.
Deleting file
flash:cat3k_caa-srdriver.BLD_V161_0_THROTTLE_LATEST_20151116_230450.SSA.pkg
... done.
Deleting file
flash:cat3k_caa-universalk9.BLD_V161_0_THROTTLE_LATEST_20151116_230450.SSA.bin
... done.
Deleting file flash:cat3k_caa-wcm.BLD_V161_0_THROTTLE_LATEST_20151116_230450.SSA.pkg ...
done.
Deleting file flash:cat3k_caa-webui.BLD_V161_0_THROTTLE_LATEST_20151116_230450.SSA.pkg
...
done.

```

```

Deleting file flash:packages.conf ... done.
Deleting file flash:packages.conf.00- ... done.
Deleting file flash:packages.conf.01- ... done.
Deleting file flash:packages.conf.02- ... done.
SUCCESS: Files deleted.
[2]:
Deleting file flash:cat3k_caa-rpbase.BLD_V161_0_THROTTLE_LATEST_20151116_230450.SSA.pkg
...
done.
Deleting file
flash:cat3k_caa-srdriver.BLD_V161_0_THROTTLE_LATEST_20151116_230450.SSA.pkg
... done.
Deleting file
flash:cat3k_caa-universalk9.BLD_V161_0_THROTTLE_LATEST_20151116_230450.SSA.bin
... done.
Deleting file flash:cat3k_caa-wcm.BLD_V161_0_THROTTLE_LATEST_20151116_230450.SSA.pkg ...
done.
Deleting file flash:cat3k_caa-webui.BLD_V161_0_THROTTLE_LATEST_20151116_230450.SSA.pkg
...
done.
Deleting file flash:packages.conf ... done.
Deleting file flash:packages.conf.00- ... done.
Deleting file flash:packages.conf.01- ... done.
Deleting file flash:packages.conf.02- ... done.
SUCCESS: Files deleted.

```

Step 10 Copy the switch image to the TFTP server using the **copy tftp://flash** command.

The following example shows that the TFTP server (192.168.254.12) requires a user name (admin) and password (cisco), which can easily be integrated into the **copy** command:

```

copy
tftp://admin:cisco@192.168.254.12/IOS/3850/cat3k_caa-universalk9.SSA.16.1.0.
EFT3-1.bin flash:

```

Update the Switch Stack Image

Step 11 Upload the image to the stack members, and then reload the switch.

The image download and installation can be performed while the stack is in-service, but to complete the update install, you must perform a switch reload, which causes a service outage.

```

software install file flash: cat3k_caa-universalk9.SSA.16.1.0.EFT3-1.bin

[1 2]: Do you want to proceed with reload? [yes/no]

```

Step 12 After the reload completes, run the **request platform software package clean switch all file flash** command.

```
.
request platform software package clean switch all file flash
Device# request platform software package clean switch all file flash:
Running command on switch 1
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
```

```
done.
Running command on switch 2
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
done.
```

To verify that stack members are using the same software, use the **show version** command on all members of the switch stack.

Enable Switch Image Auto-Upgrade

Step 13 Enable auto-upgrade so that new or replacement stack members are automatically upgraded with the software running on the switch stack.

If you are adding a new member, or replacing a stack member, we recommend that you enable the auto-upgrade feature within the stack. This feature helps to avoid stack mismatch issues and ensures that any new switches are upgraded to the version currently running on the stack and also converts a member in bundle mode to install mode.

The auto-upgrade feature automatically installs the software packages from an existing stack member to the stack member that is running incompatible software.



Note Auto-upgrade is disabled by default.



Note The rolling-upgrade feature is not supported.

```
software auto-upgrade enable
end
```




Initial Switch Configuration

This workflow explains how to configure the basic settings on a switch.

Whether the configuration deployment of a switch is completed all at once or done in phases, the basic switch settings must first be configured. The initial management configuration includes setting IP addresses, passwords, and VLANs, which are the prerequisites for future feature configuration.

Prerequisites for Initial Switch configuration

Refer to the switch [Hardware Installation Guide](#) to complete the following tasks:

1. Rack-mount the switch.
2. Connect the StackWise cables.
3. Connect the switch ports.
4. Perform power on.
5. Provision your upstream switch.
6. Connect at least one Ethernet cable from the uplink interface on the switch to the upstream switch or router.

Identify Configuration Values

We recommend that you identify certain switch configuration values in advance so that you can proceed with this section without interruption. We recommend that you take a print out of Table 2, and, as you follow the configuration sequence, replace the values in column B with your values in column C.



Note

Replace the blue italicized example values with your own values.



Table 3 Initial Configuration Values

A. Value Name	B. Example Value Names	C. Your Value
Hostname	<i>3850-access-Bld1Flr1</i>	
SNMP community strings for read-only and read-write access	<i>my-SNMP-RO-name</i> <i>my-SNMP-RW-name</i>	
Management VLAN ID	<i>100</i>	
In-band management IP address and mask	<i>192.168.1.2 255.255.255.0</i>	
Default gateway	<i>192.168.1.1</i>	
Secret password	<i>my-secret-password</i>	
TACAS server IP address	<i>192.168.254.10</i>	
TACAS server secret key	<i>cisco123</i>	
Uplink interface ID	GigabitEthernet 1/1/1	
Management VRF IP address for out-of-band interface	<i>Mgmt-vrf 192.168.128.5</i> <i>255.255.255.0</i>	
Mgmt-VRF default route next hop	<i>192.168.128.1</i>	
Native VLAN	<i>999, dummy</i>	

**Note**

The configuration examples provided in this document begin in global configuration mode, unless noted otherwise.

Assign Initial Management Information

- The following configurations should be performed in the same sequence in which they are listed here.
- Users can now proceed to the Configure Secure HTTPS and Secure Shell for Secure LAN Management section.
- Configure SNMP for Remote Management
- Configure Local Login and Password for Switch Access
- Configure Centralized User Authentication Through TACACS+
- Configure a Management IP Address on an Out-of-Band Interface
- Configure a Management IP Address on an In-Band Interface
- Create a Management VLAN in Hardware
- Enter the show running-configuration command to display the initial management information for the switch.

**Note**

The following configurations should be performed in the same sequence in which they are listed here.

Configure the Hostname for Switch Identification

Step 1 Configure the hostname on a switch to identify the switch in your network. By default, the system name and prompt are *Switch*.

Set the hostname for the switch product family, the role of the switch in your network, and the switch location.

Note that the system name is also used as the system prompt.

If you have not configured a system prompt, the first 20 characters of the system name are used as the system prompt. A greater-than symbol [>] is appended. The prompt is updated whenever the system name changes.

This example is for the switch serving as an access layer switch located on the first floor of Building 1

```
hostname 3850-access-Bld1Flr1
```

**Note**

Users can now proceed to the Configure Secure HTTPS and Secure Shell for Secure LAN Management section.

Configure Secure HTTPS and Secure Shell for Secure LAN Management

Step 2 Disable the HTTP and Telnet unencrypted protocols on the switch.

```
no ip http server
```

Step 3 Configure Secure HTTP (HTTPS) and Secure Shell (SSH) to enable secure management of the switch.

Enabling HTTPS automatically generates a cryptographic key to use the service. When SSH is configured after HTTPS, you do not have to explicitly generate the cryptographic key that SSH requires, unless you want to change the default key size.

We recommend that you use the **transport preferred none** command on the VTY lines to prevent connection attempt errors from the CLI prompt. Without this command, your IP name server may become unreachable, and long timeout delays may occur..

```
ip http secure-server
ip ssh version 2
!
line vty 0 15
  transport input ssh
  transport preferred none
```

**Note**

If the switch acts as a Web authentication server or as an authentication proxy, then do not disable the HTTP server by executing the **no ip http server** command.

Configure SNMP for Remote Management

- Step 4** Enable Simple Network Management Protocol (SNMP) to allow the network infrastructure devices to be managed by a remote Network Management System (NMS). Configure SNMPv2c read-only and read-write community strings, as shown in the following example. Once SNMP community strings are configured, then SNMP tools can be used to monitor the 3850 which includes statistics.

```
snmp-server community my-SNMP-RO-name RO
snmp-server community my-SNMP-RW-name RW
```

Configure Local Login and Password for Switch Access

- Step 5** Configure a local user ID and password to secure access to the switch. We recommend that you encrypt passwords to secure access to the device configuration mode and prevent the display of plain text passwords in configuration files.

```
username admin privilege 15 secret my-password
enable secret my-secret-password
service password-encryption
```

Configure Centralized User Authentication Through TACACS+



Note Configuring the TACACS+ protocol is optional and recommended only when using TACACS to manage all of your network devices.

- Step 6** Configure centralized user authentication through the TACACS+ protocol. As networks increase the number of devices to maintain, there is an operational burden to maintain local user accounts on every device. A centralized authentication, authorization, and accounting (AAA) service reduces operational tasks on each device and provides an audit log of user access for security compliance and root-cause analysis. When AAA is enabled for access control, all management access to the network infrastructure devices (SSH and HTTPS) is controlled by the AAA service. TACACS+ is the primary protocol used to authenticate management infrastructure devices to determine whether access can be allowed to the AAA server. A local AAA user database defined on each network infrastructure device to provide a fallback authentication source in case the centralized TACACS+ server is unavailable.

This example shows how to configure the switch for TACACS administrative access.


```
aaa new-model
tacacs server TACACS-SERVER-1
  address ipv4 192.168.254.10
  key cisco123
  exit
!
aaa group server tacacs+ TACACS-SERVERS
  server name TACACS-SERVER-1
  exit
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization exec default group TACACS-SERVERS local
ip http authentication local
```

Step 7 To save your configuration, use the **write memory EXEC** command in privileged mode.

```
write memory
```

Assign an IP Address to the Switch

Assign an IP to the switch, so that the switch can be managed remotely instead of being restricted to management through a direct connection to the console port.

Although the switch supports multiple IP addresses for switch management, only primary IP address is responsible for switch management.

Two types of IP addresses are used for switch management—in-band and out-of-band.

An in-band IP address is an address assigned to an interface that is reached through the production network. Examples of in-band interfaces that have assigned IP addresses are VLAN, Ethernet, and loopback interfaces.

An out-of-band IP address is an address assigned to an interface that is unreachable through the production network. Out-of-band networks are more common in large network deployments. If you do not have an Out-of-band network, use only an in-band network for management.

On the switch, the out-of-band interface is GigabitEthernet 0/0. The GigabitEthernet 0/0 interface is not connected to the internal switching hardware, but directly to the CPU. IP traffic on GigabitEthernet 0/0 does not use the operating network. If the physical topology of the switch deployment does not support out-of-band, then the switch can be managed with an in-band IP address.

We recommend that the switch be assigned multiple IP addresses for high availability; one IP address on the out-of-band interface, and one on the in-band interface. High availability for switch management ensures that the most available switch on the switch stack is the active switch and that it has a management IP address so that all the stack members are accessible for management. You can have both an in-band and out-of-band IP addresses as long as they are not in the same subnet. The preferred method for management is out-of-band, because it is highly available and less likely to be impacted by DOS and broadcast storms. The GigabitEthernet 0/0 interface on the switch is used for out-of-band management.

Configure the management IP addresses, as described in these sections:

- [Configure a Management IP Address on an Out-of-Band Interface](#)
- [Configure a Management IP Address on an In-Band Interface](#)
- [Create a Management VLAN in Hardware](#)

Configure a Management IP Address on an Out-of-Band Interface

Step 8 Assign an IP address to an out-of-band interface.

```
interface GigabitEthernet 0/0
ip address 192.168.128.5 255.255.255.0
exit
```

Out-of-band management is managing the switch and all other networking devices through a physical network, which is separate from the production network that carries end-user traffic. To manage the switch with an out-of-band network, the switch uses the GigabitEthernet 0/0 interface. The GigabitEthernet0/0 interface is physically located on the rear of the switch, next to the blue console port.

The following are the advantages of a GigabitEthernet 0/0 interface:

- The interface is not susceptible to network outages, such as broadcast storms or other potential issues on the production network because it is separated from the data plane.
- The interface is out-of-band and allows the switch and all other networking devices to always be manageable so that you can quickly respond whenever there is a network issue.

Step 9 Configure a Virtual Routing and Forwarding (VRF) instance.

The out-of-band management interface is in its own VRF instance. This means that the routing database and protocol exchange are also separate for this interface from the other data network interfaces.

The following are the limitations of a GigabitEthernet 0/0 interface.

- Management traffic originating from the switch must be associated with the GigabitEthernet 0/0 VRF instance. A Mgmt-vrf is used to segment management traffic from the global routing table of the switch.
- A default route for the Mgmt-vrf is required.

```
ip default-gateway 192.168.2.1
```

- This interface cannot be used as the source interface for sending SNMP traps. Sending traps to an SNMP trap server requires an IP address on a VLAN interface, see the [“Configure a Management IP Address on an In-Band Interface”](#) section.



Note

Use the IP address value that you listed in the print-out ([Table 3](#)) for the out-of-band management configuration.

In the following example, the GigabitEthernet 0/0 interface is not on the switch data plane. This interface (also referred to as the service port) is terminated on the CPU of the switch as opposed to a logical interface of the forwarding ASIC. The GigabitEthernet 0/0 differs from the Ethernet interfaces on the front of the switch because it is only a Layer 3 interface (also referred to as a routable interface). The Ethernet interfaces on the front of the switch default to Layer 2 mode and are used for bridging.

The Ethernet interfaces on the front can be configured to be a routable interface using the **no switchport** interface command. The GigabitEthernet 0/0 interface will not function without an IP address assigned to it.

Mgmt-vrf is built-in; you do not have to create one for out-of-band management.

```
ip route vrf Mgmt-vrf 192.168.128.5 255.255.255.0 192.168.128.1
exit
```

Step 10 Following is the example for **show ip route vrf** command.

```

show ip route vrf Mgmt-vrf

Routing Table: Mgmt-vrf
C- IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
   ia - IS-IS inter area, * - candidate default, U - per-user static
route
   o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
   + - replicated route, % - next hop override

Gateway of last resort is not set

      192.168.128.5/16 is variably subnetted, 3 subnets, 2 masks
S       192.168.128.5/24 [1/0] via 192.168.128.1
C       192.168.128.5/24 is directly connected, GigabitEthernet0/0
L       192.168.128.2/32 is directly connected, GigabitEthernet0/0

ping vrf Mgmt-vrf 192.168.128.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.128.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
odes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
   D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
   N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
   E1 - OSPF external type 1, E2 - OSPF external type 2
   i

```

Configure a Management IP Address on an In-Band Interface

Step 11 Assign your management IP address to a VLAN interface that is used only for management, and not used to carry other network traffic.

A VLAN interface is a Layer 3 endpoint on the subnet assigned to the corresponding VLAN.



Note Do not use VLAN 1 as the management VLAN for security purposes.

The management VLAN is a separate VLAN for managing the switch and all other network devices in the same subnet. You should assign an in-band IP address to a VLAN interface regardless of whether an IP address is assigned to the out-of-band interface.

With in-band management, the IP address can be reached through the production network. For management purposes, the in-band IP address can be used the same way as the out-of-band IP address. There is no functional difference. However, the in-band IP address has more capabilities because this is the source IP address for some of the auto-generated traffic that comes from the switch, for instance, SNMP traps use the in-band IP address.

You can assign an IP address to your VLAN interface before you configure the VLAN on the switch. The VLAN interface is not operational until the VLAN is created in hardware, and at least one physical interface, which is a member of the VLAN, is in a forwarding state.

This example shows a VLAN created for management and indicates that the IP address is reachable.

```
interface vlan 100
ip address 192.168.1.2 255.255.255.0
no shutdown
exit
```

**Note**

The switch supports IP address assignments to physical Ethernet interfaces that have been configured to operate in Layer 3 mode.

- Step 12** Configure the default gateway, as shown in the following example. This gateway functions as the default route.

When using a VLAN interface, a default route is not required.

```
ip default-gateway 192.168.1.1
```

Create a Management VLAN in Hardware

Earlier you assigned an IP address to the interface for VLAN 100. Refer to the "[Appendix 3, “Configure a Management IP Address on an In-Band Interface”](#) section to assign an IP address to the interface. However, merely assigning the IP address to VLAN 100 does not create the VLAN in hardware. Perform the below step to make the switch reachable through the assigned IP address.

- Step 13** Configure a management VLAN in hardware and configure an uplink interface as a member of this VLAN.

**Note**

This is an intermediate step required only to make the switch Layer 3 reachable and manageable from SSH or HTTPS as well as the console or Express Setup. You can skip this step if you continue to use the console to complete the configuration, but required if you use another tool to complete the configuration of the switch. The complete best-practice configuration for uplink connectivity is explained in the "[Uplink Interface Connectivity](#)" workflow.

We recommend that you use a *dummy* VLAN as the native VLAN on trunk interfaces instead of the default VLAN 1. Because all interfaces are assigned to VLAN 1 by default on the switch, this step limits the traffic associated with potential user configuration and possible connection errors propagating across the trunk.

All other VLANs on the uplink interfaces are tagged with IEEE 802.1q which encapsulates the Layer 2 head of the Frame packet.

The following example shows how to configure VLAN IDs in hardware and assign the names. The upstream interfaces to the switch or router are modified to make them members of the new VLANs. You must have the same VLAN ID on both ends of the Ethernet link to properly configure the management VLAN in hardware. A “dummy” VLAN is used as the native VLAN on trunk interfaces. A *dummy* VLAN is not used for data or management traffic.

**Note**

The Shortest Path Tree (SPT) and **ping** command used in this example require that the upstream layer device (switch or router) to be configured to operate in a production network, and without any additional configuration changes being required.

