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

LARGE

BORDERLESS NETWORKS

LAN Deployment Guide

SBA FOR GOVERNMENT

Revision: H2CY10

Who Should Read This Guide

This document is for the reader who:

- Has in total 2000 to 10,000 connected employees
- Has one or more Local Area Networks that support up to 5000 connected employees each
- Needs wired and wireless network access for employees
- Requires wireless guest access
- Requires solutions for wired and wireless voice access
- Has IT workers with a CCNA® certification or equivalent experience
- Wants to deploy their network infrastructure efficiently
- Wants the assurance of a tested solution
- Requires a migration path for growth

Related Documents

Before reading this guide

BN ● Design Overview

BN ● Internet Edge Deployment Guide

BN ● WAN Deployment Guide

Optional documents

BN ● Midsize Foundation Design Overview

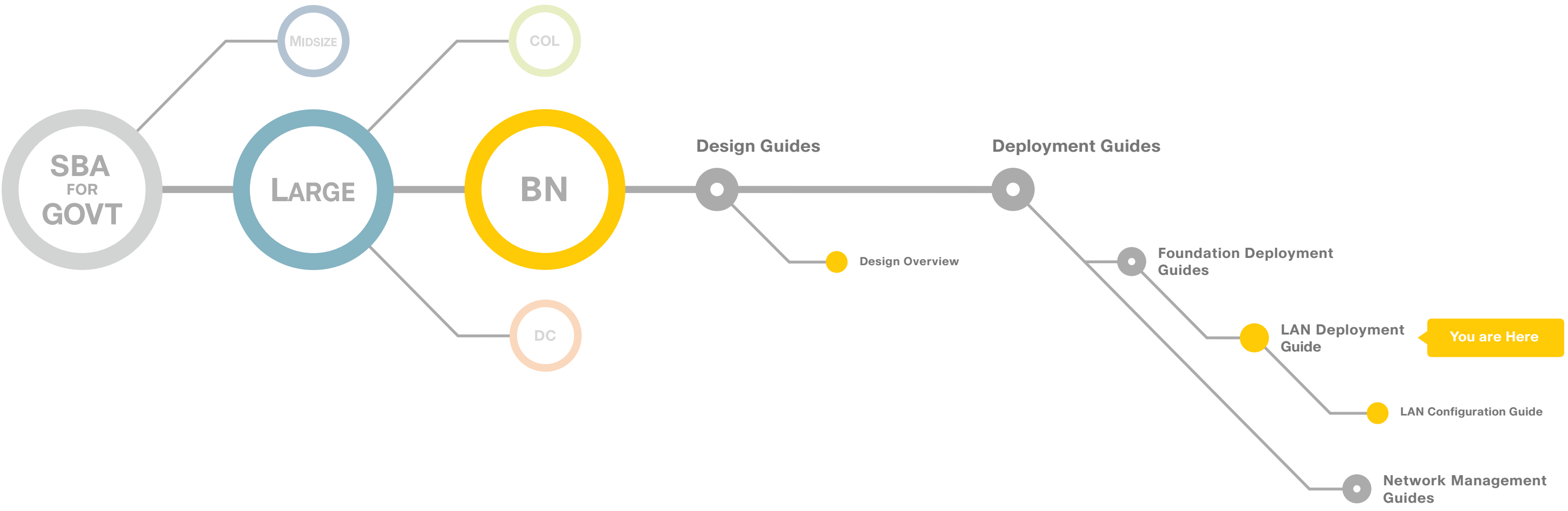


Table of Contents

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 Smart Business Architecture (SBA) for Government Large Agencies—Borderless Networks is designed for networks that have 2000 to 10,000 connected users. We created a prescriptive, out-of-the-box deployment guide that is based on best-practice design principles and that delivers flexibility and scalability. The deployment guides are designed to make the SBA for Large Agencies—Borderless Networks easy—easy to configure, easy to deploy, and easy to manage.

The goal of any network implementation is to support the applications that benefit the users and the agency that it is built for. As they guide you through the depth and breadth of the architecture, the SBA deployment guides are intended to simplify navigating among and learning the various networking technologies that we used to build the architecture. SBA is a solid network foundation that provides the flexibility to support new users or network services without re-engineering the network.

Using the Deployment Guides

The Large Agency architecture was designed, built, and validated as an end-to-end system. To focus on specific elements of the architecture, there are three primary deployment guides, one each for Local Area Network (LAN), Wide Area Network (WAN), and Internet Edge.

To enhance the Large Agency architecture, there are a number of supplemental guides that address specific functions, technologies, or features that may be important to solving your operational problems. Within each of these deployment guides, you will find a modular approach that allows you to start at the beginning and work your way through or to jump to a specific module. Each deployment guide and the modules within are designed to stand alone, so that you can deploy the specific Cisco technology in a module without completing each previous module. Each deployment guide includes a complete list of the products and the software revisions tested, and a companion supplemental guide contains all configuration files used.

The deployment guides begin with a agency overview of the common operational problems addressed, followed by an architecture overview to assist you with matching the value of a technology solution to your operational problems.

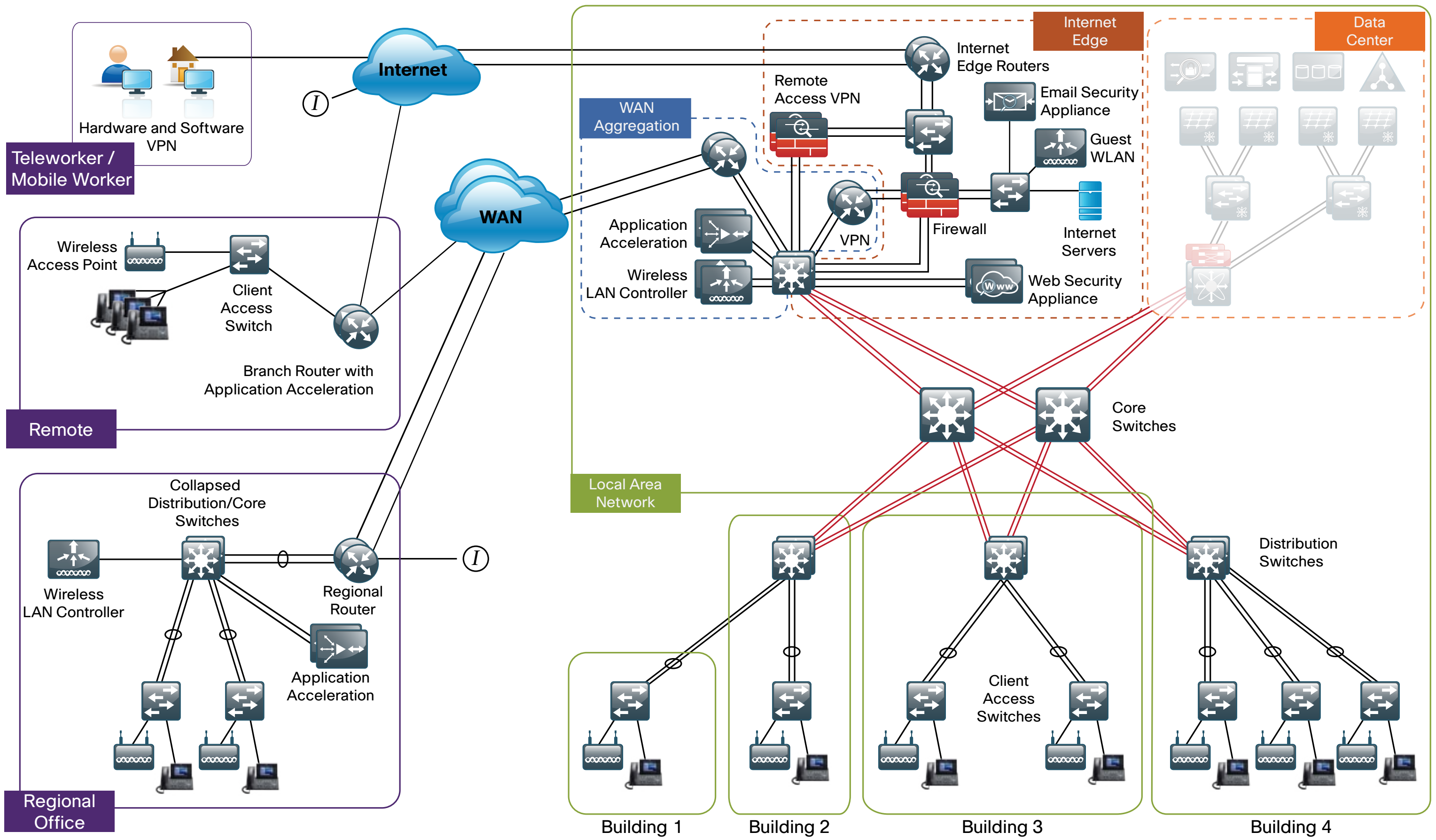
The Local Area Network Deployment Guide covers wired and wireless network access with ubiquitous capabilities for both the larger campus-size LAN as well as the smaller remote-site LAN. Resiliency, security, and scalability is included to provide a robust communications environment. Quality of service (QoS) is integrated to ensure that the base architecture can support a multitude of applications including low latency, drop-sensitive multimedia applications coexisting with data applications on a single network. The guide also provides a guest and partner access solution that is secured from accessing internal confidential information while using the same wireless infrastructure that employees use.

The Wide Area Network Deployment Guide includes the primary site aggregation design as well as multiple remote site designs to accommodate varying scale and service-level requirements in a common approach. The flexibility in the WAN deployment guide provides guidance and configuration for Multiprotocol Label Switching (MPLS) transport as well as broadband or Internet transport in a primary or backup role. QoS is integrated to ensure that the base architecture can support a multitude of applications on a single transport. The design integrates application optimization and the deployment guide provides details on optimizing WAN traffic to ensure economical use of bandwidth while providing a good user experience.

The Internet Edge Deployment Guide focuses on security services such as firewalls and intrusion prevention systems to protect your agency's gateway to the Internet. Internet service-provider connectivity and routing options, combined with server load balancing, provide resiliency to the design. The E-Mail Security module covers protecting e-mail from spam and malware. The Web Security module provides acceptable-use control and monitoring as well as guidance on managing the increasing risk associated with clients browsing the Internet. The Virtual Private Network (VPN) design supports the teleworker and mobile user with secure remote access. All of these elements are covered in separate modules and yet are designed to work together to provide a secure Internet Edge solution.

Figure 1 shows the components of the SBA for Large Agencies—Borderless Networks.

Figure 1. Borderless Networks for Large Agencies Overview



Design Goals

This architecture is based on requirements gathered from customers, partners, and Cisco field personnel for agencies with 2000 to 10,000 connected users. When designing the architecture, we considered the gathered requirements and the following design goals:

- Ease of Deployment: Agencies can deploy the design consistently across all products included in the architecture. The configurations used in the deployment represent a best-practice methodology to enable a fast and resilient deployment.
- Flexibility and Scalability: The architecture can grow with the agency without being redesigned.
- Resiliency and Security: The architecture keeps the network operating even during unplanned outages and attacks.
- Easy to Manage: The deployment guidance includes configuring devices to be managed by a network management system (NMS) or as unique elements of the network.
- Advanced Technology Ready: Implementing advanced technologies like collaboration is easy because the network foundation is already configured with the required baseline network services.

Ease of Deployment, Flexibility and Scalability

Agencies of 2000 to 10,000 users are often are spread out among different geographical locations. The locations might have labels like remote site, regional site, or headquarters. This architecture addresses how to build a network for all these locations, irrespective of the label.

In this design, several methods are used to create and maintain a scalable network. Defining a common framework with a convergence of design standards drives global consistency and optimizes the design process, which ultimately results in lower cost and less complexity. Standardization is the key to scalability; by keeping a small number of standard designs for common portions of the network, support staff are able to design services for, implement, and support these network areas more effectively.

To enhance scalability, we take a modular design approach; beginning with a set of standard, global building blocks, we can assemble a scalable network to meet requirements. For instance, to build a campus network, we might start with a LAN module, connect an Internet edge module, and then add a WAN module.

Many of these plug-in modules look identical for several different service areas; this common look provides consistency and scalability in that the same support methods can be used in multiple areas of the network to maintain the network. These modules follow standard core-distribution-access network design models and use layer separation to ensure that interfaces between the plug-ins are well defined.

Resiliency and Security

One of the keys to maintaining a highly available network is building the appropriate redundancy to guard against failure in the network, whether it is link, port, card, or chassis failure. But systems can be engineered to be too redundant, as is evident when they exhibit failures of overly complex redundancy features, which result in a complete communications failure. The redundancy in our architecture is carefully balanced with the complexity inherent in redundant systems.

Building production network services without any form of redundancy is unacceptable to most agencies. When building in the necessary redundancy, care must also be taken to prevent large dependency chains that result in greater risk of system failure. For example, chains of devices that do not have cross-connections may create a dependency on both chains being completely available.

With the addition of a significant amount of delay-sensitive and drop-sensitive traffic such as voice and video conferencing, we also place a strong emphasis on recovery times. Choosing designs that reduce the time between failure detection and recovery is important for ensuring that the network stays available even in the face of a minor component failure.

Security of the network is also a very strong component of the architecture. In a large network, there are many entry points and we ensure that they are as secure as possible without making the network too difficult to use. Securing the network not only helps keep the network safe from attacks but is also a key component to network-wide resiliency.

Easy to Manage

While this guide focuses on the deployment of the network foundation, the next phase management and operation are considered. The configurations in the deployment guides are designed to allow the devices to be managed both via normal device management connections, such as SSH and HTTPS, but also via NMS. The configuration of the NMS is not covered in this guide.

Advanced Technology Ready

Flexibility, scalability, resiliency, and security all are characteristics of an advanced technology-ready network. The modular design of the architecture means that technologies can be added when the agency is ready to deploy them. However, the deployment of advanced technologies, such as collaboration, is eased because the architecture includes products and configurations that are ready to support collaboration from day one. For example, access switches provide Power over Ethernet (PoE) for phone deployments without the need for a local power outlet. The entire network is preconfigured with QoS to support high-quality voice. Multicast is configured in the network to support efficient voice and broadcast-video delivery.

Beyond the wired network, the wireless network is also preconfigured for devices that send voice over the wireless LAN, providing IP telephony over 802.11 Wi-Fi (referred to as mobility) at all locations. The Internet edge is also ready to provide soft phones via VPN, as well as traditional hard or desk phones.

Agency Overview

The *Cisco SBA for Large Agencies—Borderless Networks LAN Deployment Guide* is designed to address five primary issues encountered by large agencies:

- Offering reliable access to agency resources
- Minimizing time required to absorb technology investments
- Allowing workforce mobility
- Providing guest access
- Reducing operation costs

Offer Reliable Access to Agency Resources

Data networks are critical to large-agency' viability and productivity. Online workforce-enablement tools only offer benefit if the data network provides reliable access to information resources. Collaboration tools and content distribution rely on high-speed, low-latency network infrastructure to provide an effective user experience. However, as networks become more complex, the level of risk increases for network availability loss or poor performance due to inadequate design, configuration errors, maintenance and upgrade outages, or hardware and software faults. The design and methods used in this deployment guide were created to minimize these risks.

Minimize Time Required to Absorb Technology Investments

New technology can impose significant costs, from the perspective of the investment in the equipment, as well as the time and workforce investment that is required to deploy the new technology and establish operational readiness. When new technology is introduced it takes time to understand how the technology operates, and to ascertain how to effectively integrate the new technology into the existing infrastructure. Over time the methods and procedures used to deploy a new technology are refined to be more efficient and accurate.

This deployment guide eases the agency's cost of technology implementation by providing methods and procedures that have been developed and tested by Cisco. Applying the guidance within this document reduces the time required for assimilation of the technology into the agency's network, and allows the technology to be deployed quickly and accurately, so the agency can achieve a head start realizing the return on its investment.

Allow Workforce Mobility

The number of users in an agency's location can vary dramatically as an agency grows and adapts to changes in agency activity. Preparing space for worker occupation takes time, and might not be possible because of the building infrastructure. In some cases, short-term space requirements may be impractical due to the lead-time and cost restrictions. Overhead costs are a common place an agency looks to control costs. One way to control overhead costs is using office space efficiently. Examples include sharing workspace between multiple users and adapting square footage that is not typically viewed as work space to serve multiple purposes.

This design provides mobility services that control costs by maximizing the use of existing office space, and increase productivity by allowing users to move throughout the agency' physical plant and get to work quickly.

Provide Guest Access

Agencies' facilities are frequently called up to host a wide range of guests, including customers, partners, and vendors. Many of these guests desire network connectivity to gain access to permitted agency resources, as well as VPN connectivity to their employer's network and the Internet, while they are on-site so they can be as productive as possible. However, offering guests the same level of network access as the agency's users exposes the agency to a significant risk. Additionally, variations in frequency and number of guests can cause difficulty predicting when and where the connectivity will be required.

The design describes wireless service that offers authenticated guest access to the internet without allowing access to the agency's internal resources.

Reduce Operational Costs

Agencies constantly pursue opportunities to reduce network operationalcosts, while maintaining the network's effectiveness for the end users. Operational costs include not only on the cost of the physical operation (power, cooling, etc), but also the labor cost required to staff an IT department that monitors and maintains the network. Additionally, network outages and performance issues impose costs that are more difficult to quantify, in the form of loss of productivity and interruption of operational continuity.

The network described by this deployment guide offers network resilience in its ability to tolerate failure or outage of portions of the network, along with a sufficiently robust-yet-simple design that staff should be able to operate, troubleshoot and return the network to service in the event of a network outage.

Notes

Architecture Overview

The Local Area Network (LAN) is the networking infrastructure that provides wired and wireless access to network communication services and resources for end users and devices spread over a single floor or building. A campus network occurs when a group of building based LANs that are spread over a small geographic area are interconnected.

The *Cisco SBA for Large Agencies—Borderless Networks LAN Deployment Guide* provides a design that enables communications between devices in a building or group of buildings as well as interconnection to the Wide Area Network (WAN) and Internet Modules.

Specifically, this document shows you how to deploy the network foundation and services to enable

- LAN connectivity for up to 5000 connected users
- Wired and wireless network access for employees
- Wireless guest access
- Wired and wireless infrastructure ready for voice services

Hierarchical Design Model

This architecture uses a hierarchical design model to break the design up into modular groups or layers. Breaking the design up into layers allows each layer to focus on specific functions, which simplifies the design and provides simplified deployment and management.

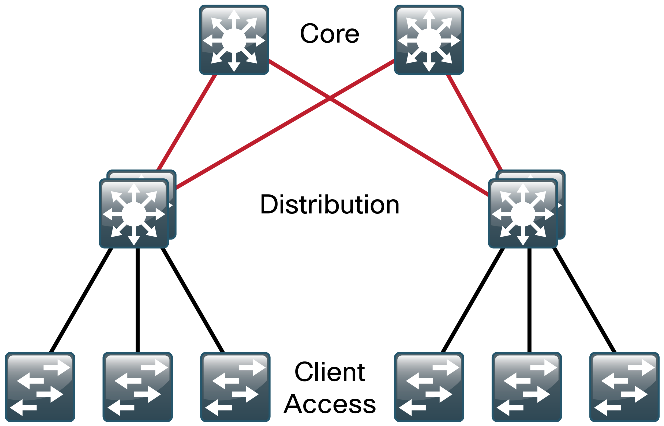
Modularity in network design allows you to create design elements that can be replicated throughout the network. Replication provides an easy way to scale the network as well as a consistent deployment method.

In flat or meshed network architectures, changes tend to impact a large number of systems. Hierarchical design helps constrain operational changes to a subset of the network, which makes it easy to manage as well as improve resiliency. Modular structuring of the network into small, easy-to-understand elements also facilitates resiliency via improved fault isolation.

