



# Compact Switch Deployment Guide

● ● ● SMART BUSINESS ARCHITECTURE

February 2013 Series

# Preface

## Who Should Read This Guide

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

## Release Series

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

The Release Notes for a series provides a summary of additions and changes made in the series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

**month year** Series

For example, the series of guides that we released in February 2013 is the “February Series”.

You can find the most recent series of SBA guides at the following sites:

Customer access: <http://www.cisco.com/go/sba>

Partner access: <http://www.cisco.com/go/sbachannel>

## How to Read Commands

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

```
class-map [highest class name]
```

Commands shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
wrr-queue random-detect max-threshold 1 100 100 100 100 100  
100 100 100
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

```
interface Vlan64  
ip address 10.5.204.5 255.255.255.0
```

## Comments and Questions

If you would like to comment on a guide or ask questions, please use the [SBA feedback form](#).

If you would like to be notified when new comments are posted, an RSS feed is available from the SBA customer and partner pages.

# Table of Contents

<b>What's In This SBA Guide</b> .....	<b>1</b>	<b>Deployment Details</b> .....	<b>6</b>
Cisco SBA Borderless Networks.....	1	Preparing the Access Layer Switch Ports.....	6
Route to Success.....	1	Setting Up the Compact Switch.....	8
About This Guide.....	1	<b>Appendix A: Product List</b> .....	<b>16</b>
<b>Introduction</b> .....	<b>2</b>	<b>Appendix B: Configuration Example</b> .....	<b>18</b>
Business Overview.....	2	<b>Appendix C: Changes</b> .....	<b>24</b>
Technology Overview.....	2		

# What's In This SBA Guide

## Cisco SBA Borderless Networks

Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization's problems—without worrying about the technical complexity.

Cisco SBA Borderless Networks is a comprehensive network design targeted at organizations with up to 10,000 connected users. The SBA Borderless Network architecture incorporates wired and wireless local area network (LAN) access, wide-area network (WAN) connectivity, WAN application optimization, and Internet edge security infrastructure.

## Route to Success

To ensure your success when implementing the designs in this guide, you should first read any guides that this guide depends upon—shown to the left of this guide on the route below. As you read this guide, specific prerequisites are cited where they are applicable.



## About This Guide

This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- **Business Overview**—Describes the business use case for the design. Business decision makers may find this section especially useful.
- **Technology Overview**—Describes the technical design for the business use case, including an introduction to the Cisco products that make up the design. Technical decision makers can use this section to understand how the design works.
- **Deployment Details**—Provides step-by-step instructions for deploying and configuring the design. Systems engineers can use this section to get the design up and running quickly and reliably.

You can find the most recent series of Cisco SBA guides at the following sites:

Customer access: <http://www.cisco.com/go/sba>

Partner access: <http://www.cisco.com/go/sbachannel>

# Introduction

## Business Overview

In some situations, organizations need more flexibility in providing a greater number of access ports to a specific location without adding more cabling. It may be a temporary requirement, such as hosting a training session in a conference room for the day. Or it may be a situation in which it is difficult or expensive to run additional cabling; such as a retail environment, a cruise ship, a classroom, or a historical building. Also, organizations often need to respond to a sudden need for additional port density very quickly when there is not enough time to get new cabling installed and tested before it is needed. In such circumstances, using an additional compact switch attached directly to the existing access layer can provide the needed connectivity within the constraints of the existing cable plant. The wiring closet is extended, while maintaining device manageability.

## Technology Overview

The Cisco Smart Business Architecture (SBA) LAN access layer provides network connections for end-user PCs, laptops, phones, printers, and other devices in the work environment. The primary access layer switches are designed to be housed in 19-inch equipment racks in a wiring closet or other room appropriate for such equipment. Typical cabling plants dictate that every device that needs access to the network has a dedicated port that is “home run” from the work environment back to the location of the nearest access layer switch.

You can sometimes use wireless network technologies to meet dynamic requirements for flexibility in the number of networked devices in a location. However, if the devices require Power over Ethernet (PoE) to operate or support only wired network connections, you need an alternate approach to meet these requirements. In this situation, Cisco SBA access layer provides for the capability to extend resilient ports from an existing access layer switch or switch stack out to an additional small switch located directly in the work area, providing up to eight or twelve ports of network connectivity. The Cisco Catalyst 3560-C and 2960-C Series Compact Switches are designed for deployment outside of the wiring closet and are ideal for this purpose, running IOS software and management, just like the standard 3560 or 2960 inside the wiring closet.

## Networking Features

The Cisco SBA access layer is designed to provide the resiliency and security required for stable operations. Cisco Catalyst Infrastructure Security Features (CISF) such as Dynamic Host Configuration Protocol (DHCP) snooping, IP Source Guard, port security, and dynamic Address Resolution Protocol (ARP) inspection (DAI), protect the vulnerable network edge from common attacks.

MAC flooding attacks are used to force a LAN switch to flood all their traffic out to all the switch interfaces. Port security limits the number of MAC addresses that can be active on a single port to protect against such attacks.

Port security lets you to configure Layer 2 interfaces to allow inbound traffic from only a restricted set of MAC addresses. The MAC addresses in the restricted set are called secure MAC addresses. In addition, the device does not allow traffic from these MAC addresses on another interface within the same VLAN.

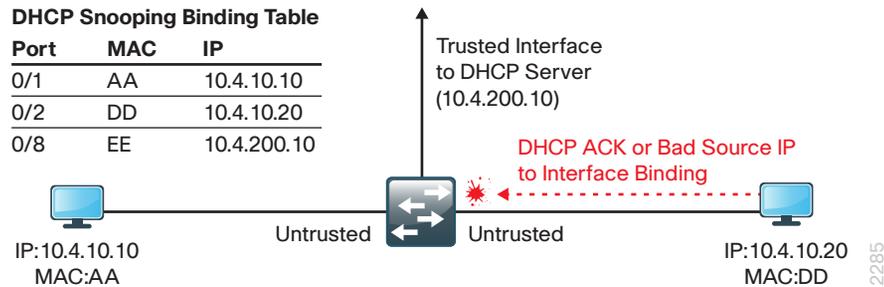
The number of MAC addresses that the device secures on each interface is configurable. For ease of management, the device can learn the addresses dynamically. Using the dynamic learning method, the device secures MAC addresses while ingress traffic passes through the interface. If the address is not yet secured and the device has not reached any applicable maximum, it secures the address and allows the traffic. The device ages dynamic addresses and drops them when the age limit is reached.

