Newer Cisco SBA for Government Guides Available

This guide is part of an older series of Cisco Smart Business Architecture for Government. To access the latest Cisco SBA for Government Guides, go to http://www.cisco.com/go/govsba

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new 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.

SBA FOR GOVT

MIDSIZE

BORDERLESS NETWORKS

Modular Access Layer Deployment Guide

SBA FOR GOVERNMENT

Revision: H2CY10

The Purpose of this Document

This guide will prepare you to deploy a modular access layer switch. It will explain:

- Why an agency might wish to use a modular switch in the access layer
- Cisco Smart Business Architecture (SBA) for Government product recommendations and the rationale behind the recommendation
- How to deploy a Modular Access Layer Switch

Who Should Read This Guide

This guide is intended for the reader with any or all of the following:

- 100-1000 connected employees
- Up to 20 branches with approximately 25 employees each
- External-facing applications, which are hosted offsite
- A server room containing agency applications
- IT workers with a CCNA® certification or equivalent experience

The reader may require:

- Wiring closets with 96 or more ports
- Power over Ethernet Plus(PoEP) support for devices requiring more than 20 watts per port
- High availability option and hitless software upgrades
- Extended product lifecycle investment protection

Related Documents

Before reading this guide

BN Foundation Deployment Guide

BN Foundation Configuration Guide

DC Data Center Deployment Guide

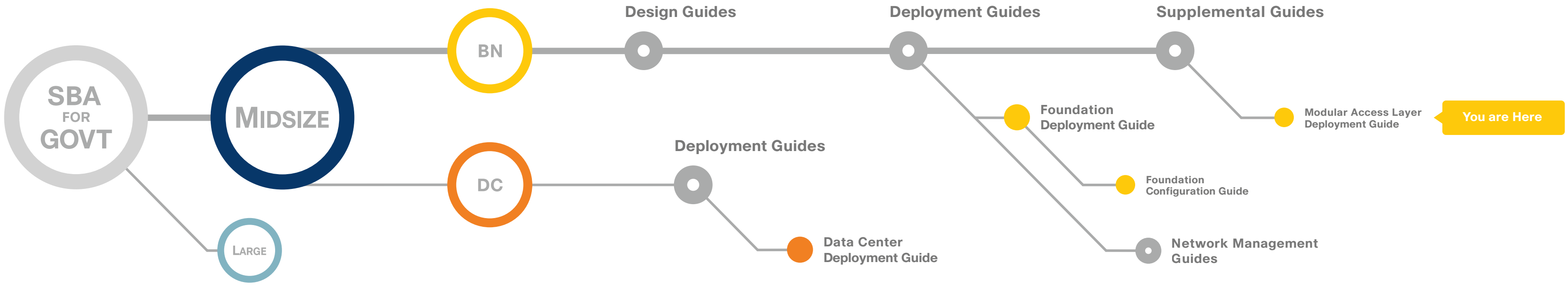

SBA FOR GOVT
MIDSIZE
LARGE
BN
DC
Design Guides
Deployment Guides
Supplemental Guides
Foundation Deployment Guide
Foundation Configuration Guide
Network Management Guides
Modular Access Layer Deployment Guide
You are Here
Deployment Guides
Data Center Deployment Guide

Table of Contents

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 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 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. Cisco Unified Communications SRND (Based on Cisco Unified Communications Manager 7.x)

Introduction

The Cisco® SBA is a comprehensive design for networks with up to 1000 users. This out-of-the-box design is simple, fast, affordable, scalable, and flexible.

The Cisco SBA for Midsize Agencies incorporates LAN, WAN, wireless, security, WAN optimization, and unified communication technologies tested together as a solution. This solution-level approach simplifies the system integration normally associated with multiple technologies, allowing you to select the modules that solve your agency's problems rather than worrying about the technical details.

We have designed the Cisco SBA to be easy to configure, deploy, and manage. This architecture:

- Provides a solid network foundation
- Makes deployment fast and easy
- Accelerates ability to easily deploy additional services
- Avoids the need for re-engineering of the core network

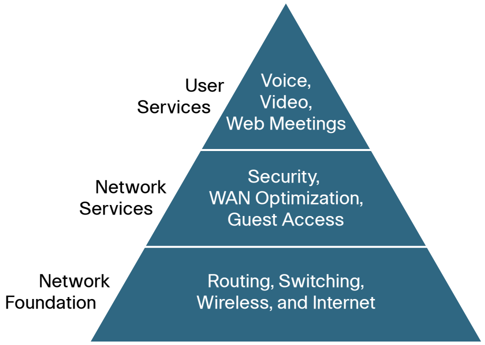
By deploying the Cisco SBA, your agency can gain:

- A standardized design, tested and supported by Cisco
- Optimized architecture for midsize agencies with up to 1000 users and up to 20 branches
- Flexible architecture to help ensure easy migration as the agency grows
- Seamless support for quick deployment of wired and wireless network access for data, voice, teleworker, and wireless guest
- Security and high availability for agency information resources, servers, and Internet-facing applications
- Improved WAN performance and cost reduction through the use of WAN optimization
- Simplified deployment and operation by IT workers with CCNA® certification or equivalent experience
- Cisco enterprise-class reliability in products designed for midsize agencies