As shown in Figure 2, a hierarchical design includes the following three layers:

- **Core Layer:** provides connection between distribution layers
- **Distribution Layer:** aggregates access layers and provides connectivity to services
- **Access Layer:** provides workgroup/user access to the network

Figure 2. LAN Hierarchical Design



The three layers—core, distribution, and access—each provide different functionality and capability to the network. Depending on the characteristics of the site where the network is being deployed, you might need one, two or all three of the layers. For example, a remote site supporting only 10 users will only require an access layer. A regional site, which occupies a single building, might only require the access and distribution layers while a campus of multiple buildings will most likely require all three layers.

Regardless of how many layers are implemented at a site, the modularity of this design ensures that each layer will always provide the same services, and in this architecture, utilize the same deployment methods.

Access Layer

The access layer is the point at which user-controlled and user-accessible devices are connected to the network. The access layer provides both wired and wireless connectivity and contains features and services that ensure security and resiliency for the entire network.

Device Connectivity

The access layer provides high-speed user-controlled and user-accessible device connectivity. Once expensive options, high-speed access technologies like Gigabit Ethernet and 802.11n wireless are now standard configurations on end-user devices. While an end-user device in most cases will not utilize the full capacity of these connections for long periods of time, the ability to burst up to these high speeds when performing routine tasks does help make the network a transparent part of an end-users day-to-day job. The longer someone has to wait to back up their machine, send an email, or open a file off an internal web page the harder it is for the network to be transparent.

It is common for many different types of devices to connect at the access layer. Personal computers, IP phones, wireless access points, and IP video surveillance cameras all might connect to the same access layer switch. Since it can be beneficial for performance, management, and security reasons to segment these different devices, the access layer provides the capability to support many logical networks on one physical infrastructure.

Resiliency and Security Services

In general the goal of the resiliency and security services in the infrastructure is to ensure that the network is available for use without impairment for everyone that needs it. Because the access layer is the connection point between the network and client devices, it plays a role in ensuring the network is protected from human error and from malicious attacks. This protection includes making sure the devices connecting to the network do not attempt to provide services to the rest of the end users that they are not authorized for, that they do not attempt to take over the role of any other device on the network, and, when possible, that they verify the device is allowed on the network.

Enabling these services in the access layer contributes not only to the overall security of the network, but also to the resiliency and availability of the network.

Advanced Technology Capabilities

Finally, the access layer provides a set of network services that support advanced technologies. Voice and Video are commonplace in today's agencies and the network must provide services that enable these technologies. This includes providing for specialized access for these devices, ensuring the traffic from these devices is not impaired by others, and providing efficient delivery of traffic that is needed by many devices in the network.

Distribution Layer

The distribution layer serves many important services for the Local Area Network. The primary function is to serve as an aggregation point for multiple access layer switches in a given location or campus. In a network where connectivity needs to transit the LAN end to end, whether that be between different access layer devices or from an access layer device to the WAN, the distribution layer facilitates this connectivity.

Scalability

In any network where multiple access layer devices exist at a location to serve end-user connectivity, it becomes impractical to interconnect each access switch as the access layer grows beyond two or three switches.

The distribution layer provides a logical point to summarize addressing and to bound protocols and features necessary for the access layer operation. Another benefit of the distribution layer boundary is that it creates fault domains that serve to contain failures or network changes to those parts of the network directly affected.

The end result to the agency is that the distribution layer can lower the cost of operating the network by making it more efficient, by requiring less memory, and by processing resources for devices elsewhere in the network. The distribution layer also increases network availability by containing failures to smaller domains.

Reduce Complexity and Increase Resiliency

This design uses a simplified distribution layer design, which consists of a single logical entity that can be implemented using a pair of physically separate switches operating as one device, a physical stack of switches operating as one device, or a single physical device with redundant components.

The benefit to the agency is the reduced complexity of configuring and operating the distribution layer as fewer protocols are required and little or no tuning is needed to provide near-second or sub-second convergence around failures or disruptions.

The design resiliency is provided by physically redundant components like power supplies, supervisors, and modules, as well as stateful switchover to redundant logical control planes. Reduced complexity and consistent design lower the operational cost of configuring and maintaining the network.

Flexible Design

The distribution layer provides connectivity to network-based services, to the WAN, and to the Internet Edge. Network-based services can include and are not limited to Wide-Area Application Services (WAAS), and Wireless LAN controllers. Depending on the size of the LAN, these services and the inter-connection to the WAN and Internet Edge may reside on a dedicated distribution layer versus sharing one with access layer devices. Like the access layer, the distribution layer also provides QoS for application flows to guarantee critical applications and multi-media applications perform as designed.

Core Layer

In a large LAN environment there often arises a need to have multiple distribution layer switches. One reason for this is when access layer switches are located in multiple geographically dispersed buildings, locating a distribution layer switch in each of those buildings can save costly fiber-optic runs between buildings. As networks grow beyond three distribution layers in a single location, a core layer should be used to optimize the design.

Another reason is when the number of access layer switches connecting to a single distribution layer exceeds the design goals of the network designer. In a modular and scalable design, you can have collocated distribution layers for Data Center, WAN connectivity, or Internet Edge Services.

As shown in Figure 3 and Figure 4, in environments where multiple distribution layer switches exist in close proximity and where fiber optics provide the ability for high-speed interconnect, a core layer reduces the network complexity.

Figure 3. LAN Topology with a Core

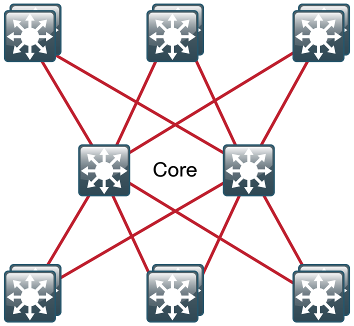
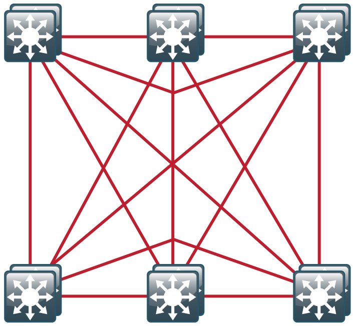


Figure 4. LAN Topology without a Core



The core layer of the LAN is a critical part of the scalable network, yet by design, is one of the simplest. The distribution layer provides the fault and control domains, and the core represents the 7x24x365 nonstop connectivity between them that agencies must have in the modern agency environment where connectivity to resources is critical to operational success.

The core layer in this design is based on two physically and logically separate switches. Connectivity to and from the core is Layer 3 only which drives increased resiliency and stability. Since the core does not need to provide the same services or boundaries that the distribution layer does, the two-box design is not an issue of any significant increase in configuration or complexity.

Quality of Service (QoS)

Because real-time traffic is very delay and drop sensitive, it is necessary to provide special handling for it on the network. The network must ensure that this type of traffic is handled with priority so that the stream of audio or video is not interrupted.

QoS allows the agency to define different traffic types and to create more deterministic handling for real-time traffic. QoS is especially useful in congestion handling, where a full communications channel might prevent voice or video streams from being intelligible at the receiving side. It is important to note, however, that QoS does not create bandwidth; rather, it takes bandwidth from one class (generally the default traffic class) to give some priority to another class.

Within this design the approach to using QoS capabilities is to keep the QoS profiles as simple as necessary to meet the goals for supporting applications that need special delivery. The primary goals in implementing QoS within the network are to:

- Support and ensure first out-the-door service for supported, real-time applications
- Provide business continuance for mission-critical applications
- Provide fairness between all other applications when congestion occurs
- Build a trusted edge around the network to guarantee that users cannot inject their own arbitrary priority values and to allow us to trust marked traffic throughout the network

To accomplish these goals, the design uses a three-step approach to implementing QoS across the network:

- Establish a limited number of traffic classes (one to six classes) within the network that need special handling (real-time voice, real-time video, high-priority data, interactive traffic, batch traffic, and default are examples of classes that may be used).
- Classify applications into the traffic classes.
- Apply special handling to the traffic classes to achieve intended network behavior.

In this design, QoS configurations are as simple as possible, and are applied only to those applications that require special handling.

This approach establishes a solid, scalable, and modular framework to implement QoS across the entire network.

Notes

Access Layer

Business Overview

Organizations rely on the flow of information to conduct business in todays competitive global economy. The ability to access applications to make informed business decisions, check email correspondence from internal and external associates or relay business directives to a dispersed workforce all rely on the ability to move information around the organization.

The ability to grow the productivity of the workforce is often driven by the ability to allow users to access this information or push communications regardless of their location using an increasingly diverse set of communications devices. The reliance on access to information and services that are on the other end of a network connection means that the speed, reliability, and availability of the transport is critical to success.

The ability to transform the communication of ideas and information from flat written text to a multimedia experience by adding audio and video improves the receivers understanding and retention of that information. As organizations evolve the ability to deliver these richer modes of communications, they face a challenge of controlling the cost of deployment by utilizing a single infrastructure to accommodate what used to require multiple parallel single purpose networks.

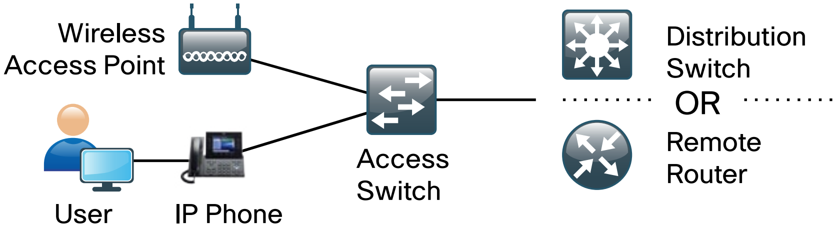
Technology Overview

The access layer is the point at which user-controlled and user-accessible devices are connected to the network and is the one architecture component that is found in every LAN. Because the access layer is the connection point between network based services and client devices it plays an important role in protecting other users, the application resources, and the network itself from human error and malicious attacks. Network resiliency and security in the Access Layer is achieved through the use of Catalyst Infrastructure Security Features (CISF) including DHCP snooping, IP Source Guard, Port Security, Dynamic ARP Inspection, and BPDU Guard.

To provide consistent access capabilities and to simplify network deployment and operation, a common deployment method is used for all access layer devices in the design whether they are located in the headquarters or at a remote site. To reduce complexity, the access layer is designed so that a single interface configuration can be used for a standalone computer, an IP phone, an IP phone with an attached computer, or a wireless access point.

The LAN access layer provides high-speed connections to devices via 10/100/1000 Ethernet with both Gigabit and 10-Gigabit uplink connectivity options. The 10 Gigabit uplinks also support Gigabit connectivity to provide flexibility and help business continuity during a transition to 10 Gigabit Ethernet. The LAN access layer is configured as a Layer 2 switch with all Layer 3 services being provided either by the directly-connected distribution layer or router (Figure 5).

Figure 5. Access Layer Overview



Features to Support the Deployment Voice and Video

Voice and Video are enabled in the access layer via network services such as Power over Ethernet+, Quality of Service, Multicast support, and CDP with the Voice VLAN.

Power over Ethernet (POE) enables devices such as IP Phones, wireless access points, and security cameras to be powered by the access layer device. This removes the expense of installing or modifying building power to support devices in difficult to reach locations and allows for the consolidation of back-up power supplies and UPSs to the access closet.

To support the increasing requirements of devices powered by the network, the access layer devices support the IEEE 802.3at standard, also known as PoE+, which is the newest industry standard for PoE. The devices, and or line cards support all the previous implementations of PoE up to 20 watts per port as well as the new IEEE 802.3at implementation of up to 30 watts per port.

Cisco Discovery Protocol (CDP) is used to support voice and video device integration into the access layer. Cisco IP Phones that are plugged into the access layer communicate bidirectionally with the access layer switch via CDP. CDP provides the IP Phone with configuration information and provides the access layer switch with the IP Phones power requirements and the ability to selectively prioritize traffic from the IP Phone.

Access Layer Platforms

Wiring Closets Requiring up to 48 Ports

The Cisco Catalyst 2960-S and 3560-X Series are both economical 10/100/1000 Ethernet fixed-port switches that provide flexibility and common features required for wiring closets that can be supported by a single fixed port switch. The Cisco Catalyst 2960-S and 3560-X are available in both PoE+ and non-powered versions.

In addition to the capabilities supported by the Catalyst 2960-S (other than stacking) the Catalyst 3560-X supports modular uplinks, an upgradable IOS feature set, and enhanced enterprise capabilities like TrustSec and Medianet.

Wiring Closets Requiring Greater than 48 Ports

When a wiring closet requires greater interface density than can be provided by a single switch, an intelligent stack of fixed configuration switches or a modular switch is recommended.

Intelligent Stacks or Modular Ethernet switches provide three major benefits:

- **Single point of management:** All switches in the stack are managed as one.
- **Built-in redundancy and high availability:** The high-speed dedicated stack connections provide redundant communication for each stack member.
- **Scalable to fit network needs:** As the need for additional access interfaces grows, adding a new switch to a stack or a module to a modular switch is easy.

Three Series of Cisco Catalyst Switches are used in this design when intelligent stacking or a modular deployment is required; The Cisco Catalyst 2960-S, 3750-X, and 4500-E.

The Cisco Catalyst 2960-S Series are fixed-configuration, stackable, 10/10/1000 Ethernet switches, with PoE+ and non-powered versions designed for entry-level enterprise, midmarket, and remote site networks.

- Cisco FlexStack is implemented by adding a stacking module to the switch. This enables up to four Catalyst 2960-S series switches to be stacked together.
- Cisco FlexStack links are full duplex 10 Gbps Ethernet links with recovery time between 1–2 seconds.

The Cisco Catalyst 3750-X Series are fixed-port, stackable, 10/100/1000 Ethernet switches, with PoE+ and non-powered versions, that provide enhanced resiliency through the StackWise Plus and StackPower technologies.

- Cisco StackWise Plus enables up to nine Cisco Catalyst 3750 switches to be stacked together using a 64-Gbps stack interconnect with subsecond failure recovery.
- Cisco StackPower shares power across the Cisco Catalyst 3750-X switch stack. This allows the flexible arrangement of power supplies in the stack, and enables a zero-footprint redundant power supply (RPS) deployment and intelligent load shedding.
- Cisco 3750-X Series have modular uplinks and support upgrading the IOS feature set and enhanced enterprise capabilities like TrustSec and Medianet, to ensure the switch functionality grows as the agency grows.

The Cisco Catalyst 4500 E-Series are modular switches that support multiple Ethernet connectivity options including 10/100/1000 Ethernet, 100 MB Fiber, Gigabit Fiber, and 10 Gigabit Fiber. The Catalyst 4500 E-Series switches also have an upgradable supervisor module which enables future functionality to be added with a supervisor module upgrade while maintaining the initial investment in the chassis and the modules.

- All key switching and forwarding components are located on the supervisor module; upgrading the supervisor upgrades the line cards.
- The Catalyst 4500 E-Series Supervisor 6L-E has uplink interfaces that can be configured as Gigabit Ethernet (with the twingig adapter) or 10-Gbps interfaces, allowing customers to easily increase bandwidth in the future.
- The Catalyst 4507R-E chassis supports redundant supervisor modules and power supplies, which increases system availability by providing 1:1 redundancy for all critical systems.
- The Catalyst 4507R-E supports stateful switchover which allows a supervisor switchover to occur with minimum disruption to the network.
- The entire software upgrade process is simplified using Cisco IOS In-Service Software Upgrades (ISSU). Not only does ISSU help eliminate errors in the software upgrade process, but additional checks are incorporated that allow the new software version to be tested and verified before completing the upgrade.

Process

1. Platform Configuration
2. LAN Switch Universal Configuration
3. Access Switch Global Configuration
4. Client Connectivity Configuration
5. Infrastructure Device Connectivity Configuration

Procedure 1 Platform Configuration

Some platforms require a one-time initial configuration prior to configuring the features and services of the switch. If you do not have a platform listed in the following steps, they can be skipped.

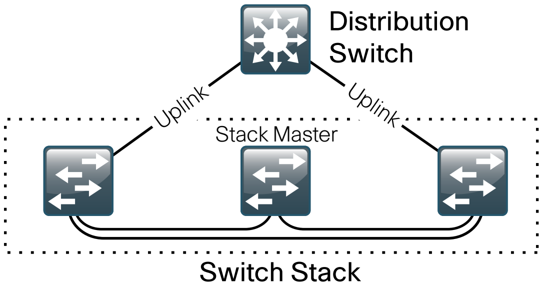
Procedure Steps:

1. Catalyst 2960-S and 3750-X Stack Configuration (Optional)
2. Catalyst 4500 Resilient Supervisor Configuration (Optional)

Step 1: Catalyst 2960-S and 3750-X Stack Configuration

When there are multiple Catalyst 2960-S or 3750-X Series switches configured in a stack, one of the switches controls the operation of the stack and is called the stack master (Figure 6).

Figure 6. Stack Master Placement in a Switch Stack



When three or more switches are configured as a stack, configure the stack master switch functionality on a switch that does not have uplinks configured. To set the stack master switch:

```
switch [switch number] priority 15
```

The default behavior when the stack master switch fails is for the newly active stack master switch to assign a new stack MAC address. This new MAC address assignment can cause the network to have to reconverge because LACP and many other protocols rely on the stack MAC address and must restart. As such, the stack-mac persistent timer 0 command should be used to ensure that the original master MAC address remains the stack MAC address after a failure.

```
stack-mac persistent timer 0
```

Step 2: Catalyst 4507R-E Resilient Supervisor Configuration

When a Catalyst 4507R-E is configured with two Supervisor 6L-Es, configure the switch to use Stateful Switchover (SSO) when moving the primary supervisor functionality between modules. To enable a fast transparent data plane failover, SSO synchronizes active process information as well as configuration information between supervisor modules.

```
redundancy
  mode sso
```

Procedure 2 LAN Switch Universal Configuration

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 will depend on your current network configuration.

Common Network Services Used in the Deployment Examples

Domain Name:	cisco.local
Active Directory, DNS, DHCP Server:	10.4.200.10
Authentication Control System:	10.4.200.15
Network Time Protocol Server:	10.4.200.17

Procedure Steps:

1. Configure the Device Hostname
2. Configure Device Resiliency Features
3. Configure Device Management Protocols
4. Configure Secure User Authentication
5. Configure a Synchronized Clock

Step 1: Configure the Device Hostname

Configure the device hostname to make it easy to identify the device.

```
hostname [hostname]
```

Step 2: Configure Device Resiliency Features

Virtual Trunk 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, adding and removing VLANs is generally not a frequent network management practice. In most cases, VLANs are defined once during switch setup with few, if any, additional modifications to the database.

The benefits of dynamic propagation of VLAN information across the network are not worth the potential for unexpected behavior due to operational error. For this reason, VTP transparent mode is configured in this architecture.

```
vtp mode transparent
```

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

While this architecture is built without any Layer 2 loops, spanning tree must still be enabled. Having spanning tree enabled ensures that if any physical or logical loops are accidentally configured, no actual layer 2 loops occur.

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

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.

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.

An easy way to remove the remote risk of this type of attack is to configure the switch to tag all native VLAN traffic. This tagging of native VLAN traffic removes any possibility that a double 802.1Q-tagged packet can hop VLANs.

```
vlan dot1q tag native
```

Unidirectional Link Detection (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.

In aggressive mode, the interface will be put into the errdisable state and will be effectively shut down when a unidirection link occurs.

```
udld aggressive
```

EtherChannels are used extensively in this design because of their resiliency capabilities. To normalize the method in which traffic is load-shared across the member links of the EtherChannel all switches should be set to use the traffic source and destination IP address when calculating which link to send the traffic across.

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

Step 3: Configure Device Management Protocols

Secure HTTP (HTTPS) and Secure Shell (SSH) are 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.