```
vlan 100
  name switch_mgmt
  exit
vlan 999
  name dummy
  exit
!
! The next step assumes the uplink interface is GigabitEthernet 1/1/1, but
! your uplink interface may be different.
!
interface GigabitEthernet 1/1/1
  Switchport mode trunk
  Switchport trunk native vlan 999
```

```
! Use "show spanning-tree vlan 100" to confirm VLAN 100 FWD on the uplink
! interface.
! Use "show interface trunk" to confirm GigabitEthernet 1/1/1 is
! operating in Trunk mode correctly.
```

show spanning-tree vlan 100

```
VLAN0100
  Spanning tree enabled protocol rstp
  Root ID    Priority    32868
            Address    0022.bdd9.4c00
            Cost      4
            Port      49 (GigabitEthernet1/1/1)
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32868 (priority 32768 sys-id-ext 100)
            Address    20bb.c05f.b300
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time 300 sec
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Gi1/1/1	Root	FWD	4	128.49	P2p
Gi1/1/2	Altn	BLK	4	128.50	P2p

show interfaces trunk

Port	Mode	Encapsulation	Status	Native vlan
Gi1/1/1	on	802.1q	trunking	999
Gi1/1/2	on	802.1q	trunking	999

Port	Vlans allowed on trunk
Gi1/1/1	1-4094
Gi1/1/2	1-4094

Port	Vlans allowed and active in management domain
Gi1/1/1	1,100,999
Gi1/1/2	1,100,999

Port	Vlans in spanning tree forwarding state and not pruned
Gi1/1/1	1,100,999
Gi1/1/2	none

```
!
! Now the default gateway will respond to pings
!
```

```
ping 182.168.1.1
```



Note

Enter the show running-configuration command to display the initial management information for the switch.



Global System Configuration

This workflow describes common global configurations for all switch deployments in the access layer.

Prerequisites for Global System Configuration

- Complete the task described in “[Initial Switch Configuration](#)” workflow.
- If you have not completed the task described in the “[Uplink Interface Connectivity](#)” workflow, the switch might not be IP reachable. If that is the case, use only the switch console to perform the Global System Configuration workflow.

If you have completed the “[Uplink Interface Connectivity](#)” workflow, you can perform the Global System Configuration workflow using the switch console, SSH, or any management tool. Using tools other than the console requires you to log in using user names and passwords configured, as described in the section the “[Initial Switch Configuration](#)” workflow.

Identify Configuration Values

We recommend that you identify certain switch configuration values in advance so that you can proceed with this workflow without interruption. We recommend that you take a print out of Table 4, and, as you follow the configuration sequence, you should replace the values in column B with your values in column C.



Note

Replace the blue italicized example values with your own values.

Table 4 **Global System: Setting Values**

A. Value Name	B. Example Value	C. Your Value
Management subnets allowed	<i>192.168.128.5/0.0.0.255</i> <i>192.168.0.0/0.0.0.255</i> <i>192.168.254.0/0.0.0.255</i>	
NTP server IP address	<i>192.168.254.11</i>	



Table 4 **Global System: Setting Values**

A. Value Name	B. Example Value	C. Your Value
Data VLAN	<i>10</i>	
Voice VLAN	<i>11</i>	
Access points VLAN	<i>12</i>	
Management VLAN ID	<i>100</i>	
Wireless clients VLAN	<i>200</i>	
VLAN name for data	<i>Data</i>	
VLAN name for voice	<i>Voice</i>	
VLAN name for access points	<i>Access_Points</i>	
VLAN name for wireless clients	<i>Wireless_Client</i>	
SNMP community strings for read-only and read-write access	<i>my-SNMP-RO-name,</i> <i>my-SNMP-RW-name</i>	
IPv6 Router Advertisement Guard policy for access interfaces	<i>endhost_ipv6_raguard</i>	
IPv6 Router Advertisement Guard policy for upstream router interfaces	<i>router_ipv6_raguard</i>	
IPv6 Router Advertisement Guard policy for upstream switch interfaces	<i>switch_ipv6_raguard</i>	
IPv6 DHCP guard policy for access interfaces	<i>endhost_ipv6_dhcp_guard</i>	
IPv6 DHCP guard policy for uplink interfaces	<i>uplink_ipv6_dhcp_guard</i>	

**Note**

Configuration examples begin in global configuration mode, unless noted otherwise.

Assign Global Configuration Information

**Note**

The following tasks should be performed in the same sequence in which they are listed here.

- [Configure High Availability on the Switch Stack](#)
- [Configure the Switch to run in VTP Transparent Mode](#)
- [Enable Rapid Per-VLAN Spanning Tree Plus](#)
- [Configure BPDU Guard for Spanning-Tree PortFast Interfaces](#)
- [Configure UDLD to Detect Link Failure](#)

- [Configure an Access List to Limit Switch Access](#)
- [Configure System Clock and Console Timestamps](#)
- [Configure DHCP Snooping Security Features](#)
- [Configure ARP Inspection](#)
- [Configure EtherChannel Load Balancing](#)
- [Create Access Layer VLANs](#)
- [Create IPv6 First-Hop Security Policies](#)
- [Increase the TFTP Block Size](#)
- [Enable New Members to Automatically Update to the Switch Stack Image](#)
-

Configure High Availability on the Switch Stack

Step 1 Assign the active switch and standby switch with high stack-member priority values, so that network operations are not affected during a stack-member failure.

Recommendation: For consistency, configure the stack-member priority used to determine the active stack member. By configuring one member to be the active stack member, you ensure that this member is always the active member through all stack elections, for the lifetime of the stack. The member with the highest configured priority becomes the active member.

In a switch stack, the member most likely to fail is the active member. Therefore, in a switch stack with three or more members, we recommend that you configure uplink connectivity on more than one stack member and do not configure uplink connectivity on the active member. This way, uplink connectivity is not affected if the active member fails.

In this document, the stack refers to a two-member stack, and the example here shows how to assign the highest priority to member 1. Assign a secondary member by giving it a slightly lower priority. The default priority is 1.

```
switch 1 priority 15
switch 2 priority 14
```



Note

For additional information about managing switch stacks and configuring high availability features on the switch, see the [Stack Manager and High Availability Configuration Guide, Cisco IOS XE Release](#).

Configure the Switch to run in VTP Transparent Mode

Step 2 Configure your switch to run in VTP transparent mode in order to avoid the VLAN configuration updates coming from the network, since they have the potential for unexpected behavior due to error operations.

Typically, VLANs are defined once during your initial switch configuration and do not require continuous VTP updates after the switch is operational.

A switch in VTP transparent mode can create, modify, and delete VLANs (the same way as VTP servers), but the switch does not send dynamic propagation of VLAN information across the network and does not synchronize its VLAN configuration based on advertisements received. Configuration changes made when the switch is in this mode are saved in the switch's running configuration, and can be saved to the switch's startup configuration file.

**Note**

The default VTP mode for the switch is VTP server mode. This mode allows you to create, modify, and delete VLANs and specify other configuration parameters for the entire VTP domain. VTP servers advertise their VLAN configuration to other switches in the same VTP domain and synchronize their VLAN configuration with other switches based on advertisements received over trunk links.

```
vtp mode transparent
```

Enable Rapid Per-VLAN Spanning Tree Plus

- Step 3** Enable Rapid Per-VLAN Spanning Tree Plus (PVST+), to improve the detection of indirect failures or linkup restoration events over classic spanning tree.

Rapid PVST+ provides an instance of RSTP (IEEE 802.1w) for each VLAN, and PVST+ improves the detection of indirect failures or linkup restoration events over the classic spanning tree (IEEE 802.1D).

Recommendation: Enable spanning tree even if your deployment is created without any Layer 2 loops. By enabling spanning tree, you ensure that if physical or logical loops are accidentally configured, no actual Layer 2 loops occur.

```
spanning-tree mode rapid-pvst
```

Configure BPDU Guard for Spanning-Tree PortFast Interfaces

- Step 4** Configure the Bridge Protocol Data Unit (BPDU) guard globally to protect all Spanning-Tree PortFast-enabled interfaces.

The BPDU guard protects against a user plugging a switch into an access port, which many cause a catastrophic, undetected spanning-tree loop.

If a Spanning-Tree PortFast-configured interface receives a BPDU, an invalid configuration exists, such as the connection of an unauthorized device. The BPDU Guard feature prevents loops by moving a nontrunking interface into an errdisable state when a BPDU is received on an interface when STPF is enabled.

The BPDU configuration protects STPF-enabled interfaces by disabling the port if another switch is plugged into the port.

This command should be configured globally, not at the interface level.

```
spanning-tree portfast bpduguard default
```

Configure UDLD to Detect Link Failure

- Step 5** Configure Unidirectional Link Detection (UDLD) in aggressive mode, not normal mode.

UDLD detects a unidirectional link, and then disables the affected interface and alerts you. Unidirectional links can cause a variety of problems, including spanning-tree loops, black holes, and nondeterministic forwarding. In addition, UDLD enables faster link-failure detection and quick reconvergence of interface trunks, especially with fiber, which can be susceptible to unidirectional failures.

```
udld aggressive
```

In aggressive mode, if the link state of a port is determined to be bidirectional and the UDLD information times out while the link on the port is still in UP state, UDLD tries to re-establish the state of the port. If this not successful, the port is put into errdisable state. In normal mode, the port state for UDLD is marked as undetermined, and operates according to its Spanning Tree Protocol state.

Do not change UDLD aggressive timers.



Note

UDLD in aggressive mode is not needed when the upstream device is a switch operating in VSS mode.

For more information about VSS-enabled campus design, see the [Campus 3.0 Virtual Switching System Design Guide](#).

Configure an Access List to Limit Switch Access

- Step 6** If your network operation support is centralized, you can increase network security by using an access list to limit the networks that can access your switch.

We recommend that you use an access list to permit IP addresses from known source management locations.

In this example, only the hosts on the 192.168.128.0, 192.168.0.0, and 192.168.254.0 networks can access your switch using SSH or SNMP. The following example shows an ACL that permits three subnets. your network may have more subnets or fewer subnets. configure the ACL that best fits your network. You can continue to add to the list, as required for your network deployment.

```
access-list 55 permit 192.168.128.0 0.0.0.255
access-list 55 permit 192.168.0.0 0.0.0.255
access-list 55 permit 192.168.254.0 0.0.0.255
line vty 0 15
  access-class 55 in vrf-also
  exit
snmp-server community sample-READONLY RO 55
snmp-server community sampe-READWRITE RW 55
!
```

Configure System Clock and Console Timestamps

- Step 7** Configure a synchronized clock by programming your network devices to synchronize to a local NTP server in the network.

The local NTP server typically references a more accurate clock feed from an outside source.

```
ntp server 192.168.0.10
!
clock timezone PST -8
clock summer-time PDT recurring
```

- Step 8** Configure console messages, logs, and debug output to provide timestamps on output, which allows cross-referencing of events in a network.

```
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

Configure DHCP Snooping Security Features

- Step 9** Enable Dynamic Host Configuration Protocol (DHCP) snooping on the data, voice, and wireless AP VLANs.

The switch intercepts and safeguards DHCP messages within the VLAN. This configuration ensures that an unauthorized DHCP server cannot allocate addresses to end-user devices.

```
ip dhcp snooping vlan 10,11,12,100
no ip dhcp snooping information option
ip dhcp snooping
ip dhcp snooping wireless bootp-broadcast enable
```

Configure ARP Inspection

ARP inspection is a security feature that prevents ARP spoofing.

- Step 10** Enable Address Resolution Protocol (ARP) inspection on the data, voice, and management VLANs.

```
ip arp inspection vlan 10,11,100
```

Configure EtherChannel Load Balancing

- Step 11** Set EtherChannels to use the traffic source and destination IP address when calculating which link to send traffic to.

EtherChannel traffic should be balanced across all physical interfaces. The default load-balancing scheme for EtherChannels is based on the source MAC address.

This configuration normalizes the method in which traffic is load-shared across the member links of an EtherChannel. EtherChannels are used extensively in this design because of their resilience.

```
port-channel load-balance src-dst-ip
```

Create Access Layer VLANs

Step 12 Create VLANs to separate traffic based on end-user devices.

When VLANs are created, they automatically join any interface that is configured for trunk mode. Earlier, the uplink interface was configured for trunk mode. Therefore, the uplink interface should now be a member of these VLANs.

Use consistent VLAN IDs and VLAN names in the access layer. Consistent IDs and names help with consistency, and network operation becomes more efficient.

**Note**

Do not use VLAN 1.

**Note**

Use VLAN 200 for wireless clients only if the switch operates as a wireless controller in the converged access mode.

```
vlan 10
  name Data
vlan 11
  name Voice
vlan 12
  name Access_Points
vlan 200
  name Wireless_Client
```

Create IPv6 First-Hop Security Policies

Step 13 Create and apply global IPv6 security policies on the uplink interfaces to define the trust and roles on the connected distribution switches or routers.

Blocking router advertisements with Router Advertisement Guard and DHCP responses from untrusted sources are an easy way to secure against the most common IPv6 problems.

**Note**

Access interfaces to end devices should not be trusted for router advertisements and IPv6 DHCP response.

This example configuration shows how to create global policies that are applied to the interfaces described in the “[Access Control on the Wired Network](#)” workflow.

```

ip6 nd rguard policy endhost_ipv6_rguard
  device-role host
!
ip6 nd rguard policy router_ipv6_rguard
  device-role router
  trusted-port
!
ip6 nd rguard policy switch_ipv6_rguard
  device-role switch
  trusted-port
!
ip6 dhcp guard policy endhost_ipv6_dhcp_guard
  device-role client
!
ip6 dhcp guard policy uplink_ipv6_dhcp_guard
  device-role server
  trusted-port

```

Increase the TFTP Block Size

Step 14 Increase the TFTP block size to the maximum allowed value of 8192.

By default, the switch uses a TFTP block size value of 512, which is the lowest possible value. Increasing this global value significantly improves the TFTP file transfer time.

```
ip tftp blocksize 8192
```

Enable New Members to Automatically Update to the Switch Stack Image

Step 15 Enable the Auto Upgrade feature so that new switch members automatically update to the Cisco IOS version that is running on the switch stack.

When new members join an existing switch stack, the Cisco IOS version of the new members must match the Cisco IOS version of the existing members. The Auto Upgrade feature provides the ability to automatically update new members when they join. However, this feature is not enabled by default.



Note

The switch stack must be running Cisco IOS XE Release 3.3.1 or higher, or later in install mode.