Guiding Principles

We divided the deployment process into modules according to the following principles:

- **Ease of use:** A top requirement of Cisco SBA was to develop a design that could be deployed with the minimal amount of configuration and day-two management.
- **Cost-effective:** Another critical requirement as we selected products was to meet the budget guidelines for midsize agencies.
- **Flexibility and scalability:** As the agency grows, so too must its infrastructure. Products selected must have the ability to grow or be repurposed within the architecture.
- **Reuse:** We strived, when possible, to reuse the same products throughout the various modules to minimize the number of products required for spares.


User Services
Voice, Video, Web Meetings
Network Services
Security, WAN Optimization, Guest Access
Network Foundation
Routing, Switching, Wireless, and Internet

The Cisco SBA can be broken down into the following three primary, modular yet interdependent components for the midsize agency.

- **Network Foundation:** A network that supports the architecture
- **Network Services:** Features that operate in the background to improve and enable the user experience without direct user awareness
- **User Services:** Applications with which a user interacts directly

Agency Overview

The Cisco SBA for Midsize Agencies is a prescriptive architecture that delivers an easy-to-use, flexible, and scalable network with wired, wireless, security, wide-area network (WAN) optimization, and unified communication components. It eliminates the challenges of integrating the various network components by using a standardized design that is reliable with comprehensive support offerings.

As part of the SBA, Cisco recommends the following switches:

- Cisco® Catalyst 4500 E-Series as the switching platform for the access layer of the network
- Cisco Catalyst 3750 and Cisco Catalyst 3560 series of switches

More specifically, the Catalyst 4500 E-Series is the recommended product for access layer designs where the wiring closets require higher port densities with extended investment protection and services.

Figure 1 shows the complete SBA foundation design with all of the modules deployed.