Secure management of the LAN device is enabled through the use of the SSH and HTTPS protocols. Both protocols are encrypted for privacy and the nonsecure protocols, Telnet and HTTP, are turned off.

```
ip domain-name cisco.local
ip ssh version 2
no ip http server
ip http secure-server
line vty 0 15
 transport input ssh
```

Simple Network Management Protocol (SNMP) is enabled to allow the network infrastructure devices to be managed by a Network Management System (NMS). SNMPv2c is configured both for a read-only and a read-write community string.

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

Step 4: Configure Secure User Authentication Configuration

Authentication, Authorization and Accounting (AAA) is enabled for access control. All management access to the network infrastructure devices (SSH and HTTPS) is controlled with AAA.

The AAA server used in this architecture is the Cisco Authentication Control System. Configuration of ACS is discussed in the ACS Deployment Supplement.

RADIUS 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 RADIUS server is unavailable.

```
enable secret c1sco123
service password-encryption
!
username admin password c1sco123
aaa new-model
aaa authentication login default group radius local
radius-server host 10.4.200.15 key SecretKey
```

Step 5: Setup Synchronized Clock and Timezone for Management

The Network Time Protocol (NTP) is designed to synchronize a network of devices. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the agency network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two devices to within a millisecond of one another.

Network devices should be programmed 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. Configuring console messages, logs, and debug output on switches, routers, and other devices in the network to provide time stamps on output allows cross-referencing of events in a network.

```
ntp server 10.4.200.17
ntp update-calendar
!
clock timezone PST -8
clock summer-time PDT recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

Procedure 3: Access Switch Global Configuration

Procedure Steps:

1. Configure Virtual LANs on the Switch
2. Configure In-Band Management
3. Configure DHCP Snooping and ARP Inspection

Step 1: Configure Virtual LANs on the Switch

The access layer devices use Virtual LANs (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.
- The voice VLAN provides access to the network for IP Phones.

  Both the data and the voice VLAN are 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.

  If the switch is the only switch at the site and is directly connected to a router or firewall, do not configure a management VLAN. Instead, configure the in-band management interface on the data VLAN.

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.

```
vlan [data vlan],[voice vlan],[management vlan]
```

Step 2: Configure In-Band Management

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]
```

The Catalyst 4500 does not support the **ip default-gateway** command since it has **ip routing** enabled by default. Instead use the following command on the Catalyst 4500.

```
ip route 0.0.0.0 0.0.0.0 [default router]
```

Step 3: Configure DHCP Snooping and ARP Inspection

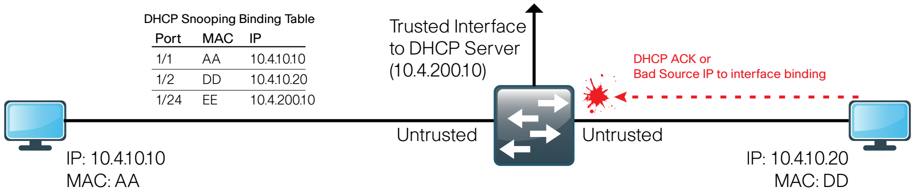
DHCP snooping is a DHCP security feature that blocks DHCP replies on an untrusted interface. An untrusted interface is any interface on the switch not specifically configured as a known DHCP server or path towards a known DHCP server.

When you enable DHCP snooping on a VLAN, the switch intercepts and safeguards DHCP messages within the VLAN. This ensures that an unauthorized DHCP server cannot serve out addresses to end-devices.

For ease of management and troubleshooting, the DHCP snooping feature tracks 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 (Figure 7). To configure DHCP Snooping, enter the following global switch commands:

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

Figure 7. DHCP Snooping and ARP inspection



DHCP Snooping Binding Table

Port	MAC	IP
1/1	AA	10.4.10.10
1/2	DD	10.4.10.20
1/24	EE	10.4.200.10

Dynamic ARP Inspection (DAI) mitigates Address Resolution Protocol (ARP) poisoning attacks. An ARP poisoning attack is a method by which an attacker sends falsified 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.

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 (Figure 7).

To configure ARP inspection, enter the following global switch commands:

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

Procedure 4 Switch Client Connectivity Configuration

Procedure Steps:

1. Configure Switch Ports to support Clients, and IP Phones
2. Configure Port Security
3. Configure DHCP Snooping and ARP Inspection
4. Configure IP Source Guard
5. Configure BPDU Guard

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. Since 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 24 interfaces (Gig 0/1 to Gig 0/24) simultaneously.

```
interface range Gigabitethernet 0/1-24
```

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 mode access
  switchport voice vlan [voice vlan]
```

Because only end-device connectivity is provided at the access layer, shorten the time it takes for the interface to go into a forwarding state by enabling portfast, disable 802.1q trunking, and disable channel grouping.

```
switchport host
```

All client facing interfaces use the cisco-phone version of AutoQoS. This allows for an untrusted PC and/or a trusted Cisco IP phone to be connected to the switch which then automatically sets QoS parameters. When a Cisco Phone is connected, trust is extended to the phone, and any device that connects to the phone will be considered untrusted and all traffic from that device will be remarked to best-effort or CoS 0.

To enable QoS, configure the following commands:

```
auto qos voip cisco-phone
```

Step 2: Configure Port Security on the Interface

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

Port security allows 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 can secure is configurable per interface. For easy management, the addresses can be learned dynamically. Using the dynamic learning method, the device secures MAC addresses as 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 once the age limit is reached.

The number of MAC addresses allowed on each interface is very agency specific. 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 agency while still protecting the network infrastructure.

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
```

Set an aging time to remove learned MAC addresses from the secured list after 2 minutes of inactivity:

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

Configure the restrict option to drop traffic from MAC addresses that are in violation, but 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 3: Configure DHCP Snooping and ARP Inspection on the Interface

Allow ARP inspection and DHCP snooping to process 100 packets per second of traffic on the port.

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

Step 4: Configure IP Source Guard on the Interface

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.

To protect against IP spoofing attacks configure:

```
ip verify source
```

The Catalyst 4500 does not support the **ip verify source** command. Instead use the following command:

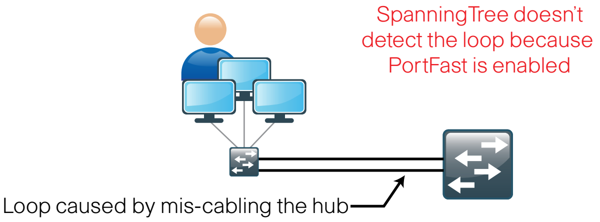
```
ip verify source vlan dhcp-snooping
```

Step 5: Configure BPDU Guard on the Interface

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 8).

Figure 8. Scenario that BPDU Guard protects against

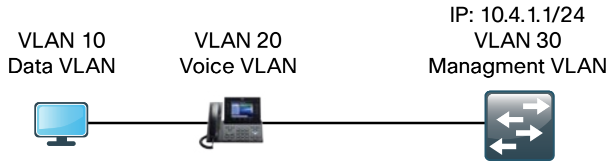

SpanningTree doesn't detect the loop because PortFast is enabled
Loop caused by mis-cabling the hub

To disable the interface if another switch is plugged into the port:

```
spanning-tree bpduguard enable
```

Procedure 3 and 4 Configuration Example

Figure 9. Procedure 3 and 4 Example



```
vlan 10,20,30
!
interface vlan 30
  description in-band management
  ip address 10.4.1.1 255.255.255.0
  no shutdown
!
ip default-gateway 10.4.1.254
!
ip dhcp snooping vlan 10,20
no ip dhcp snooping information option
ip dhcp snooping
ip arp inspection vlan 10,20
!
interface range Gigabit 0/1-24
  switchport access vlan 10
  switchport mode access
  switchport voice vlan 20
  switchport host
  auto qos voip cisco-phone
  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
  spanning-tree bpduguard enable
```

Procedure 5 Access Switch Device Configuration

Access layer devices can be one component of a larger LAN and connect to a distribution switch or, in the case of a small remote site, might be the only LAN device and connect directly to a WAN device. This procedure details how to connect an access layer device to a distribution switch or WAN router.

Procedure Steps:

1. EtherChannel Member Interface Configuration (Optional)
2. EtherChannel Member Interface QoS Configuration (Optional)
3. Trunk Configuration

Step 1: EtherChannel Member Interface Configuration

Unless the access layer device is a single fixed configuration switch connecting to a WAN router, Layer 2 EtherChannels are used to interconnect the devices in the most resilient method possible. When using EtherChannel, the member interfaces should be on different switches in the stack or different modules in the modular switch for the highest resiliency (Figure 10).

The physical interfaces that are members of a Layer 2 EtherChannel are configured prior to configuring the logical port-channel Interface. This 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 1a: EtherChannel to Distribution Switch Member Interface Configuration

Configure two or more physical interfaces to be members of the EtherChannel. It is best if they are added in multiples of two. If connecting to another switch, Link Aggregation Control Protocol is set to active on both sides to ensure a proper EtherChannel is formed and does not cause any issues.

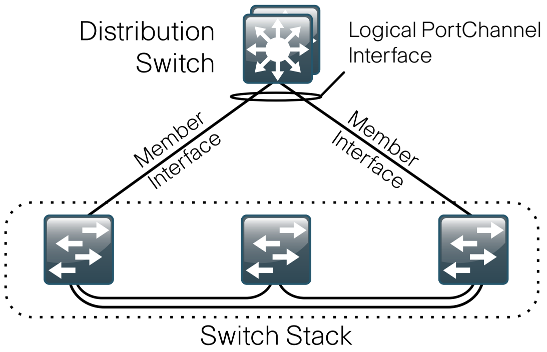
```
interface range [interface type] [port 1], [interface type] 
[port 2]
  channel-protocol lacp
  channel-group [number] mode active
```

Step 1b: EtherChannel to WAN Router Member Interface Configuration

When connecting to a network infrastructure device that does not support LACP like a router use the following commands:

```
interface range [interface type] [port 1], [interface type] 
[port 2]
  channel-group [number] mode on
```

Figure 10. EtherChannel



Step 2: EtherChannel Member Interface QoS Configuration

AutoQoS provides the majority of the configuration required to enable QoS in the access layer. However, to enable QoS on a EtherChannel link requires additional platform specific configuration.

Step 2a: Cisco Catalyst 2960-S, 3560-X, and 3750-X EtherChannel QoS

On the 2960-S, 3560-X, and 3750-X, configure QoS on the EtherChannel member interfaces . All member interfaces must be configured the same as QoS will not be invoked until all EtherChannel member interfaces are configured.

Enable QoS on the EtherChannel member interfaces, by configuring the following:

```
mls qos trust dscp
queue-set 2
srr-queue bandwidth share 10 10 60 20
priority-queue out
```

Step 2b: Cisco Catalyst 4500 Supervisor 6L-E and 6-E Etherchannel QoS

The 4500 Supervisor 6-E and Supervisor 6L-E handle QoS queuing and classification as separate functions when configuring EtherChannel and require classification commands, and policing statements to be applied to the port-channel interface and the queuing configuration commands to be applied at the physical port-level interface.

This configuration requires the creation of two policy-maps. The first policy-map contains the traffic classification commands The second, invokes queues for voice signaling and a priority queue for voice bearer traffic.

```
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
```

Enable QoS on all the EtherChannel member interfaces. Configure the following:

```
    service-policy output queue-only
```

Step 3: Trunk Configuration

An 802.1Q trunk is used for the connection to this upstream device, which allows it to provide the Layer 3 services to all the VLANs defined on the access layer switch. The VLANs allowed on the trunk are pruned to only the VLANs that are active on the access switch. DHCP Snooping and ARP Inspection are set to trust.

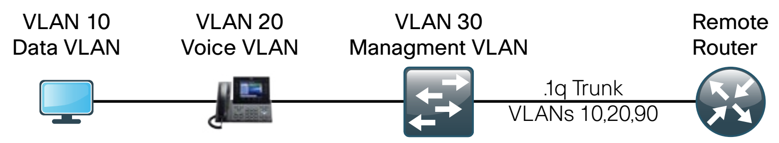
```
interface [interface type] [number]
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan [data vlan],[voice vlan],
    [mgmt vlan]
  switchport mode trunk
  ip arp inspection trust
  ip dhcp snooping trust
  no shutdown
```

The Catalyst 4500 does not require the **switchport trunk encapsulation dot1q** command. However, classification commands and policing statements must be enabled on the port-channel interface.

```
    service-policy output EC-non-queue
    service-policy input AutoQos-VoIP-Input-Dscp-Policy
```

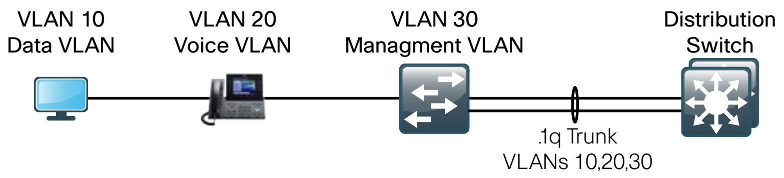
Procedure 5 Configuration Examples

Figure 11. Procedure 5 Example 1



```
interface gigabit 0/24
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 10,20,30
  switchport mode trunk
  ip arp inspection trust
  ip dhcp snooping trust
  no shutdown
```

Figure 12. Procedure 5 Example 2



```
interface range gigabit 1/25, gigabit 3/25
  channel-protocol lacp
  channel-group 1 mode active
  no shutdown
!
interface portchannel 1
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 10,20,30
  switchport mode trunk
  ip arp inspection trust
  ip dhcp snooping trust
  no shutdown
```

Notes

Distribution Layer

Agency Overview

The challenge for an agency to deliver reliably accessible user services to employees grows as the number of employees at a given location expands. As the number of access layer closets at a location grows it creates the need to aggregate the connectivity at a common point. One of the benefits of aggregation is to reduce costs by reducing the number of interconnections from each access layer switch to the rest of the network, which is used to get to the applications and resources hosted in the center of the network or across the WAN.

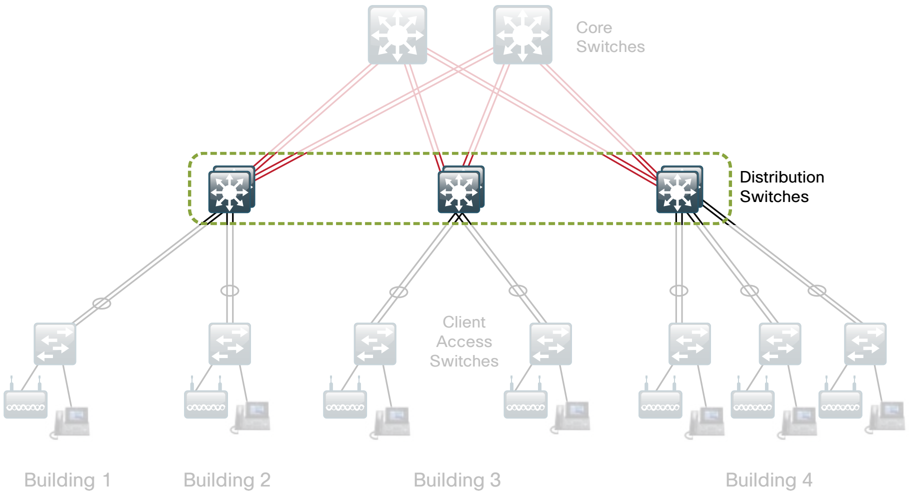
Traditional network design utilized parallel physical networks to transport different traffic types like voice or data, or to transport traffic with different security needs. To reduce costs IT organizations must create a single multi-use network infrastructure that can utilize multiple Virtual LANs (VLANs) on a single physical infrastructure. The dominant internetwork protocol in use in networks today is IP which allows a routed network topology, however some applications require that network connected endpoints are Layer 2 adjacent. The challenge for IT departments is to design a network that accommodates the application requirements without sacrificing the reliability or scalability of the network. The ability of the network design to provide an ever-increasing number of services required from the LAN and to control the increasing complexity of delivering those services without the elimination of essential functionality is the goal of the network foundation architecture.

Technology Overview

The primary function of the distribution layer is to aggregate access layer switches in a given building or campus (Figure 13). The distribution layer provides a boundary between the Layer 2 domain of the access layer and the Layer 3 domain that provides a path to the rest of the network. This boundary provides two key functions for the LAN. On the Layer 2 side the distribution layer creates a boundary for Spanning Tree Protocol limiting propagation of Layer 2 faults. On the Layer 3 side the distribution layer provides a logical point to summarize IP routing information before it enters the network and reduce IP route tables for easier troubleshooting and faster recovery from failures.

The Cisco SBA for Large Agencies Distribution Layer uses a simplified distribution layer design that is easier to operate and troubleshoot than the traditional and routed access designs.

Figure 13. Distribution Layer Overview



Traditional Distribution Layer Design

Traditional LAN designs deploy a multitier approach with Layer 2 from the access to the distribution layer where the Layer 3 boundary exists. The connectivity from the access layer to the distribution layer can result in either a loop free or looped design.

In the traditional network design, the distribution layer has two standalone switches for resiliency. It is recommended that a Layer 2 VLAN be restricted to a single wiring closet or access uplink pair to reduce or eliminate topology loops which Spanning Tree Protocol must block and that were a common point of failure in LANs (Figure 14). Restricting a VLAN to a single switch provides a loop free design but limits network flexibility. A resilient IP gateway for VLANs in this design requires the use of first-hop redundancy protocols which provide hosts with a gateway IP for a VLAN on a healthy switch. Hot Standby Routing Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP) are the most common gateway redundancy protocols, but they only allow hosts to send data out one of the access uplinks to the distribution layer. Gateway Load Balancing Protocol (GLBP) does provide greater uplink utilization for traffic exiting the access layer by balancing load from hosts across multiple uplinks, but can only be used in the non-looped topology. All of these redundancy protocols require tuning from their default settings to allow for subsecond network convergence.

Some agencies require the same Layer 2 VLAN be extended to multiple access layer closets to accommodate an application or service. The looped design causes spanning tree to block links which reduces the bandwidth from the rest of the network and can cause slower network convergence.

Figure 14. Traditional Loop Free Design with a VLAN per access switch

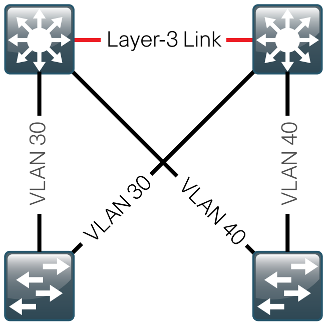


Figure 15. Traditional Looped Design with VLANs spanning access switches

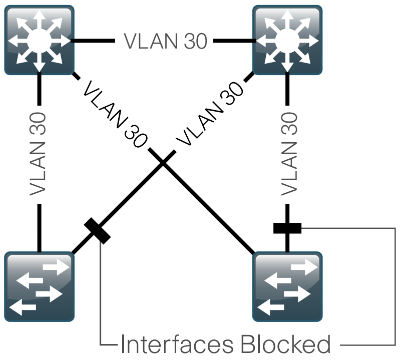


Figure 16. Simplified Design with a VLAN per access switch.

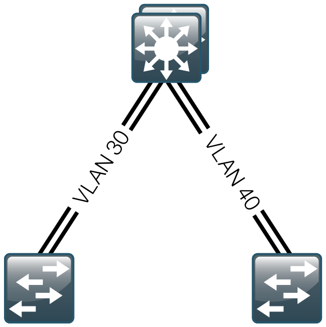
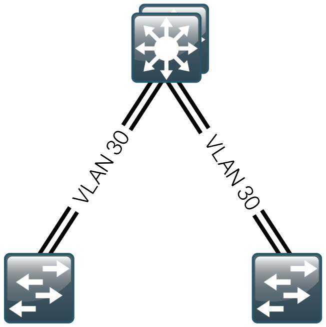


Figure 17. Simplified Design with VLANs spanning access switches



Routed Access Distribution Layer Design

Another approach to access and distribution layer design uses Layer 3 all the way to the access layer. The benefits of this design are the elimination of spanning tree loops and the reduction of protocols as the IP gateway is now the access switch. Because there are no spanning tree blocking links, we can use both uplinks to the access layer and increase effective bandwidth available to the users.