```
software auto-upgrade enable
```

For detailed information about the Auto Upgrade feature, see the [Using the Auto-Upgrade feature on the Cisco Catalyst 3850](#) document.



Uplink Interface Connectivity

This workflow describes how to configure the Ethernet interfaces that connect a switch or switch stack to distribution switches or routers. These interfaces are uplink interfaces. They are different from access interfaces that connect to non-networking end devices such as IP phones, personal computers, wireless access points, printers, and IP cameras.

The switch interface configuration recommendations are based on a switch stack deployed in the campus or branch of the access layer.

When stacking two or more physical switches into one logical switch, we recommend that the uplink interfaces are configured across the physical members to ensure that an active uplink interface always available for switch-stack members.

Prerequisites for Uplink Interface Connectivity

Ensure that the best-practice configurations are set, as described in the [Global System Configuration](#) workflow.

Restrictions for Uplink Interface Connectivity

- A maximum of only eight physical links can be active in a single EtherChannel group.
- All the ports in an EtherChannel must be assigned to the same VLAN, or must be configured as trunk ports.
- All the interfaces in an EtherChannel must be of the same type, for example, Gigabit Ethernet interfaces cannot be mixed with 10-Gbps interfaces.

Identify Configuration Values

We recommend that you identify certain switch configuration values in advance so that you can proceed with this workflow without interruption. We recommend that you take a print out of Table 5, and, as you follow the configuration sequence, replace the values in column B with your values in column C.



**Note**

Replace the blue italicized example values with your own values.

Table 5 *Uplink Connectivity Values*

A. Value Name	B. Example Value Name	C. Your Value
Uplink interfaces	<i>GigabitEthernet 1/1/1</i> <i>GigabitEthernet 1/1/2</i> <i>GigabitEthernet 2/1/1</i> <i>GigabitEthernet 2/1/2</i>	
Data VLAN	<i>10</i>	
Voice VLAN	<i>11</i>	
Access points VLAN	<i>12</i>	
Wireless clients VLAN	<i>200</i>	
Management VLAN ID	<i>100</i>	
Dummy VLAN	<i>999</i>	
IPv6 Router Advertisement Guard policy name	<i>switch_ipv6_raguard</i> <i>router_ipv6_raguard</i>	
IPv6 Router Advertisement Guard policy name	<i>uplink_ipv6__guard</i>	
QoS service policy input name	<i>AutoQos-4.0-Trust-Dscp-Input-Policy</i>	
QoS service policy output name	<i>AutoQos-4.0-Output-Policy</i>	

**Note**

Configuration examples begin in global configuration mode, unless noted otherwise.

LAN Access Switch Topology with Uplinks to a Distribution Switch or Distribution Router

The following illustration displays the LAN Access Switch Topology with Uplinks to a distribution switch or distribution router:

Figure 6 LAN Access Switch Topology with Uplinks to a Distribution Switch

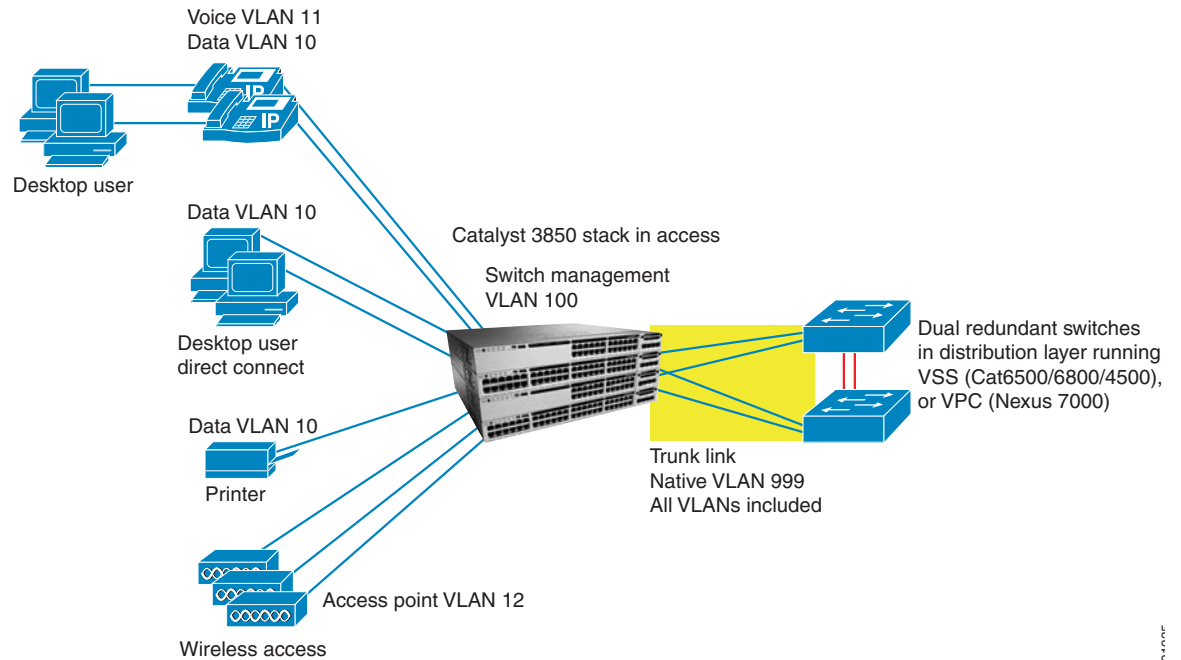
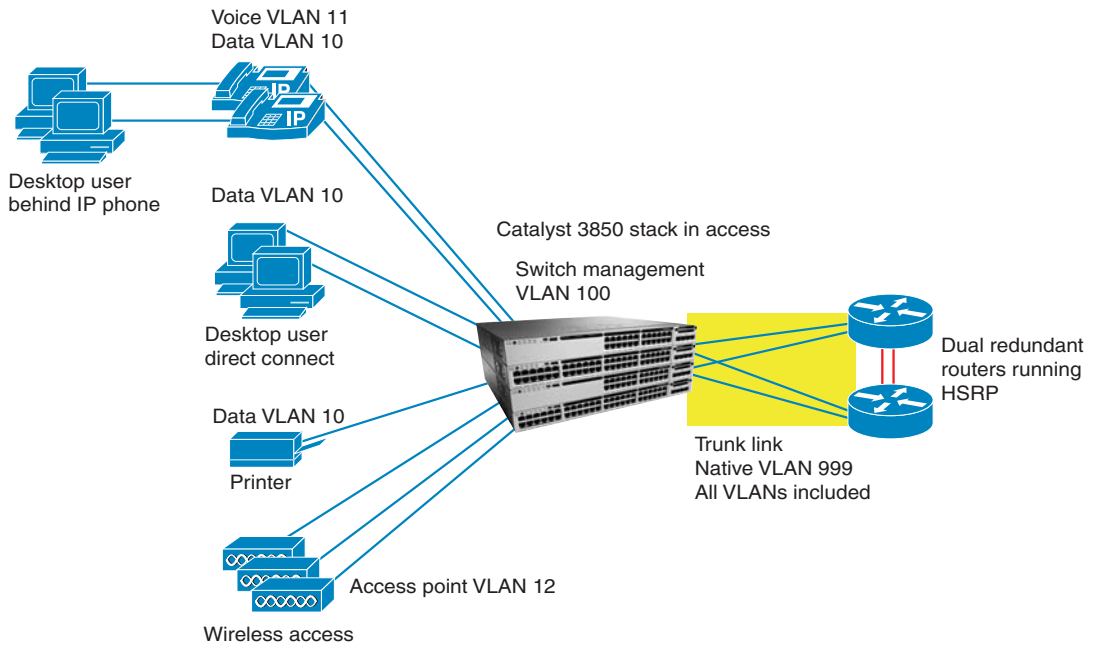


Figure 7 Uplinks for a Distribution Router



991996

Configure Uplink Interface Connectivity

- [Recommendations for Configuring an Uplink Interface to a Router or Switch](#)
- [Configure QoS on an Uplink EtherChannel Interfaces](#)
- [Configure an Uplink Interface as an EtherChannel and as a Trunk](#)
- [Configure Security Features on an Uplink EtherChannel Interface](#)
- [Spanning-Tree Recommendations for an Uplink Interface Connecting to a Distribution Switch](#)
- [Verify Uplink Interface Configurations](#)

Recommendations for Configuring an Uplink Interface to a Router or Switch

When configuring your uplink interface, follow the below recommendations to guide you through the configuration from interface to upstream router or switch:

- Make sure that the uplink connections from the switch stack to the distribution switches have enough bandwidth to carry the traffic associated with all of the access interfaces on the switch stack.
- Use EtherChannels to increase resilience of in case an uplink interface fails.
- For EtherChannels, use Link Aggregation Control Protocol (LACP) active-active mode, which adheres to the IEEE 802.3ad standard. The active-active mode implies that both the switch stack as well as the distribution switch side of the EtherChannel must be configured in LACP active mode.
- Use uplink ports on the different switches in the switch stack to connect back to the distribution switches. This configuration ensures that there is no single source of failure for the switch stack. If a switch in the stack owning one of the uplink connections fails, there will still be an uplink port connection from a remaining member of the switch stack connecting back to the distribution switches.
- All the interfaces are assigned to VLAN 1 by default. Do not configure VLAN 1 on the trunk; this is to prevent traffic associated with potential user connection errors from propagating across the trunk.

Configure QoS on an Uplink EtherChannel Interfaces

**Note**

This configuration should be applied to the physical uplink interfaces before adding them to an EtherChannel.

Step 1

Apply the Trust Differentiated Services Code Point (DSCP) service policy on an interface in the ingress direction, and then apply the 2P6Q3T policy in order to ensure proper congestion management and egress bandwidth distribution on the interface in the egress direction.

Ethernet traffic that is received from the upstream switch or router contains trusted QoS markings and is classified to guarantee a type of service.

Additional service policies should be applied after traffic is transmitted in order to ease congestion. For more information see, [“Configure QoS on an Access Interface” on page 56](#)

```

interface GigabitEthernet 1/1/1
  auto qos trust dscp
  service-policy input AutoQos-4.0-Trust-Dscp-input-Policy
  service-policy output 2P6Q3T
  exit

interface GigabitEthernet 1/1/2
  auto qos trust dscp
  service-policy input AutoQos-4.0-Trust-Dscp-input-Policy
  service-policy output 2P6Q3T
  exit

interface GigabitEthernet 2/1/1
  auto qos trust dscp
  service-policy input AutoQos-4.0-Trust-Dscp-input-Policy
  service-policy output 2P6Q3T
  exit

interface GigabitEthernet 2/1/2
  auto qos trust dscp
  service-policy input AutoQos-4.0-Trust-Dscp-input-Policy
  service-policy output 2P6Q3T

```

Configure an Uplink Interface as an EtherChannel and as a Trunk

- Step 1** Choose one of the following configurations based on your network topology:
- [“Configure an Uplink Interface to Connect to a Distribution VSS or VPC Switch”](#)
 - [“Configure an Uplink Interface to Connect to a Distribution Router \(or Standalone Distribution Switch\)”](#)

Configure an Uplink Interface to Connect to a Distribution VSS or VPC Switch

1. Ensure that the distribution Virtual Switch System (VSS) or Virtual Port Channel (VPC) switch connections are configured the same way and that the EtherChannel is configured in LACP active mode.
2. For additional resilience, ensure that the uplink interfaces are located on different switches in the switch stack.

[Figure 6](#), shows the switch stack that has a single EtherChannel connection to a distribution VSS or VPC switch pair.

The VSS and VPC systems have an explicit configuration between the Cisco distribution switch pair. That allows them to act as a single logical switch when connected to the EtherChannel. The EtherChannel is configured as a trunk with VLANs 10, 11, 12, and 100, with the native VLAN set to 999.



Note

Use this switch-stack uplink interface configuration only when connecting the switch stack to a VSS or VPC distribution switch pair, and not when the distribution switch pair is configured as two standalone switches.

```
interface GigabitEthernet 1/1/1
  description connection to Distribution VSS or VPC switch 1
  switchport mode trunk
  switchport trunk native vlan 999
  switchport trunk allowed vlan 10,11,12,100,200
  channel-protocol lacp
  channel-group 1 mode active
!
interface GigabitEthernet 2/1/1
  description connection to Distribution VSS or VPC switch 1
  switchport mode trunk
  switchport trunk native vlan 999
  switchport trunk allowed vlan 10,11,12,100,200
  channel-protocol lacp
  channel-group 1 mode active
!
interface GigabitEthernet 1/1/2
  description connection to Distribution VSS or VPC switch 2
  switchport mode trunk
  switchport trunk native vlan 999
  switchport trunk allowed vlan 10,11,12,100,200
  channel-protocol lacp
  channel-group 1 mode active
!
interface GigabitEthernet 2/1/2
  description connection to Distribution VSS or VPC switch 2
  switchport mode trunk
  switchport trunk native vlan 999
  switchport trunk allowed vlan 10,11,12,100,200
  channel-protocol lacp
  channel-group 1 mode active
```

Configure an Uplink Interface to Connect to a Distribution Router (or Standalone Distribution Switch)



Note

Use this configuration when connecting the switch stack to two standalone distribution switches (not configured as a VSS or VPC pair). However, do not use the **spanning-tree portfast trunk** command for switch configuration.

- Ensure that the distribution VSS or VPC router side of the connections are configured the same and that the EtherChannel is configured with the LACP active mode.
- For additional resilience, the configured uplink interfaces should be located on different switches in the switch stack.
- Use the **spanning-tree portfast trunk** command to allow the switch side of the uplink to immediately transition to a spanning-tree forwarding state when the link becomes available, because routers do not participate in a spanning tree.

Figure 7 shows a switch stack having a separate EtherChannel to each distribution router. Each EtherChannel is configured as a trunk with VLANs 10, 11, 12, 100, 200, and 999, with the native VLAN set to 999.

EtherChannel Connection to Router 1

```

interface GigabitEthernet 1/1/1
  description connection to Distribution router 1
  switchport mode trunk
  switchport trunk native vlan 999
  switchport trunk allowed vlan 10,11,12,100,200
  spanning-tree portfast trunk
  channel-protocol lacp
  channel-group 1 mode active
interface GigabitEthernet 2/1/1
  description connection to Distribution router 1
  switchport mode trunk
  switchport trunk native vlan 999
  switchport trunk allowed vlan 10,11,12,100,200
  spanning-tree portfast trunk
  channel-protocol lacp
  channel-group 1 mode active

```

EtherChannel Connection to Router 2

```

interface GigabitEthernet 1/1/2
  description connection to Distribution router 2
  switchport mode trunk
  switchport trunk native vlan 999
  switchport trunk allowed vlan 10,11,12,100,200
  spanning-tree portfast trunk
  channel-protocol lacp
  channel-group 2 mode active
interface GigabitEthernet 2/1/2
  description connection to Distribution router 2
  switchport mode trunk
  switchport trunk native vlan 999
  switchport trunk allowed vlan 10,11,12,100,200
  spanning-tree portfast trunk
  channel-protocol lacp
  channel-group 2 mode active

```

Configure Security Features on an Uplink EtherChannel Interface

Step 2 Configure IPv4 and IPv6 security features on uplink EtherChannel interfaces.

The uplink EtherChannel interfaces to distribution routers and switches should be configured to trust router advertisements and IP response, because Layer 3 routing and server functionality resides on the distribution switches and routers. This step is different from the access interface-to-end device configuration, which should not be trusted, as specified in the [“Access Interface Connectivity”](#) workflow.

The policies that should be applied are defined in the [“Global System Configuration”](#) workflow.

In the following example, security is applied to the uplink interfaces connecting to VPC, VSS, or standalone switch.


```
interface Port-channel 1
 ip arp inspection trust
 ip snooping trust
 ipv6 nd raguard attach-policy switch_ipv6_raguard
 ipv6 guard attach-policy uplink_ipv6_guard
```

In the following example, security is applied to the uplink interfaces connecting to routers:

```
interface Port-channel 1
 ip arp inspection trust
 ip snooping trust
 ipv6 nd raguard attach-policy router_ipv6_raguard
 ipv6 guard attach-policy uplink_ipv6_guard
 exit
!
interface Port-channel 2
 ip arp inspection trust
 ip snooping trust
 ipv6 nd raguard attach-policy router_ipv6_raguard
 ipv6 guard attach-policy uplink_ipv6_guard
```

Spanning-Tree Recommendations for an Uplink Interface Connecting to a Distribution Switch



Note

Complete this configuration on the distribution switches and not on the switch. The recommendations listed below are not applicable when routers are used at the distribution layer.

Step 3

On uplink interfaces to distribution switches (Figure 6), ensure that the spanning-tree root for the switch-stack VLANs is configured on the distribution switch pair.

Follow the below recommendations when the standalone distribution switches are used instead of a VSS or VPC system:

- Make sure that the spanning-tree roots for the VLANs are distributed evenly between two standalone distribution switches. For example, configure one switch as the spanning-tree root for all the even VLANs, and configure the other switch as the spanning-tree root for all the odd VLANs. This distribution configuration ensures that the spanning tree does not block all the VLANs on a single uplink interface, and results in an even traffic flow on the uplink interfaces.
- If Hot Standby Router Protocol (HSRP) or Virtual Router Redundancy Protocol (VRRP) is configured for the VLANs located on the standalone distribution switches, make sure that the VLAN configuration on the active switch is the same on the switch that is the spanning-tree root for that VLAN.
- Avoid flooding of traffic caused by asymmetric routing of traffic flows, by configuring the **arp timeout** interface configuration command. This command adjusts the ARP aging timer to less than the MAC address table aging timer on the Layer 3 VLAN interfaces of the distribution switches. By default, the MAC address table aging timer is set to 5 minutes (300 seconds) on the switch.

For more information about spanning tree root configuration on the VSS, see the “Spanning Tree Configuration Best Practice with VSS” section of the *VSS Enabled Campus Design Guide*.

For more information about spanning-tree root on distribution switches, see the “Spanning VLANs across Access Layer Switches” section of the *Campus Network for High Availability Design Guide*.

For more information about spanning-tree root configuration and asymmetric routing, see the “Spanning VLANs Across Access Layer Switches” and “Asymmetric Routing and Unicast Flooding” sections of the *Campus Network for High Availability Design Guide*.

Verify Uplink Interface Configurations

Use the following commands to verify if configurations in this workflow are correctly applied to your uplink interfaces:

- **show etherchannel summary**
- **show interface**
- **show interface trunk**
- **show cdp neighbors**
- **show auto qos interface**
- **show policy-map interface**

Display Uplink Interface Connectivity for the Switch

Step 1 Enter the **show running-configuration** command to display uplink interface connectivity for the switch.