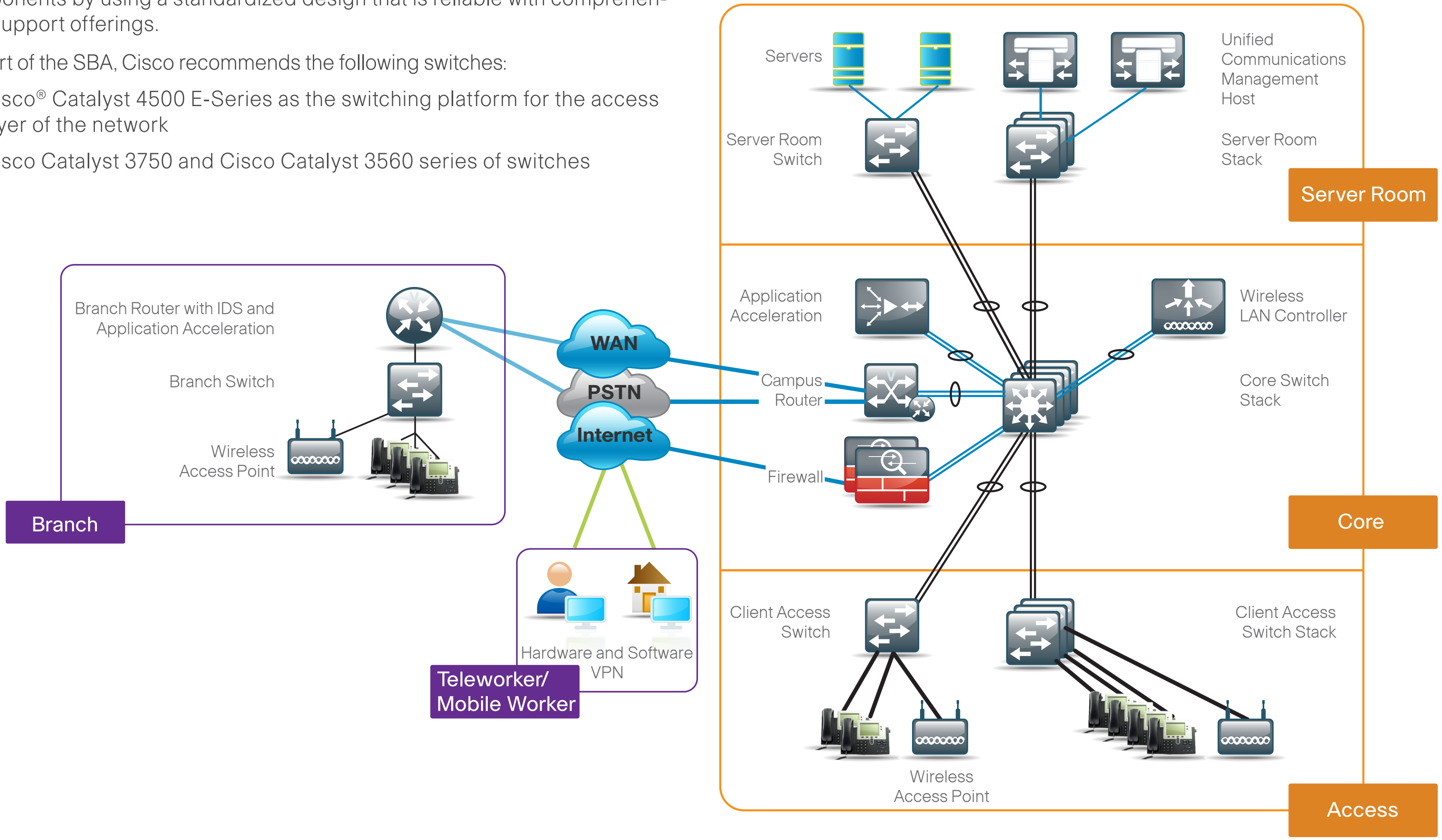


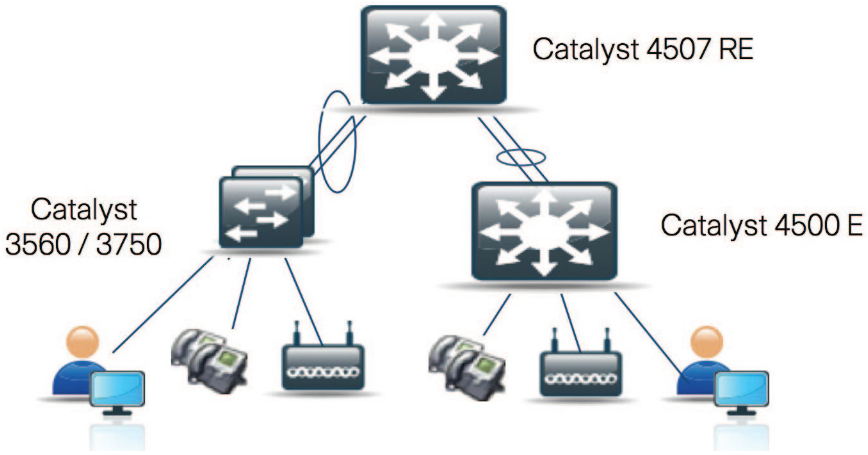
Figure 1. Network Architecture Baseline

Catalyst 4500 Client Access Overview

The Catalyst 4500 E-Series is the recommended product for access layer designs with one or more of the following requirements:

- **Long Lasting Investment Protection:** Agencies that require 5+ years of product lifecycle
- **Port Density:** Wiring closets with 96 ports or greater
- **Enhanced Power Over Ethernet (PoE):** PoE deployments requiring more than 20 watts per port
- **High Availability:** No single-point-of-failure designs, hitless software upgrades

Figure 2. Access Layer



Long-Lasting Investment Protection

The Catalyst 4500 E-Series is designed for long lasting investment protection where products are expected to remain in service well beyond 5 years. This level of investment protection is achieved primarily through:

- A hardware and software design that utilizes centralized switching,
- Forwarding architecture with a passive backplane design,
- A centralized switching and forwarding architecture.

All of the key switching and forwarding components are located on the Supervisor module itself. The line cards in the Catalyst 4500 E-Series are functionally transparent, meaning the line cards have minimal active components.

The passive-backplane design minimizes the active components on the chassis backplane and ensures full 1:1 hardware redundancy for active components.

The design allows future functionality to be added with a simple Supervisor module upgrade, while still maintaining the initial investment with existing chassis common equipment including the line cards. This not only minimizes capital expense, but also a great deal of the operations expense associated with network hardware upgrades.

The original Catalyst 4500 Series started shipping in February 2002. Customers who purchased this chassis still have software maintenance support on this product as of May 2010. Catalyst 4500 Series customers have had the option of upgrading their Supervisor module as the network requirements evolved, all the while maintaining the majority of their investment in the line cards, chassis, and common equipment.

The long-lasting investment protection continues with the Catalyst 4500 E-Series Switches as well. Initially released in November 2007, the Catalyst 4500 E-Series Switches:

- Are fully backward compatible with the traditional Catalyst 4500 Series Supervisor modules and line cards.
- Support new higher-performance E-Series line cards and higher levels of Power over Ethernet.

The new E-series line cards scale performance from 6 Gbps per slot to 24 Gbps per slot. Going forward, the E-Series chassis is capable of supporting even higher-performance line cards when the next generation Supervisor modules are released. Once again, the centralized switching and forwarding architecture with the passive backplane design is the key to the long-lasting investment protection.

The Catalyst 4500 E-Series Supervisor 6L-E provides investment protection in uplink technologies as well.

The Supervisor uplink ports can be configured as Gigabit Ethernet interfaces or 10 Gigabit interfaces, allowing you to increase bandwidth in the future with minimal downtime and operational expense.