The challenge with the routed access layer design is that Layer 2 domains are confined to the access closet served by the Layer 3 access switch, which increases operational complexity, requires more IP address planning, and limits flexibility for applications that require Layer 2 connectivity.

Simplified Distribution Layer Design

The distribution layer design in the Borderless Network for Large Agencies uses multiple physical switches that act as a single logical switch or a single, highly-redundant physical switch. One advantage of this design is that Spanning Tree dependence is minimized and even in the distributed VLAN design, Spanning Tree blocked links due to looped topologies are eliminated, and all uplinks from the access layer to the distribution are active and passing traffic. Reducing the dependence on Spanning Tree is accomplished by using EtherChannel. EtherChannel to the access layer with dual homed uplinks is a key characteristic of this design and can load balance up to eight links if needed for additional bandwidth.

There are several other advantages to the simplified distribution layer design. IP gateway redundancy protocols like HSRP, VRRP, and GLBP are no longer needed because the default IP gateway is now on a single logical interface and resiliency is provided by the distribution layer switch or switches themselves. Also, the network will converge faster now that it is not depending on spanning tree to unblock links when a failure occurs because EtherChannel provides fast subsecond failover between links in an uplink bundle.

The topology of the network from the distribution layer to the access layer is logically hub-and-spoke which reduces complexity of design and troubleshooting. The hub and spoke design provides a more efficient operation for IP Multicast in the distribution layer because there is now a single logical designated router to forward IP Multicast packets to a given VLAN in the access layer.

Finally, by using the single logical distribution layer design, there are fewer boxes to manage which eases ongoing provisioning and maintenance.

Distribution Layer Platforms

Multiple platforms can be used to deploy the simplified distribution layer design. Physically, the distribution layer can be a Cisco Catalyst 6500 Virtual Switching System (VSS) 1440, a highly available Cisco Catalyst 4507R-E switch, or a stack of Cisco Catalyst 3750 switches. It is important to note that although each switch has different physical characteristics, each appears to the rest of the network as a single node and provides a fully resilient design.

Cisco Catalyst 6500 VSS 1440 effectively allows the clustering of two physical chassis into a logical entity that can be operated as a single device. This configuration provides redundant chassis, supervisors, line cards, and power supplies and can provide the highest density of the product options for Gigabit Ethernet and 10 Gigabit Ethernet EtherChannel uplinks using Cisco Multi-chassis EtherChannel. The Cisco Catalyst 6500 VSS 1440 provides stateful switchover between supervisors in each chassis for Nonstop Forwarding in the event of a failure and provides Enhanced Fast Software Upgrades for minimizing downtime for upgrades. The Cisco Catalyst 6500 VSS 1440 is the premier distribution layer platform in this design. It allows for high density aggregation of Gigabit Ethernet and 10 Gigabit Ethernet connected wiring closets, while providing an advanced feature set and the highest resiliency of the available platforms.

The Cisco Catalyst 4507R-E switch has redundant supervisors, line cards, and power supplies. A single 4507R-E chassis configured with resilient components is used as a distribution layer platform in this design. The Supervisor 6E has the ability to provide a medium density of Gigabit Ethernet and even 10 Gigabit Ethernet EtherChannel links to the access layer. The dual supervisor Cisco Catalyst 4507R provides stateful switchover which is critical to Nonstop Forwarding in the event of a failure and allows in-service software upgrades for the system. The Cisco Catalyst 4507R-E should be utilized at locations where there is only a small number of Gigabit Ethernet or 10 Gigabit Ethernet connected wiring closets that need to be aggregated.

The Cisco Catalyst 3750 stack configures as a single unit, but has an independent power supply and processor for each switch in the StackWise stack. The Cisco SBA for Large Agencies—Borderless Networks LAN design uses a pair of stacked Cisco Catalyst 3750-12S-E switches that provide Layer 2 and Layer 3 switching and use Small Form Pluggable transceivers for a port-by-port option of copper or fiber optic Gigabit Ethernet EtherChannel uplinks. The Cisco Catalyst 3750-12S-E should be used at locations where there is only a small number of gigabit connected wiring closests that need to be aggregated.

Configuration Procedure Details

The single, logical, resilient, distribution-layer design simplifies the distribution switch configuration over traditional dual system designs.

Process

1. Platform Configuration
2. LAN Switch Universal Configuration
3. Distribution Switch Global Configuration
4. Access Layer Aggregation Configuration
5. Connectivity to WAN Routers and the LAN Core Configuration

Procedure 1 Platform Configuration

Some platforms require a one-time initial configuration prior to configuring the features and services of the switch. If you do not have a platform listed in the following steps, they can be skipped.

Procedure 1a Cisco Catalyst 6500 Virtual Switching System 1440

The Cisco Catalyst 6500 Virtual Switching System 1440 clusters two physical 6500 switches with a single supervisor in each switch together as a single logical switch. One of the supervisors acts as the active control plane for both chassis by controlling protocols such as EIGRP, Spanning Tree, CDP, and so forth, and both supervisors actively switch packets in each chassis.

The following configuration example shows you how to configure the Virtual Switching System between the two new unconfigured chassis. If you are migrating your switches from an existing in-service dual chassis role to a VSS system, go to www.cisco.com and search on “Migrate Standalone Cisco Catalyst 6500 Switch to Cisco Catalyst 6500 Virtual Switching System” for information that describes hot to do this migration. For an in-depth VSS configuration guide and configuration options, go to www.cisco.com and search for the Campus 3.0 Virtual Switching System Design Guide.

In the setup for the Cisco Catalyst 6500 Virtual Switching System 1440, connect two 10 Gigabit Ethernet links between the chassis to provides the Virtual Switch Link (VSL). Use at least two links, however there are restrictions on which 10 Gigabit Ethernet interfaces can be used for the VSL. This design uses the two 10 Gigabit Ethernet interfaces on each supervisor; the interfaces must be cabled together before the VSS can be configured.

This design uses IOS 12.2(33) SXI3 with the IP Services Feature Set. for all configuration examples. Prior IOS versions need additional commands, and should not be used with this deployment guide.

Virtual Switching System Platform Configuration Procedure Details

Procedure Steps

1. Convert standalone 6500s to VSS
2. Configure the Virtual Switch Link
3. Enable Virtual Mode Operation
4. Configure Dual Active Detection
5. Configure the System Virtual MAC Address
6. Save and Reload the Switch
7. Configure Quality of Service

Step 1: Convert standalone 6500s to VSS

Configure a hostname on each switch so you can keep track of your programming steps:

On the Catalyst 6500 standalone switch #1:

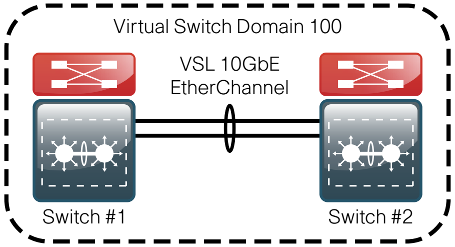
```
Router#config t
Router#(config)#hostname VSS-Sw1
```

On the Catalyst 6500 standalone switch #2:

```
Router#config t
Router#(config)#hostname VSS-Sw2
```

Each VSS switch pair must have a unique domain assigned that the pair shares. The domain number 100 is used in this example (Figure 18). Each switch is also given a unique number in the domain, switch 1 or switch 2.

Figure 18. VSS Domain



On the standalone switch #1:

```
VSS-Sw1(config)#switch virtual domain 100
VSS-Sw1(config-vs-domain)# switch 1
```

On the standalone switch #2:

```
VSS-Sw2(config)#switch virtual domain 100
VSS-Sw2(config-vs-domain)# switch 2
```

Step 2: Configure the Virtual Switch Link

The VSL link is a critical component of the Virtual Switching System. Use unique port-channel numbers on each switch even though they connect to each other because both switches will soon become a single logical switch. This example uses port-channel number 101 on switch 1 and port-channel number 102 on switch 2. For the physical interfaces of the VSL EtherChannel, this example uses the 10 Gigabit Ethernet interfaces on the Supervisor.

On standalone switch #1:

```
VSS-Sw1(config)#interface port-channel 101
VSS-Sw1(config-if)#switch virtual link 1
VSS-Sw1(config)#interface range tengigabit 5/4-5
VSS-Sw1(config-if)#channel-group 101 mode on
VSS-Sw1(config-if)#no shutdown
```

On standalone switch #2:

```
VSS-Sw2(config)#interface port-channel 102
VSS-Sw2(config-if)#switch virtual link 2
VSS-Sw2(config)#interface range tengigabit 5/4-5
VSS-Sw2(config-if)#channel-group 102 mode on
VSS-Sw2(config-if)#no shutdown
```

At this point you should be able to see that port-channel 101 and 102 are up and both links are active, but the switch is not in VSS mode yet.

```
VSS-Sw1# show etherchannel 101 port
VSS-Sw2# show etherchannel 102 port
VSS-Sw2#show etherchannel 102 port

        Ports in the group:
        -------------------
Port: Te5/4
------------
Port state  = Up Mstr In-Bndl
Port: Te5/5
------------
Port state  = Up Mstr In-Bndl
```

Step 3: Enable Virtual Mode Operation

Now that a port-channel has been established between the switches, convert each switch to virtual mode operation. At the enable prompt (not in configuration mode) on each switch, enter the following command:

```
VSS-Sw1# switch convert mode virtual
VSS-Sw2# switch convert mode virtual
```

When asked if you want to proceed answer yes.

Each switch now renumbers its interfaces from interface y/z where y is the slot number and z is the interface number, to interface x/y/z where x is the switch number, y is the module number in that switch, and z is the interface on that module. This numbering scheme allows the two chassis to be addressed and configured as a single system from a single supervisor, which is the supervisor with the active control plane.

Once the configuration changes, it prompts to save the configuration to bootflash. Press Return <CR> or Enter to accept the destination filename and location on each switch.

Both switches reload and become a Virtual Switching System and one of the switches is resolved as the ACTIVE supervisor for the VSS cluster. All configuration commands now must be entered on the single active switch console; the standby switch console displays the Standby prompt.

The following command checks that both switches see each other, that they are in SSO mode, and that the second supervisor is in standby hot status.

```
VSS-Sw1#show switch virtual redundancy
```

To recognize that the two Catalyst 6500 switches are now operating as a single VSS system, rename the switch hostname.

```
VSS-Sw1(config)#hostname 6500VSS
6500VSS(config)#
```

Step 4: Configure Dual-Active Detection

A critical aspect of the Cisco Catalyst 6500 VSS 1440 is that a single supervisor is active for the control plane in both switches. Recall that each supervisor is active for its respective chassis and it switches data packets from input interfaces to output interfaces , but a single supervisor is active for EIGRP, Spanning Tree, and so on for the control plane. The Virtual Switch Link (VSL) allows the supervisors to stay in synchronization.

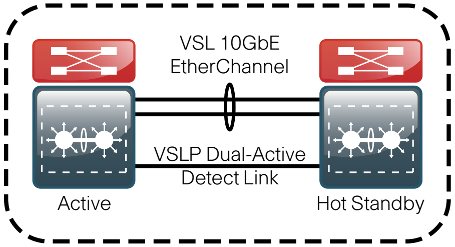
In the event that the VSL link is severed (all links), or for any other reason, both supervisors assume the active role, there are safeguards to have the previously active supervisor shut down all of its interfaces to prevent loops in the network and to have the previous standby supervisor become the active supervisor.

There are three methods to detect this dual-active condition:

- Ethernet Fast-Hello (VSLP) packet mode link
- Port Aggregation Protocol (PAgP) hellos between an adjacent switch to the VSS
- A configured Bidirectional Forwarding Detect (BFD) peer configuration between supervisors

This design uses the Fast-Hello (VSLP) packet mode link for dual-active detection. To configure the link, use a Gigabit Ethernet interface on each VSS switch chassis and cable them together (similar to a VSL link) in a back-to-back fashion (Figure 19). This link does not require high bandwidth as it is only a detection link with control plane hellos on it.

Figure 19. VSLP



```
VSS-Sw1(config)# switch virtual domain 100
VSS-Sw1(config-vs-domain)#dual-active detection fast-hello
VSS-Sw1(config)#interface range gigabit1/1/8, gigabit2/1/8
VSS-Sw1(config-if-range)#dual-active fast-hello
VSS-Sw1(config-if-range)#no shutdown

*Feb 25 14:28:39.294: %VSDA-SW2_SPSTBY-5-LINK_UP: Interface
Gi2/1/8 is now dual-active detection capable
*Feb 25 14:28:39.323: %VSDA-SW1_SP-5-LINK_UP: Interface
Gi1/1/8 is now dual-active detection capable
```

Step 5: Configure the System Virtual MAC Address

By default, the VSS system uses the default chassis-based MAC-address pool assigned to the switch that is resolved to be the active switch when the switches initialize. Although the MAC addresses do not change when the active supervisor is switched to the standby, it is best to avoid gratuitous ARP updates to connected devices. If both switches are reloaded at the same time and the opposite supervisor comes up first and becomes the active supervisor, it would use the MAC address pool assigned to that switch. Set a virtual MAC address for the VSS system so that either active supervisor will use the same MAC address pool, regardless of which supervisor is active, even across a system reboot.

```
6500-VSS(config)# switch virtual domain 100
6500-VSS(config-vs-domain)# mac-address use-virtual
Configured Router mac address is different from operational
value. Change will take effect after config is saved and
the entire Virtual Switching System (Active and Standby) is
reloaded.
```

Step 6: Save and Reload the Switch

Save the running configuration and then reload the entire system (both chassis):

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

When the switches initialize after this final reload, the VSS programming is complete.

Step 7: Configure Quality of Service

On the Catalyst 6500 Series switches, QoS is enabled globally and primarily configured at the port level. When you enable QoS with the **mls qos** command, default queuing is enabled on all interfaces and they are considered untrusted. All connections in the distribution and core are configured to trust DSCP.

Even though this design is configured to trust DSCP markings, it is a best practice to ensure proper mapping of CoS to DSCP for VoIP. This mapping is accomplished by overriding the default mapping of CoS 5 “voice bearer traffic” to DSCP 40, with DSCP 46, which is the EF per-hop behavior for voice.

Enable QoS globally and modify the global default COS to DSCP mapping.

```
mls qos
mls qos map cos-dscp 0 8 16 24 32 46 48 56
```

Procedure 1b Catalyst 4507R-E Resilient Supervisor Configuration

When a Catalyst 4507R-E is configured with two Supervisor 6L-Es, configure the switch to use Stateful Switchover (SSO) when moving the primary supervisor functionality between modules. To enable a fast transparent data plane failover, SSO synchronizes active process information as well as configuration information between supervisor modules.

```
redundancy
  mode sso
```

Since AutoQoS may not be configured on this device, manually configure the global QoS settings by enter the following:

```
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
```

The 4500 Supervisor 6-E and Supervisor 6L-E handle QoS queuing and classification as separate functions when configuring EtherChannel. Both supervisors require classification commands, and policing statements to be applied to the port-channel interface and the queuing configuration commands to be applied at the physical port-level interface.

This configuration requires the creation of two policy-maps. The first policy-map contains the traffic classification commands. The second, invokes queues for voice signaling and a priority queue for voice bearer traffic.

```
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
```

Procedure 1c Catalyst 3750G-12S and 3750-X Platform Configuration

When there are multiple switches configured in a stack, one of the switches controls the operation of the stack and is called the stack master.

When three or more switches are configured as a stack, configure the stack master switch functionality on a switch that does not have uplinks configured. To set the stack master switch:

```
switch [switch number] priority 15
```

The default behavior when the stack master switch fails is for the newly active stack master switch to assign a new stack MAC address. This new MAC address assignment can cause the network to have to reconverge because LACP and many other protocols rely on the stack MAC address and must restart. As such, the **stack-mac persistent timer 0** command should be used to ensure that the original master MAC address remains the stack MAC address after a failure.

```
stack-mac persistent timer 0
```

Since AutoQoS may not be configured on this device, manually configure the global QoS settings by entering the following commands:

```
mls qos
mls qos map policed-dscp 24 26 46 to 0
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue input bandwidth 90 10
mls qos srr-queue input threshold 1 8 16
mls qos srr-queue input threshold 2 34 66
mls qos srr-queue input buffers 67 33
mls qos srr-queue input cos-map queue 1 threshold 2 1
mls qos srr-queue input cos-map queue 1 threshold 3 0
mls qos srr-queue input cos-map queue 2 threshold 1 2
mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7
mls qos srr-queue input cos-map queue 2 threshold 3 3 5
mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14
15
mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7
mls qos srr-queue input dscp-map queue 1 threshold 3 32
mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20
21 22 23
mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37
38 39 48
mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53
54 55 56
mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61
62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44
45 46 47
mls qos srr-queue output cos-map queue 1 threshold 3 5
mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 2 4
mls qos srr-queue output cos-map queue 4 threshold 2 1
mls qos srr-queue output cos-map queue 4 threshold 3 0
mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44
45 46 47
mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28
29 30 31
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 16 17 18 19 20
21 22 23
mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36
37 38 39
mls qos srr-queue output dscp-map queue 4 threshold 1 8
mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13
14 15
mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7
mls qos queue-set output 1 threshold 1 138 138 92 138
mls qos queue-set output 1 threshold 2 138 138 92 400
mls qos queue-set output 1 threshold 3 36 77 100 318
mls qos queue-set output 1 threshold 4 20 50 67 400
mls qos queue-set output 2 threshold 1 149 149 100 149
mls qos queue-set output 2 threshold 2 118 118 100 235
mls qos queue-set output 2 threshold 3 41 68 100 272
mls qos queue-set output 2 threshold 4 42 72 100 242
mls qos queue-set output 1 buffers 10 10 26 54
mls qos queue-set output 2 buffers 16 6 17 61
```

Procedure 2 LAN Switch Universal Configuration

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 will depend on your current network configuration.

Common Network Services Used in the Deployment Examples

Domain Name:	cisco.local
Active Directory, DNS, DHCP Server:	10.4.200.10
Authentication Control System:	10.4.200.15
Network Time Protocol Server:	10.4.200.17

Procedure Steps:

1. Configure the Device Hostname
2. Configure Device Resiliency Features
3. Configure Device Management Protocols
4. Configure Secure User Authentication
5. Configure a Synchronized Clock and Timezone for Management

Step 1: Configure the Device Hostname

Configure the device hostname to make it easy to identify the device.

```
hostname [hostname]
```

Step 2: Configure Device Resiliency Features

Virtual Trunk 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, adding and removing VLANs is generally not a frequent network management practice. In most cases, VLANs are defined once during switch setup with few, if any, additional modifications to the database.

The benefits of dynamic propagation of VLAN information across the network are not worth the potential for unexpected behavior due to operational error. For this reason, VTP transparent mode is configured in this architecture.

```
vtp mode transparent
```

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

While this architecture is built without any Layer 2 loops, spanning tree must still be enabled. Having spanning tree enabled ensures that if any physical or logical loops are accidentally configured, no actual Layer 2 loops occur.

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

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.

At first glance, this form of attack 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.

An easy way to remove the remote risk of this type of attack is to configure the switch to tag all native VLAN traffic. This tagging of native VLAN traffic removes any possibility that a double 802.1Q-tagged packet can hop VLANs.

```
vlan dot1q tag native
```

Unidirectional Link Detection (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. 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.

In aggressive mode, the interface will be put into the errdisable state and will be effectively shut down when a unidirection link occurs.

```
udld aggressive
```

EtherChannels are used extensively in this design because of their resiliency capabilities. To normalize the method in which traffic is load-shared across the member links of the EtherChannel, all switches should be set to use the traffics source and destination IP Address when calculating which link to send the traffic across.