DHCP snooping is a DHCP security feature that blocks DHCP replies on an untrusted interface. An untrusted interface is any interface on the switch not specifically configured as a known DHCP server or path towards a known DHCP server.

The DHCP snooping feature helps simplify management and troubleshooting by tracking MAC address, IP address, lease time, binding type, VLAN number, and interface information that correspond to the local untrusted interfaces on the switch. DHCP snooping stores that information in the DHCP binding table.

Dynamic ARP inspection (DAI) mitigates ARP poisoning attacks. An ARP poisoning attack is a method by which an attacker sends false ARP information to a local segment. This information is designed to poison the ARP cache of devices on the LAN, allowing the attacker to execute man-in-the-middle attacks.

Figure 1 - DHCP snooping and ARP inspection



DAI uses the data generated by the DHCP snooping feature and intercepts and validates the IP-to-MAC address relationship of all ARP packets on untrusted interfaces. ARP packets that are received on trusted interfaces are not validated and invalid packets on untrusted interfaces are discarded.

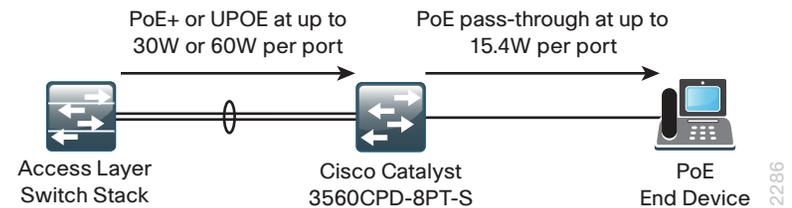
IP Source Guard is a means of preventing a packet from using an incorrect source IP address to obscure its true source, also known as *IP spoofing*. IP Source Guard uses information from DHCP snooping to dynamically configure a port access control list (PACL) on the interface that denies any traffic from IP addresses that are not in the DHCP binding table.

Voice and video support is enabled through network services such as Power over Ethernet+ (PoE+), Quality of Service (QoS), IP Multicast, and Cisco Discovery Protocol (CDP) with the Voice VLAN. When the access layer is extended by use of an additional compact switch, it is important that you ensure consistency of feature support for these additional access layer ports. The Cisco Catalyst Compact Switch family supports a common feature set with the networking platforms that are already a part of your Cisco SBA access layer. Using Cisco SBA configuration procedures similar to those used for your access layer switches promotes greater ease of deployment.

## Power over Ethernet Options

PoE pass-through allows a switch to power PoE end devices by using power received from the upstream wiring closet switch. The Cisco Catalyst Compact Switch is available in models that provide eight PoE-capable Ethernet ports able to power edge devices up to the pass-through power budget, and two Gigabit Ethernet uplink ports that receive IEEE PoE+ power or Cisco UPOE from the upstream switch. This switch model is a PoE-powered device, because it does not require a separate connection for wall power, but instead can receive power from the upstream switch. This allows the compact switch to benefit from any power resiliency that is provided in the upstream wiring closet.

Figure 2 - Pass-through PoE



To power both the switch and one or more attached devices, the upstream switch must be able to provide enough power over the uplinks to satisfy total device power requirements. Power can be used from one or both uplink ports to power the switch, with remaining power available as pass-through from the Cisco Compact Switch to powered devices, up to the power budget limit for that device.

The Cisco Catalyst Compact Switches can also draw power from an external auxiliary adapter, allowing the flexibility to use the same switch in situations where the upstream switch does not provide PoE. You can also use the auxiliary adapter to provide greater resiliency for attached PoE devices in the event power available from the uplink connections is reduced, such as with a PoE+ uplink failure. With the auxiliary adapter in use, the maximum available power for edge ports is unchanged.

Table 1 - Pass-through power available to powered devices

Uplink power source	Nominal uplink source power supplied	Catalyst 2960CPD maximum pass-through power	Catalyst 3560CPD maximum pass-through power
1 PoE	15.4 W	0 W	Insufficient to power switch
2 PoE	30.8 W	7 W	0 W
1 PoE+	30 W	7 W	0 W
1 PoE+ and 1 PoE	45.4 W	15.4 W	0 W
2 PoE+	60 W	22.4 W	15.4 W
1 Cisco UPOE	60 W	30.8 W	23.8 W
Auxiliary power input	-	22.4 W	15.4 W
Auxiliary power input with UPOE uplink	-	30.8 W	23.8 W

### Tech Tip

For more details about the available power with different uplink configurations, see the following:  
[Cisco Catalyst 3560-C and 2960-C Series Compact Switches Data Sheet](#)

The Cisco Catalyst 3560CPD-8PT-S has eight 10/100/1000 Mbps ports and includes layer 3 IP Base features. The Cisco Catalyst 2960CPD-8PT-L has eight 10/100 Mbps ports and layer 2 focused LAN Base features.

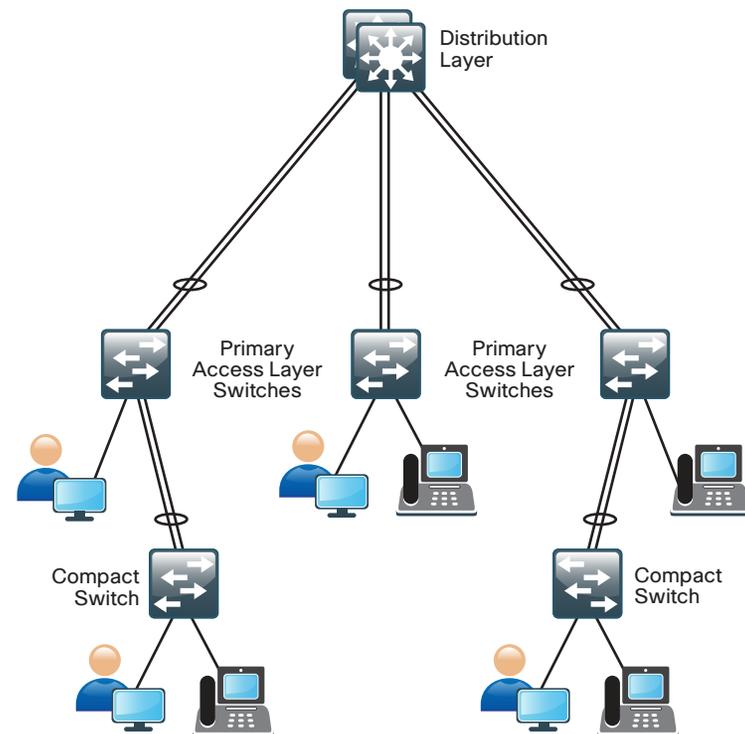
When PoE pass-through power is insufficient for the deployment, Cisco Catalyst Series Compact Switches are available in models that use a traditional internal power supply. The supply must be plugged in separately, allowing the Catalyst 2960-C to support a maximum of 15.4W of PoE per port and the Catalyst 3560-C to support a maximum of 30W of PoE+ per port. The switch allows a total maximum power consumption of 124W that

can be spread across all ports in any combination with up to 30W consumed by any single port supporting PoE+. The Catalyst 3560-C switch is an appropriate choice if you need to use it to drive multiple PoE+ devices, such as IP phones, wireless access points, or video surveillance cameras.