The Supervisor 6L-E provides up to four Gigabit Ethernet Small Form-Factor Pluggable (SFP) interfaces. These SFP interfaces are available via two 10 Gigabit Ethernet X2 optic slots populated with TwinGig adapters. The TwinGig adapters convert a single X2 slot into two SFP slots. Note that to enable the interfaces for 10 Gigabit Ethernet, an additional software license is required.

Port Density

For wiring closets that require more than 96 ports of connectivity, the Catalyst 4500 E-Series is the recommended and validated solution. At port densities above 96 ports, the cost differential between the Catalyst 3750 and Catalyst 3560 Switches versus the Catalyst 4500 E-Series becomes less than 10% and the benefits of the Catalyst 4500 E-Series make it the best choice.

IEEE 802.3at Power over Ethernet (PoE)

The newest industry standard for Power over Ethernet is the IEEE 802.3at standard, also known as PoE+, and was ratified in September 2009. The new standard allows for inline power up to 30 watts per port.

The Catalyst 4500 E-Series line cards validated in this Deployment Guide are PoE+ ready, meaning that these line cards support all the previous implementations of PoE up to 20 watts per port, and with a future software upgrade, will support the new IEEE 802.3at implementation up to 30 watts per port.

Now that the standard has been ratified, new end¬point devices requiring the higher power levels will quickly begin to reach the market. Devices such as higher-powered, dual-band, wireless access points, high-definition cameras with enhanced zoom and motion capabilities, powering thin clients and more.

High Availability

Environments where network availability is a critical requirement should deploy a Catalyst 4507R-E chassis or 4510R-E chassis and configure the system with redundant Supervisor modules. Once again, because the Catalyst 4500 E-Series is designed with the centralized forwarding and switching architecture, with all of the key switching and forwarding components located on the Supervisor module, system availability is increased by having all of the critical switching and forwarding components made 1:1 redundant.

The redundant Supervisor model is enhanced further with Cisco IOS® high-availably technologies, including:

- Stateful switchover
- Nonstop forwarding routing protocol extensions
- In-service software upgrades

These technologies synchronize critical information between the two Supervisor modules in an Active and Hot-Standby model. This enables a Supervisor switchover event to occur without disruption to the network Layer 2 or Layer 3 topologies, ensuring that:

- Link status is maintained on all ports
- Data forwarding is maintained with less than a 10-millisecond interruption

This allows sensitive user applications such as voice and video to continue uninterrupted until the Supervisor module switchover event.

The redundant Supervisor configuration also allows system software upgrades to be performed using the stateful Supervisor switchover capabilities. The entire software upgrade process is simplified and streamlined using Cisco IOS In-Service Software Upgrades (ISSU). Not only does ISSU help eliminate misconfigurations associated with the software upgrade process, but an additional testing phase is incorporated that allows the new software version to be tested and verified before committing to the full upgrade.

Deploying Catalyst 4500 E-Series Client Access

In keeping with the SBA design principles, the access configuration is made as simple as possible: For example, a common access port configuration is used for a number of devices, including a computer, a phone, and a computer connected to a phone.

Access security features are recommended as part of a strategy using layers of defense tools to protect the network from accidental or malicious forms of denial-of-service attacks. These features include:

- Port Security, which limits the number of Media Access Control (MAC) addresses allowed on a given port. This prevents MAC flooding attacks and limits the exposure to the network in case someone inserts a non-authorized switch or wireless access point.
- Dynamic Host Configuration Protocol (DHCP) snooping prevents rogue DHCP servers from operating on the network and helps protect against DHCP starvation attacks.
- Address Resolution Protocol (ARP) inspection ties an IP address to a MAC address and protects against ARP spoofing attacks.
- IP Source Guard prevents attacks that use spoofed source IP addresses.

The uplinks from the Catalyst 4500 E-Series to the Core should be built using an EtherChannel comprised of ports on the Supervisor module. If redundant Supervisor modules are installed, then using ports from each Supervisor module for added resiliency is recommended.

Reader Tip

Any underlined command is wrapped to fit this document's format and should be entered at the command line as one complete command.

Process

Configuring Catalyst 4500 E-Series Client Access

1. Configure 10 Gb Ethernet X2 Optics Slots
2. Configure VLAN Trunking
3. Configure Access Ports
4. Configure Spanning Tree Protocol
5. Configure Auto QoS
6. Apply the Auto QoS Macros to the EtherChannel

Complete each of the following procedures to completely configure Catalyst 4500 E-Series client access.

Procedure 1 Configure10Gb Ethernet X2 Optics Slots

The Supervisor 6L-E uplink ports are 10 Gigabit Ethernet X2 optics slots. In the standard configuration, these X2 optics slots ship with a TwinGig converter module installed in each slot. The TwinGig converter module allows for two SFP Gigabit Ethernet transceivers to be installed in each X2 optic slot, providing four Gigabit Ethernet ports total.

In order to use the 10 Gigabit Ethernet X2 optics slots with the TwinGig converter modules you must configure the interfaces for the Gigabit Ethernet mode.