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

Step 3: Configure Device Management Protocols

Secure HTTP (HTTPS) and Secure Shell (SSH) are 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.

Secure management of the LAN device is enabled through the use of the SSH and HTTPS protocols. Both protocols are encrypted for privacy and the nonsecure protocols, Telnet and HTTP, are turned off.

```
ip domain-name cisco.local
ip ssh version 2
no ip http server
ip http secure-server
line vty 0 15
  transport input ssh
```

Simple Network Management Protocol (SNMP) is enabled to allow the network infrastructure devices to be managed by a Network Management System (NMS). SNMPv2c is configured both for a read-only and a read-write community string.

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

Step 4: Configure Secure User Authentication Configuration

Authentication, Authorization and Accounting (AAA) is enabled for access control. All management access to the network infrastructure devices (SSH and HTTPS) is controlled with AAA.

The AAA server used in this architecture is the Cisco Authentication Control System. Configuration of ACS is discussed in the ACS Deployment Supplement.

RADIUS 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 RADIUS server is unavailable.

```
enable secret c1sco123
service password-encryption
!
username admin password c1sco123
aaa new-model
aaa authentication login default group radius local
radius-server host 10.4.200.15 key SecretKey
```

Step 5: Configure a Synchronized Clock and Timezone for Management

The Network Time Protocol (NTP) is designed to synchronize a network of devices. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the agency network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two devices to within a millisecond of one another.

Network devices should be programmed 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. Configuring console messages, logs, and debug output on switches, routers, and other devices in the network to provide timestamps on output allows cross-referencing of events in a network.

```
ntp server 10.4.200.17
ntp update-calendar
!
clock timezone PST -8
clock summer-time PDT recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

Procedure 3 Distribution Layer Switch Global Configuration

1. Configure an In-Band Management Interface
2. Configure IP Unicast Routing
3. Configure IP Multicast Routing

Step 1: Configure an In-Band Management Interface

The loopback interface is a logical interface that is always reachable as long as the device is powered on and any IP interface is reachable to the network. Because of this capability, the loopback address is the best way to manage the switch in-band. Layer 3 process and features are also bound to the Loopback interface to ensure process resiliency.

The loopback address is commonly a host address with a 32-bit address mask. Allocate the loopback address from the IP address block that the distribution switch summarizes to the rest of the network. .

```
interface loopback 1
  ip address [ip address] 255.255.255.255
  ip pim sparse-mode
```

The **ip pim sparse-mode** command will be explained further in step 3.

Bind the SNMP and SSH processes to the Loopback interface address for optimal resiliency:

```
snmp-server trap-source loopback 1
ip ssh source-interface loopback 1
```

Step 2: Configure IP Unicast Routing

EIGRP is the IP unicast routing protocol used in this design because it is easy to configure, does not require a large amount of planning, has flexible summarization and filtering, and can scale to large networks.

Enable EIGRP for the IP address space that the network will be using. If needed for your network, you can enter multiple network statements. Disable auto summarization of the IP networks and enable all routed links to be passive by default. The Loopback 1 IP address is used for the EIGRP router ID to ensure maximum resiliency.

The single logical distribution layer design uses stateful switchover and non-stop forwarding to provide subsecond failover in the event of a supervisor data or control plane failure. This ability reduces packet loss in switchover to redundant logic and keeps packets flowing when the data plane is still intact to adjacent nodes. In the stack-based distribution layer approach, a single logical control point still exists and the master control plane in a stack can fail over to another member in the stack providing near-second or subsecond resiliency.

When the supervisor or master switch of a distribution platform switches over from the Active to the Hot-Standby supervisor, it will continue switching IP data traffic flows in hardware. However, the supervisor requires time to reestablish control plane two-way peering with EIGRP routing neighbors and avoid the peer router from tearing down adjacencies due to missed hellos that would cause a reroute and disruption of traffic. To allow this time for the supervisor to recover, there is a Nonstop Forwarding (NSF) setting for the routing protocol to wait for the dual supervisor peer switch to recover. The neighboring router is said to be NSF aware if it has a newer release of IOS that recognizes an NSF peer. All of the platforms used in this design are NSF aware for the routing protocols in use.

The distribution layer switch must be configured to enable Nonstop Forwarding for the protocol in use so that it can signal a peer when it switches over to a Hot-Standby supervisor for the peering neighbor to allow it time to reestablish the EIGRP protocol to that node. No tuning of the default NSF timers is needed in this network. Nothing has to be configured for an NSF aware peer router.

```
ip routing
!
router eigrp [as number]
  network [network] [inverse mask]
  no auto-summary
  passive-interface default
  eigrp router-id [ip address of loopback 1]
  nsf
```

The Cisco Catalyst 6500 does not require the **ip routing** command, it is enabled by default on that platform.

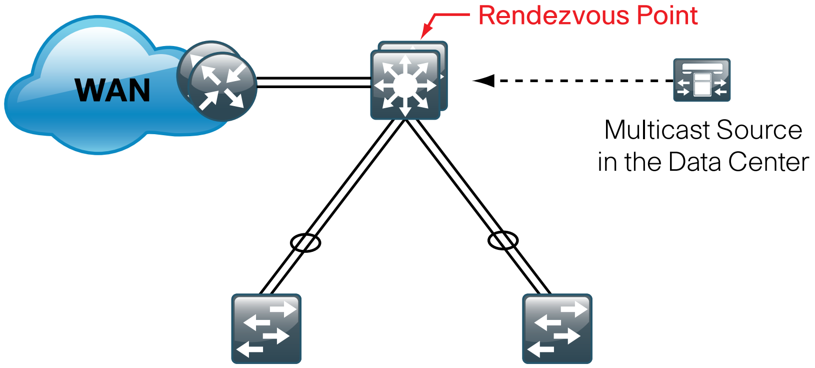
Step 3: Configure IP Multicast Routing

IP multicast allows a single IP data stream to be replicated by the infrastructure (routers and switches) and sent from a single source to multiple receivers. Using IP multicast is much more efficient than multiple individual unicast streams or a Broadcast stream that would propagate everywhere. IP Telephony Music on Hold and IP Video Broadcast Streaming are two examples of IP Multicast applications.

To receive a particular IP multicast data stream, end hosts must join a multicast group by sending an Internet Group Membership Protocol (IGMP) message to their local multicast router. In a traditional IP multicast design, the local router consults another router in the network that is acting as a Rendezvous Point (RP) to map the receivers to active sources so they can join their streams.

The RP is a control plane operation that should be placed in the core of the network or close to the IP multicast sources on a pair of Layer 3 switches or routers (Figure 20). IP multicast routing begins at the distribution layer if the access layer is Layer 2 and provides connectivity to the IP Multicast Rendezvous Point (RP). In designs without a core layer, the distribution layer will perform the RP function.

Figure 20. Rendezvous Point Placement in the Network



In this design, based on sparse mode multicast operation, Anycast RP is used to provide a simple yet scalable way to provide a highly resilient RP environment.

Enable IP multicast routing on the platforms in the global configuration mode.

```
ip multicast-routing
```

The Cisco Catalyst 3750 Series switches instead require the **ip multicast-routing distributed** command.

Every Layer 3 switch and router must be configured with the address of the IP multicast RP. Use the **rp-address** command in conjunction with an access-list to limit the network size that the RP is responsible for. This configuration provides for future scaling and control of the IP multicast environment and can change based on network needs and design.

```
ip pim rp-address [rp address] [acl number]
access-list [acl number] permit [multicast network] [inverse 
mask]
```

All Layer 3 interfaces in the network must be enabled for sparse mode multicast operation.

```
ip pim sparse-mode
```

Procedure 3 Example

```
interface loopback 1
  ip address 10.4.60.252 255.255.255.255
  ip pim sparse-mode
!
snmp-server trap-source loopback 1
ip ssh source-interface loopback 1
!
ip routing
!
router eigrp 100
  network 10.4.0.0 0.0.255.255
  no auto-summary
  passive-interface default
  eigrp router-id 10.4.60.252
  nsf
!
ip multicast-routing
!
ip pim rp-address 10.4.60.252 10
access-list 10 permit 239.1.0.0 0.0.255.255
```

Procedure 4 Distribution Layer Connectivity to Access Layer

1. Configure Layer 2
2. Configure EtherChannel Member Interfaces
3. Configure EtherChannel Member Interface QoS
4. Configure Trunk
5. Configure Layer 3

The resilient, single, logical, distribution layer switch design is based on a hub-and-spoke or star design. The links to access layer switches and connected routers are Layer 2 EtherChannels. Links to other distribution layers, and the optional core are Layer 3 links or Layer 3 EtherChannels.

Step 1: Configure Layer 2

With the hub-and-spoke design, there are no spanning-tree loops or blocked links; however, Rapid PVST is still enabled to protect against unintentional loops.

Set the distribution layer switch to be the Spanning Tree Root for the VLANs on the access layer switches that you are connecting to the distribution switch.

```
vlan [data vlan],[voice vlan],[management vlan]
spanning-tree vlan [data vlan],[voice vlan],[mgmt vlan] root 
primary
```

Step 2: Configure EtherChannel Member Interfaces

We use Layer 2 EtherChannels to connect all access layer switches to the distribution layer and thereby create the hub-and-spoke resilient design that eliminates spanning-tree loops.

EtherChannel is a logical interface which can use a control plane protocol to manage the physical members of the bundle. Running a channel protocol is desired over forced-on mode because it performs consistency checks for interfaces programmed to be in the channel and provides protection to the system from inconsistent configurations. Cisco Catalyst switches provide both Port Aggregation Protocol (PAgP), which is a widely deployed Cisco designed protocol, and Link Aggregation Protocol (LACP) based on IEEE 802.3ad. This design uses LACP for EtherChannel because it is the only protocol supported in a Catalyst 3750 cross-stack configuration and can be used in all configurations in this design.

Connect the access layer EtherChannel uplinks to separate switches in the distribution layer switches or stack, and in the case of the Cisco Catalyst 4507R-E distribution layer, to separate redundant modules for additional resiliency.

The physical interfaces that are members of a Layer 2 EtherChannel are configured prior to configuring the logical port-channel interface. Doing the configuration in this order 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.

Configure two or more physical interfaces to be members of the EtherChannel. It is best if they are added in multiples of two. If connecting to another switch, Link Aggregation Control Protocol is set to active on both sides to ensure a proper EtherChannel is formed and does not cause any issues.

```
interface range [interface type] [port 1], [interface type] 
[port 2]
  switchport
  channel-protocol lacp
  channel-group [number] mode active
```

Step 3: Configure EtherChannel Member Interface QoS

To enable QoS on a EtherChannel link, some platforms require configuration on the EtherChannel Member Interfaces.

Step 3a: Cisco Catalyst 3750 EtherChannel QoS

On the Catalyst 3750 switch, configure QoS on the EtherChannel member interfaces . All member interfaces must be configured the same as QoS will not be invoked until all EtherChannel member interfaces are configured.

Enable QoS on the EtherChannel member interfaces, configure the following :

```
mls qos trust dscp
queue-set 2
srr-queue bandwidth share 10 10 60 20
priority-queue out
```

Step 3b: Cisco Catalyst 4500 Supervisor 6L-E and 6-E Etherchannel QoS

The 4500 Supervisor 6-E and Supervisor 6L-E handle QoS queuing and classification as separate functions when configuring EtherChannel. Both supervisors require classification commands, and policing statements to be applied to the port-channel interface and the queuing configuration commands to be applied at the physical port-level interface.

Enable QoS on all the EtherChannel member interfaces , configure the following:

```
service-policy output queue-only
```

Step 4: Configure Trunk

An 802.1Q trunk is used for the connection to the access layer which allows the distribution switch to provide the Layer 3 services to all the VLANs defined on the access layer switch. The VLANs allowed on the trunk are pruned to only the VLANs that are active on the access switch. .

```
interface [interface type] [number]
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan [data vlan],[voice vlan],
    [mgmt vlan]
  switchport mode trunk
  no shutdown
```

The Catalyst 4500 does not require the **switchport trunk encapsulation dot1q** command. However, classification commands and policing statements that were configured in Procedure 1 must be enabled on the port-channel interface.

```
service-policy output EC-non-queue
service-policy input AutoQos-VoIP-Input-Dscp-Policy
```

The Catalyst 6500 additionally must be configured to trust the QoS markings entering the switch on the port-channel interface.

```
mls qos trust dscp
```

Step 5: Configure Layer 3

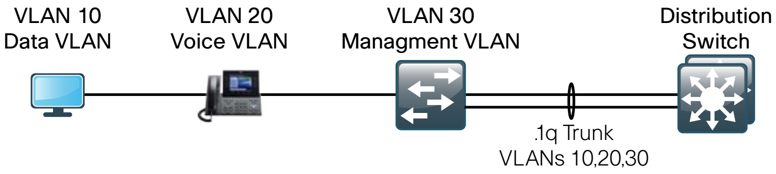
Configure a VLAN interface (SVI) for every access layer VLAN so devices in the VLAN can communicate with the rest of the network.

Use the **ip helper-address** command to allow remote DHCP servers to provide IP Addresses for this network. The address that the helper command points to is the DHCP server and if you have more than one DHCP server, multiple helper commands can be listed on an interface.

```
interface vlan [number]
  ip address [ip address] [mask]
  ip helper-address [dhcp server ip]
  ip pim sparse-mode
```

Procedure 4 Example

Figure 21. Procedure 4 Example



```
vlan 10,20,30
spanning-tree vlan 10,20,30 root primary
!
interface range gigabit 1/1/1, gigabit 2/1/1
  channel-protocol lacp
  channel-group 10 mode active
  no shutdown
!
interface portchannel 10
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 10,20,30
  switchport mode trunk
  no shutdown
!
interface vlan 10
  ip address 10.4.1.0 255.255.255.0
  ip helper-address 10.4.200.10
  ip pim sparse-mode
!
interface vlan 20
  ip address 10.4.2.0 255.255.255.0
  ip helper-address 10.4.200.10
  ip pim sparse-mode
!
interface vlan 30
  ip address 10.4.3.0 255.255.255.0
  ip helper-address 10.4.200.10
  ip pim sparse-mode
```

Procedure 5 Connectivity to WAN Routers and LAN Core

1. Configure Layer 3 EtherChannel Interface
2. Configure EtherChannel Member Interfaces
3. Conifugre EtherChannel Member Interface QoS
4. Configure the EIGRP Interface

Step 1: Configure Layer 3 EtherChannel Interface

Any links to connected WAN routers, adjacent distribution layers, or a core layer should be Layer 3 links or Layer 3 EtherChannels. When creating a Layer 3 EtherChannel, create the logical port-channel interface first.

```
interface port-channel [number]
  no switchport
  ip address [ip address] [mask]
  ip pim sparse-mode
  no shutdown
```

As networks grow, the number of IP subnets or routes in the routing tables grows as well. To reduce the amount of bandwidth, processor, and memory necessary to carry large route tables and to reduce convergence time around a link failure, configure IP summarization on links where logical boundaries exist.

The Catalyst 4500 requires classification commands and policing statements to be enabled on the port-channel interface.

```
  service-policy output EC-non-queue
  service-policy input AutoQos-VoIP-Input-Dscp-Policy
```

The Catalyst 6500 must be configured to trust the QoS markings entering the switch on the port-channel interface.

```
  mls qos trust dscp
```

Configure EIGRP summarization on the interface if the connected device provides connectivity to another piece of the network like the WAN, Internet, or LAN core.

```
  ip summary-address eigrp [as number] [network] [mask]
```

Step 2: Configure EtherChannel Member Interfaces

Configure the physical interfaces to tie to the logical port-channel using the **channel-group** command. The number for the port-channel and channel-group will match.

```
interface range [interface type] [port 1], [interface type] 
[port 2]
  no switchport
  channel-protocol lacp
  channel-group [number] mode active
  no shutdown
```

Step 3: Configure EtherChannel Member Interface QoS

To enable QoS on a EtherChannel link, some platforms require configuration on the EtherChannel Member Interfaces.

Step 3a: Cisco Catalyst 3750 EtherChannel QoS

On the Catalyst 3750 switch, configure QoS on the EtherChannel member interfaces . All member interfaces must be configured the same as QoS will not be invoked until all EtherChannel member interfaces are configured.

Enable QoS on the EtherChannel member interfaces, configure the following :

```
mls qos trust dscp
queue-set 2
srr-queue bandwidth share 10 10 60 20
priority-queue out
```

Step 3b: Cisco Catalyst 4500 Supervisor 6L-E and 6-E Etherchannel QoS

The 4500 Supervisor 6-E and Supervisor 6L-E handle QoS queuing and classification as separate functions when configuring EtherChannel. Both supervisors require classification commands, and policing statements to be applied to the port-channel interface and the queuing configuration commands to be applied at the physical port-level interface. To enable QoS on all the EtherChannel member interfaces , configure the following:

```
service-policy output queue-only
```

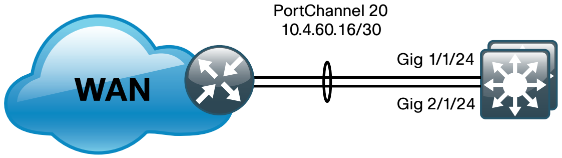
Step 4: Configure the EIGRP Interface

After the Layer 3 interfaces and Layer 3 port-channels connecting to other Layer 3 devices have been configured, allow EIGRP to form neighbor relationships across these interfaces to establish peering adjacencies and exchange route tables.