### Compact Switch Access Topology

Because the cabling in a typical network environment connects back to the nearest access layer wiring closet, connecting a small switch to the nearest access switch is a common configuration. This approach extends the local LAN access ports in the workspace to allow a greater density of attached devices in a given location. The compact switch fits into the existing Cisco SBA design as shown in the following figure.

Figure 3 - Compact switch access topology



2287

While the compact switches could also be connected directly to the distribution layer and configured as access switches, this would be a less common use case. The cabling plant in your specific physical environment dictates the available options in your network. Cabling from the workspace is normally copper to the nearest wiring closet, and the links from the access layer switches in the closet up to the distribution are normally fiber optic. Cisco compact switches use copper cabling for uplinks, consistent with placement directly in the workspace, and are also available with fiber uplink options. The target use for the solution outlined in this guide is expanding port count rapidly in the workspace with existing cabling.

## Notes

# Deployment Details

Ideally, when you extend access layer ports to increase port density in the workspace, it is desirable to maintain the resiliency inherent in the Cisco SBA network architecture. Using two uplink ports allows the compact switch to maintain connectivity to the network even if one of the cable connections fails. Using a second uplink also provides a greater overall power budget when the uplinks use PoE or PoE+; however, it is possible that some pass-through PoE edge devices could lose power with a single uplink failure, even though the switch itself is still powered. A single Cisco UPOE link is sufficient to offer the maximum power budget to connected powered devices.

To maintain maximum resiliency, select ports from different line cards of a chassis-based access layer switch or, if you are using a stacked access layer, from different physical stack members. Creating this arrangement may require a visit to the wiring closet to repatch the specific LAN ports in the work area. Using two uplink ports, of course, requires that enough copper runs are available from the work area.



## Reader Tip

Deployment procedures provided in this section are designed to be used in conjunction with an existing Cisco Catalyst switch running the Cisco SBA LAN access layer configuration. For details of this configuration, please see the *Cisco SBA—Borderless Networks LAN Deployment Guide*.

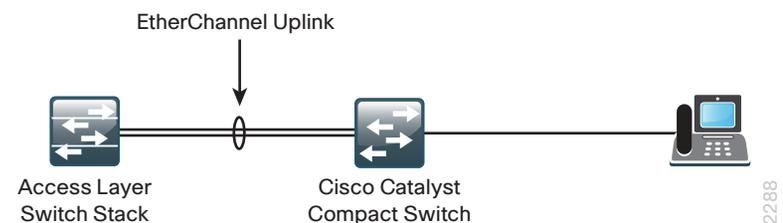
## Process

Preparing the Access Layer Switch Ports

1. Identify access layer switch ports
2. Configure the trunk and port channel

The compact switch requires a configuration process similar to other access layer switches. The main difference is that its upstream switch is a member of the existing layer-2 access layer switch, as opposed to a layer-3 capable distribution layer switch. Prepare the configuration of the upstream access layer switch before connecting the links to the compact switch. This process ensures the Cisco SBA access layer switch does not disable the uplink ports on the access switch when it begins to see spanning tree BPDU packets from the compact switch.

Figure 4 - Access layer topology with Cisco Catalyst Compact Switch



## Procedure 1

### Identify access layer switch ports

**Step 1:** Identify the switch ports to be used as uplinks from the compact switch, and ensure that the cable runs from the work area are properly patched into the correct switch ports. If possible, choose ports from different line cards or switch stack members to attach the compact switch. If the compact switch is being powered by PoE, choose ports with the required PoE power sourcing capabilities to support the switch and pass-through power requirements.

**Step 2:** Connect to the console or open a Secure Shell (SSH) session to the access switch, and then examine the existing configuration of the switch ports to be used as uplinks to the compact switch. If the configuration of the selected ports is currently blank, move on to Procedure 2.

**Step 3:** If the existing switch ports are set up with an access layer edge port configuration, use the **default interface** command prior to setting up the port as a trunk connection for the compact switch. This clears any existing configuration on the port.

```
default interface GigabitEthernet [slot/port]
```

## Procedure 2

### Configure the trunk and port channel

You should configure the physical interfaces that are members of a Layer 2 EtherChannel prior to configuring the logical port-channel interface. This sequence allows for minimal configuration because most of the commands entered to a port-channel interface are copied to its members interfaces and do not require manual replication.

**Step 1:** Configure the EtherChannel member interface by setting Link Aggregation Control Protocol (LACP) negotiation to active on both sides to ensure a proper EtherChannel is formed. If the access layer switch adheres to a Cisco SBA LAN Access Layer configuration, the egress QoS macro specific to the access platform in use. The Cisco Catalyst 2960S does not require the **switchport** command, and the Cisco Catalyst 4500 does not require the **logging event bundle-status** command.

```
interface [interface type] [port 1]
  description Link to Compact Switch port 1
interface [interface type] [port 2]
```

```
  description Link to Compact Switch port 2
!
interface range [interface type] [port 1], [interface type]
[port 2]
  switchport
  macro apply EgressQoS
  channel-protocol lacp
  channel-group [number] mode active
  logging event link-status
  logging event trunk-status
  logging event bundle-status
```

**Step 2:** Configure the trunk. Use an 802.1Q trunk for the connection to the compact switch. This allows it to provide connectivity for all the VLANs defined on the access layer switch. Prune the VLANs allowed on the trunk to only those that are required. Set DHCP snooping and ARP inspection to trust. When using EtherChannel, the interface type will be "port-channel," and the number must match the channel-group configured in Step 1.