Step 1: Enter the following commands to configure each 10 Gigabit X2 Optic Slot, or port-group as they are referred to in the Command Line Interface, for gigabit Ethernet mode:

```
hw-module module 3 port-group 1 select gigabitethernet
hw-module module 3 port-group 2 select gigabitethernet
```

The configuration file provides separate interfaces for all ports. Keep in mind that the port-group configuration setting determines which interfaces are active. Assuming the Supervisor module is installed in slot 3, physical port-group 1 contains interface TenGigabitEthernet 3/1, it also contains GigabitEthernet 3/3 and 3/4 when using the TwinGig Converter Module. Likewise, port-group 2 contains interface TenGigabitEthernet 3/2 and GigabitEthernet 3/5 and 3/6.

The following is an example:

```
4500Access#show run module 3
Building configuration...
Current configuration : 541 bytes
!
interface TenGigabitEthernet3/1
!
interface TenGigabitEthernet3/2
!
interface GigabitEthernet3/3
   switchport trunk allowed vlan 1,8,12
switchport mode trunk
   ip arp inspection trust
   channel-group 1 mode on
   service-policy output queue-only
   ip dhcp snooping trust
!
interface GigabitEthernet3/4
   switchport trunk allowed vlan 1,8,12
   switchport mode trunk
   ip arp inspection trust
   channel-group 1 mode on
   service-policy output queue-only
   ip dhcp snooping trust
!
interface GigabitEthernet3/5
!
interface GigabitEthernet3/6
end
4500Access#
```

Step 2: Be sure you have a software license to use these interfaces as 10 Gigabit Ethernet interfaces. This allows for an easy future-proof upgrade path to 10 Gigabit Ethernet uplinks later if needed.

Procedure 2 Configure VLAN Trunking

The access uplinks are configured as Layer 2 switch-ports using VLAN Trunking. As a best practice, only the configured VLANs should be allowed on the trunk. For our example, the configuration uses VLAN ID 8 for the data VLAN, and VLAN ID 12 for the voice VLAN.

Step 1: Enter the following text at the command line:

```
switchport trunk allowed vlan 1,8,12
switchport mode trunk
```

Procedure 3 Configure Access Ports

The DHCP snooping, IP ARP Inspection, and IP Source Guard are all part of the access port configuration. These features require some global configuration commands as well as some interface specific commands.

Step 1: Enter the global configuration mode commands:

```
ip dhcp snooping vlan 1,8,12
no ip dhcp snooping information option
ip dhcp snooping
```

Step 2: The uplink interfaces are the trusted interfaces for the DHCP snooping and IP ARP inspection. Enter the following interface-specific commands:

```
ip dhcp snooping trust
ip arp inspection trust
```

Step 3: The access port configurations are simplified and are able to support a variety of devices including PCs, phones, and wireless access points. This way, you can apply the same configuration to all the access ports. Therefore, you can make use of the interface range macro command and apply the configuration in one step as opposed to configuring all the interfaces individually. Assuming a Catalyst 4500 E-Series with a single Supervisor module in slot 3, and slots 1 and 2 populated with the WS-4648-GETX+E line card, the following interface range command would be used to configure all of the access ports in one step:

```
4500Access(config)#interface range gigabitEthernet 1/1-
48,gi2/1-48
4500Access(config-if-range)#
```

Step 4: Configure the host ports as Layer 2 access ports with the specific data VLAN and voice VLANs:

```
switchport access vlan 8
switchport mode access
switchport voice vlan 12
```

Step 5: The following host port configurations enable the port-security functionality and allows 11 MAC addresses to be active on the port; additional MAC addresses are considered to be in violation and their traffic will be dropped:

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

Step 6: Enter the following command to set the aging time to 2 minutes:

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

Step 7: The following command will restrict traffic from MAC addresses that are in violation, but will not shut down the port, so an IP phone will still function:

```
switchport port-security violation restrict
switchport port-security aging type inactivity
```

Procedure 4 Configure Spanning Tree Protocol

Step 1: Enter the following command to shorten the time it takes for the port to go into a forwarding state:

```
spanning-tree portfast
```

Step 2: Enter the following command to disable the port if another switch is plugged into the port:

```
spanning-tree bpduguard enable
```

Step 3: Enter the following command to enable the IP Source Guard feature, which prevents IP address spoofing:

```
ip verify source
```

Step 4: As an added safeguard to harden the network from a DHCP-based denial-of-service attack, configure rate limiting the DHCP service on the host ports:

```
ip dhcp snooping limit rate 100
```

Procedure 5 Configure Auto QoS

QoS configurations are simplified with the use of AutoQoS macrocommands. The AutoQoS macros will create the Modular QoS CLI (MQC)-based class-maps, policy-maps, and even apply the correct Layer 2 or Layer 3 service policies to the interface.