```
router eigrp [as number]
  no passive-interface [interface type] [number]
```

Procedure 5 Example

Figure 22. Procedure 5 Example



```
interface port-channel 20
  no switchport
  ip address 10.4.60.17 255.255.255.252
  ip pim sparse-mode
  ip summary-address eigrp 100 10.4.0.0 255.255.240.0
!
interface range gig 1/1/24, gig 2/1/24
  no switchport
  channel-group 20 mode on
  no shutdown
!
router eigrp 100
  no passive-interface port-channel 20
```

Core Layer

Agency Overview

Modern agencies require non-stop connectivity and uninterrupted access to the resources essential to operational success. The risk of a single link outage or device failure cascading throughout the facility and disrupting communications for a large number of users increases as networks grow in size and scale at a given location . IT departments tasked with providing reliable access to resources require a network architecture that can provide a highly available service.

As the LAN environment at a larger facility grows it often creates the need to use multiple LAN distribution layer blocks. The creation of multiple distribution layer blocks may be due to the physical layout of the site or based on the density of access layer switches connecting to a single distribution layer. As the number of required distribution layer blocks in a facility grows beyond two or three, a solution is required to reduce the need and cost of fully meshing all interconnectivity while maintaining a design that provides a reliable infrastructure.

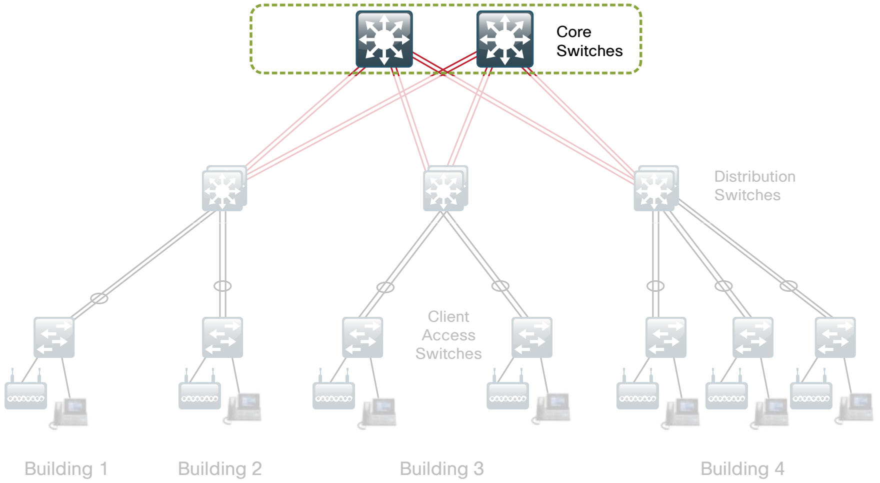
An important component in the consideration to invest in new technology and services to drive agency productivity is the time required to implement the technology in a usable fashion. Agencies must design an architecture of compute, storage, application, and network foundation that allows them to reduce the time required to utilize new technology investments by exploiting a flexible and scalable infrastructure.

Technology Overview

The core layer of the LAN is a critical part of the scalable network, yet by design, is one of the simplest. Like the distribution layer, the core layer aggregates connectivity, but for multiple distribution layers instead of access layers. As networks grow beyond three distribution layers in a single location, a core layer should be used to optimize the design.

Beyond the simple aggregation of connectivity, the core layer serves to reduce the number of paths between distribution layers which in turn lowers the time required to converge the network after a failure. By upgrading bandwidth between a distribution layer and the core, multiple distribution layer blocks can benefit from the increase versus the need to upgrade the bandwidth to every other device in a design without a core. The core layer is especially relevant to designs where the data center resources might be collocated with the LAN.

Figure 23. Core Layer Overview



In large modular and scalable LAN designs, a core layer is used to aggregate multiple user connectivity distribution layer blocks. In designs with a collocated data center, the core provides high speed fanout connectivity to the rest of the network. The core layer also serves as the interconnect for the Wide Area Network (WAN) and Internet Edge distribution layer blocks. Because of this central point of connectivity for all data flows, the core is part of the backbone IP routing address space and is designed to be highly resilient to protect from component-, power-, or operational-induced outages. The core layer should not contain highly complex or high touch services that require constant care and tuning, to avoid downtime required by complex configuration changes, increased software upgrades for new services, or links that toggle up/down as part of normal operations like user endpoint connectivity.

The core layer in the SBA design is based on two physically and logically separate switches. Connectivity to and from the core should be Layer 3 only. No VLANs should span the core to drive increased resiliency and stability. Since the core does not need to provide the same services or boundaries that the distribution layer does, the two-box design does not significantly increase the complexity of the solution. Because the Layer 3 core has no need to provide access layer services or Layer 2 connectivity, the single logical device approach used in the distribution layer to prevent spanning tree and reduce IP gateway protocols is not as beneficial.

The core is built on dual switches to provide a completely separate control plane housed on each switch, that provides redundant logic, line cards, hardware, and power for the backbone operation. Each distribution layer block, router, or other appliance connecting to the core should be dual homed with an EtherChannel or link to each core switch. This dual-homed approach provides Equal Cost Multiple Path (ECMP) load sharing of IP traffic across links for traffic traversing the core, and fast failover based on either EtherChannel or ECMP alternate routes without waiting for routing protocol topology changes to propagate the network.

The core is designed to be high speed and provides for connectivity ranging from Gigabit Ethernet, Gigabit EtherChannel, 10 Gigabit Ethernet, and up to 10Gigabit EtherChannel. The core can provide non-blocking bandwidth based on design and configuration. EtherChannel links homed to a switch should be spread across line cards when possible.

The core switches can be provisioned with dual supervisors for Stateful Switchover (SSO) operation to protect the core bandwidth in the event a control plane hardware or software failure occurs. The core switches are Nonstop Forwarding (NSF) aware to provide enhanced resilience for any dual supervisor connected devices and NSF capable if provisioned with dual supervisors per switch.

Core Layer Platforms

The Cisco Catalyst 6500 Series Switch is the premiere LAN core platform. It delivers scalable performance, intelligence, and a broad set of features to address the needs of the most demanding large-agency deployment requirements for building modular, resilient, scalable, and secure Layer 2 or Layer 3 solutions. With support for interfaces from Gigabit Ethernet to 10 Gigabit Ethernet, copper or fiber optic media, as well as the ability to support a wide range of WAN and Metro interfaces, the Cisco Catalyst 6500 provides the necessary versatility for the core of any network. The Catalyst 6500 used in this design can use the same supervisor engine, chassis, and power supplies as the Cisco Catalyst 6500 VSS 1440 systems used for the distribution layer, which helps with sparing of parts and reduction of platforms to support.

The **Collapsed Core with Nexus 7000 Supplemental** discuss the use of the Cisco Nexus 7000 Series Switch as the core layer platform when the LAN and data center core functionality are combined on one set of devices.

Procedure 1 LAN Switch Universal Configuration

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 will depend on your current network configuration.

Common Network Services Used in the Deployment Examples

Domain Name:	cisco.local
Active Directory, DNS, DHCP Server:	10.4.200.10
Authentication Control System:	10.4.200.15
Network Time Protocol Server:	10.4.200.17

Procedure Steps:

1. Configure the Device Hostname
2. Configure Device Resiliency Features
3. Configure Device Management Protocols
4. Configure Secure User Authentication
5. Configure Synchronized Clock and Timezone for Management

Step 1: Configure the Device Hostname

Configure the device hostname to make it easy to identify the device.

```
hostname [hostname]
```

Step 2: Configure Device Resiliency Features

Virtual Trunk 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, adding and removing VLANs is generally not a frequent network management practice. In most cases, VLANs are defined once during switch setup with few, if any, additional modifications to the database.

The benefits of dynamic propagation of VLAN information across the network are not worth the potential for unexpected behavior due to operational error. For this reason, VTP transparent mode is configured in this architecture.

```
vtp mode transparent
```

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

While this architecture is built without any Layer 2 loops, spanning tree must still be enabled. Having spanning tree enabled ensures that if any physical or logical loops are accidentally configured, no actual layer 2 loops occur.

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

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.

At first glance, this form of attack 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.

An easy way to remove the remote risk of this type of attack is to configure the switch to tag all native VLAN traffic. This tagging of native VLAN traffic removes any possibility that a double 802.1Q-tagged packet can hop VLANs.

```
vlan dot1q tag native
```

Unidirectional Link Detection (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. 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.

In aggressive mode, the interface will be put into the errdisable state and will be effectively shut down when a unidirection link occurs.

```
udld aggressive
```

EtherChannels are used extensively in this design because of their resiliency capabilities. To normalize the method in which traffic is load-shared across the member links of the EtherChannel. All switches should be set to use the traffic source and destination IP Address when calculating which link to send the traffic across.

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

Step 3: Configure Device Management Protocols

Secure HTTP (HTTPS) and Secure Shell (SSH) are 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.

Secure management of the LAN device is enabled through the use of the SSH and HTTPS protocols. Both protocols are encrypted for privacy and the nonsecure protocols, Telnet and HTTP, are turned off.

```
ip domain-name cisco.local
ip ssh version 2
no ip http server
ip http secure-server
line vty 0 15
  transport input ssh
```

Simple Network Management Protocol (SNMP) is enabled to allow the network infrastructure devices to be managed by a Network Management System (NMS). SNMPv2c is configured both for a read-only and a read-write community string.

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

Step 4: Configure Secure User Authentication Configuration

Authentication, Authorization and Accounting (AAA) is enabled for access control. All management access to the network infrastructure devices (SSH and HTTPS) is controlled with AAA.

The AAA server used in this architecture is the Cisco Authentication Control System. Configuration of ACS is discussed in the ACS Deployment Supplement.

RADIUS 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 RADIUS server is unavailable.

```
enable secret c1sco123
service password-encryption
!
username admin password c1sco123
aaa new-model
aaa authentication login default group radius local
radius-server host 10.4.200.15 key SecretKey
```

Step 5: Configure Synchronized Clock and Timezone for Management

The Network Time Protocol (NTP) is designed to synchronize a network of devices. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the agency network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two devices to within a millisecond of one another.

Network devices should be programmed 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. Configuring console messages, logs, and debug output on switches, routers, and other devices in the network to provide timestamps on output allows cross-referencing of events in a network.

```
ntp server 10.4.200.17
ntp update-calendar
!
clock timezone PST -8
clock summer-time PDT recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

Procedure 2 Core Switch Global Configuration

1. Configure the In-Band Management Interface
2. Configure IP Unicast Routing
3. Configure IP Multicast Routing

Step 1: Configure the In-Band Management Interface

The loopback interface for Cisco Layer 3 devices is a logical interface that is always reachable as long as the device is powered on and any IP interface is reachable to the network. Layer 3 process and features are also bound to the Loopback interface to ensure resiliency of the processes. The loopback address is commonly a host address with a 32-bit address mask and has been allocated out of the core network address range. We have included the **ip pim sparse-mode** command that will be explained further in step 3.

```
interface loopback 1
 ip address [ip address] 255.255.255.255
 ip pim sparse-mode
```

Now that we have created an IP loopback interface, we can tie SNMP and SSH to that interface address.

```
snmp-server trap-source loopback 1
ip ssh source-interface loopback 1
```

Step 2: Configure IP Unicast Routing

Enable EIGRP for the IP address space that the network will be using and disable auto summarization of the IP networks. If needed for your network, you can enter multiple network statements. The Loopback 1 IP address is used for the EIGRP router ID to ensure maximum resiliency.

```
router eigrp [as number]
 network [network] [inverse mask]
 no auto-summary
 eigrp router-id [ip address of loopback 1]
```

Step 3: Configure IP Multicast Routing

Enable IP multicast routing on the platforms in the global configuration mode.

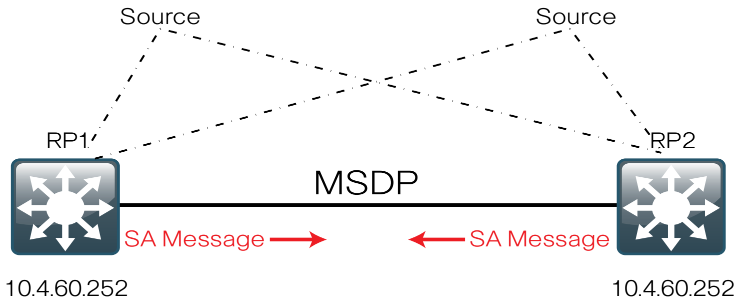
```
ip multicast-routing
```

To enable Anycast RP operation, the first step is to configure a second loopback interface on each of the core switches. The key is that this second loopback interface will have the same IP address on both core switches and will use a host address mask (32 bits). All routers will then point to this common IP address on Loopback 2 for their RP in their configuration. We have configured the RP address from the core IP address space.

```
interface Loopback2
 ip address 10.4.60.252 255.255.255.255
 ip pim sparse-mode
```

The final step for the Anycast RP configuration is to enable Multicast Source Discovery Protocol (MSDP) to run between the two core RP switches. To enable MSDP, you must use unique addresses at each end of the link; therefore, we will use the loopback 1 addresses of each core router to configure the MSDP session.

Figure 24. MSDP Overview



On core switch #1:

```
ip msdp peer 10.4.60.253 connect-source loopback 1
ip msdp originator-id loopback 1
! The IP address for the listed above is the core switch #2 
loopback
```

On core switch #2:

```
ip msdp peer 10.4.60.254 connect-source loopback1
ip msdp originator-id loopback1
! The IP address for the listed above is the core switch #1 
loopback
```

The MSDP configuration is complete and convergence around a failed RP is now as fast as the unicast routing protocol (EIGRP) convergence. You will see the MSDP protocol session activate later on as you enable the routing links between the core switches and the distribution layer blocks establishing Layer 3 connectivity:

```
*Mar 3 06:32:21.659: %MSDP-5-PEER_UPDOWN: Session to peer 
10.4.60.253 going up
```

Every Layer 3 switch and router must be configured with the address of the IP multicast RP, including the core switches that are serving as the RP. Configure the core switches to point their RP address to the loopback 2 IP address as well as every other remote router and Layer 3 switch. Use the **rp-address** command in conjunction with an access list to limit the network size that the RP is responsible for. This configuration provides for future scaling and control of the IP multicast environment and can change based on network needs and design.

```
ip pim rp-address [rp address] [acl number]
access-list [acl number] permit [multicast network] [inverse 
mask]
```

In the event you add a core layer to your existing network and the RP is currently configured on a distribution layer, you may want to move the RP to the core.

With AnyCast RP, you can move the RP to a new location by programming the RP address on the loopback 2 interfaces at the new location, and enable and establish IP multicast and MSDP peering.

All remote routers should still point to the same RP address, which simplifies the move and reduces disruption to the IP Multicast environment.

All Layer 3 interfaces in the network must be enabled for sparse mode multicast operation.

```
ip pim sparse-mode
```

Procedure 3 Distribution Layer Aggregation Configuration

In this design, links in the core layer are configured as point-to-point Layer 3 routed links or Layer 3 routed EtherChannels. If you are using the Cisco Catalyst 6500 VSS 1440 system in the distribution layer, we recommend that all peer-connected links are EtherChannel links. EtherChannel to the Catalyst 6500 VSS provides for optimal forwarding as a packet that is received on the switch will be forwarded out a link on that same switch in normal operation versus traversing the VSL link.

Other benefits of EtherChannel to any single physical or logical device are the ease of growing bandwidth without changing the topology and that a single link failure uses EtherChannel recovery versus using ECMP or a routing topology change to reroute the data flows for fastest recovery.

Since the core links are point-to-point routed links, use 30-bit IP address subnets and masks and do not use Switched Virtual Interfaces (SVI).

For Layer 3 connected devices that do not require EtherChannel, configure the routed interfaces with the IP address directly on the physical interface and do not use a Switch Virtual Interface (SVI).

```
interface [interface type] [number]
  no switchport
  ip address [ip address] [mask]
  ip pim sparse-mode
  mls qos trust dscp
```

When creating a Layer 3 EtherChannel, we create the logical port-channel interface first.

```
interface port-channel [number]
  no switchport
  ip address [ip address] [mask]
  ip pim sparse-mode
  mls qos trust dscp
```

Configure the physical interfaces to tie to the logical port channel using the **channel-group** command. The number for the port channel and channel group will match.

```
interface range [interface type] [port 1], [interface type] 
[port 2]
  no switchport
  channel-protocol lacp
  channel-group [number] mode active
```

Notes

Wireless Local Area Network

Agency Overview

The effectiveness and efficiency of today's employee can be improved with the ability to stay connected regardless of location. As an integrated part of the wired networking port design that provides connectivity when a user is at their desk or another prewired location, wireless allows connectivity in transit to meetings and turns cafeterias or other meeting places into ad-hoc conference rooms. Wireless networks enable the users to stay connected and the flow of information moving regardless of any physical building limitations.

In the Cisco SBA for Large Agencies—Borderless Networks design, wireless uses Wi-Fi technology to transport data, voice and even video traffic rather than using cellular technology.

Remote site and headquarters users can connect to voice and data services via the same methods creating a seamless operational environment for the agency.

Benefits

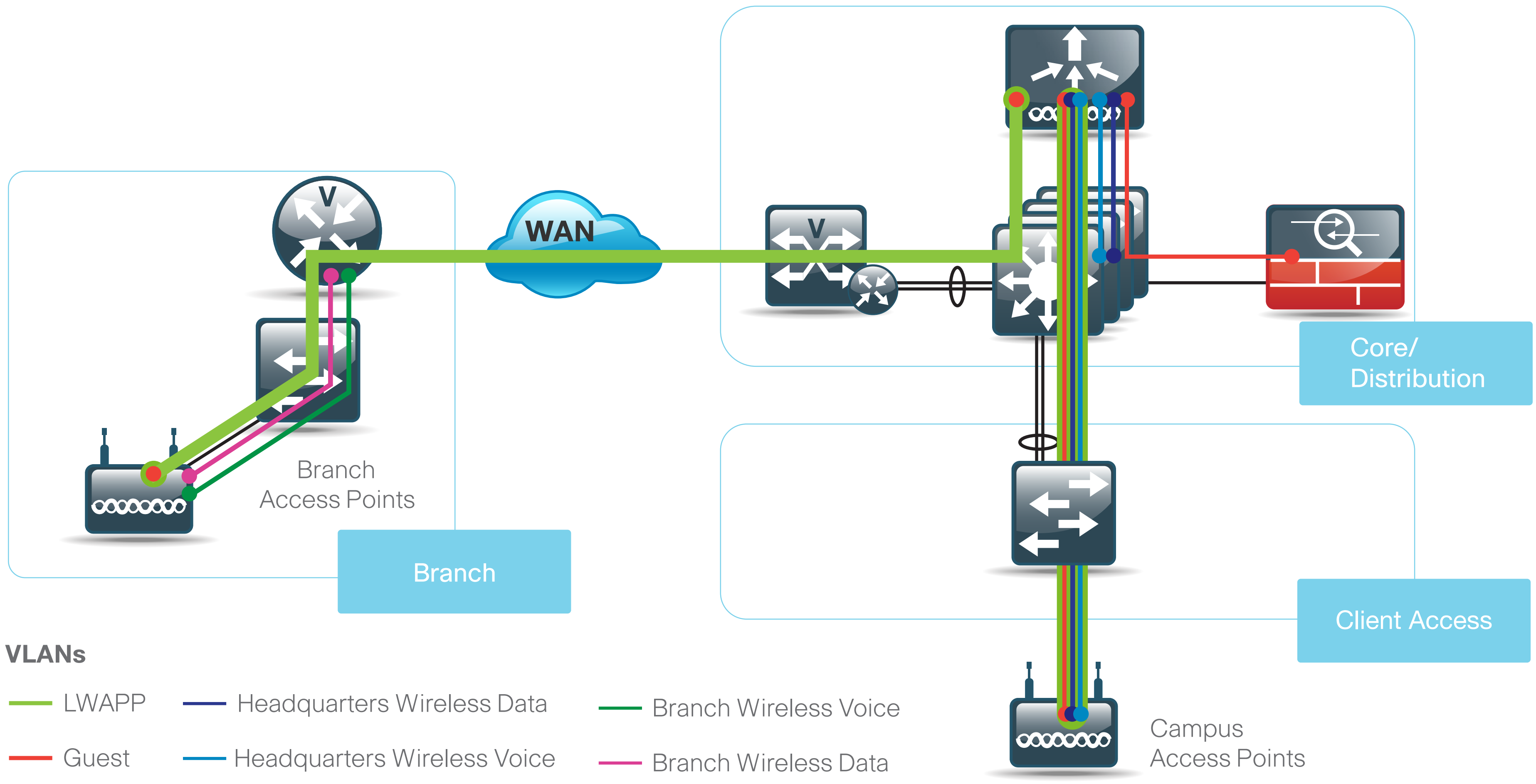
- Location independent network access improves employee productivity
- Additional Network Flexibility: hard-to-wire locations can be reached without costly construction
- Easy to manage and operate: there us centralized control of distributed wireless environment
- Plug and play deployment: network core preconfigured to recognize new access points connected to any access port

Technology Overview

Cisco recommends using a wireless mobility network for voice and data services in order to provide data connectivity for employees, voice connectivity for wireless IP phones, and wireless guest access for visitors to connect to the Internet.

With ease of deployment one of the core goals, this wireless network design is secure and scalable, and it covers the headquarters and remote sites connected via a WAN. It does not cover the radio frequency (RF) design.

Figure 25. Wireless Overview



What Is Our Approach to Wireless?

In the past, the simplest approach was to use standalone access points (APs), yet each needed to be managed individually and lacked the ability to expand wireless functionality.

At the center of this new design is a Wireless LAN Controller (WLC) appliance that can be scaled to support the required number of access points to match the required coverage area. For this design, Cisco recommends using a Cisco 5500 Series Wireless LAN Controller that provides support for up to 250 APs each. For simplicity, the design uses a Wireless LAN Controller for guest, four Wireless LAN Controllers for LAN (Primary Site and Remotes) where they are split up in pairs. Two Wireless LAN Controllers are designated for a resilient LAN while the other two controllers are designated for the remote site connectivity. Although more WLCs can be added to provide additional capacity and resiliency to this design, we specifically used the Cisco 5508 WLC, which has eight Small Form-Factor Pluggable (SFP)-based distribution ports that are used to provide EtherChannel connectivity to the access and application switches and can be either copper or fiber, depending on distance and choice.