The Cisco Catalyst 2960-S and 4500 do not require the **switchport trunk encapsulation dot1q** command.

```
interface [port-channel] [number]
  description EtherChannel Link to Compact Switch
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan [data vlan],[voice vlan],[mgmt
vlan]
  switchport trunk native vlan 999
  switchport mode trunk
  ip arp inspection trust
  ip dhcp snooping trust
  logging event link-status
  no shutdown
```

### Example

```
interface GigabitEthernet 1/0/24
  description Link to Compact Switch port 1
interface GigabitEthernet 2/0/24
  description Link to Compact Switch port 2
interface range GigabitEthernet 1/0/24, GigabitEthernet 2/0/24
```

```

macro apply EgressQoS
logging event link-status
logging event trunk-status
logging event bundle-status
channel-protocol lacp
channel-group 7 mode active
no shutdown
!
interface Port-channel 7
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 100,101,115
switchport mode trunk
ip arp inspection trust
ip dhcp snooping trust
no shutdown

```

## Process

### Setting Up the Compact Switch

1. Configure the platform
2. Configure the LAN switch
3. Configure Layer 2 and Layer 3 setup
4. Configure client connections
5. Configure connection to upstream switch

The following procedures assume that:

- You have connected a console terminal to the console port of the Cisco Catalyst compact access switch you are deploying. Set the console for 9600 baud, Async, 8 databits, no parity.
- You have connected the uplink ports of the compact switch to the ports on the access layer switches, which you configured as trunk and port channel in the previous process.

- The Cisco Catalyst Compact Switch is automatically powered by using the PoE power from the access-layer switch. If you are not sourcing power by this method, you have connected power to the Cisco Catalyst Compact Switch.

The previous process allows the port channel to come up when you complete the configuration in this process.

## Procedure 1 Configure the platform

**Step 1:** After the compact switch completes loading, cancel the initial system configuration dialogue, enter enable mode, and then enter configuration mode.

**Step 2:** Create two QoS macros, one to be used for edge ports facing end hosts and the other to be applied to the uplinks for egress traffic, by entering the following sequence of commands.

```

macro name AccessEdgeQoS
  auto qos voip cisco-phone
@
!
macro name EgressQoS
  mls qos trust dscp
  queue-set 1
  srr-queue bandwidth share 1 30 35 5
  priority-queue out
@

```

## Procedure 2 Configure the LAN switch

Within this design, there are features and services that are common across all LAN switches, regardless of the type of platform or role in the network. These are system settings that simplify and secure the management of the solution.

This procedure provides examples for some of those settings. The actual settings and values depend on your current network configuration.

Table 2 - Common network services used in the deployment examples

Setting	Value
Domain name	cisco.local
Active Directory, DNS, DHCP server	10.4.48.10
Authentication Control System	10.4.48.15
Network Time Protocol server	10.4.48.17

**Step 1:** Configure the device hostname. This makes it easy to identify the device.

```
hostname [hostname]
```

**Step 2:** If the switch VTP mode has been changed from the default, configure VTP transparent mode. This deployment uses VTP transparent mode because the benefits of dynamic propagation of VLAN information across the network are not worth the potential for unexpected behavior that is due to operational error.

VLAN Trunking Protocol (VTP) allows network managers to configure a VLAN in one location of the network and have that configuration dynamically propagate out to other network devices. However, in most cases, VLANs are defined once during switch setup with few, if any, additional modifications.

```
ntp mode transparent
```

**Step 3:** Enable Rapid Per-VLAN Spanning-Tree (PVST+). PVST+ provides an instance of Rapid Spanning Tree Protocol (RSTP) (802.1w) per VLAN. Rapid PVST+ greatly improves the detection of indirect failures or linkup restoration events over classic spanning tree (802.1D).

Although this architecture is built without any Layer 2 loops, you must still enable spanning tree. By enabling spanning tree, you ensure that if any physical or logical loops are accidentally configured, no actual layer 2 loops occur.

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

**Step 4:** Enable Unidirectional Link Detection (UDLD) as the default for fiber ports.

UDLD is a Layer 2 protocol that enables devices connected through fiber-optic or twisted-pair Ethernet cables to monitor the physical configuration of the cables and detect when a unidirectional link exists. When UDLD detects a unidirectional link, it disables the affected interface and alerts you.

Unidirectional links can cause a variety of problems, including spanning-tree loops, black holes, and non-deterministic 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 enable
```

**Step 5:** Set EtherChannels to use the traffic source and destination IP address when calculating which link to send the traffic across. This normalizes the method in which traffic is load-shared across the member links of the EtherChannel. EtherChannels are used extensively in this design because of their resiliency capabilities.

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

**Step 6:** Configure DNS for host lookup.

At the command line of a Cisco IOS device, it is helpful to be able to type a domain name instead of the IP address for a destination.

```
ip name-server 10.4.48.10
```

**Step 7:** Configure device management protocols.

Secure HTTP (HTTPS) and Secure Shell (SSH) are more secure replacements for the HTTP and Telnet protocols. They use Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to provide device authentication and data encryption.

The SSH and HTTPS protocols enable secure management of the LAN device. Both protocols are encrypted for privacy, and the unencrypted protocols, Telnet and HTTP, are turned off.

Specify the **transport preferred none** on vty lines to prevent errant connection attempts from the CLI prompt. Without this command, if the ip name-server is unreachable, long timeout delays may occur for mistyped commands.

```
ip domain-name cisco.local
ip ssh version 2
no ip http server
ip http secure-server
line vty 0 15
  transport input ssh
  transport preferred none
```

**Step 8:** Enable Simple Network Management Protocol (SNMP) in order to allow the network infrastructure devices to be managed by a Network Management System (NMS), and then configure SNMPv2c both for a read-only and a read-write community string.

```
snmp-server community cisco RO
snmp-server community cisco123 RW
```

**Step 9:** In networks where network operational support is centralized, you can increase network security by using an access list to limit the networks that can access your device. In this example, only devices on the 10.4.48.0/24 network are able to access the device via SSH or SNMP.

```
access-list 55 permit 10.4.48.0 0.0.0.255
line vty 0 15
access-class 55 in
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
```



### Caution

If you configure an access-list on the vty interface, you may lose the ability to use ssh to log in from one device to the next for hop-by-hop troubleshooting.

**Step 10:** Configure local login and password.

The local login account and password provides basic device access authentication to view platform operation. The enable password secures access to the device configuration mode. By enabling password encryption, you prevent the use of plain text passwords when viewing configuration files.

```
username admin password cisco123
enable secret cisco123
service password-encryption
aaa new-model
```

By default, https access to the switch uses the enable password for authentication.

**Step 11:** If you want to reduce operational tasks per device, configure centralized user authentication by using the TACACS+ protocol to authenticate management logins on the infrastructure devices to the authentication, authorization and accounting (AAA) server.

As networks scale in the number of devices to maintain, there is an operational burden to maintain local user accounts on every device. A centralized AAA service reduces operational tasks per 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 AAA.

TACACS+ is the primary protocol used to authenticate management logins on the infrastructure devices to the AAA server. A local AAA user database is also defined on each network infrastructure device to provide a fallback authentication source in case the centralized TACACS+ server is unavailable.