Step 1: Issue the “AutoQoS macro” and the “trust” command so QoS markings on the traffic are trusted when a Cisco IP-phone is detected.

```
auto qos voip cisco-phone
qos trust device cisco-phone
```

Step 2: The macro automatically creates and applies the class-maps, policy-maps, and service-polices. Apply the following example to apply a service policy for input traffic and another for output traffic to each interface:

```
interface GigabitEthernet1/1
   switchport access vlan 8
   switchport mode access
   switchport voice vlan 12
   switchport port-security maximum 11
   switchport port-security aging time 2
   switchport port-security violation restrict
   switchport port-security aging type inactivity
   ip arp inspection limit rate 100
   auto qos voip cisco-phone
   qos trust device cisco-phone
   spanning-tree portfast
   spanning-tree bpduguard enable
   service-policy input AutoQos-VoIP-Input- Cos-Policy
   service-policy output AutoQos-VoIP-Output- Policy
   ip verify source vlan dhcp-snooping
!
```

Procedure 6 Apply the Auto QoS Macro

The recommended configuration utilizes the Supervisor uplink ports in an EtherChannel configuration. However, applying the AutoQoS macros to the EtherChannel requires a few additional steps. The Supervisor 6-E and Supervisor 6L-E handle QoS queuing and classification as separate functions and require that the QoS queuing configuration commands be applied at the physical port-level interface. Therefore, the traffic classification com¬mands such as set cos, set dscp, and any policing statements must be applied in the port-channel interface, while commands related to traffic queuing such as bandwidth, priority, and dbl must be applied on the physical-port interface. This requires the AutoQoS policy maps be modified before they can be applied correctly.

Step 1: The policy-maps created with the AutoQoS macros include both classification and queuing commands in the policy; therefore, in order to apply the same functionality to port-channel interfaces, simply create two new policy-maps where one contains the traffic queuing commands and the other contains the traffic classification commands.

Step 2: Then apply the classification policy-map to the port-channel interface and the queuing policy-map to the individual physical interfaces.

For example, consider the default AutoQoS policy-map that is applied to outbound traffic:

```
policy-map AutoQos-VoIP-Output-Policy
   class AutoQos-VoIP-Bearer-QosGroup
      set dscp ef
      set cos 5
         priority
         police cir percent 33
   class AutoQos-VoIP-Control-QosGroup26
      set dscp af31
      set cos 3
         bandwidth remaining percent 5
   class AutoQos-VoIP-Control-QosGroup24
      set dscp cs3
      set cos 3
         bandwidth remaining percent 5
   class class-default
         dbl
```

Step 3: In order to apply this policy-map to an EtherChannel using the Supervisor 6-E or Supervisor 6-LE, break the policy-map into two different policy-maps, one that includes the classification and marking commands and one that performs the queuing. Such as the following two policies below:

```
policy-map EC-non-queue
   class AutoQos-VoIP-Bearer-QosGroup
      set dscp ef
      set cos 5
         police cir 33000000
   class AutoQos-VoIP-Control-QosGroup26
      set dscp af31
      set cos 3
   class AutoQos-VoIP-Control-QosGroup24
      set dscp cs3
      set cos 3
policy-map queue-only
   class AutoQos-VoIP-Bearer-QosGroup
      priority
   class AutoQos-VoIP-Control-QosGroup26
      bandwidth remaining percent 5
   class AutoQos-VoIP-Control-QosGroup24
      bandwidth remaining percent 5
   class class-default
      dbl
```

Note the change to the policing command in the EC-non-queue policy-map. The change from the percent 33 to a specific value 33000000 is done because the port-channel interface does not support the percent argument. Therefore, a specific value is given. The value chosen here is more than sufficient to handle the voice calls even under the worst-case scenarios. Configuring a traffic policer is a recommended best practice for the traffic assigned to the priority queue in order to prevent the traffic from consuming all the remaining bandwidth.

Finally, keep in mind that the AutoQoS feature was designed to simplify the deployment of QoS polices in the network. The macro commands are based on years of real-world experience, industry standards, and internal lab testing. The policies created by the AutoQos macros are an excellent deployment tool, especially for basic voice-over-IP network environments. You should, however, consider your own specific requirements and be prepared to make modifications to the QoS policies as needed; especially when more advanced voice and video applications are deployed.

Reader Tip

Complete and current information on the Cisco SBA can be found at: http://www.cisco.com/en/US/solutions/ns340/ ns414/ns742/ns982/ landing_sBus_archit.html

Appendix A: Product Part Numbers

The following products and software version have been validated for the Cisco SBA:

Functional Area	Product	Part Numbers	Software Version
Headquarter access for PC, phones, APs, other devices	Catalyst 4500 E-Series Chassis Supervisor Engine 6L-E 48-port 10/100/1000 Line Card PoE+ ready	WS-C3750G-12S-S Catalyst 3750 12 SFP + IPB Image WS-Sup6L-E WS-X4648-RJ45V+E Special Bundle Pricing available includes reduced service pricing WS-C4506E-S6L-96V+ WS-C4503E-S6L-48V+ When ordering via Cisco distribution channels please use the following part numbers: WS-C4503E-S6L-1300 WS-C4506E-S6L-1300 WS-C4506E-S6L-2800 WS-C4506E-S6L-4200 Consult the Cisco Power Calculator for sizing the appropriate power supply[1]	12.2(53)SG