```
Switch#sh int te2/1/3
TenGigabitEthernet2/1/3 is up, line protocol is up (connected)
  Hardware is Ten Gigabit Ethernet, address is 381c.1a24.d537 (bia
381c.1a24.d537)
  MTU 1500 bytes, BW 10000000 Kbit/sec, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not set
  Full-duplex, 10Gb/s, link type is auto, media type is SFP-10GBase-SR
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:19, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 1000 bits/sec, 1 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    2596461 packets input, 426179392 bytes, 0 no buffer
    Received 2596461 broadcasts (2596461 multicasts)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 2596461 multicast, 0 pause input
    0 input packets with dribble condition detected
  303459 packets output, 45794121 bytes, 0 underruns
    0 output errors, 0 collisions, 2 interface resets
    0 unknown protocol drops
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier, 0 pause output
    0 output buffer failures, 0 output buffers swapped out
```


■ Display Uplink Interface Connectivity for the Switch



Access Interface Connectivity

This workflow describes how to configure the Ethernet interfaces that connect to the end devices of a switch. End devices are the non-networking devices that connect to the network, such as IP phones, personal computers, wireless access points, printers, and IP cameras. The Ethernet interfaces that connect to end devices are referred to as access interfaces. They differ from uplink interfaces that link to other networking devices.

The workflow for configuring access interfaces is based on a switch deployed at the access layer in a campus or branch network ([Figure 8](#)). The switch interfaces connected to end devices are the edge of the network, which network security and QoS begins.

Prerequisites for Access Interface Connectivity

- Complete the procedure described in the [Global System Configuration](#) workflow, which includes the necessary configurations for the access interface configuration.
- Complete the procedure described in the [“Configure QoS on an Uplink EtherChannel Interfaces”](#) workflow, which includes the creation of input services policies for end devices.

Identify Configuration Values

We recommend that you identify certain switch configuration values in advance so that can proceed with this section without interruption. We also recommend that you take a print out of [Table 6](#), and, as you follow the configuration sequence, replace the values in column B with your values in column C.



Note

Replace the blue italicized example values with your own values.



Table 6 Access Interface Connectivity Values

A. Value Name	B. Example Value Name	C. Your Value
Access interface ranges	<i>interface range GigabitEthernet1/0/1-48 interface range GigabitEthernet2/0/1-48</i>	
Data VLAN	<i>10</i>	
Voice VLAN	<i>11</i>	
Access Points VLAN	<i>12</i>	
Management VLAN ID	<i>100</i>	
Wireless Clients VLAN	<i>200</i>	
IPv6 Router Advertisement Guard policy name	<i>endhost_ipv6_raguard</i>	
IPv6 Router Advertisement Guard policy name	<i>endhost_ipv6__guard</i>	
QoS service policy input names (See the “Configure QoS on an Uplink EtherChannel Interfaces” section.)	<i>IPPhone-Input-Policy Classify-Police-Input-Policy Classify-Police-Input-Policy Trust-Dscp-Input-Policy SoftPhone-Input-Policy Trust-Dscp-Input-Policy Trust-Dscp-Input-Policy Trust-COS-Input-Policy No-Trust-Input-Policy</i>	
QoS service policy output name	<i>2P6Q3T</i>	

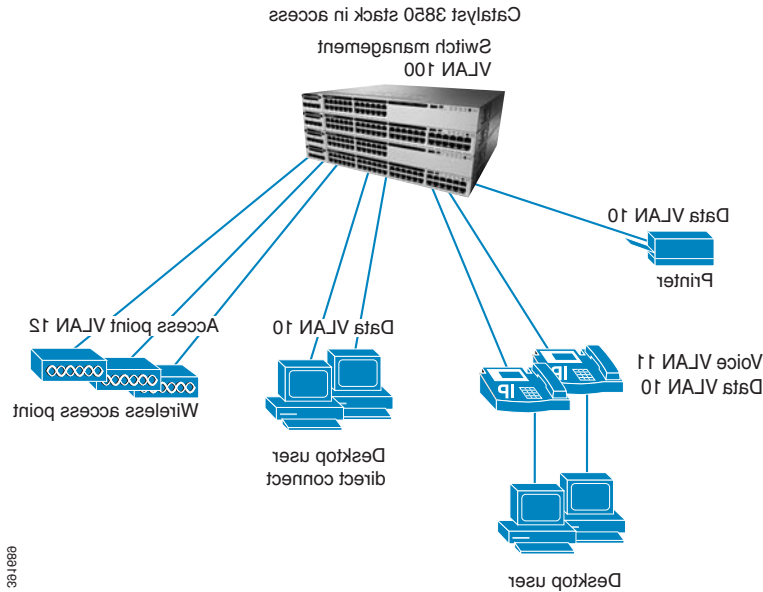
**Note**

Configuration examples begin in global configuration mode, unless noted otherwise.

LAN Access Switch Topology with Connections to End Devices

The following illustration shows the topology of LAN Access Switch to end devices:

Figure 8 LAN Access Switch Topology with Connections to End Devices



Configure Access Interface Connectivity

- [Recommendations for Configuring an Access Interface](#)
- [Configure an Interface for Access Mode](#)
- [Configure VLAN Membership](#)
- [Create an Interface Description](#)
- [Configure Security Features on an Access Interfaces](#)
- [Configure QoS on an Access Interface](#)
- [Verify Access Interface Configurations](#)

Recommendations for Configuring an Access Interface

Although some end devices do not require the following access interface configurations, we recommend that you perform them to ensure consistency. The configurations do not interfere with the operation of the network or the attached end device, and is considered safe to use.

When configuring your access interface, you should complete the following tasks:

- [Configure an Interface for Access Mode](#)
- [Configure VLAN Membership](#)
- [Create an Interface Description](#)

- [Configure Security Features on an Access Interfaces](#)
- [Configure QoS on an Access Interface](#)
- [Verify Access Interface Configurations](#)

IP Device Tracking



Caution

The IP Device Tracking (IPDT) feature could have some negative side effects that may impact the normal day-to-day operation of your switch.



Note

Symptoms as a result of IPDT issues are seen on the end device. For instance on Windows PC, an error message report for a duplicate IP Address 0.0.0.0 appears.

IPDT is enabled globally, but it cannot be globally disabled. To disable IPDT, you must disable it at the interface level.



Note

To disable IPDT on a port channel, you must first unbundle the physical Ethernet interfaces from the port channel.

We recommend that you disable IPDT on all access interfaces except under these situations where a feature explicitly has IPDT enabled:

- IPDT is required for Centralized Web Authentication with Identity Services Engine (ISE).
- Network Mobility Services communicates with the Mobility Services Engine to track location.
- Device Sensor watches the control packets that ingress from the attached end device and determine what type of device is attached. Device Sensor uses multiple sources (such as IPDT) to determine the device type. Device Sensor is critical to other features, such as Auto Smart Ports, and AutoConf.
- Auto Smart Ports and AutoConf are indirectly affected, because they are clients of Device Sensor. The Device Sensor feature uses IPDT to aid in detection of attached device types.
- Address Resolution Protocol (ARP) snooping will be impacted if IPDT is disabled.

Recommended ways to disable IPDT at the interface levels:

```
interface GigabitEthernet1/0/1
  nmsp attach suppress
```

Alternately, you can use the following method:

```
interface GigabitEthernet1/0/1
  ip device tracking maximum 0
```

Configure an Interface for Access Mode

- Step 1** Use the **switchport host** command to perform the following configurations for the end devices on your switch:

- Configure the access interface for static access mode, which is single VLAN mode with no negotiation.
- Configure the interface for Spanning Tree PortFast (STPF), which shortens the time it takes for the interface to go into forwarding mode. We recommend STPF on interfaces that do not connect to other bridging devices (Ethernet switches).

The default Administrative mode for Ethernet interfaces on a switch is dynamic auto. Dynamic mode means the interface will negotiate to trunk mode if the networking device on the side of the link initiates the negotiation to trunk (administrative mode “dynamic desirable”).

Configure VLAN Membership

Step 2 Configure the VLANs for voice and data traffic.

VLAN configuration on an interface is dependent on the end device being used:

- IP phones, IP cameras, and access points are typically configured on separate VLANs.
- VLANs 10 and 11 are defined as the data and voice VLANs, respectively.

Recommendation: Do not use VLAN 1 for data or voice. VLAN 1 is the default VLAN on the 3850. This is well documented and understood by experienced networking personnel. Thus VLAN 1 will be more susceptible to attacks. Changing the VLAN IDs to something other than VLAN1 has been a long standing Cisco recommendation for Ethernet switching

```
switchport access vlan 10
switchport voice vlan 11
```

Create an Interface Description

Step 3 Create a description for the interface to identify the end-device type.



Tip

When you create an interface description, you can quickly scan a long list of interfaces to learn how they are used in your network.

```
description IP Phone
```

Configure Security Features on an Access Interfaces

Step 4 Enable port security features to protect the network from malicious or troublesome end devices.

The primary purpose of port security is to prevent an end device from overloading the switch with too many source MAC addresses. Port security controls the MAC addresses remembered from the attached network device. Port security controls how many MAC addresses are remembered, how long they are remembered, and what happens when too many are remembered.

The MAC address limit is 11. When the end device exceeds 11 source MAC addresses, the ingress traffic to the switch on those source MAC addresses is dropped.

```

switchport port-security maximum 11
switchport port-security
switchport port-security aging time 2
switchport port-security aging type inactivity
switchport port-security violation restrict

```



Note MAC addresses that are remembered on interfaces with port security do not appear in the dynamic MAC address table; they appear in the static MAC address table.

Step 5 Configure IP ARP inspection and (DHCP, IGMP, and so on) snooping to 100 p/s on the interface. (Incoming ARP packets exceeding 100 p/s is not typical and is considered malicious. Those packets are dropped and a syslog message is raised).

```

ip arp inspection limit rate 100
ip snooping limit rate 100

```

Step 6 Configure IP source guard to prevent IP address spoofing on the interface.

```

ip verify source

```

Step 7 Enable storm control on broadcast and multicast packets on the interface to protect the network from a flood of broadcast or multicast packets.

```

storm-control broadcast level pps 1k
storm-control multicast level pps 2k
storm-control action trap
switchport block unicast

```

When the configured levels are exceeded, the switch sends an SNMP trap. The interfaces are not put into a disabled state.

Unicast packets are blocked on egress and not ingress traffic. The switch drops unknown unicast packets from being egressed to the end device, ensuring that only the packets intended for the end device are forwarded.

Step 8 Configure IPv6 security on the interface to secure the end devices from malicious or unexpected operation by preventing them from transmitting IPv6 router advertisements, and IPv6 responses. The applied policies are defined in the “[Global System Configuration](#)” workflow.

```

ipv6 nd rguard attach-policy endhost_ipv6_rguard
ipv6 guard attach-policy endhost_ipv6__guard

```

Configure QoS on an Access Interface

Quality of Service (QoS) provides preferential treatment to certain types of traffic at the expense of others. Without QoS, the switch offers best-effort service to each packet, regardless of the packet contents or size. It sends the packets without any assurance of reliability, delay bounds, or throughput.

AutQoS on the switch generates multiple service policies for various end devices. The service policy that is generated depends with the end device type.

Step 9 Apply service policies to a single access interface.

The switch then automatically generates the modular QoS command-line interface (MQC) service policies needed for access.

This example identifies some of the service policy configurations.

```
auto qos voip cisco-phone  
service-policy input AutoQos-4.0-CiscoPhone-Input-Policy  
service-policy output 2P6Q3T
```

Step 10 Apply ingress and egress service policies.

Check the end device-specific configuration to see which service policy is recommended for an end device.

Verify Access Interface Configurations

The following section describes the commands that you should use to use to confirm that your configurations in this workflow are correctly applied to your switch:

Step 11 Use the **show running-configuration** command to verify the operational configuration of the access interfaces.

Use the **show ip verify source** command to confirm that the IP source guard is configured and working.

```

show ip verify source
Interface  Filter-type  Filter-mode  IP-address  Mac-address  Vlan
-----
Gi1/0/1   ip           active       deny-all   -----
Gi1/0/2   ip           active       deny-all   10-11
Gi1/0/3   ip           active       deny-all   10
Gi1/0/4   ip           active       deny-all   12
Gi1/0/4   ip           active       deny-all   10

```

Use the **show port-security** command to confirm that access interfaces are configured for port security.

```

show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
              (Count)          (Count)          (Count)
-----
Gi1/0/1      11              1              0                  Restrict
Gi1/0/2      11              1              0                  Restrict
Gi1/0/3      11              1              0                  Restrict
Gi1/0/4      11              1              0                  Restrict
-----
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 4096

```

Use the **show ip arp inspection interfaces** command to confirm the rate and untrusted state of access interfaces.

```

show ip arp inspection interfaces
Interface      Trust State      Rate (pps)      Burst Interval
-----
Gi1/0/1        Untrusted        100              1
Gi1/0/2        Untrusted        100              1
Gi1/0/3        Untrusted        100              1
Gi1/0/4        Untrusted        100              1

```

Use the **show ipv6 nd raguard policy** command to confirm that access interfaces are configured for Router Advertisement Guard with specific policies.

```

show ipv6 nd raguard policy endhost_ipv6_raguard
Policy endhost_ipv6_raguard configuration:
  device-role host
Policy endhost_ipv6_raguard is applied on the following targets:
Target      Type  Policy          Feature      Target range
Gi1/0/1     PORT endhost_ipv6_raguard RA guard     vlan all
Gi1/0/2     PORT endhost_ipv6_raguard RA guard     vlan all
Gi1/0/3     PORT endhost_ipv6_raguard RA guard     vlan all
Gi1/0/4     PORT endhost_ipv6_raguard RA guard     vlan all

```

Use the **show ipv6 guard policy** command to confirm the guard on access interfaces.

```
show ipv6 guard policy endhost_ipv6__guard
guard policy: endhost_ipv6__guard
Device Role: client
Target: Gi1/0/1 Gi1/0/2 Gi1/0/3 Gi1/0/4
```

Use the **show policy-map interface** command to confirm the input and output service policies applied to access interfaces.

```
show policy-map interface GigabitEthernet1/0/1
GigabitEthernet1/0/1

Service-policy input: AutoQos-4.0-CiscoPhone-Input-Policy
<snip>
Service-policy output: AutoQos-4.0-Output-Policy
```

Display Running Configuration for Access Interface Connectivity

Step 1 Show the recommended configuration for each end device type described in the beginning of this workflow.



Tip

To use the same interface configuration for multiple interfaces on the switch, use the **interface range** command. This command allows you to issue a command once and have it apply to many interfaces. Because most of the interfaces in the access layer are configured identically, using this command can save a lot of time. For example, the following command allows you to enter commands simultaneously on all 48 interfaces (GigabitEthernet 1/0/1 to GigabitEthernet 1/0/48).

```
interface range GigabitEthernet 1/0/1-1/0/48
```



Note

Apply the **interface range** command to every switch stack member. This range command will work for all interfaces on a single switch member. Enter the range command for each member.

IP Phone Access Interface

The following example displays the IP phone Access Interface information:

show running-configuration

```
.  
. .  
.  
  
Description IP Phone  
switchport host  
switchport access vlan 10  
switchport voice vlan 11  
switchport port-security maximum 11  
switchport port-security  
switchport port-security aging time 2  
switchport port-security aging type inactivity  
switchport port-security violation restrict  
ip arp inspection limit rate 100  
ip snooping limit rate 100  
ip verify source  
switchport block unicast  
storm-control broadcast level pps 1k  
storm-control multicast level pps 2k  
storm-control action trap  
ipv6 nd raguard attach-policy endhost_ipv6_raguard  
ipv6 guard attach-policy endhost_ipv6__guard  
auto qos voip cisco-phone  
service-policy input AutoQos-4.0-CiscoPhone-Input-Policy  
service-policy output 2P6Q3T
```

Personal Computer Access Interface

The following example displays the Personal Computer access interface information.