Four Controllers allows for complete redundancy that is referenced as the N to N redundancy model within Cisco Documentation. All four controllers are configured in a robust fashion to provide management and control for either the LAN or the Remote site solutions.

The access points used around the LAN are the Cisco 1140 Series Lightweight access points with 802.11a/b/g/n support. Power is provided by standard PoE from the switches, allowing APs to be deployed without installing or modifying existing building electrical outlets (which is often the case as APs are typically mounted on the ceiling.)

The access points selected for the remote sites are Cisco 1140 APs providing 802.11a/b/g/n service. In normal conditions, they operate in Lightweight mode; if connectivity between the remote sites and headquarters is lost, they operate in Standalone mode (switching traffic locally without the use of a Wireless LAN Controller) commonly referred to as HREAP.

Deployment Summary

Deploying wireless mobility initially requires only a RADIUS server for authentication and DNS entry for the APs to locate the manager Wireless LAN Controller.

At the headquarters, there is a site-wide data wireless LAN (WLAN) and a separate voice WLAN that terminates at the WLC where they are put into their separate broadcast domains.

Each remote site also carries the same data and voice WLANs (also known as SSIDs) that are locally switched within the remote site to avoid traversing the WAN when accessing local resources. A single guest WLAN is deployed for the headquarters and all the remote sites, which is then tunneled back to the Guest Wireless LAN Controller and onto a DMZ VLAN that connects to the Adaptive Security Appliance (ASA) on the Edge that provides secure access to the Internet without compromising LAN Security.

The guest WLAN uses OPEN authentication with an HTTP redirect. Access to the Internet is controlled using web authentication that uses an expiring guest account created with the Next Generation Guest Access Server.

Configuration Procedure Details:

LAN Wireless

1. LAN Distribution Switch Configuration
2. Wireless LAN Controller Configuration
3. Create Wireless LAN Controller Data Interface
4. Create Wireless LAN Controller Voice Interface
5. Configure Data Wireless LAN
6. Configure Voice Wireless LAN
7. Wireless Mobility Group
8. Assign APs to Controllers for High Availability
9. Cisco Access Control Server (Radius)

Guest Wireless

1. Firewall DMZ Configuration
2. Firewall Address Translation (NAT/PAT) Configuration
3. Configure Firewall Policy for Wireless Guest Access
4. DMZ Switch Configuration
5. WLC Configuration
6. Create Wireless Guest Interface
7. Add Guest Anchor to BN Mobility Group
8. Configure Auto-Anchor for Guest
9. Configure Guest WLAN for WebAuth
10. Create the BN-Guest Wireless LAN Controller Login Page
11. Create the Lobby Admin User Account

Remote Site Wireless

1. Provision Branch Site Access Points
2. Map Voice and Data to each AP

Procedure 1 LAN Distribution Switch Configuration

After all the Wireless LAN Controllers are physically installed and powered up, configure an EtherChannel between each controller and the LAN distribution switch.

1. Layer 2 Configuration
2. EtherChannel Member Interface Configuration
3. EtherChannel Member Interface QoS Configuration
4. Trunk Configuration
5. Layer 3 Configuration

The VLANs used in the following configuration examples are:

- Wireless data: VLAN 148, IP: 10.4.48.0/22
- Wireless voice: VLAN 152, IP 10.4.52.0/22
- WLC management: VLAN 156, IP 10.4.56.0/24

Step 1: Layer 2 Configuration

Set the distribution layer switch to be the Spanning Tree Root for the Wireless VLANs that you are connecting to the distribution switch.

```
vlan 148,152,156
spanning-tree vlan 148,152,156 root primary
```

Step 2: EtherChannel Member Interface Configuration

This design uses Layer 2 EtherChannels to connect Wireless LAN Controllers to the distribution switch. Connect the WLC EtherChannel uplinks to separate devices in the distribution layer virtual switch or stack, and in the case of the Cisco Catalyst 4507R-E distribution layer switch, connect to separate redundant line cards for additional resiliency.

On the distribution switch, the physical interfaces that are members of a Layer 2 EtherChannel are configured prior to configuring the logical PortChannel Interface. Doing the configuration in this order 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.

Configure two or more physical interfaces to be members of the EtherChannel. It is best if they are added in multiples of two.

```
interface range [interface type] [port 1], [interface type] 
[port 2]
  channel-group [number] mode on
```

Step 3: EtherChannel Member Interface QoS Configuration

To enable QoS on a EtherChannel link, some platforms require configuration on the EtherChannel Member Interfaces.

Step 3a: Cisco Catalyst 3750 EtherChannel QoS

On the Catalyst 3750 switch configure QoS on the EtherChannel member interfaces . All member interfaces must be configured the same as QoS will not be invoked until all EtherChannel member interfaces are configured.

Enable QoS on the EtherChannel member interfaces, configure the following :

```
mls qos trust dscp
queue-set 2
srr-queue bandwidth share 10 10 60 20
priority-queue out
```

Step 3b: Cisco Catalyst 4500 Supervisor 6L-E and 6-E Etherchannel QoS

The Catalyst 4500 Supervisor 6-E and Supervisor 6L-E handle QoS queuing and classification as separate functions when configuring EtherChannel. Both supervisors require classification commands, and policing statements to be applied to the port-channel interface and the queuing configuration commands to be applied at the physical port-level interface.

Enable QoS on all the EtherChannel member interfaces , configure the following:

```
service-policy output queue-only
```

Step 4: Trunk Configuration

An 802.1Q trunk is used for the connection to the WLC which allows the distribution switch to provide the Layer 3 services to all the VLANs defined on the access layer switch. The VLANs allowed on the trunk are pruned to only the VLANs that are active on the access switch.

```
interface [interface type] [number]
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 148,152,156
  switchport mode trunk
  no shutdown
```

The Catalyst 4500 does not require the **switchport trunk encapsulation dot1q** command. However, classification commands and policing statements that are configured in the distribution platform must be enabled on the port-channel interface.

```
service-policy output EC-non-queue
service-policy input AutoQos-VoIP-Input-Dscp-Policy
```

The Catalyst 6500 additionally must be configured to trust the QoS markings that enter the switch on the port-channel interface.

```
mls qos trust dscp
```

Step 5: Layer 3 Configuration

Configure a VLAN interface (SVI) for each VLAN so devices in the VLAN can communicate with the rest of the network.

```
interface Vlan148
 description Data WLAN
 ip address 10.4.48.1 255.255.252.0
!
interface Vlan152
 description Voice WLAN
 ip address 10.4.52.1 255.255.252.0
!
interface Vlan156
 description Management
 ip address 10.4.56.1 255.255.252.0
```

Procedure 2 Wireless LAN Controller Configuration

The following steps should be repeated for all Wireless LAN Controllers. In this design, there are four controllers and the management IP address of each controller is increased by one.

Controller	Management IP Address
BN-WLC1	10.4.56.64
BN-WLC2	10.4.56.65
BN-WLC3	10.4.56.66
BN-WLC4	10.4.56.67

Next, using the console port and after powering up each Wireless LAN Controller, you will be prompted by a setup script. The answers to the onscreen prompts are in **bold**.

After the initial hardware boot process is complete, you will see the following on the screen:

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
Would you like to terminate autoinstall? [yes]:no
```

Step1: Enter a system name. Use a different for each controller.

```
System Name [Cisco_7e:8e:43] (31 characters max): BN-WLC1
```

Step 2: Enter an administrator username and password.

Tech Tip

Do not use the username below. When entering the passwords, the characters echo back as "*" symbols.

```
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Re-enter Administrative Password     : *****
```

Step 3: Use DHCP for the service port interface address.

```
Service Interface IP address Configuration [none] [DHCP]: DHCP
```

Step 4: Enable Link Aggregation.

```
Enable Link Aggregation (LAG) [yes][NO]: YES
```

Step 5: Enter the IP address and subnet mask for the management interface (that is, IP address 10.4.56.64, netmask 255.255.255.0, default gateway 10.4.56.1, and VLAN 156)

```
Management Interface IP Address: 10.4.56.64
Management Interface Netmask: 255.255.255.0
Management interface Default Router: 10.4.56.1
Management Interface VLAN Identifier (0 = untagged): 156
```

Tech Tip

All interfaces are tagged. We do not use the untagged VLAN or native VLAN of the Layer 2 port-channel for any interface.

Step 6: Enter the default DHCP server for clients.

Tech Tip

In this deployment example, the DHCP Server is 10.4.200.10. Configure this with the IP Address of the DHCP server in your agency.

```
Management Interface DHCP Server IP Address: 10.4.200.10
```

Step 7: The virtual interface is used by the WLC for Mobility DHCP relay and inter-controller communication (that is, 1.1.1.1)

```
Virtual Gateway IP Address: 1.1.1.1
```

Step 8: Enter a name that will be used as the default mobility and RF group (i.e. default).

Tech Tip

Use something OTHER than default like the building or campus name.

```
Mobility/RF Group Name: BN
```

Step 9: Enter an initial SSID of guest or the guest SSID you wish to use as you will be able to leverage this for your guest WLAN later.

```
Network Name (SSID): guest
```

Step 10: Enter no to make clients use DHCP IP addresses, as you do not want users to be able to assign their own address when connecting to your network. This type of addressing works much the same way as DHCP snooping.

```
Allow Static IP Addresses {YES][no]: NO
```

Step 11: Enter no to configure RADIUS as we will configure this later using the Graphical User Interface (GUI).

```
Configure a RADIUS Server now? [YES][no]: NO
```

The default WLAN security policy requires a RADIUS server.

Step 12: Enter the correct country code for the country where you are deploying.

```
Enter Country Code list (enter ‘help’ for a list of countries)
[US]: US
```

Step 13: Enter yes to enable all wireless networks, (802.11a will typically be used for wireless Voice traffic while 802.11b/g/n will typically be used for data.)

```
Enable 802.11b network [YES][no]: YES
Enable 802.11a network [YES][no]: YES
Enable 802.11g network [YES][no]: YES
```

Step 14: Enable the WLC's radio resource management (RRM) auto RF feature by entering yes, RRM is an important and unique feature of the Cisco Wireless LAN controller that can help you keep your network up and operational.

```
Enable Auto-RF [YES][no]: YES
```

Step 15: Configuring NTP can be done later, so we can skip this section by entering the current date and time as there is no way to ensure an NTP server is reachable until the entire network is configured up to and including network connectivity. Once NTP can be reached, setting up a server will help ensure proper configuration.

```
Configure a NTP server now? [YES][no]: NO
Enter the date in MM/DD/YY format: 02/16/10
Enter the time in HH:MM:SS format: 10:10:10
```

Step 16: Type yes to save the configuration, if you respond with no the system will restart from step 1 and guide you through this same process without saving what you have already configured.

```
Configuration correct? If yes, system will save it and reset 
[yes][NO]: YES
Configuration saved!
```

Repeat the preceding procedure for each controller; remember to change the name and the management IP address.

```
Resetting system with new configuration…
```

At this point, the WLC will save the configuration and reboot. When the onscreen prompt appears, enter the username and password used in Step 2.

To verify the basic installation, use the show port summary command from the CLI to confirm that both ports are up and enabled. Used the show interface summary command to confirm that the IP addresses and VLAN for the Management interface is correct. Notably, the port used by both is Link Aggregation Group (LAG), which groups the two distribution ports together so that they can provide load balancing and high availability to the two core switches configured for EtherChannel.

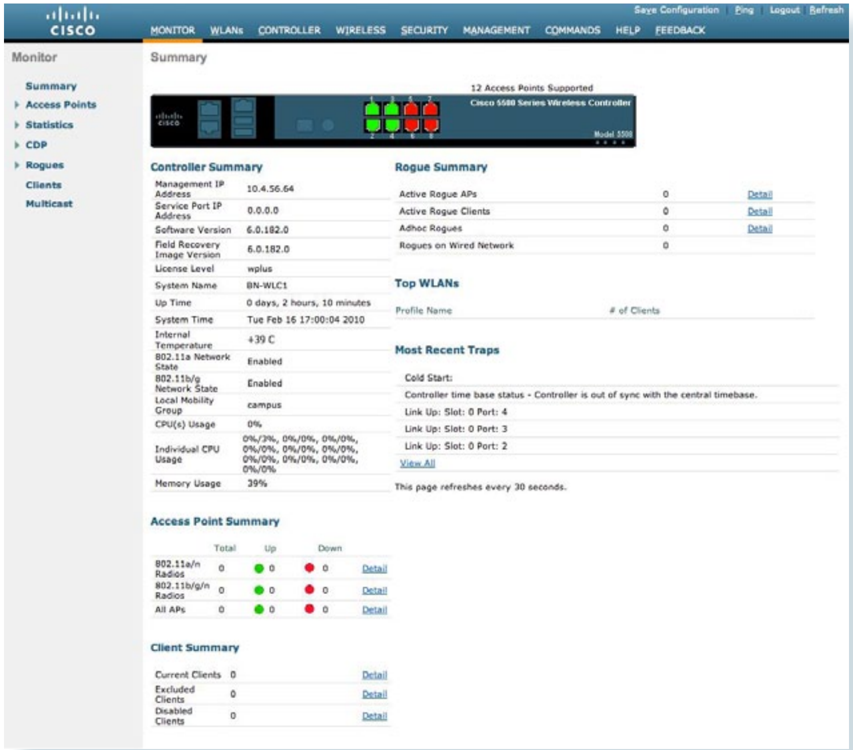
```
(Cisco Controller) >show interface summary

Interface Name   Port Vlan Id IP Address   Type    Ap Mgr Guest
---------------- ---- ------- ----------- ------- ------ -----
management       LAG   156    10.4.56.64  Static   Yes    No
service-port     N/A   N/A    0.0.0.0     Static   No     No
virtual          N/A   N/A    1.1.1.1     Static   No     No
```

Once you have confirmed the configuration, access the GUI for each WLC by using a web browser through a client connected to the wired network:

You may also use a DNS name if you have added a host entry for the management IP address.

After logging into the web interface, you can verify the basic health of the WLC by selecting **Monitor>Summary** (Figure 26).

Figure 26. Logon Page



Summary

Controller Summary

Management IP Address	10.4.56.64
Service Port IP Address	0.0.0.0
Software Version	6.0.182.0
Field Recovery Image Version	6.0.182.0
License Level	wplus
System Name	BN-WLC1
Up Time	0 days, 2 hours, 10 minutes
System Time	Tue Feb 16 17:00:04 2010
Internal Temperature	+39 C
802.11a Network State	Enabled
802.11b/g Network State	Enabled
Local Mobility Group	campus
CPU(s) Usage	0%
Individual CPU Usage	0%/3%, 0%/0%, 0%/0%, 0%/0%, 0%/0%, 0%/0%, 0%/0%, 0%/0%, 0%/0%, 0%/0%
Memory Usage	39%

Access Point Summary

	Total	Up	Down	
802.11a/n Radios	0	● 0	● 0	Detail
802.11b/g/n Radios	0	● 0	● 0	Detail
All APs	0	● 0	● 0	Detail

Client Summary

Current Clients	0	Detail
Excluded Clients	0	Detail
Disabled Clients	0	Detail

Rogue Summary

Active Rogue APs	0	Detail
Active Rogue Clients	0	Detail
Adhoc Rogues	0	Detail
Rogues on Wired Network	0	

Top WLANs

Profile Name	# of Clients

Most Recent Traps

Cold Start:
Controller time base status - Controller is out of sync with the central timebase.
Link Up: Slot: 0 Port: 4
Link Up: Slot: 0 Port: 3
Link Up: Slot: 0 Port: 2
View All

This page refreshes every 30 seconds.

This page shows the distribution ports that are up (green) and any APs that have established communications.

Prerequisites for Access Point Configuration

Before further configuration on the WLC, confirm that there is a Host entry for CISCO-CAPWAP-CONTROLLER with the Manager IP address in the DNS server specified in the DHCP server scopes. (In this case, the DNS server is 10.4.200.10.)

```
dhcp-10.4.20.12:~ noname$ nslookup cisco-lwapp-controller
Server:     10.4.200.10
Address:    10.4.200.10#53