[1] Cisco Power Calculator – http://tools.cisco.com/cpc/

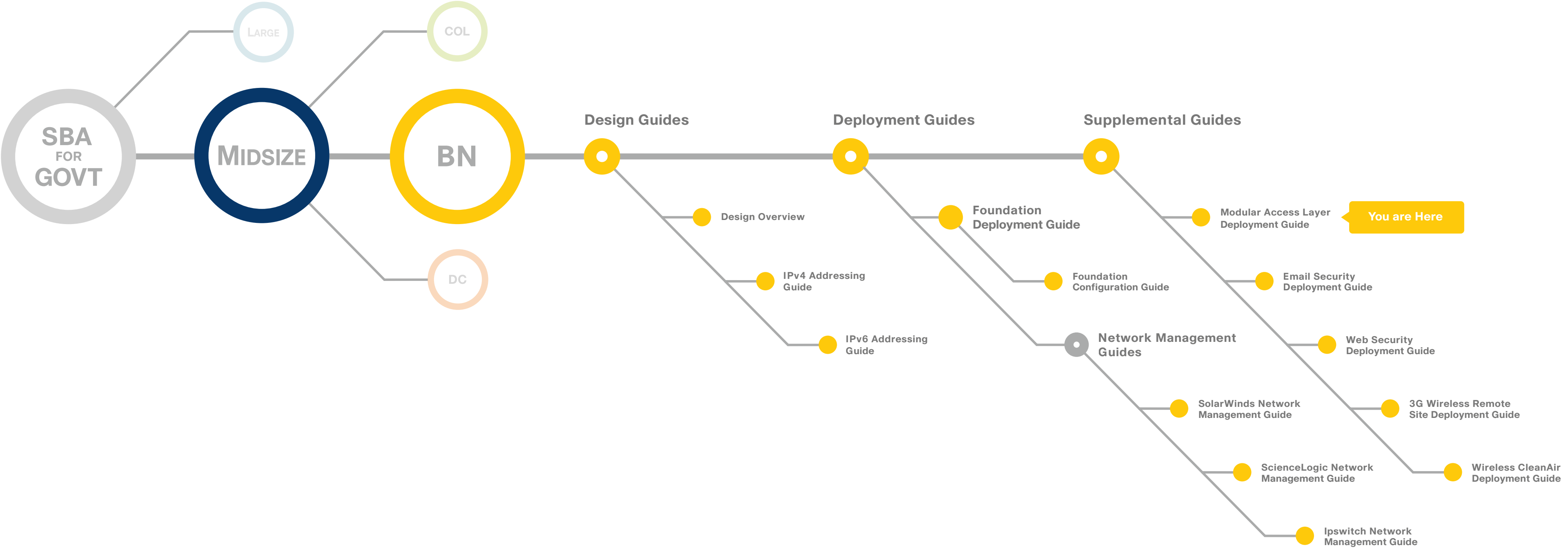
Appendix B: Catalyst 4500 E-Series Access Configuration File

```
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname 4500Access
!
boot-start-marker
boot system flash:cat4500e-lanbasek9-mz.122-53.SG.bin
boot-end-marker
!
!
no aaa new-model
hw-module module 3 port-group 1 select gigabitethernet
hw-module module 3 port-group 2 select gigabitethernet
udld aggressive
vtp mode transparent
ip subnet-zero
ip arp inspection vlan 1,8,12
!
!
ip dhcp snooping vlan 1,8,12
no ip dhcp snooping information option
ip dhcp snooping
ip vrf mgmtVrf
!
!
!
!
power redundancy-mode redundant
!
!
!
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
redundancy
   mode rpr
!
vlan internal allocation policy ascending
!
vlan 8,12
!
!
class-map match-all AutoQos-VoIP-Control-Dscp26
   match dscp af31
class-map match-all AutoQos-VoIP-Control-Dscp24
   match dscp cs3
class-map match-all AutoQos-VoIP-Bearer-Cos
   match cos 5
class-map match-all AutoQos-VoIP-Control-QosGroup24
   match qos-group 24
class-map match-all AutoQos-VoIP-Control-QosGroup26
   match qos-group 26
class-map match-all AutoQos-VoIP-Bearer-QosGroup
   match qos-group 46
class-map match-all AutoQos-VoIP-Bearer-Dscp
   match dscp ef
class-map match-all AutoQos-VoIP-Control-Cos
   match cos 3
!
!
policy-map AutoQos-VoIP-Input-Dscp-Policy
   class AutoQos-VoIP-Bearer-Dscp
      set qos-group 46
   class AutoQos-VoIP-Control-Dscp26
      set qos-group 26
   class AutoQos-VoIP-Control-Dscp24
      set qos-group 24
policy-map EC-non-queue
   class AutoQos-VoIP-Bearer-QosGroup
      set dscp ef
      set cos 5
         police cir 33000000
   class AutoQos-VoIP-Control-QosGroup26
      set dscp af31
      set cos 3
   class AutoQos-VoIP-Control-QosGroup24
```

```
      set dscp cs3
      set cos 3
policy-map queue-only
   class AutoQos-VoIP-Bearer-QosGroup
      priority
   class AutoQos-VoIP-Control-QosGroup26
      bandwidth remaining percent 5
   class AutoQos-VoIP-Control-QosGroup24
      bandwidth remaining percent 5
   class class-default
      dbl
policy-map AutoQos-VoIP-Input-Cos-Policy
   class AutoQos-VoIP-Bearer-Cos
      set qos-group 46
   class AutoQos-VoIP-Control-Cos
      set qos-group 24
policy-map AutoQos-VoIP-Output-Policy
   class AutoQos-VoIP-Bearer-QosGroup
      set dscp ef
      set cos 5
         priority
         police cir percent 33
   class AutoQos-VoIP-Control-QosGroup26
      set dscp af31
      set cos 3
         bandwidth remaining percent 5
   class AutoQos-VoIP-Control-QosGroup24
      set dscp cs3
      set cos 3
         bandwidth remaining percent 5
   class class-default
         dbl
!
!
!
interface Port-channel1
   switchport
   switchport trunk allowed vlan 1,8,12
   switchport mode trunk
   ip arp inspection trust
   service-policy input AutoQos-VoIP-Input-Cos-Policy
   service-policy output EC-non-queue
   ip dhcp snooping trust
!
interface FastEthernet1
   ip vrf forwarding mgmtVrf
   no ip address
   speed auto
   duplex auto
!
```

```
interface GigabitEthernet1/1
   switchport access vlan 8
   switchport mode access
   switchport voice vlan 12
   switchport port-security maximum 11