```

show running-configuration
.
.
.
Description Personal Computer
switchport host
switchport access vlan 10
switchport port-security maximum 11
switchport port-security
switchport port-security aging time 2
switchport port-security aging type inactivity
switchport port-security violation restrict
ip arp inspection limit rate 100
ip snooping limit rate 100
ip verify source
switchport block unicast
storm-control broadcast level pps 1k
storm-control multicast level pps 2k
storm-control action trap
ipv6 nd raguard attach-policy endhost_ipv6_raguard
ipv6 guard attach-policy endhost_ipv6__guard
auto qos trust dscp
service-policy input AutoQos-4.0-Classify-Input-Policy
service-policy output 2P6Q3T

```

Lightweight Access Point Access Interface

The following example displays the Lightweight Access Point Access interface information:

```

show running-configuration
.
.
.
Description Lightweight Access Point
switchport host
switchport access vlan 12
switchport port-security maximum 11
switchport port-security
switchport port-security aging time 2
switchport port-security aging type inactivity
switchport port-security violation restrict
ip snooping limit rate 100
switchport block unicast
storm-control broadcast level pps 1k
storm-control multicast level pps 2k
storm-control action trap

```

Printer Access Interface

The following example displays the Printer Access Interface information.


```
show running-configuration
.
.
.
Description Printer
switchport host
switchport access vlan 10
switchport port-security maximum 11
switchport port-security
switchport port-security aging time 2
switchport port-security aging type inactivity
switchport port-security violation restrict
ip arp inspection limit rate 100
ip snoopig limit rate 100
ip verify source
switchport block unicast
storm-control broadcast level pps 1k
storm-control multicast level pps 2k
storm-control action trap
ipv6 nd rguard attach-policy endhost_ipv6_rguard
ipv6 guard attach-policy endhost_ipv6__guard
auto qos classify police
service-policy input AutoQos-4.0-Classify-Police-Input-Policy
service-policy output 2P6Q3T
```




Access Control on the Wired Network

This workflow describes a phased approach to deploy IEEE 802.1x port-based authentication to provide secure and identity-based access control at the edge of the switch stack network.

Prerequisites for Access Control on the Wired Network

- Before globally enabling IEEE 802.1x authentication, remove the EtherChannel configuration from all of the interfaces.
- Define the authenticator (switch) to RADIUS server communication.
- Initiate Extensible Authentication Protocol (EAP) over LAN (EAPoL) messaging to successfully authenticate the end device (or supplicant).
- Based on your requirements, choose an appropriate EAP method. For information, see the [Wired 802.1x Deployment Guide](#).
- Automate the certificate enrollment process for supplicants, as described in the [Certificate Autoenrollment in Windows Server 2003](#).
- Enable machine authentication for end points, such as printers, to ensure that user login is supported.

Restrictions for Access Control on the Wired Network

- You cannot configure an IEEE 802.1x port that is a member of an EtherChannel.
- Destination ports configured with Switched Port Analyzer (SPAN) and remote SPAN (RSPAN) cannot be enabled with IEEE 802.1x authentication.
- You cannot enable an IEEE 802.1x port on trunk or dynamic ports. Dynamic ports can negotiate with its neighbors to become a trunk.
- Do not use port security with IEEE 802.1x. When IEEE 802.1x is enabled, port security then becomes redundant and might interfere with the IEEE 802.1x functionality.

Identify Configuration Values



We recommend that you identify certain switch configuration values in advance so that you can proceed without interruption. We recommend that you take a print out of Table 7, and, as you follow the configuration sequence, replace the values in column B with your values in column C.



Note Depending on your authentication server settings, the authentication and accounting ports could be assigned the values 1812 and 1813 respectively.



Note Replace the blue italicized example values with your own values.

Table 7 *Secure Access Control for Wired Network Values*

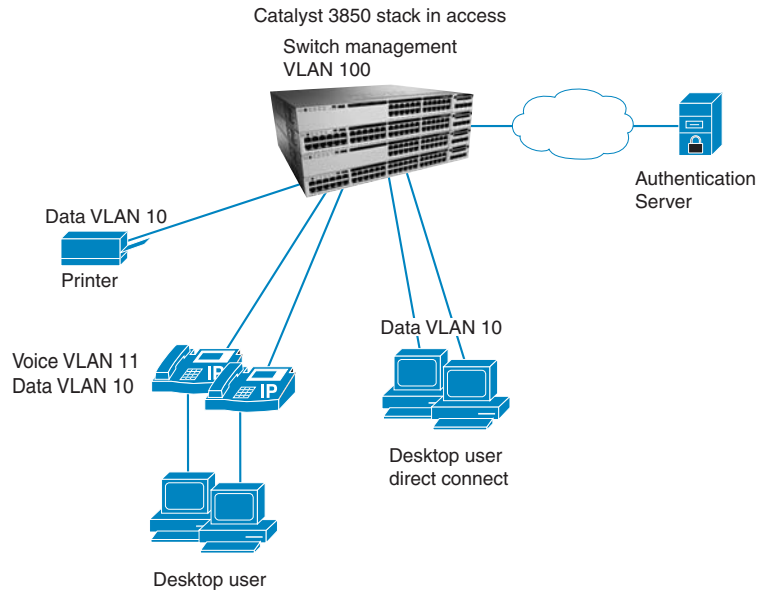
A. Value Name	B. Example Value Names	C. Your Value
Interface range	<i>GigabitEthernet 1/0/1-1/0/24</i>	
RADIUS server	<i>AuthServer</i>	
RADIUS server IPv4 address	<i>192.168.254.14</i>	
Auth-port	<i>1656</i>	
Acct-port	<i>1646</i>	
RADIUS server encryption key	<i>cisco123</i>	
Data VLAN	<i>10</i>	
Voice VLAN	<i>11</i>	
Auth-server dead vlan	<i>20</i>	
Extended IP ACL	<i>LowImpactSecurity-acl</i>	



Note Configuration examples begin in global configuration mode, unless noted otherwise.

LAN Access Switch Topology with IEEE 802.1x Secure Access Control

Figure 9 LAN Access Switch Topology with IEEE 802.1x Secure Access Control



391703

Securing Access Using 802.1x on a wired LAN

The following tasks are to be performed in the same order that is listed here.

- [Recommendations for Configuring Security on a Wired LAN](#)
- [Provision Common Wired Security Access](#)
- [Provision in Monitor Mode](#)
- [Provision in Low-Impact Mode](#)
- [Provision in High-Impact Mode](#)
-

Recommendations for Configuring Security on a Wired LAN

IEEE 802.1x permits or denies network connectivity based on the identity of users and devices. It provides a link between the user name and IP address, MAC address, and a port on a switch. It also provides customized network access based on the identity of the end device or user.

The main components of IEEE 802.1x are:

- Supplicant (end device)
- Authenticator (switch)
- Authentication server (RADIUS or ISE)

To provide secure access to your wired switch network, we recommend that you first provision your common wired security features. Provision security modes in phased deployments (monitor mode to high-security mode) of IEEE 802.1x authentication along with MAC Authentication Bypass (MAB), which uses the MAC address of the end device (or supplicant) to make decisions about access.

**Note**

Each phased deployment should occur over time after ensuring that your network is ready to transition to the next security mode.

Table 8 describes the recommended IEEE 802.1x deployment scenarios that will have limited impact on network access. Test your network infrastructure while in monitor mode. If you are satisfied, then transition to low-impact mode and allow a subset of network traffic to pass through. Finally, transition to high-security mode, requiring authorization from all end devices.

Table 8 IEEE 802.1x Deployment Modes

Monitor Mode	Low-Impact Mode	High-Security Mode (Closed)
<ul style="list-style-type: none"> Open access for unauthorized supplicants. Extensive network visibility. Monitor the network. No impact to end devices. 	<ul style="list-style-type: none"> Limited access for unauthorized supplicants. Differentiated access control using dynamic ACLs. Limited impact to end devices. 	<ul style="list-style-type: none"> No access for unauthorized supplicants. Heavily impacts supplicants.

Reference

For detailed information about wired mode deployments, see the [TrustSec Phased Deployment Configuration Guide](#).

For basic information about IEEE 802.1x protocols, see the “8021X Protocols” section of the [Wired 802.1X Deployment Guide](#).

Provision Common Wired Security Access

IEEE 802.1x port host modes determine whether more than one client can be authenticated on the port and how authentications is enforced:

Table 9 Types of IEEE 802.1x Port Host Modes

Single-Host	Multi-Host	Multi-Domain	Multi-Authentication
Allows only one end device to the IEEE 802.1x enabled switch port.	Authenticates the first MAC address and then allows an unlimited number of other MAC addresses.	Allows two endpoints on the port: one data endpoint and one voice endpoint.	Allows only one voice end device, but allows multiple data end devices. In this mode, all devices are authenticated.

Unless otherwise noted, we recommend that multiple-authentication mode be configured instead of single-host mode, for increased security:

- Multi-authentication mode authenticates all the devices that gain access to the network through a single switch port, such as devices connected through IP phones.
- Multi-authentication mode is more secure than multi-host mode (which also allows multiple data devices) because it authenticates all the devices that try to gain access to the network.

Step 1 Run the **show run** command on your switch to ensure that your access interface connections are set up.

This output is what you inherit after performing the “[Access Interface Connectivity](#)” workflow configuration for an interface connected to an IP phone.

```
Switch#show running-config int Te3/0/12
Building configuration...

Current configuration : 766 bytes
!
interface TenGigabitEthernet3/0/12
switchport mode access
switchport block unicast
switchport voice vlan 2
switchport port-security maximum 3
switchport port-security maximum 2 vlan access
switchport port-security violation restrict
switchport port-security aging time 1
switchport port-security aging type inactivity
switchport port-security
load-interval 30
trust device cisco-phone
storm-control broadcast level pps 1k
storm-control multicast level pps 2k
storm-control action trap
auto qos voip cisco-phone
  macro description CISCO_PHONE_EVENT
spanning-tree portfast
spanning-tree bpduguard enable
service-policy input AutoQos-4.0-CiscoPhone-Input-Policy
service-policy output AutoQos-4.0-Output-Policy
ip dhcp snooping limit rate 15
end
```

Step 2 (Optional) If you observe excessive timeouts, fine-tune the IEEE 802.1x timers and variables. Timers and variables are important for controlling the IEEE 802.1x authenticator process on the switch.

We recommend that you do not change the IEEE 802.1x timer and variable default settings, unless necessary.

Begin in interface configuration mode:

```
dot1x timeout tx
-period 30
dot1x max-reauth-req 2
authentication timer restart 60
dot1x timeout quiet-period 60
```

Step 3 Set the timers on the appropriate interfaces.

These timers and variables control IEEE 802.1x authenticator operations when end devices stop functioning during authentication.

Begin in interface configuration mode.

```
dot1x timeout supp-timeout 30
dot1x max-req 2
```

Reference

For detailed information about the IEEE 802.1x timers and variables, see the [Wired 802.1x Deployment Guide](#).

Step 4 Enable MAC authentication bypass (MAB) from interface configuration mode to authenticate supplicants that do not support IEEE 802.1x authentication.

When MAB is enabled, the switch uses the MAC address of the device as its identity. The authentication has a database of MAC addresses that are allowed network access.

We recommend that you enable MAB to support non-802.1x-compliant devices. MAB also is an alternate authentication method when end devices fail IEEE 802.1x authentication due to restricted ACL access.

Begin in interface configuration mode.

```
mab
```

Step 5 Configure IEEE 802.1x on the appropriate interfaces.

When you configure an IEEE 802.1x parameter on a port, a dot1x authenticator is automatically created on the port. When that occurs, the **dot1x pae authenticator** command must also be configured to ensure that the dot1x authentication will work on legacy configurations.

Begin in interface configuration mode:

```
authentication port-control auto
dot1x pae authenticator
```

Step 6 Enable access control and IEEE 802.1x authentications.

Begin in global configuration mode.

```
!Enable new access control
!
aaa new-model
!
!Set authentication list for 802.1x
!
aaa authentication dot1x default group radius
!
!Enable 802.1x authentication
!
dot1x system-auth-control
```


- Step 7** To establish the radius server, configure the RADIUS server with IP address, UDP port for authentication and accounting server, and server encryption key.

```
radius server AuthServer
address ipv4 192.168.254.14 auth-port 1656 acct-port 1646
key cisco123
```

Provision in Monitor Mode

Monitor mode enables IEEE 802.1x authentication without impacting the access of the end devices (supplicants) to a switch (authenticator). This mode allows you to continuously gather the following types of data for all the devices connected to your network:

- List of IEEE 802.1x-capable devices
- List of devices that are not capable of IEEE 802.1x
- Devices with good credentials
- Devices with bad credentials.
- List of valid MAC addresses (for MAB)
- List of unknown or invalid MAC addresses (for MAB)

We recommend monitor mode as a first-phase approach to provide secure access with IEEE 802.1x. Although this mode authenticates the end devices and users (supplicants), traffic is not impacted if authentication fails.

In monitor mode, IEEE 802.1x and MAB are enabled, but access is open to all users.

- Step 8** To allow hosts to gain access to a controlled port, configure multi-authentication host mode and open authentication.

```
authentication host-mode multi-auth
authentication open
```

- Step 9** Disable the Port Security feature, because when IEEE 802.1x is enabled, the Port Security feature becomes redundant and might interfere with the IEEE 802.1x functionality.

Begin in interface configuration mode.

```
no switchport port-security
no switchport port-security violation
no switchport port-security aging type
no switchport port-security aging time
no switchport port-security maximum
```

Provision in Low-Impact Mode

The next deployment phase in securing your network is to provision in low impact mode, which allows differentiated network access to authenticated users while permitting basic network services for all users.



Note

For information about configuration of multiple-authentication mode on IEEE 802.1x ports, see [“Provision Common Wired Security Access”](#).

Minimize the impact to your initial network access settings and add differentiated network access to authenticated users with low-impact mode provisioning. In low-impact mode, authentication is open and network access is contained using less restrictive port ACLs. After authentication, dACLs are used to allow full network access to end devices.

- Step 10** configure multi-domain mode to prevent unauthorized users from accessing an interface after an authorized user has been authenticated.

```
authentication host-mode multi-domain
```

- Step 11** Add a static ACL to allow basic network access.

Configure a restrictive port ACL that allows access for configuration and a Configured Trust List (CTL). Begin in global configuration mode.

```
ip access-list extended LowImpactSecurity-acl
  permit tcp any any established
  permit udp any any eq bootps
  permit udp any any eq tftp
  permit udp any any eq domain
  exit
interface GigabitEthernet1/0/1
  ip access-group LowImpactSecurity-acl in
```

Provision in High-Impact Mode

The final deployment phase of securing your wired network is high-impact mode.

This phase goes beyond low-impact mode and provisions tight access control on the network port by configuring the default IEEE 802.1x authentication mode with dynamic VLAN for differentiated access.

- Step 12** Configure multi-authentication host mode, and open authentication.

```
authentication host-mode multi-auth
authentication open
```

- Step 13** Disable RADIUS for this deployment phase.

High-impact mode provides no network access to devices and users that fail authentication. In monitor mode and low-impact mode, we recommend that you identify and resolve the devices and user accounts that have failed authentication. Transition to high-impact mode when you are confident that end devices (that need network access) authenticate successfully, and authentication fails for devices and users that do not need access.

Begin in global configuration mode.

```
interface GigabitEthernet 1/0/1-1/0/24
  no authentication open
```

- Step 14** Assign critical VLAN assignments for situations where the authentication server is unavailable.

The following command is used to configure a port to send both new and existing hosts to the critical VLAN when the RADIUS server is unavailable. Use this command for ports in multiple authentication (multiauth) mode or if the voice domain of the port is in MDA mode.

```
authentication event server dead action authorize vlan 20
```

- Step 15** If the authentication server does not respond, authorize voice.