```
tacacs server TACACS-SERVER-1
address ipv4 10.4.48.15
key SecretKey
!
aaa group server tacacs+ TACACS-SERVERS
server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization exec default group TACACS-SERVERS local
aaa authorization console
ip http authentication aaa
```



### Reader Tip

The AAA server used in this architecture is the Cisco Authentication Control System. Configuration of ACS is discussed in the *Cisco SBA—Borderless Networks Device Management Using ACS Deployment Guide*.

**Step 12:** Configure a synchronized clock by programming 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. Configure console messages, logs, and debug output to provide time stamps on output, which allows cross-referencing of events in a network.

```
ntp server 10.4.48.17
!
clock timezone PST -8
clock summer-time PDT recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

### Procedure 3 Configure Layer 2 and Layer 3 setup

The access layer devices use VLANs to separate traffic from different devices into three logical networks:

- The data VLAN provides access to the network for all attached devices other than IP phones. This network is configured on all user-facing interfaces.
- The voice VLAN provides access to the network for IP phones. This network is configured on all user-facing interfaces.
- The management VLAN provides in-band access to the network for the switches' management interface. The management VLAN is not configured on any user-facing interface, and the VLAN interface of the switch is the only member.

**Step 1:** Configure the data, voice, and management VLANs on the switch so connectivity to clients, IP phones, and the in-band management interfaces can be configured. You will extend the VLANs from the active upstream Access Layer switch.

```
vlan [data vlan]
name Data
vlan [voice vlan]
name Voice
vlan [management vlan]
name Management
```

**Step 2:** Configure the switch with an IP address so that it can be managed via in-band connectivity.

```
interface vlan [management vlan]
ip address [ip address] [mask]
no shutdown
ip default-gateway [default router]
```

**Step 3:** Configure DHCP snooping and enable it on the data and voice VLANs. The switch intercepts and safeguards DHCP messages within the VLAN. This ensures that an unauthorized DHCP server cannot serve up addresses to end-user devices.

```
ip dhcp snooping vlan [data vlan],[voice vlan]
no ip dhcp snooping information option
ip dhcp snooping
```

**Step 4:** Configure ARP inspection on the data and voice VLANs.

```
ip arp inspection vlan [data vlan],[voice vlan]
```

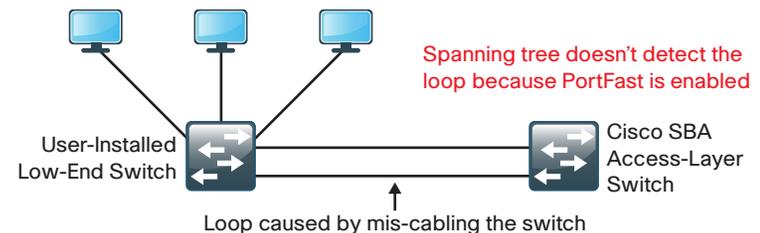
**Step 5:** Configure BPDU Guard globally. This protects PortFast-enabled interfaces by disabling the port if another switch is plugged into the port.

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

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

If a 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 PortFast is enabled.

Figure 5 - Scenario that BPDU guard protects against



## Procedure 4

### Configure client connections

To make configuration easier when the same configuration will be applied to 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 at the same time. Because most of the interfaces in the access layer are configured identically, it can save a lot of time. For example, the following command allows you to enter commands on all eight interfaces (Gig 0/1 to Gig 0/8) simultaneously.

```
interface range GigabitEthernet 0/1-8
```

**Step 1:** Configure switch interfaces to support clients and IP phones.

The host interface configurations support PCs, phones, or wireless access points. Inline power is available on switches that support 802.3AF/AT for capable devices.

```
interface range [interface type] [port number]-[port number]
  switchport access vlan [data vlan]
  switchport voice vlan [voice vlan]
```

**Step 2:** Because only end-device connectivity is provided at the access layer, enable PortFast. PortFast shortens the time it takes for the interface to go into a forwarding state by disabling 802.1q trunking and channel group negotiation.

```
switchport host
```

**Step 3:** Enable QoS by applying the access edge QoS macro that was defined in the platform configuration procedure.

```
macro apply AccessEdgeQoS
```

All client-facing interfaces allow for an untrusted PC and/or a trusted Cisco IP Phone to be connected to the switch and automatically set QoS parameters. When a Cisco Phone is connected, trust is extended to the phone. Any device that connects to the Cisco phone is considered untrusted, and all traffic from that device is remarked to best-effort or class of service (CoS) of 0.

Next, configure port security on the interface.

**Step 4:** Configure 11 MAC addresses to be active on the interface at one time; additional MAC addresses are considered to be in violation, and their traffic will be dropped.

```
switchport port-security maximum 11
switchport port-security
```

The number of MAC addresses allowed on each interface is specific to the organization. However, the popularity of virtualization applications, IP phones, and passive hubs on the desktop drives the need for the number to be larger than one might guess at first glance. This design uses a number that allows flexibility in the organization while still protecting the network infrastructure.

**Step 5:** Set an aging time to remove learned MAC addresses from the secured list after two minutes of inactivity.

```
switchport port-security aging time 2
switchport port-security aging type inactivity
```

**Step 6:** Configure the restrict option to drop traffic from MAC addresses that are in violation, but do not shut down the port. This configuration ensures that an IP phone can still function on this interface when there is a port security violation.

```
switchport port-security violation restrict
```

**Step 7:** Configure DHCP snooping and ARP inspection on the interface to process 100 packets per second of traffic on the port.

```
ip arp inspection limit rate 100
ip dhcp snooping limit rate 100
```

**Step 8:** Configure IP Source Guard on the interface.

```
ip verify source
```

### Example



```

vlan 100
  name Data
vlan 101
  name Voice
vlan 115
  name Management
!
interface Vlan 115
  description in-band management
  ip address 10.4.15.7 255.255.255.0
  no shutdown
!
ip default-gateway 10.4.15.1
!
ip dhcp snooping vlan 100,101
no ip dhcp snooping information option
ip dhcp snooping
ip arp inspection vlan 100,101
!
interface range GigabitEthernet 0/1-8
  switchport access vlan 100
  switchport voice vlan 101
  switchport host
  macro apply AccessEdgeQoS
  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 dhcp snooping limit rate 100
  ip verify source

```

### Procedure 5 Configure connection to upstream switch

This procedure details how to configure the links from the compact switch to the upstream access layer switch.