   switchport port-security aging time 2
   switchport port-security violation restrict
   switchport port-security aging type inactivity
   ip arp inspection limit rate 100
   auto qos voip cisco-phone
   qos trust device cisco-phone
   spanning-tree portfast
   spanning-tree bpduguard enable
   service-policy input AutoQos-VoIP-Input-Cos-Policy
   service-policy output AutoQos-VoIP-Output-Policy
   ip verify source vlan dhcp-snooping
!
interface GigabitEthernet1/2
   switchport access vlan 8
   switchport mode access
   switchport voice vlan 12
   switchport port-security maximum 11
   switchport port-security aging time 2
   switchport port-security violation restrict
   switchport port-security aging type inactivity
   ip arp inspection limit rate 100
   auto qos voip cisco-phone
   qos trust device cisco-phone
   spanning-tree portfast
   spanning-tree bpduguard enable
   service-policy input AutoQos-VoIP-Input-Cos-Policy
   service-policy output AutoQos-VoIP-Output-Policy
   ip verify source vlan dhcp-snooping
!
!*************************************************************
*
! Interface GigabitEthernet 1/3 – 2/48 are all configured the
! same as 1/1 ! and 1/2 and have been removed for conciseness
!*************************************************************
*
!
interface GigabitEthernet1/12
   description Wireless AP port
   switchport access vlan 8
   switchport mode access
   switchport voice vlan 12
   switchport port-security maximum 11
   switchport port-security aging time 2
   switchport port-security violation restrict
   switchport port-security aging type inactivity
   ip arp inspection limit rate 100
   auto qos voip cisco-phone
   qos trust device cisco-phone
   spanning-tree portfast
   spanning-tree bpduguard enable
   service-policy input AutoQos-VoIP-Input-Cos-Policy
   service-policy output AutoQos-VoIP-Output-Policy
   ip verify source vlan dhcp-snooping
!
interface TenGigabitEthernet3/1
!
interface TenGigabitEthernet3/2
!
interface GigabitEthernet3/3
   switchport trunk allowed vlan 8,12
   switchport mode trunk
   ip arp inspection trust
   channel-group 1 mode on
   service-policy output queue-only
   ip dhcp snooping trust
!
interface GigabitEthernet3/4
   switchport trunk allowed vlan 8,12
   switchport mode trunk
   ip arp inspection trust
   channel-group 1 mode on
   service-policy output queue-only
   ip dhcp snooping trust
!
interface GigabitEthernet3/5
!
interface GigabitEthernet3/6
!
interface Vlan1
   no ip address
!
ip http server
no ip http secure-server
!
!
!
!
line con 0
   stopbits 1
line vty 0 4
!
end
4500Access#
```

Appendix C: SBA for Midsize Agencies Document System


SBA FOR GOVT
LARGE
MIDSIZE
COL
DC
BN
Design Guides
Design Overview
IPv4 Addressing Guide
IPv6 Addressing Guide
Deployment Guides
Foundation Deployment Guide
Foundation Configuration Guide
Network Management Guides
SolarWinds Network Management Guide
ScienceLogic Network Management Guide
Ipswitch Network Management Guide
Supplemental Guides
Modular Access Layer Deployment Guide
You are Here
Email Security Deployment Guide
Web Security Deployment Guide
3G Wireless Remote Site Deployment Guide
Wireless CleanAir Deployment Guide

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.**