```
authentication dead action authorize voice
```

Show Running Configuration for Provisioning Modes

Step 1 Enter the **show running-configuration** command to display provisioning modes for the switch.

Figure 10 *show running-configuration command for Provision in Monitor Mode*

```

show running-configuration

hostname 3850-access-Bld1Flr1
!
!
aaa new-model
!
aaa authentication dot1x default group radius
!
ip device tracking
!
!
dot1x system-auth-control
!
!
interface GigabitEthernet1/0/1
  switchport access vlan 10
  switchport mode access
  switchport block unicast
  switchport voice vlan 11
  ip arp inspection limit rate 100
  trust device cisco-phone
  authentication host-mode multi-auth
  authentication open
  authentication port-control auto
  mab
  dot1x pae authenticator
  storm-control broadcast level pps 1k
  storm-control multicast level pps 2k
  storm-control action trap
  Ipv6 nd raguard attach-policy endhost_ipv6_raguard
  Ipv6 guard attach-policy endhost_ipv6__guard
  auto qos voip cisco-phone
  service-policy input AutoQos-4.0-CiscoPhone-Input-Policy
  service-policy output AutoQos-4.0-Output-Policy
  ip verify source
  ip snooping limit rate 100
!
!
radius server AuthServer
  address ipv4 192.168.254.14 auth-port 1645 acct-port 1646
  key cisco123
!

```

Figure 11 *how running-configuration command for Provision in Low-Impact Mode*

```
show running-configuration

hostname 3850-access-Bld1Flr1
!
!
aaa new-model
!
aaa authentication dot1x default group radius
!
ip device tracking
!
!
dot1x system-auth-control
!
!
aaa session-id common
interface GigabitEthernet1/0/1
  switchport access vlan 10
  switchport mode access
switchport block unicast
switchport voice vlan 11
ip arp inspection limit rate 100
trust device cisco-phone
ip access-group LowImpactSecurity-acl in
authentication event fail action next-method
authentication host-mode multi-domain
authentication open
authentication port-control auto
mab
dot1x pae authenticator
storm-control broadcast level pps 1k
storm-control multicast level pps 2k
storm-control action trap
Ipv6 nd rguard attach-policy endhost_ipv6_rguard
Ipv6 guard attach-policy endhost_ipv6__guard
auto qos voip cisco-phone
service-policy input AutoQos-4.0-CiscoPhone-Input-Policy
service-policy output AutoQos-4.0-Output-Policy
ip verify source
ip snooping limit rate 100
!
!
ip access-group LowImpactSecurity-acl in
permit tcp any any established
permit udp any any eq bootps
permit udp any any eq tftp
permit udp any any eq domain
!
radius server AuthServer
address ipv4 192.168.254.14 auth-port 1645 acct-port 1646
key cisco123
```

Figure 12 *how running-configuration command for Provision in High-Impact Mode*

```

show running-configuration

hostname 3850-access-Bld1Flr1
!
!
aaa new-model
!
aaa authentication dot1x default group radius
!
ip device tracking
!
!
dot1x system-auth-control
!
!
aaa session-id common
interface GigabitEthernet1/0/1
  switchport access vlan 10
  switchport mode access
switchport block unicast
  switchport voice vlan 11
  ip arp inspection limit rate 100
  trust device cisco-phone
  authentication event server dead action authorize vlan 20
  authentication event server dead action authorize voice
  authentication host-mode multi-auth
  authentication port-control auto
  mab
  dot1x pae authenticator
  storm-control broadcast level pps 1k
  storm-control multicast level pps 2k
  storm-control action trap
  Ipv6 nd rguard attach-policy endhost_ipv6_rguard
  Ipv6 guard attach-policy endhost_ipv6__guard
  auto qos voip cisco-phone
  service-policy input AutoQos-4.0-CiscoPhone-Input-Policy
  service-policy output AutoQos-4.0-Output-Policy
  ip verify source
  ip snooping limit rate 100
!
!
radius server AuthServer
  address ipv4 192.168.254.14 auth-port 1645 acct-port 1646
  key cisco123

```

Monitoring IEEE 802.1x Status and Statistics

- Step 1** Use the **show dot1x statistics** command to display switch-related and port-related IEEE 802.1x statistics.

To detect errors, filter the dot1x verbose messages that are enabled by default.

```
show dot1x statistics
```

```
Dot1x Global Statistics for
-----
RxStart = 7      RxLogoff = 0      RxResp = 0      RxRespID = 8
RxReq = 0        RxInvalid = 0    RxLenErr = 0
RxTotal = 29

TxStart = 0      TxLogoff = 0      TxResp = 0
TxReq = 0        ReTxReq = 0      ReTxReqFail = 0
TxReqID = 8     ReTxReqID = 0    ReTxReqIDFail = 0
TxTotal = 8
```

Step 2 Use the **show dot1x interface statistics** command to display IEEE 802.1x statistics for a specific port.

```
show dot1x interface g1/0/1 statistics
```

```
Dot1x Authenticator Port Statistics for GigabitEthernet1/0/1
-----
RxStart = 10     RxLogoff = 0     RxResp = 0     RxRespID = 10
RxInvalid = 0    RxLenErr = 0     RxTotal = 37

TxReq = 0        TxReqID = 11     TxTotal = 11

RxVersion = 1    LastRxSrcMAC = 0023.33db.e970
```

Step 3 Use the **show dot1x all** command to display the IEEE 802.1x administrative and operational status for a switch.

```
show dot1x all
```

```
Sysauthcontrol          Enabled
Dot1x Protocol Version      3

Dot1x Info for GigabitEthernet1/0/1
-----
PAE                      = AUTHENTICATOR
QuietPeriod              = 60
ServerTimeout            = 0
SuppTimeout              = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
```

- Step 4** Use the **show dot1x interface** command to display the IEEE 802.1x administrative and operational status for a specific port.

```
show dot1x interface g1/0/1

Dot1x Info for GigabitEthernet1/0/1
-----
PAE = AUTHENTICATOR
QuietPeriod = 60
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
```




Converged Wired and Wireless Access

This workflow explains how to enable the converged access functionality of the switch, and explains how the switch can operate as the wireless mobility controller (MC) as well as the wireless mobility anchor (MA) in a small branch deployment.

Wired and wireless features that are enabled in the same platform is referred to as *converged access*. The wired plus wireless features are bundled into a single Cisco IOS Software image, which reduces the number of software images that users have to qualify and certify before enabling them in their network.

Converged access improves wireless bandwidth across the network and the scale of wireless deployment. For example, a 48-port Catalyst 3850 switch provides 40 Gbps of wireless throughput. This wireless capacity increases with the number of members in the stack. This ensures that the network will scale with current wireless bandwidth requirements, as dictated by IEEE 802.11n-based access points and with future wireless standards such as IEEE 802.11ac.

Prerequisites

Complete the following tasks before proceeding with wireless configuration:

- Switch stack must function in Stateful Switchover (SSO) mode.
- Interface configuration is completed, as explained in the [“Access Interface Connectivity”](#) workflow.
- Lightweight access points are used.
- NTP configuration should be present and operational, as explained in the [“Global System Configuration”](#) workflow.
- A wireless site survey should be completed. The site survey identifies the proper placement of wireless access points for the best coverage. For detailed information about the site survey process and the tool to use, see the [Wireless Site Survey FAQ](#).
- Complete the QoS workflow.

Restrictions

- AP-count licenses are supported only on IP Base and IP Services licenses. See the [Cisco Catalyst 3850 Switch Right-to-Use Licensing Model](#).



- A Catalyst 3850 switch stack can support a maximum of 50 access points.
- A Cisco Catalyst 3650 stack can support a maximum of 25 access points.
- WLAN cannot use client VLAN 0.

Identify Configuration Values

We recommend that you identify certain switch configuration values in advance so that you are ready to proceed with this section without interruption. As you follow the configuration sequence, replace the values in column B with your values in column C.



Note

This workflow contains two separate IP subnets that contain VLANs used for access points and wireless clients. The access points are on VLAN 12, and use IP subnet 192.168.12.x. The wireless clients are on VLAN 200, and use IP subnet 192.168.13.x.



Note

In the configuration examples, you must replace the blue italicized example values with your own values.

Table 10 **Wireless LAN Controller Values**

A. Value Name	B. Example Value Names	C. Your Value
Number of access point count licenses and slots	<i>10/1, 15/2</i>	
Management VLAN	<i>wireless-management-vlan</i>	
Management VLAN access point and description	<i>Wireless VLAN</i> <i>Wireless Management VLAN Interface</i>	
IP address for VLAN interface managing access points	<i>192.168.12.2 255.255.255.0</i>	
Access point pool	<i>APVlan10-Pool</i>	
Access point client pool	<i>192.168.12.0 255.255.255.0</i>	
Default router for client	<i>10.1.1.1</i>	
excluded address	<i>192.168.12.1</i>	
Wireless management interface	<i>vlan12</i>	
Access interface	<i>GigabitEthernet1/0/3</i>	
Description	<i>Lightweight Access Point</i>	
WLAN interface for client VLAN	<i>200</i>	
WLAN profile and ID	<i>Wireless_Client</i>	
Wireless client VLAN IP address	<i>192.168.13.2 255.255.254.0</i>	
WLAN for easy-RADIUS and ID	<i>OPEN_WLAN 1 open_wlan</i>	
RADIUS server	<i>AuthServer</i>	

Table 10 **Wireless LAN Controller Values**

A. Value Name	B. Example Value Names	C. Your Value
IPv4 address for RADIUS	<i>192.168.254.14</i>	
Auth-port	<i>1645</i>	
Acct-port	<i>1646</i>	
AAA group	<i>RADIUS-GROUP</i>	
RADIUS server dead-criteria time/tries	<i>10/3</i>	
RADIUS server deadtime	<i>1</i>	
WLAN with WPA2 and IEEE 802.1x enabled	<i>Secure_WLAN1 CISCO_WLAN</i>	
Input service policy	<i>wlan-Guest-Client-Input-Policy</i>	
Output service policy	<i>wlan-Guest-SSID-Output-Policy</i>	



Note

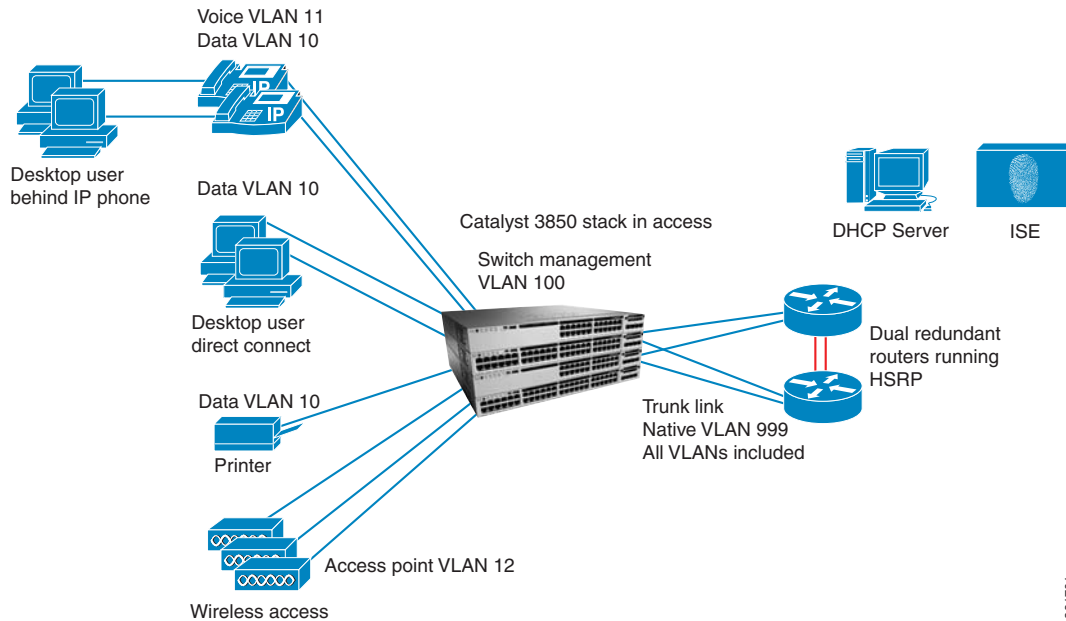
Configuration examples begin in global configuration mode, unless noted otherwise.

LAN Access Switch Topology with Wireless Connectivity

This topology shows the switch stack connected to multiple routers. The most common deployment of converged access is in a branch scenario, but this workflow also applies to a campus deployment.

The switch is stacked and acts as both the MC and MA. In a single stack converged access deployment, the switch can support up to 50 directly connected access points. For converged access, at least one lightweight access point is required. A maximum of 50 access points can be supported by a switch stack.

We recommend that you distribute the access points equally across the stack to achieve reliability during switchover scenarios preventing connectivity loss to access points connected to a member or standby switch.

Figure 13 LAN Access Switch Topology with Wireless Connectivity

391701

Enable the Switch as a Wireless Controller

- [Install Access Point Licenses on the Switch](#)
- [Configure a Wireless Management VLAN](#)
- [Configure Service Connectivity](#)
- [Enable Wireless Controller Functionality](#)
- [Change a Switch to Run in Mobility Controller Mode](#)
- [Enable the Access Point Connections](#)

Install Access Point Licenses on the Switch

For ease of use, an evaluation license is preinstalled on your switch, but you are required to accept the End-User-License Agreement (EULA) before the 90-day period expires.

The IP Base and IP Services image-based licenses support wireless functionality. The minimum license level for wireless functionality is IP Base.

The total AP-count license of a switch stack is equal to the sum of all the individual member AP-count licenses, up to a maximum of 50 AP-count licenses.

The total AP-count license of the stack is affected when stack members are added or removed:

- When a new member is added to the stack that has an existing AP-count license, then the total available AP-count license for the switch stack is automatically recalculated.
- When members are removed from the stack, the total AP-count license is decremented from the total available AP-count license in the stack.

- If more access points are connected that exceed the total number of accepted AP-count licenses, a syslog warning message is sent without disconnecting the newly connected access points until a stack reload.
- After a stack reload, the newly connected access points are removed from the total access point count.

You can activate permanent RTU licenses after you accept the EULA. The EULA assumes you have purchased the permanent license. Use AP-count adder type licenses to activate access point licenses. The adder AP-Count license is an “add as you grow” license. You can add access point licenses as your network grows. You activate an adder AP-count license by using EXEC commands, and it is activated without a switch reload.

Step 1 Activate a permanent access point license and accept the EULA.

Access point licenses are configured for permanent or for evaluation purposes. To prevent disruptions in operation, the switch does not change licenses when an evaluation license expires. You get a warning that your evaluation license will expire and you must disable the evaluation license and purchase a permanent one.

We recommend that you purchase and activate a permanent license and accept the EULA to avoid an untimely expiration.

The following examples activate 10 access point licenses on member 1 and 15 on member 2.

```
license right-to-use activate apcount 10 slot 1 acceptEULA
license right-to-use activate apcount 15 slot 2 acceptEULA
```

For more information about RTU licenses, see the “[Configuring Right-To-Use Licenses](#)” chapter in the *System Management Configuration Guide, Cisco IOS SE Release 3E*.

Verify AP-Count License Installation

Step 2 Verify the allocation of the access point licenses on the switch.

The following example shows two members in the stack:

```
show license right-to-use
```

Slot#	License name	Type	Count	Period left
1	ibase	permanent	N/A	Lifetime
1	lanbase	permanent	N/A	Lifetime
1	apcount	adder	10	Lifetime
License Level on Reboot: ibase				
Slot#	License name	Type	Count	Period left
2	ibase	permanent	N/A	Lifetime
2	lanbase	permanent	N/A	Lifetime
2	apcount	adder	15	Lifetime
License Level on Reboot: ibase				

Step 3 Verify the RTU license summary details.

The example shows that a permanent IP Services license is installed and is available upon switch reboot: Five AP-count licenses are in use.

```
show license right-to-use summary
```

License Name	Type	Count	Period left
ipservices	permanent	N/A	Lifetime
apcount	base	0	Lifetime
apcount	adder	25	Lifetime

```

License Level In Use: ipservices
License Level on Reboot: ipservices
Evaluation AP-Count: Disabled
Total AP Count Licenses: 25
AP Count Licenses In-use: 5
AP Count Licenses Remaining: 20

```

Configure a Wireless Management VLAN

Step 4 Configure the VLAN and SVI and assign it an IP address.

A wireless management VLAN is used for access point CAPWAP and other CAWAP mobility tunnels. The creation of a wireless management VLAN is mandatory. First, configure the VLAN in hardware and then create the SVI and assign it to an IP address. (See the [“Create a Management VLAN in Hardware”](#) section in the [Initial Switch Configuration](#) workflow.)

```
! To activate the VLAN in the database if it does not exist.
interface vlan 12
 name Wireless VLAN
 description Wireless Management VLAN Interface
 ip address 192.168.12.2 255.255.255.0
 no shutdown
 end
```

Configure Service Connectivity

Step 5 Create a name for the server address pool and specify the subnet network number and mask of the address pool client, and the default router for the client.

If you want the switch to receive IP address information you must configure the server with the IP address and subnet mask of the client and a router IP address to provide a default gateway for the switch. The server uses the DNS server to resolve the TFTP server name to an IP address, but configuration of the DNS server IP address is optional.

In small branch deployments in which the MC and MA are combined, we recommend using the switch as the server for the lightweight access points. In this deployment, the switch operates in Layer 2 mode, and the upstream router provides all routing functions.

We recommend that you exclude the IP address already used for the default router and the in-use wireless management SVI address to prevent an upstream router from allocating this IP address to an access point.

```
ip pool APVlan10-Pool
network 192.168.12.0 255.255.255.0
default-router 192.168.12.1
ip excluded-address 192.168.12.1 192.168.12.2
```

Enable Wireless Controller Functionality

Step 6 Configure an SVI (rather than a physical interface) as the management VLAN.

The **wireless management interface** command is used to source the access point CAPWAP and other CAPWAP mobility tunnels.

An SVI must be configured with an IP address before enabling the wireless controller.