### Tech Tip

The configuration steps to be applied to the compact switch for creating the upstream trunk and port channel are identical to the steps used earlier on the access switch. They are reiterated here for context clarity.

Configure the physical interfaces that are members of a Layer 2 EtherChannel prior to configuring the logical port-channel interface. This sequence allows for minimal configuration because most of the commands entered to a port-channel interface are copied to its members interfaces and do not require manual replication.

**Step 1:** Configure the EtherChannel member interface.

Set Link Aggregation Control Protocol (LACP) negotiation to active on both sides to ensure a proper EtherChannel is formed. Also, apply the egress QoS macro that was defined in Procedure 1, “Configure the platform,” to ensure traffic is prioritized appropriately.

The Cisco Catalyst 2960C switch does not require the **switchport** command.

```

interface [interface type] [port 1]
  description Link to Upstream Switch port 1
interface [interface type] [port 2]
  description Link to Upstream Switch port 2
!
interface range [interface type] [port 1], [interface type]
[port 2]
  switchport
  macro apply EgressQoS
  channel-protocol lacp
  channel-group [number] mode active
  logging event link-status
  logging event trunk-status
  logging event bundle-status

```

## Step 2: Configure the trunk.

An 802.1Q trunk is used for the connection to this upstream device, which allows the uplink to provide Layer 3 services to all the VLANs defined on the access layer switch. Prune the VLANs allowed on the trunk to only the VLANs that are active on the access switch. Set DHCP snooping and ARP inspection to trust. When using EtherChannel, the interface type is port-channel, and the number must match the channel-group configured in Step 1.

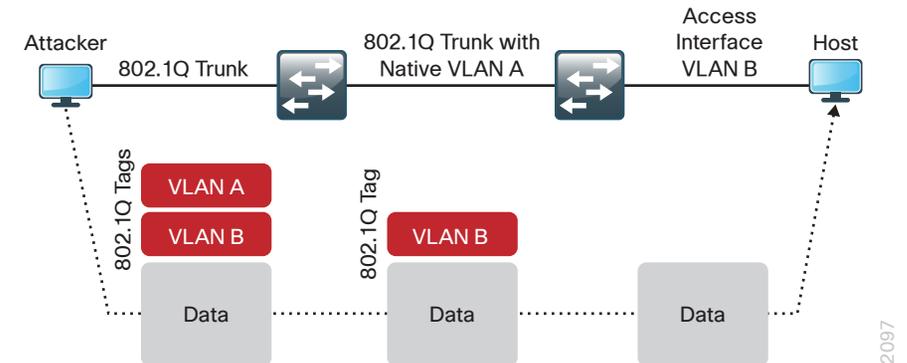
The Cisco Catalyst 2960C switch does not require the `switchport trunk encapsulation dot1q` command.

```
interface [port-channel] [number]
  description EtherChannel Link to Upstream Switch
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan [data vlan],[voice vlan], [mgmt
vlan]
  switchport mode trunk
  ip arp inspection trust
  ip dhcp snooping trust
  logging event link-status
  no shutdown
```

Next, mitigate VLAN hopping on the trunk.

There is a remote possibility that an attacker can create a double 802.1Q encapsulated packet. If the attacker has specific knowledge of the 802.1Q native VLAN, a packet could be crafted that when processed, the first or outermost tag is removed when the packet is switched onto the untagged native VLAN. When the packet reaches the target switch, the inner or second tag is then processed and the potentially malicious packet is switched to the target VLAN.

Figure 6 - VLAN hopping attack



At first glance, this appears to be a serious risk. However, the traffic in this attack scenario is in a single direction and no return traffic can be switched by this mechanism. Additionally, this attack cannot work unless the attacker knows the native VLAN ID.

**Step 3:** If you want to remove the remote risk of this type of attack, configure an unused VLAN on all switch-to-switch 802.1Q trunk links from access layer to distribution layer. Choosing an arbitrary, non-default, unused VLAN assignment for the native VLAN reduces the possibility that a double 802.1Q-tagged packet can hop VLANs. If you are running the recommended EtherChannel uplink to the LAN access layer switch, configure the `switchport trunk native vlan` on the port-channel interface.

```
Vlan 999
!
interface [interface type] [number]
  switchport trunk native vlan 999
```

**Step 4:** If you used the QoS macros, the default queue should be tuned by increasing the buffers. This improves the queue's ability to handle high-bandwidth, bursty traffic.

```
mls qos queue-set output 1 threshold 3 100 100 100 3200
```

**Step 5:** Save the running configuration that you have entered so it will be used as the startup configuration file when your switch is reloaded or power-cycled.

```
copy running-config startup-config
```

## Example

```
interface GigabitEthernet 0/9
  description Link to Upstream Switch port 1
interface GigabitEthernet 0/10
  description Link to Upstream Switch port 2
!
interface range GigabitEthernet 0/9, GigabitEthernet 0/10
  macro apply EgressQoS
  logging event link-status
  logging event trunk-status
  logging event bundle-status
  channel-protocol lacp
  channel-group 2 mode active
  no shutdown
!
interface Port-channel 2
  description EtherChannel Link to Upstream Switch
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 999
  switchport trunk allowed vlan 100,101,115
  switchport mode trunk
  ip arp inspection trust
  ip dhcp snooping trust
  no shutdown
```

## Notes

# Appendix A: Product List

## Extended LAN Access Layer

Functional Area	Product Description	Part Numbers	Software
Compact Switch	Cisco Catalyst Compact 3560 Switch - 8 GE PoE and 2 x 1GE copper uplink ports	WS-C3560CPD-8PT-S	15.0(2)SE IP Base license

## LAN Access Layer

Functional Area	Product Description	Part Numbers	Software
Modular Access Layer Switch	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.3.0.SG(15.1-1SG) IP Base license
	Cisco Catalyst 4500 E-Series Supervisor Engine 7L-E	WS-X45-SUP7L-E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+ ports	WS-X4648-RJ45V+E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+,UPoE ports	WS-X4748-UPOE+E	
Stackable Access Layer Switch	Cisco Catalyst 3750-X Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-48PF-S	15.0(2)SE IP Base license
	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-24P-S	
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	
Standalone Access Layer Switch	Cisco Catalyst 3560-X Series Standalone 48 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-48PF-S	15.0(2)SE IP Base license
	Cisco Catalyst 3560-X Series Standalone 24 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-24P-S	
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	

Functional Area	Product Description	Part Numbers	Software
Stackable Access Layer Switch	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-48FPD-L	15.0(2)SE LAN Base license
	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-48FPS-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-24PD-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-24PS-L	
	Cisco Catalyst 2960-S Series Flexstack Stack Module	C2960S-STACK	

# Appendix B: Configuration Example

```
version 15.0
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname A3560CPD
!
boot-start-marker
boot-end-marker
!
enable secret 4 /DtCCr53Q4B18jsIm1UEqu7cNVZTOhxTZyUnZdsSrsW
!
username admin password 7 121A540411045D5679
aaa new-model
!
aaa group server tacacs+ TACACS-SERVERS
  server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PDT recurring
system mtu routing 1500
ip arp inspection vlan 100-101
!
ip dhcp snooping vlan 100-101
no ip dhcp snooping information option
ip dhcp snooping
```

```
ip domain-name cisco.local
ip name-server 10.4.48.10
vtp mode transparent
udld enable
!
mls qos map policed-dscp 0 10 18 24 46 to 8
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue output cos-map queue 1 threshold 3 4 5
mls qos srr-queue output cos-map queue 2 threshold 1 2
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 0
mls qos srr-queue output cos-map queue 4 threshold 3 1
mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40 41
42 43 44 45
mls qos srr-queue output dscp-map queue 1 threshold 3 46 47
mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18 19
20 21 22 23
mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28 29
30 31 34 35
mls qos srr-queue output dscp-map queue 2 threshold 1 36 37 38 39
mls qos srr-queue output dscp-map queue 2 threshold 2 24
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51
52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59
60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3 4 5
6 7
mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11 13
15
mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
mls qos queue-set output 1 threshold 1 100 100 50 200
```

```

mls qos queue-set output 1 threshold 2 125 125 100 400
mls qos queue-set output 1 threshold 3 100 100 100 3200
mls qos queue-set output 1 threshold 4 60 150 50 200
mls qos queue-set output 1 buffers 15 25 40 20
mls qos
!
crypto pki trustpoint TP-self-signed-1311523712
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-1311523712
  revocation-check none
  rsakeypair TP-self-signed-1311523712
!
crypto pki certificate chain TP-self-signed-1311523712
  certificate self-signed 02
    3082022B 30820194 A0030201 02020102 300D0609 2A864886 F70D0101
05050030
    31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D
43657274
    69666963 6174652D 31333131 35323337 3132301E 170D3933 30333031
30303432
    33315A17 0D323030 31303130 30303030 305A3031 312F302D 06035504
03132649
    4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31
33313135
    32333731 3230819F 300D0609 2A864886 F70D0101 01050003 818D0030
81890281
    8100D7D9 ACFC0888 FC89CDFE 56AD5AC7 01E31D50 1E8B6256 47BF6C3B
983AE1E4
    49D69C0F A4854B6A 57FCAECD 53F22841 5092E7CF 63F00949 F68C5BB6
FD8C87FB
    146E5620 397D6E11 9F2A9CBA 0A984601 E15822D9 734B6ED6 74127AEE
D67667EB
    8C99EC1B 7063A9D5 8C5A6DA3 3D842C8D E37427A9 FD87E5B8 1B4022E3
0A347A27
    610B0203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF
301F0603
    551D2304 18301680 14067B4A BC7105C1 F775A42F F7FB6E52 75304E1B

```

```

6B301D06
03551D0E 04160414 067B4ABC 7105C1F7 75A42FF7 FB6E5275 304E1B6B
300D0609
2A864886 F70D0101 05050003 81810073 D66B7E76 3F8C6860 C9B21E79
075BE4D3
ADD8B597 3A7ABF96 3B020001 D747158A 60C823EB EA83CCA9 A55A7AB6
F8CB7319
A58D50ED 93B28D19 467730DA B775FFDF C3850E98 65DD5124 F9A0186F
8195FF23
66F5E9D4 BAD5B9A9 16DB8F4A 42061B5B F60665B6 AAB9F9C0 0B8A6FFA
E3D94855
36EF29AA 10A03B83 B083FF9D D2E27B
quit
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
port-channel load-balance src-dst-ip
!
vlan internal allocation policy ascending
!
vlan 100
  name Data
!
vlan 101
  name Voice
!
vlan 115
  name Management
!
vlan 999
!
ip ssh version 2
!
class-map match-all AUTOQOS_VOIP_DATA_CLASS
  match ip dscp ef
class-map match-all AUTOQOS_DEFAULT_CLASS

```

```

    match access-group name AUTOQOS-ACL-DEFAULT
class-map match-all AUTOQOS_VOIP_SIGNAL_CLASS
    match ip dscp cs3
!
policy-map AUTOQOS-SRND4-CISCOPHONE-POLICY
    class AUTOQOS_VOIP_DATA_CLASS
        set dscp ef
        police 128000 8000 exceed-action policed-dscp-transmit
    class AUTOQOS_VOIP_SIGNAL_CLASS
        set dscp cs3
        police 32000 8000 exceed-action policed-dscp-transmit
    class AUTOQOS_DEFAULT_CLASS
        set dscp default
        police 10000000 8000 exceed-action policed-dscp-transmit
!
macro name AccessEdgeQoS
    auto qos voip cisco-phone
@
macro name EgressQoS
    mls qos trust dscp
    queue-set 1
    srr-queue bandwidth share 1 30 35 5
    priority-queue out
@
!
interface Port-channel2
    description EtherChannel Link to Upstream Switch
    switchport trunk encapsulation dot1q
    switchport trunk native vlan 999
    switchport trunk allowed vlan 100,101,115
    switchport mode trunk
    ip arp inspection trust
    ip dhcp snooping trust
!
interface GigabitEthernet0/1
    switchport access vlan 100
    switchport mode access

```

```

    switchport voice vlan 101
    switchport port-security maximum 11
    switchport port-security
    switchport port-security aging time 2
    switchport port-security violation restrict
    switchport port-security aging type inactivity
    ip arp inspection limit rate 100
    srr-queue bandwidth share 1 30 35 5
    priority-queue out
    mls qos trust device cisco-phone
    mls qos trust cos
    macro description AccessEdgeQoS
    auto qos voip cisco-phone
    spanning-tree portfast
    service-policy input AUTOQOS-SRND4-CISCOPHONE-POLICY
    ip verify source
    ip dhcp snooping limit rate 100
!
interface GigabitEthernet0/2
    switchport access vlan 100
    switchport mode access
    switchport voice vlan 101
    switchport port-security maximum 11
    switchport port-security
    switchport port-security aging time 2
    switchport port-security violation restrict
    switchport port-security aging type inactivity
    ip arp inspection limit rate 100
    srr-queue bandwidth share 1 30 35 5
    priority-queue out
    mls qos trust device cisco-phone
    mls qos trust cos
    macro description AccessEdgeQoS
    auto qos voip cisco-phone
    spanning-tree portfast
    service-policy input AUTOQOS-SRND4-CISCOPHONE-POLICY
    ip verify source