```
wireless management interface vlan12
```

Change a Switch to Run in Mobility Controller Mode

Step 7 Enable the switch as an MC before the AP-count license installation.

In the wireless licensing model, the MA is the access point enforcer and the MC is the gatekeeper of the access points. The MC allows an access point to join the switch or not. The default role of the switch after boot up is an MA.

It is mandatory to save the configuration and reload the switch for the MC role to take effect.

```
wireless mobility controller
%
Mobility role changed to Mobility Controller. Please save config and
reboot the whole stack.
end
write memory
reload
proceed with reload? [confirm] y
```

Step 8 After the switch reboots, verify that the role of the switch has changed to Mobility Controller.

show wireless mobility summary

Mobility Controller Summary:

```

Mobility Role                : Mobility Controller
Mobility Protocol Port       : 16666
Mobility Group Name          : default
Mobility Oracle IP Address   : 0.0.0.0
DTLS Mode                    : Enabled
Mobility Domain ID for 802.11r : 0xac34
Mobility Keepalive Interval  : 10
Mobility Keepalive Count     : 3
Mobility Control Message DSCP Value : 48
Mobility Domain Member Count : 3

```

Link Status is Control Link Status : Data Link Status

Controllers configured in the Mobility Domain:

IP	Public IP	Group Name	Multicast IP	Link Status
192.168.102.210	-N/A	default	0.0.0.0	UP : UP

Enable the Access Point Connections

Step 9 Connect the access points directly to the switch ports to complete installation.

It is mandatory that the access point connection port be configured as an access port. The access point does not register if the port is configured as a trunk.



Note

The access VLAN on the switch port should be the same as the wireless management VLAN configured in [Step 4](#) in this workflow.


```
interface GigabitEthernet1/0/3
  description Lightweight Access Point
  switchport host
  switchport access vlan 12
  switchport port-security maximum 11
  switchport port-security
  switchport port-security aging time 2
  switchport port-security aging type inactivity
  switchport port-security violation restrict
  ip snooping limit rate 100
  switchport block unicast
  storm-control broadcast level pps 1k
  storm-control multicast level pps 2k
  storm-control action trap
```

Enable a Client VLAN

- Step 10** Configure an external server to allocate IP addresses for clients. Define a client VLAN and activate the VLAN in the database.

Every WLAN profile must be associated with a client VLAN.

```
!Activate the client VLAN in the VLAN database.
!Configure VLAN 200 if not already configured.
!
vlan 200
name Wireless_Client
end
!
interface vlan 200
  description Client VLAN
  ip address 192.168.13.2 255.255.254.0
  no shutdown
end
```

Provisioning a Small Branch WLAN

- [Provision in Easy-RADIUS](#)—Easiest to configure and does not rely on outside services.
- [Provision in Secure Mode](#)—End-users are authenticated by the external RADIUS server or ISE.
- [Manage Radio Frequency and Channel Settings](#)

We highly recommend that secure mode be provisioned for security concerns. However, both WLAN modes can co-exist if the network design requires it. For example, you can provision both WLANs on a single switch with each WLAN having its own purpose in the network.



Note

If your network does not permit open access for any wireless device, proceed to the [“Provision in Secure Mode”](#) section and provision your wireless network in secure mode.



Note

Guest Access network deployment is beyond the scope of this document. For detailed information, see the [“Configuring Wireless Guest Access”](#) chapter in the *Security Configuration Guide, Cisco IOS XE Release 3E, (Catalyst 3850 Switches)*.

Provision in Easy-RADIUS

Easy-RADIUS allows access to the network without authentication and is not secure.

- [Disable Authentication to Enable Easy-RADIUS](#)
- [Configure QoS to Secure the WLAN](#)
- [Verify Client Connectivity in RADIUS](#)



Note

If your network does not permit open access for any wireless device, proceed to the [“Provision in Secure Mode”](#) section and provision your wireless network in secure mode.

Disable Authentication to Enable Easy-RADIUS

- Step 1** To provision in easy-RADIUS, use the **no security EXEC** commands to disable authentication for a WLAN.

By default, the WLAN is enabled for security with Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2). To make the WLAN open, use the **no security wpa wpa2** command.

```
wlan OPEN_WLAN 1 open_wlan
client vlan 200
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
no shutdown
```

**Note**

By default, the broadcast SSID is enabled, and the WLAN/SSID information is sent in the beacons. The **no broadcast-ssid** command can be used to hide the SSID from being broadcast or made visible to end clients. When the SSID broadcast is disabled, the end-users will still be able to connect to the SSID by explicitly entering the SSID information manually in the wireless client network properties.

Configure QoS to Secure the WLAN

Step 2 Configure a service policy on the ingress direction to properly classify traffic.

All ingress traffic is classified the same as wired traffic. On egress, the secure WLAN is given the majority of the available bandwidth.

QoS configuration for a secure WLAN assumes that there is another WLAN with lower priority, such as a guest or open WLAN. The end users on a secure WLAN should not be impacted by non-critical traffic on other WLANs.

All WLANs share the default `port_child_policy` egress service policy. This policy is configured by default and does not need to be explicitly configured on a WLAN.

```
wlan secure_WLAN 2 CISCO_WLAN
shutdown
service-policy client input wlan-Entr-Client-Input-Policy
service-policy output wlan-Entr-SSID-Output-policy
no shutdown
exit
```

Verify Client Connectivity in RADIUS

Step 3 Associate clients and verify connectivity

Clients are associated to the WLAN end device by choosing the appropriate SSID.

Client connectivity can be verified by using wireless **show** commands that display state and authentication information.

```
pol-edu-3850-mc-12#show wireless client summary
```

```
Number of Local Clients : 2
```

MAC Address	AP Name	WLAN State		
Protocol				
0000.3a40.0001	pol-edu-tsim-40-6	4	UP	11a
0000.3a40.0002	pol-edu-tsim-40-1	4	UP	11a

```
pol-edu-3850-mc-12#show wcdb database all
```

```

Total Number of Wireless Clients = 2
  Clients Waiting to Join      = 0
  Local Clients                 = 2
  Anchor Clients                = 0
  Foreign Clients              = 0
  MTE Clients                   = 0

```

Mac Address	VlanId	IPv4 Address	Src If	Mob
0000.3a40.0001	340	153.40.125.100	0x00000000800000E2	LOCAL
0000.3a40.0002	340	153.40.125.101	0x00000000800000A1	LOCAL

```
!  
!Look for client open auth state.  
  
pol-edu-3850-mc-12#show access-session mac 0000.3a40.0001 details  
    Interface: Capwap33  
    MAC Address: 0000.3a40.0001  
    IPv6 Address: fe80::200:3aff:fe40:1  
    IPv4 Address: 153.40.125.100  
    User-Name: cisco  
    Status: Authorized  
    Domain: DATA  
    Oper host mode: multi-auth  
    Oper control dir: both  
    Session timeout: N/A  
    Common Session ID: 000000000000002D000B81FD  
    Acct Session ID: Unknown  
    Handle: 0xe9000023  
    Current Policy: (No Policy)  
    Blocked On:  
  
Server Policies:  
    Vlan Group: Name: 340, Vlan: 340  
  
Method status list:  
    Method          State  
    dot1x           Authc Success  
  
!
```

Provision in Secure Mode

Secure mode allows secure wireless connectivity. End users are authenticated by an external RADIUS server or ISE. Provision in secure mode if your network does not permit open access for any wireless device.

- [Enable the AAA RADIUS Server](#)
- [Configure the WLAN with IEEE 802.1x Authentication](#)
- [Configure QoS Service Policies for an Open WLAN](#)
- [DHCP Snooping](#)

Enable the AAA RADIUS Server

The configuration of the RADIUS server is dependent on the RADIUS service that you choose.

Step 1 Enable the AAA RADIUS server.

You must match the following configuration with an equivalent configuration on the RADIUS server.

```

aaa new-model
aaa session-id common
aaa authentication dot1x default group RADIUS
aaa authorization network default group RADIUS
aaa accounting dot1x default start-stop group RADIUS
!
! Enable 802.1X authentication globally on the switch
!
dot1x system-auth-control
! Radius Server definition (adds ISE to the Radius Group)
!
RADIUS server AuthServer
  address ipv4 192.168.254.14 auth-port 1645 acct-port 1646
  key cisco123
!
!
aaa group server RADIUS RADIUS-GROUP
server name AuthServer

```

Configure the WLAN with IEEE 802.1x Authentication

Step 2 Create a WLAN with WPA2 and IEEE 802.1x enabled.

Although the controller and access points support WLAN with SSID using WPA and WPA2 simultaneously, some wireless client drivers cannot support complex SSID settings.

Whenever possible, we recommend only WPA2 be configured with Advanced Encryption Standard (AES).

```

wlan Secure_WLAN1 CISCO_WLAN
client vlan 200
no shutdown

```



Note

WPA2 with AES encryption and IEEE 802.1x key management are enabled by default on the WLAN for the switch so you do not need to explicitly configure these security settings.

Configure QoS Service Policies for an Open WLAN

Step 3 Configure service policies for ingress and egress traffic for an open WLAN.

All ingress traffic is classified the same as wired traffic, but egress traffic is allocated only 30% of the available bandwidth.

When configuring QoS for an open WLAN, a low priority WLAN should be created for guest usage. The end users on an open WLAN are restricted and should not impact business-critical traffic on secure enterprise WLANs.

All WLANs share the port_child_policy egress policy. The policy is configured by default and is not explicitly configured on a WLAN.

```
wlan OPEN_WLAN 1 open_wlan
shutdown
service-policy client input wlan-Guest-Client-Input-Policy
service-policy output wlan-Guest-SSID-Output-Policy
no shutdown
exit
```

DHCP Snooping

Step 4 DHCP snooping configuration is required on the controller for proper client join functionality. DHCP snooping needs to be enabled on each client VLAN including the override VLAN if override is applied on the WLAN.

```
ip dhcp snooping
ip dhcp snooping vlan 100
```

Enable bootp-broadcast command. It is needed for clients that send the DHCP messages with broadcast addresses and broadcast bit is set in the DHCP message.

```
ip dhcp snooping wireless bootp-broadcast enable
```

On the interface:



Note If upstream is via a port channel, the trust Config should be on the port channel interface as well.

```
interface TenGigabitEthernet1/0/1
switchport trunk allowed vlan 100
switchport mode trunk
ip dhcp snooping trust
```



Note DHCP snooping should be configured on the Guest Anchor controller for guest access similar to the Config above.

To allow ingress and egress traffic on the network, the -required option in the WLAN settings forces clients to perform an address request and renew operation each time an association is made with the WLAN. This option allows strict control of used IP addresses.

Manage Radio Frequency and Channel Settings

Radio Resource Management (RRM), also known as Auto-RF, helps with channel and power setting management, but Auto-RF cannot correct for a poor radio frequency design.

- [Disable Low Data Rates](#)
- [Enable Clean Air](#)
- [Enable Dynamic Channel Assignment](#)
- [Associate WLAN Clients](#)
- [Verify WLAN Client Connectivity](#)

For any wireless deployment, we recommend a site survey to ensure a proper quality service design for your wireless clients.

Disable Low Data Rates

Step 1 Disable the 5-GHz and 2.4-GHz networks to successfully modify wireless spectrum rates.

In a well-designed wireless network with good radio frequency coverage, lower data rates can be disabled. Low data rates consume the most airtime.

Limiting the number of supported data rates allows clients to down-shift faster when retransmitting. Wireless clients try to send at the fastest data rate. If the transmitted frame is unsuccessful, the wireless client will retransmit at the next lowest available data rate. The removal of some supported data rates means that clients that need to retransmit a frame directly down-shift several data rates, which increases the chance for the frame to go through at the second attempt. IEEE 802.11b-only devices no longer need to be accommodated. Disable speeds used by IEEE 802.11b-only devices.

```
!Shutdown 5ghz network.
!
ap dot11 5ghz shutdown
!
!Enable 802.11n and 802.11ac for the 5Ghz spectrum.
!
ap dot11 5ghz dot11n
ap dot11 5ghz rate RATE_6M disable
ap dot11 5ghz rate RATE_9M disable
ap dot11 5ghz rate RATE_12M mandatory
ap dot11 5ghz rate RATE_18M supported
ap dot11 5ghz rate RATE_24M mandatory
ap dot11 5ghz rate RATE_36M supported
ap dot11 5ghz rate RATE_48M supported
ap dot11 5ghz rate RATE_54M supported
no ap dot11 5ghz shutdown
!
!Shutdown 2.4Ghz network
!
ap dot11 24ghz shutdown
!
```


Step 2 Enable wireless spectrums.

The lightweight access points support two wireless spectrums: 5 GHz and 2.4 GHz. You must enable and disable speeds in each spectrum, but the speeds do not have to match.

- Enable IEEE 802.11n and IEEE 802.11ac for the 5-GHz spectrum.
- Enable IEEE 802.11n and IEEE 802.11g for the 2.4-GHz spectrum.

**Note**

Beacons are sent at the lowest mandatory rate that define the cell size.

When deploying the switch in converged access mode as a hotspot, the lowest data rate should be enabled to increase coverage gain versus speed. In addition, the recommended data rates are to be used in a wireless network with good radio frequency coverage. Data rates are contingent upon the nature of your radio frequency deployment.

```
!Enable 802.11n and 802.11g for the 2.4Ghz spectrum.
!
ap dot11 24ghz dot11g
ap dot11 24ghz dot11n
ap dot11 24ghz rate RATE_24M mandatory
ap dot11 24ghz rate RATE_1M disable
ap dot11 24ghz rate RATE_2M disable
ap dot11 24ghz rate RATE_5_5M disable
ap dot11 24ghz rate RATE_6M disable
ap dot11 24ghz rate RATE_9M disable
ap dot11 24ghz rate RATE_11M disable
ap dot11 24ghz rate RATE_12M mandatory
ap dot11 24ghz rate RATE_18M supported
ap dot11 24ghz rate RATE_36M supported
ap dot11 24ghz rate RATE_48M supported
ap dot11 24ghz rate RATE_54M supported
no ap dot11 24ghz shutdown
```

Enable Clean Air

Step 3 Enable Clean Air on the switch and on devices that are common in your deployment environment.

The switch detects and reduces radio frequency interference when Clean Air is enabled. Some sources of interference are jammers, microwave ovens, and bluetooth devices.

```
ap dot11 24ghz cleanair
ap dot11 5ghz cleanair
ap dot11 24ghz cleanair device jammer
ap dot11 24ghz cleanair device cont-tx
ap dot11 24ghz cleanair device dect-like
ap dot11 24ghz cleanair device mw-oven
ap dot11 24ghz cleanair device video
!
ap dot11 5ghz cleanair device jammer
ap dot11 5ghz cleanair device cont-tx
ap dot11 5ghz cleanair device dect-like
ap dot11 5ghz cleanair device video
```

- Step 4** Verify that Clean Air is enabled on devices.

```
show ap dot11 24ghz cleanair config
show ap dot11 5ghz cleanair config
```

Enable Dynamic Channel Assignment

- Step 5** Make sure that the wireless 2.4-GHz and 5-GHz networks are shut down, as described in the “[Disable Low Data Rates](#)” section.
- Step 6** Enable Dynamic Channel Assignment (DCA) on both the 2.4-GHz and 5-GHz wireless spectrums to optimize channel assignments on radios for interference-free operation. For the 5-GHz spectrum, enable channel bonding to increase throughput.

DCA uses over-the-air metrics reported by each radio on every possible channel and provides a solution that maximizes channel bandwidth and minimizes radio frequency interference from all sources: self (signal), other networks (foreign interference), and noise (everything else).

```
ap dot11 24ghz rrm channel dca global auto
ap dot11 5ghz rrm channel dca global auto

ap dot11 5ghz shutdown
ap dot11 5ghz rrm channel dca chan-width 80
no ap dot11 5ghz shutdown
```

Associate WLAN Clients

- Step 7**

Association of WLAN clients is done on the end-client device by choosing the appropriate SSID and supplying the required credentials for authentication. Client connectivity depends on the type of device used which can be verified by looking at the wireless network interface details.

Verify WLAN Client Connectivity

Step 8 Verify client connectivity.