```

```

ip dhcp snooping limit rate 100
!
interface GigabitEthernet0/3
  switchport access vlan 100
  switchport mode access
  switchport voice vlan 101
  switchport port-security maximum 11
  switchport port-security
  switchport port-security aging time 2
  switchport port-security violation restrict
  switchport port-security aging type inactivity
  ip arp inspection limit rate 100
  srr-queue bandwidth share 1 30 35 5
  priority-queue out
  mls qos trust device cisco-phone
  mls qos trust cos
  macro description AccessEdgeQoS
  auto qos voip cisco-phone
  spanning-tree portfast
  service-policy input AUTOQOS-SRND4-CISCOPHONE-POLICY
  ip verify source
  ip dhcp snooping limit rate 100
!
interface GigabitEthernet0/4
  switchport access vlan 100
  switchport mode access
  switchport voice vlan 101
  switchport port-security maximum 11
  switchport port-security
  switchport port-security aging time 2
  switchport port-security violation restrict
  switchport port-security aging type inactivity
  ip arp inspection limit rate 100
  srr-queue bandwidth share 1 30 35 5
  priority-queue out
  mls qos trust device cisco-phone
  mls qos trust cos

```

```

macro description AccessEdgeQoS
auto qos voip cisco-phone
spanning-tree portfast
service-policy input AUTOQOS-SRND4-CISCOPHONE-POLICY
ip verify source
ip dhcp snooping limit rate 100
!
interface GigabitEthernet0/5
  switchport access vlan 100
  switchport mode access
  switchport voice vlan 101
  switchport port-security maximum 11
  switchport port-security
  switchport port-security aging time 2
  switchport port-security violation restrict
  switchport port-security aging type inactivity
  ip arp inspection limit rate 100
  srr-queue bandwidth share 1 30 35 5
  priority-queue out
  mls qos trust device cisco-phone
  mls qos trust cos
  macro description AccessEdgeQoS
  auto qos voip cisco-phone
  spanning-tree portfast
  service-policy input AUTOQOS-SRND4-CISCOPHONE-POLICY
  ip verify source
  ip dhcp snooping limit rate 100
!
interface GigabitEthernet0/6
  switchport access vlan 100
  switchport mode access
  switchport voice vlan 101
  switchport port-security maximum 11
  switchport port-security
  switchport port-security aging time 2
  switchport port-security violation restrict
  switchport port-security aging type inactivity

```

```

ip arp inspection limit rate 100
srr-queue bandwidth share 1 30 35 5
priority-queue out
mls qos trust device cisco-phone
mls qos trust cos
macro description AccessEdgeQoS
auto qos voip cisco-phone
spanning-tree portfast
service-policy input AUTOQOS-SRND4-CISCOPHONE-POLICY
ip verify source
ip dhcp snooping limit rate 100
!
interface GigabitEthernet0/7
switchport access vlan 100
switchport mode access
switchport voice vlan 101
switchport port-security maximum 11
switchport port-security
switchport port-security aging time 2
switchport port-security violation restrict
switchport port-security aging type inactivity
ip arp inspection limit rate 100
srr-queue bandwidth share 1 30 35 5
priority-queue out
mls qos trust device cisco-phone
mls qos trust cos
macro description AccessEdgeQoS
auto qos voip cisco-phone
spanning-tree portfast
service-policy input AUTOQOS-SRND4-CISCOPHONE-POLICY
ip verify source
ip dhcp snooping limit rate 100
!
interface GigabitEthernet0/8
switchport access vlan 100
switchport mode access
switchport voice vlan 101

switchport port-security maximum 11
switchport port-security
switchport port-security aging time 2
switchport port-security violation restrict
switchport port-security aging type inactivity
ip arp inspection limit rate 100
srr-queue bandwidth share 1 30 35 5
priority-queue out
mls qos trust device cisco-phone
mls qos trust cos
macro description AccessEdgeQoS
auto qos voip cisco-phone
spanning-tree portfast
service-policy input AUTOQOS-SRND4-CISCOPHONE-POLICY
ip verify source
ip dhcp snooping limit rate 100
!
interface GigabitEthernet0/9
description Link to Upstream Switch port 1
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 100,101,115
switchport mode trunk
ip arp inspection trust
logging event link-status
logging event trunk-status
logging event bundle-status
srr-queue bandwidth share 1 30 35 5
priority-queue out
mls qos trust dscp
macro description EgressQoS
channel-protocol lacp
channel-group 2 mode active
ip dhcp snooping trust
!
interface GigabitEthernet0/10
description Link to Upstream Switch port 2

```

```

switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 100,101,115
switchport mode trunk
ip arp inspection trust
logging event link-status
logging event trunk-status
logging event bundle-status
srr-queue bandwidth share 1 30 35 5
priority-queue out
mls qos trust dscp
macro description EgressQoS
channel-protocol lacp
channel-group 2 mode active
ip dhcp snooping trust
!
interface Vlan1
no ip address
shutdown
!
interface Vlan115
description in-band management
ip address 10.4.15.7 255.255.255.128
!
ip default-gateway 10.4.15.1
no ip http server
ip http authentication aaa
ip http secure-server
!
ip access-list extended AUTOQOS-ACL-DEFAULT
permit ip any any
!
access-list 55 permit 10.4.48.0 0.0.0.255
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
tacacs server TACACS-SERVER-1

```

```

address ipv4 10.4.48.15
key 7 13361211190910012E3D
!
line con 0
line vty 0 4
access-class 55 in
length 0
transport preferred none
transport input ssh
line vty 5 15
access-class 55 in
transport preferred none
transport input ssh
!
ntp server 10.4.48.17
end

```

# Appendix C: Changes

This appendix summarizes the changes to this guide since the previous Cisco SBA series.

- We upgraded the device software versions and hardware model. For specific version and model information, see “Appendix A: Product List” in this guide.
- We updated the centralized user authentication template to the newer method that allows IPv4 and IPv6 TACACS+ server definition. The older method will be deprecated from Cisco IOS over time.
- We added information describing powering the Cisco Catalyst Compact Switch by using Cisco UPOE.

## Notes

## Feedback

Please use the [feedback form](#) to send comments and suggestions about this guide.



## SMART BUSINESS ARCHITECTURE



**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV Amsterdam,  
The Netherlands

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](http://www.cisco.com/go/offices).

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT 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 THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

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

© 2013 Cisco Systems, Inc. All rights reserved.

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](http://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)