```
show authentication sessions mac ec55.f9c6.266b detail
```

```

Interface: Capwap4
  IIF-ID: 0x506280000033A0
  MAC Address: ec55.f9c6.266b
  IPv6 Address: Unknown
  IPv4 Address: 121.1.0.253
  User-Name: Employee1
  Status: Authorized
  Domain: DATA
  Oper host mode: multi-auth
  Oper control dir: both
  Session timeout: N/A
  Common Session ID: 64010101539f285900003353
  Acct Session ID: Unknown
  Handle: 0xDB000467
  Current Policy: (No Policy)

```

```
Server Policies (priority 100)
```

```
Method status list:
```

```

Method      State
dot1x      Authc Success

```

```
show wcb database all
```

```
!Need to look for the output of 'AUTH' equals to 'RUN'.
!
```

```

Total Number of Wireless Clients = 1
  Clients Waiting to Join = 0
  Local Clients = 1
  Anchor Clients = 0
  Foreign Clients = 0
  MTE Clients = 0

```

Mac Address	VlanId	IP Address	Src If	Auth	Mob
ec55.f9c6.266b	200	121.1.0.253	0x006B2F4000002844	RUN	LOCAL

Show Running Configuration for Wireless LAN Converged Access

Step 1 Enter the **show running-configuration** command to display the wireless configuration settings for the switch.

show running configuration

```
ip arp inspection vlan 10-11,100
!
ip device tracking
ip snoop vlan 10-13,100,200
no ip snoop information option
ip snoop wireless bootp-broadcast enable
!
! the default router for subnet 192.168.12.x /24 is the upstream router
! 192.168.12.2 is the layer 3 address of the 3850 vlan interface on vlan 12
!
ip excluded-address 192.168.12.1
ip excluded-address 192.168.12.2
!
!
!Access Point IP pool defined locally on the 3850
!
ip pool APVlan12-pool
network 192.168.12.0 255.255.255.0
default-router 192.168.12.1
!
! Vlan 200 for wireless clients, and the subnet 192.168.13.x /23
! the server is external to the 3850.
vlan 200
 name Wireless_Client
!
<snip>
!
! remember to exclude 192.168.13.2 on the server. Its statically defined
on the vlan 200 intf
interface Vlan200
description wireless Clients
ip address 192.168.13.2 255.255.255.0
!
wireless mobility controller
wireless management interface Vlan12
!
! this is copied from the "show run" output.
wlan OPEN_WLAN 1 WiFi_Open
client vlan 200
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
no shutdown
!
```

(Continued)

```
! Radio Resource management features
ap dot11 24ghz shutdown
ap dot11 24ghz cleanair
ap dot11 24ghz rate RATE_1M disable
ap dot11 24ghz rate RATE_2M disable
ap dot11 24ghz rate RATE_5_5M disable
ap dot11 24ghz rate RATE_6M disable
ap dot11 24ghz rate RATE_9M disable
ap dot11 24ghz rate RATE_11M disable
ap dot11 24ghz rate RATE_12M supported
ap dot11 24ghz rate RATE_18M supported
ap dot11 24ghz rate RATE_24M mandatory
ap dot11 24ghz rate RATE_36M supported
ap dot11 24ghz rate RATE_48M supported
ap dot11 24ghz rate RATE_54M supported
no ap dot11 24ghz shutdown
!
ap dot11 5ghz shutdown
ap dot11 5ghz rrm channel dca chan-width 80
ap dot11 5ghz cleanair
ap dot11 5ghz rate RATE_6M disable
ap dot11 5ghz rate RATE_9M disable
ap dot11 5ghz rate RATE_12M disable
ap dot11 5ghz rate RATE_18M disable
ap dot11 5ghz rate RATE_24M mandatory
ap dot11 5ghz rate RATE_36M supported
ap dot11 5ghz rate RATE_48M supported
ap dot11 5ghz rate RATE_54M supported
no ap dot11 5ghz shutdown
ap group default-group
end
```




System Health Monitoring

Monitoring critical system resources is very important to maintain stability of the network. We recommend that you monitor the switch CPU, memory, file systems, and environmental resources on a regular basis.

This workflow discusses the commonly used commands and procedures to monitor and maintain system health.

Prerequisites for System Health Monitoring

Obtain information about your switch such as the running software release, duration of switch run time, and the reason for the most recent reload. To obtain this information, use the **show version** command. The command with the pipe feature gives the duration of uptime and any reload information.

```
show version|inc software|uptime|Last
Cisco IOS Software, IOS-XE Software, Catalyst L3 Switch Software
(CAT3K_CAA-UNIVERSALK9-M), Version 03.03.02.SE RELEASE SOFTWARE (fc2)
3850-access-Bld1Flr1 uptime is 5 weeks, 3 days, 2 hours, 59 minutes
Last reload reason: reload
```

Show Running Status

Identify the reasons for uptime and reload. Over time, switches can crash and reload without your knowledge.

Step 1 Use the **show version** command to retrieve the overall switch status.

If you are only interested in the switch uptime and last reload, you can run a more direct command using the pipe “|” feature built into Cisco IOS XE (and Cisco IOS) software.

This example shows that Cisco IOS XE release 3.3.2 SE was running for five weeks before a privileged user initiated a switch reload.



```
show version|inc software|uptime|Last
Cisco IOS Software, IOS-XE Software, Catalyst L3 Switch Software
(CAT3K_CAA-UNIVERSALK9-M), Version 03.03.02.SE RELEASE SOFTWARE (fc2)

3850-access-Bld1Flr1 uptime is 5 weeks, 3 days, 2 hours, 59 minutes

Last reload reason: reload
```

Run a System Baseline for Core Resources

Set your system baseline usage during normal production time and determine if there is a change from your expected resource values. If the increase in usage is not justified, investigate to find the cause. Ideally, it is best to setup some form of Network Monitoring System (NMS) to automatically monitor these values, however it is also important to learn how to manually poll these values.

After you have identified the switch running status, examine core resources to ensure that they are all at optimal values.

Obtain CPU and Core Processor Usage

Step 2 Use the **show process cpu** command to display CPU and core processor usage.

To find CPU usage due to the subprocesses and tasks operating under a specific process, use the **show process cpu detailed** command. To sort for high activity usage, use **show process cpu sorted** command.

CPU usage can be monitored on a per-switch basis in a stacked environment.

At periodic intervals, we recommend that you run the following variations of the **show process cpu** command.



Note

The switch is a multicore platform that is different from its predecessors. A single core can experience high CPU, so it is important to monitor each core when running these commands.

This output shows the five-second, one-minute, and five-minute periods on each CPU core. It also shows the Forwarding Engine Driver (FED), IOS daemon IOSd, and Wireless Controller Module (WCM) processes have the highest CPU utilization.

Obtain Switch Memory Usage

Step 4 Use the **show process memory** command to display the state of memory usage on your switch.

To find memory usage due to the subprocesses and tasks operating under a specific process, use the **show process memory detailed** command. To sort for high activity usage, use the **show process memory detailed sorted** command.

Memory usage can be monitored on a per-switch basis in a stacked environment.

```
show process memory sorted
System memory : 3930840K total, 1487028K used, 2443812K free, 222004K kernel
reserved
Lowest(b)      : 1915568076
PID   Text      Data      Stack    Heap     RSS      Total    Process
5681  9988      269088    92       476     233060   584844   fed
10162 72268     34364     104      288     206548   343980   iosd
10158 24260     519732    88       10628   108612   662328   wcm
```

Monitor File Systems Usage

Step 5 At regular intervals, use the **show file systems** command to monitor the file systems within the switch to ensure that there is always sufficient space available.

Unlike previous platforms, the switch writes crash files to a separate directory. For example, the **show file systems** command output shows that the crashinfo folder is populated. Compare the size of the folder against the free space available.

The switch has different file systems that can be listed by using the **show file systems** command.

```
show file systems
File Systems:

      Size(b)      Free(b)      Type  Flags  Prefixes
      248354816    148799488    disk  rw     crashinfo: crashinfo-1:
      248512512    178782208    disk  rw     crashinfo-2: stby-crashinfo:
*    1621966848    346673152    disk  rw     flash: flash-1:
      1622147072    350224384    disk  rw     flash-2: stby-flash:
```



Note

An (*) asterisk indicates the default file system. If the file system has a dash (-) or a zero (0) for the Size(b) field, that indicates that the file system is not present or not recognized.

Step 6 Use the **dir filesystem** or the **show filesystem** command to list the files under a specific file system. When you find crash files, it is important to immediately retrieve them to diagnose a system failure or unexpected crash.

This example shows that crash files were created in the directory.

```

dir crashinfo
Directory of crashinfo:/

 6073  drwx          1024  Jul 17 2013 17:53:48 +00:00  ap_crash
   12  -rwx           0     Jan 1 1970 00:00:06 +00:00  koops.dat
   11  -rwx           357   Jun 1 2014 13:05:15 +00:00  last_systemreport_log
   13  -rwx       1128623  Nov 22 2013 12:33:27 +00:00
system-report_2_20131122-123229-UTC.gz
   14  -rwx           39   Jun 1 2014 13:05:15 +00:00  last_systemreport
   15  -rwx       657766   Jun 5 2013 09:17:03 +00:00
system-report_1_20130605-091616-UTC.gz
   16  -rwx       737390   Jun 26 2013 22:48:22 +00:00
system-report_1_20130626-224726-UTC.gz

```

Run a System Baseline for Environmental Resources

Step 7 Use the **show environment** command to display an overview of switch health.

It is important to monitor environmental resource values because something as small as a fan failure can lead to a serious hardware problem. If your switches provide Power Over Ethernet (POE), then the **show environment** command will also provide a view into the power supplies and if they are performing as expected.

```

show environment all
Switch 1 FAN 1 is OK
Switch 1 FAN 2 is OK
Switch 1 FAN 3 is OK
FAN PS-1 is OK
FAN PS-2 is OK
Switch 1: SYSTEM TEMPERATURE is OK
SW  PID                      Serial#      Status      Sys Pwr  PoE Pwr  Watts
--  -----
1A  PWR-C1-715WAC              LIT171310MT  OK          Good     Good     715
1B  PWR-C1-715WAC              LIT171310PS  OK          Good     Good     715

```

Step 8 If your switches are in a stack, run the **show environment stack** command to view all of the environmental outputs stack wide.

Although some of settings are adjustable, we recommend leaving the settings with their default values.

```
show environment stack
SWITCH: 1
Switch 1 FAN 1 is OK
Switch 1 FAN 2 is OK
Switch 1 FAN 3 is OK
FAN PS-1 is OK
FAN PS-2 is OK
Switch 1: SYSTEM TEMPERATURE is OK
Inlet Temperature Value: 34 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 41 Degree Celsius
Red Threshold    : 56 Degree Celsius
Hotspot Temperature Value: 45 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 105 Degree Celsius
Red Threshold    : 125 Degree Celsius
SWITCH: 2
Switch 2 FAN 1 is OK
Switch 2 FAN 2 is OK
.
.
.
```

Other System Monitoring Considerations

Spanning Tree Monitoring

Spanning tree design is beyond the scope of this document, however, the goal of this procedure is to provide simple spanning tree monitoring commands. It is important to always understand your spanning tree topology within your network. There are a number of simple commands that you can run to verify that your switch is performing the expected spanning tree role.

- Step 9** Use the **show spanning-tree summary** command to periodically monitor the stability of your spanning tree environment and ensure a loop-free environment.

This example output shows that the switch is actually operating as the root bridge for all of the VLANs which can cause extreme network degradation if incorrectly configured.

```

show spanning-tree summary
Switch is in pvst mode
Root bridge for: VLAN0001, VLAN0011, VLAN0015, VLAN0100-VLAN0101
VLAN0881-VLAN0883
Extended system ID          is enabled
Portfast Default            is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default          is disabled
EtherChannel misconfig guard is enabled
UplinkFast                 is disabled
BackboneFast               is disabled
Configured Pathcost method used is short

```

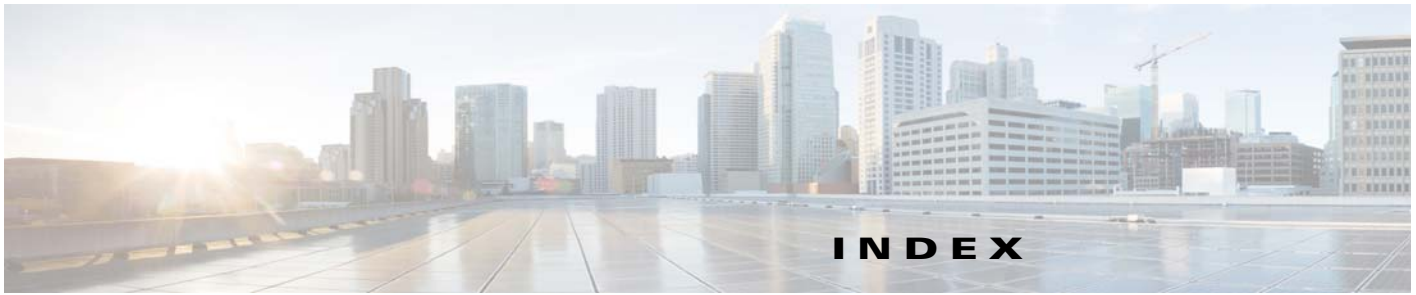
Name	Blocking	Listening	Learning	Forwarding	STP Active
VLAN0001	0	0	0	2	2
VLAN0011	0	0	0	1	1
VLAN0015	0	0	0	1	1
VLAN0100	0	0	0	1	1
VLAN0101	0	0	0	1	1
VLAN0777	0	0	0	2	2
VLAN0881	0	0	0	1	1

Name	Blocking	Listening	Learning	Forwarding	STP Active
VLAN0882	0	0	0	1	1
VLAN0883	0	0	0	1	1
9 vlans	0	0	0	11	11

Step 10 Use the **show spanning-tree detail** command to frequently check STP stability.

This command displays network stability information about the number of topology changes within each VLAN, the last time a TCN was received, and so forth. Frequently monitoring this information is critical to maintaining overall health of the switch and network.

```
show spanning-tree detail |inc ieee|occur|from|is|exec
VLAN0001 is executing the ieee compatible Spanning Tree protocol
  Number of topology changes 55 last change ed 4d07h ago
    from GigabitEthernet1/0/1
VLAN0011 is executing the ieee compatible Spanning Tree protocol
  Number of topology changes 7 last change ed 4d07h ago
    from GigabitEthernet1/0/1
VLAN0015 is executing the ieee compatible Spanning Tree protocol
  Number of topology changes 7 last change ed 4d07h ago
    from GigabitEthernet1/0/1
VLAN0100 is executing the ieee compatible Spanning Tree protocol
  Number of topology changes 7 last change ed 4d07h ago
    from GigabitEthernet1/0/1
VLAN0101 is executing the ieee compatible Spanning Tree protocol
  Number of topology changes 7 last change ed 4d07h ago
    from GigabitEthernet1/0/1
VLAN0777 is executing the ieee compatible Spanning Tree protocol
  Number of topology changes 12 last change ed 4d07h ago
    from GigabitEthernet1/0/1
VLAN0881 is executing the ieee compatible Spanning Tree protocol
  Number of topology changes 7 last change ed 4d07h ago
    from GigabitEthernet1/0/1
```



A

active stack member [131](#)
AP licenses [185](#)
auto-upgrade [127, 136](#)

B

Bridge Protocol Data Unit (BPDU) [132](#)
bundle mode [124](#)

C

crashinfo folder [1106](#)

D

DHCP server [187](#)
DHCP snooping [134](#)
Dynamic Channel Assignment (DCA) [198](#)

E

Easy-open mode [190](#)
End-User-License Agreement (EULA) [184](#)
EtherChannels [135, 144](#)
evaluation license [184](#)

H

high impact mode [173](#)
HSRP (Hot Standby Router Protocol) [149](#)
HTTP (HTTPS) [19](#)

I

in-band IP Address [114](#)
install mode [124](#)
IP device tracking (IPDT) [154](#)
IPv6 security policies [135](#)

L

LACP (Link Aggregation Control Protocol) [144](#)
low impact mode [172](#)

M

MAC Authentication Bypass (MAB) [168](#)
management IP address [114](#)
monitor mode [171](#)

N

NTP server [134](#)

O

out-of-band management [112](#)

P

password [110](#)
provision in phased deployments [168](#)

R

Rapid Per-VLAN Spanning-Tree (PVST+) [132](#)
Rapid PVST+ [132](#)
Router Advertisement Guard [135](#)
router advertisements [136, 157](#)

S

Secure mode [193](#)
Secure Shell (SSH) [19](#)
show environment command [1107](#)
show process cpu command [1104](#)
Show Running Configuration for Global Management Assignments [138](#)
Show Running Configuration for Initial Management Assignments [118](#)
show version command [1103](#)
software clean [125, 127](#)
software expand [124](#)
spanning tree monitoring commands [1108](#)
stack member priority [131](#)
standalone Distribution switches [148](#)
synchronized clock [134](#)

T

TACACS+ [110](#)
TFTP and FTP server [125](#)
TFTP block size [121, 136](#)

U

Unidirectional Link Detection (UDLD) [133](#)
uplink to distribution switches [148](#)
user id [110](#)

V

VLAN 1 [144](#)
VLAN management interface [114](#)
VRRP (Virtual Router Redundancy Protocol) [149](#)
VTP transparent mode [132](#)

W

Wi-Fi Protected Access (WPA) [190](#)
Wi-Fi Protected Access II (WPA2) [190](#)