cisco-lwapp-controller.cisco.local     canonical name = wlc.
cisco.local.
Name:       wlc.cisco.local
Address: 10.4.56.64
```

Using DHCP for the IP address, netmask, gateway, and DNS server information, the AP then uses DNS to resolve **cisco-lwapp-controller.yourdomain.com** and establish a connection with the WLC to allow the enabling of the radios (they are disabled by default) and additional configuration. Define a DNS Host entry for the management IP address, although it is not required.

At the headquarters, the access ports, which are connected to the APs, should use standard access switchport configuration, with one exception: the default trust must be changed from CoS to DSCP by using the interface command **mls qos trust dscp**.

Configuring Voice and Data Connectivity

Separating voice and data is essential in any good network design to ensure proper treatment of the respective IP traffic, regardless of the medium it is traversing.

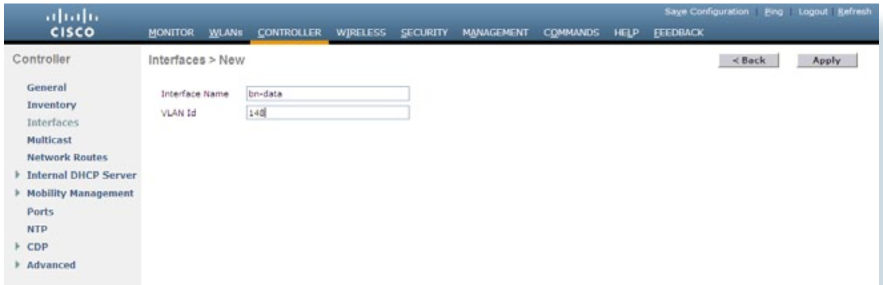
Procedure 3 Create Wireless LAN Data Interface

Step 1: Add Wireless Data Interface

From **Controller>Interfaces** click **New**.

Enter the Interface name of **Wireless-Data** and the VLAN identifier of **148** and click **Apply**.

Figure 27. New Data Interface



Interfaces > New

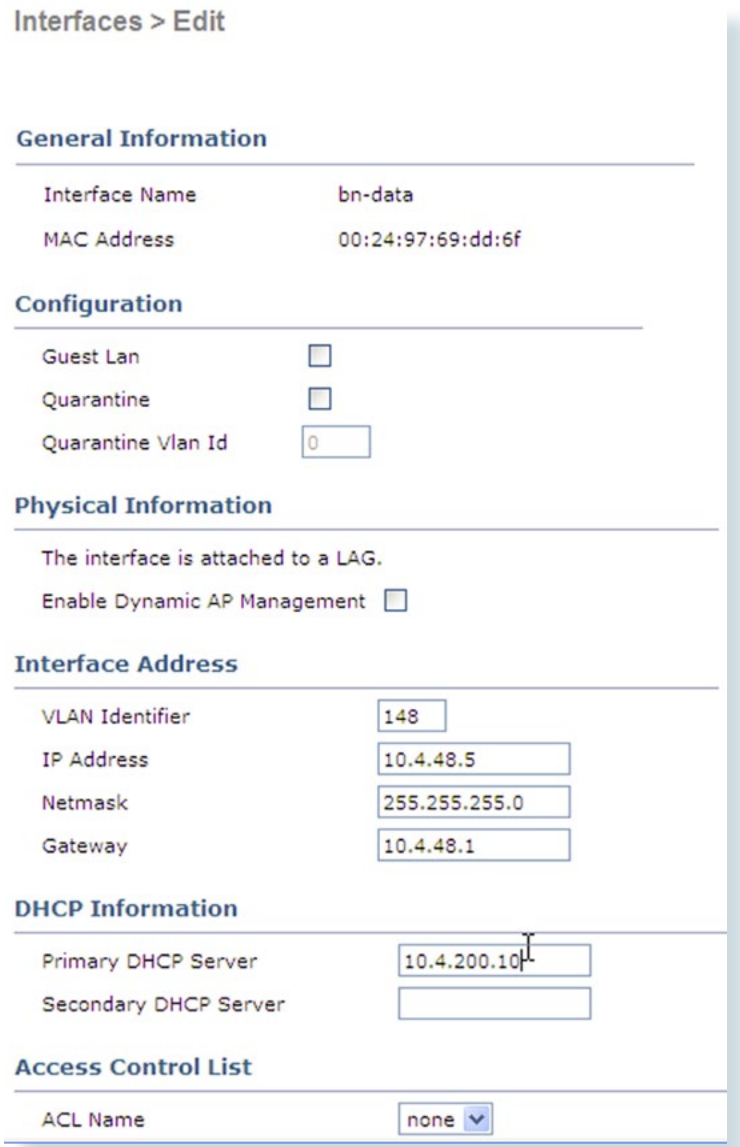
Interface Name: bn-data

VLAN Id: 148

Step 2: Enter all necessary information for this interface (Figure 28). Each Wireless LAN Controller has a unique IP address in the data network.

Controller	Data Interface IP Address
BN-WLC1	10.4.48.5 255.255.255.0
BN-WLC2	10.4.48.6 255.255.255.0
BN-WLC3	10.4.48.7 255.255.255.0
BN-WLC4	10.4.48.8 255.255.255.0

Figure 28. Data Interface Details



Interfaces > Edit

General Information

Interface Name: bn-data

MAC Address: 00:24:97:69:dd:6f

Configuration

Guest Lan □

Quarantine □

Quarantine Vlan Id: 0

Physical Information

The interface is attached to a LAG.

Enable Dynamic AP Management □

Interface Address

VLAN Identifier: 148

IP Address: 10.4.48.5

Netmask: 255.255.255.0

Gateway: 10.4.48.1

DHCP Information

Primary DHCP Server: 10.4.200.10

Secondary DHCP Server:

Access Control List

ACL Name: none

Step 3: Click **Apply.**

Repeat this procedure for each Wireless LAN Controller in the LAN, giving each a unique IP address.

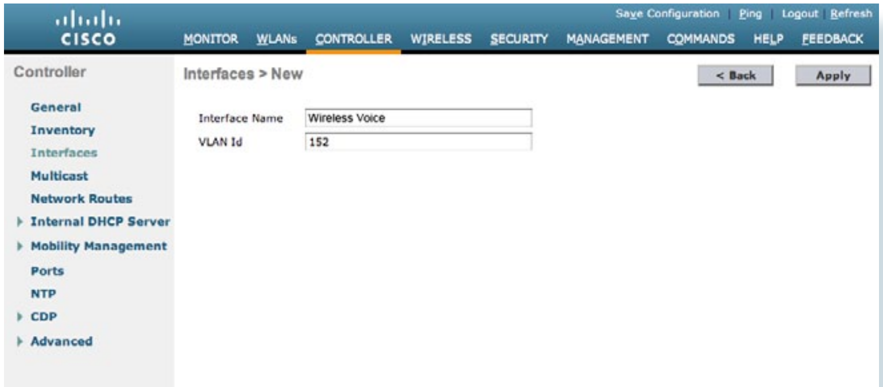
Procedure 4 Create Wireless LAN Voice Interface

Step 1: Add Wireless Voice Interface

From **Controller>Interfaces** click **New**.

Add the Interface name of **Wireless-Voice** and the VLAN identifier of **152** and click **Apply.**

Figure 29. New Voice Interface



Interfaces > New

Interface Name: Wireless Voice

VLAN Id: 152

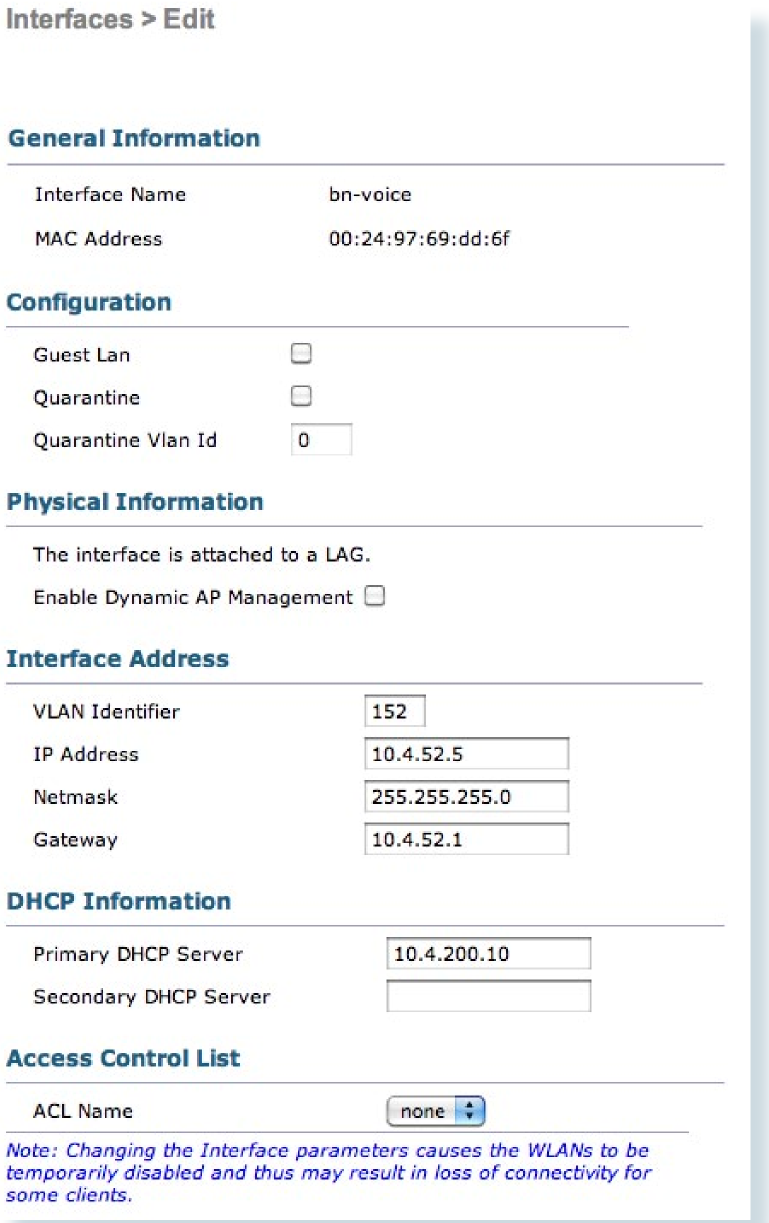
Step 2: Enter all necessary information for this interface (Figure 30). Each Wireless LAN Controller has a unique IP address in the data network.

Controller	Voice Interface IP Address
BN-WLC1	10.4.52.5 255.255.255.0
BN-WLC2	10.4.52.6 255.255.255.0
BN-WLC3	10.4.52.7 255.255.255.0
BN-WLC4	10.4.52.8 255.255.255.0

Step 3: Click **Apply**.

Repeat this procedure for each Wireless LAN Controller in the LAN, giving each a unique IP address.

Figure 30. Voice Interface Details



Interfaces > Edit

General Information

Interface Name	bn-voice
MAC Address	00:24:97:69:dd:6f

Configuration

Guest Lan	□
Quarantine	□
Quarantine Vlan Id	0

Physical Information

The interface is attached to a LAG.

Enable Dynamic AP Management □

Interface Address

VLAN Identifier	152
IP Address	10.4.52.5
Netmask	255.255.255.0
Gateway	10.4.52.1

DHCP Information

Primary DHCP Server	10.4.200.10
Secondary DHCP Server	

Access Control List

ACL Name	none

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

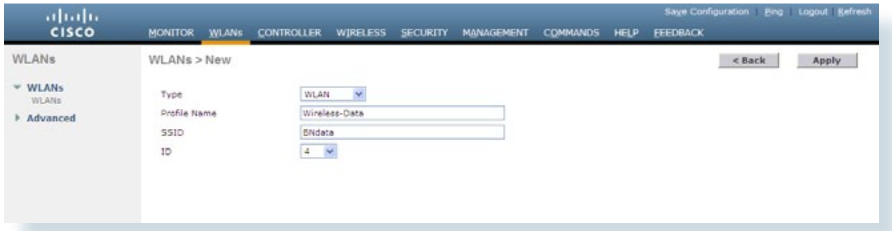
Procedure 5 Configure Data Wireless LAN

Wireless data traffic is unique to voice traffic in that it can more efficiently handle delay and jitter as well as greater packet loss. To configure the data wireless LAN keep the default QoS settings and segment the data traffic onto the data wired VLAN.Enabling Hybrid Remote Edge Access Point (H-REAP) local Switching for this WLAN prepares this WLAN to be used at the remote sites where H-REAP can be leveraged.

Step 1: From the GUI Navigate to **WLANs,** select **Create New,** and then click **Go**.

Step 2: Enter Wireless-Data as the profile name and BNdata as the SSID.

Figure 31. Create Wireless LAN for Data



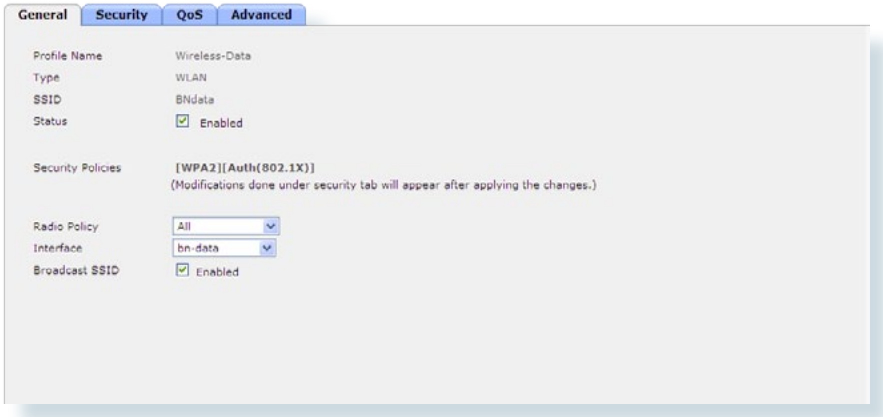
WLANs > New

Type	WLAN
Profile Name	Wireless-Data
SSID	BNdata
ID	4

Step 3: Modify this new WLAN.

From the **General** tab, check the **Status** checkbox to enable the WLAN. Select **bn-data** from the Interface drop-down list.

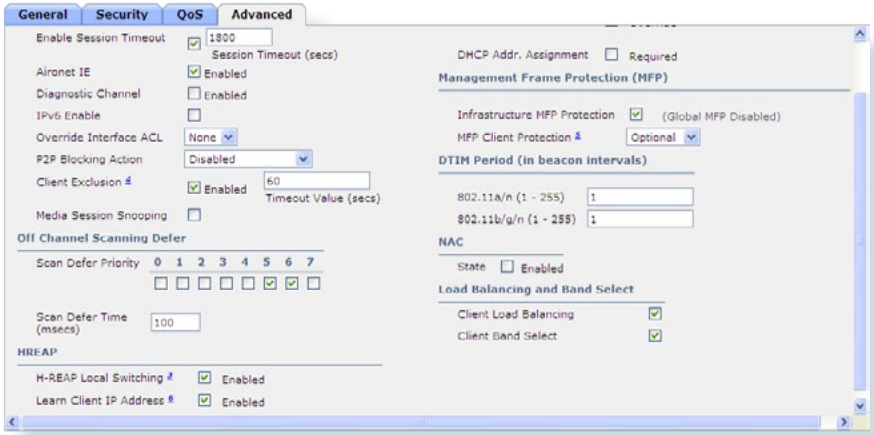
Figure 32. Data WLAN General Tab



Profile Name	Wireless-Data
Type	WLAN
SSID	BNdata
Status	☑ Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface	bn-data
Broadcast SSID	☑ Enabled

Step 4: Under the Advanced tab, check the H-REAP Local Switching checkbox, and then **Apply**.

Figure 33. Data WLAN Advanced Tab



Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE ☑ Enabled
Diagnostic Channel □ Enabled
IPv6 Enable □
Override Interface ACL None
P2P Blocking Action Disabled
Client Exclusion ☑ Enabled 60 Timeout Value (secs)
Media Session Snooping □

Off Channel Scanning Defer

Scan Defer Priority 0 □ 1 □ 2 □ 3 □ 4 □ 5 ☑ 6 ☑ 7 □
Scan Defer Time (msecs) 100

HREAP

H-REAP Local Switching ☑ Enabled
Learn Client IP Address ☑ Enabled

DHCP Addr. Assignment □ Required

Management Frame Protection (MFP)

Infrastructure MFP Protection ☑ (Global MFP Disabled)
MFP Client Protection Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

NAC

State □ Enabled

Load Balancing and Band Select

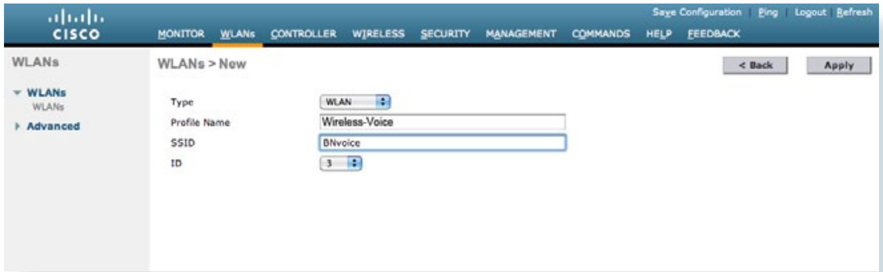
Client Load Balancing ☑
Client Band Select ☑

Procedure 6 Configure Voice Wireless LAN

Wireless voice traffic is unique to data traffic in that it cannot effectively handle delay and jitter as well as packet loss. To configure the voice wireless LAN change the default QoS settings to Platinum and segment the voice traffic onto the voice wired VLAN. Enabling Hybrid Remote Edge Access Point (H-REAP) local Switching for this WLAN prepares this WLAN to be used at the remote sites where H-REAP can be leveraged.

Step 1: Navigate to **WLANs**, select **Create New**, and then click **Go**.

Figure 34. Create Voice WLAN



WLANs > New

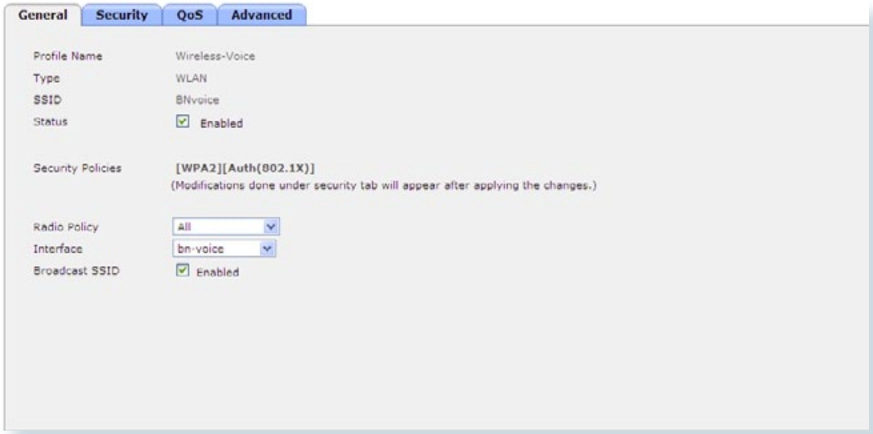
Type WLAN
Profile Name Wireless-Voice
SSID BNvoice
ID 3

Step 2: Create the **Wireless-Voice** profile name and the **BNvoice** SSID.

Step 3: Modify this new WLAN.

From the General tab, check the **Status** checkbox to enable the WLAN, and select **bn-data** from the Interface dropdown list.

Figure 35. Voice WLAN General Tab



Profile Name Wireless-Voice
Type WLAN
SSID BNvoice
Status ☑ Enabled

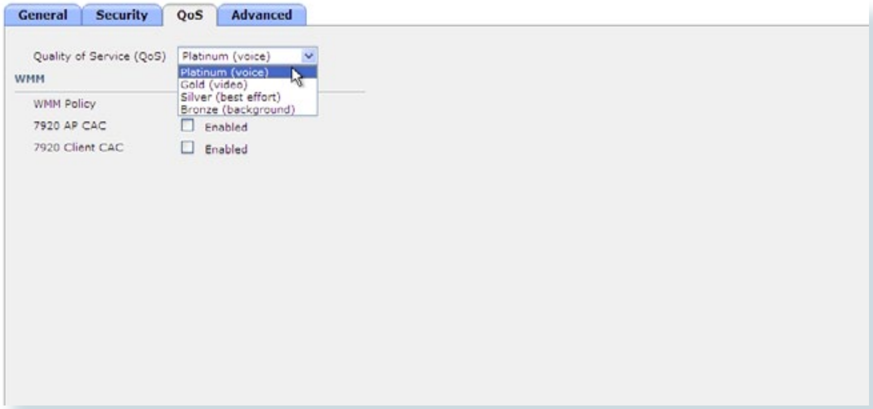
Security Policies [WPA2][Auth(802.1X)]
(Modifications done under security tab will appear after applying the changes.)

Radio Policy All
Interface bn-voice
Broadcast SSID ☑ Enabled

Step 4: Select the **QoS** tab

From the drop-down list next to Quality of Service (QoS), Select **Platinum**.

Figure 36. Voice QoS Configuration Tab



Quality of Service (QoS) Platinum (voice)

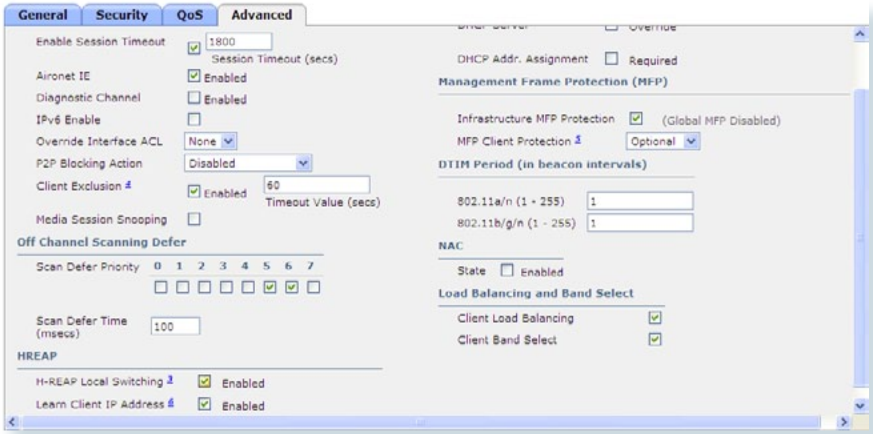
WMM

WMM Policy
7920 AP CAC □ Enabled
7920 Client CAC □ Enabled

Step 5: Select the **Advanced** tab

Check the **H-REAP Local Switching checkbox** and then click **Apply**.

Figure 37. Voice WLAN Advanced Tab



Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE ☑ Enabled
Diagnostic Channel □ Enabled
IPv6 Enable □
Override Interface ACL None
P2P Blocking Action Disabled
Client Exclusion [3] ☑ Enabled 60 Timeout Value (secs)
Media Session Snooping □

Off Channel Scanning Defer

Scan Defer Priority 0 □ 1 □ 2 □ 3 □ 4 □ 5 ☑ 6 ☑ 7 □
Scan Defer Time (msecs) 100

HREAP

H-REAP Local Switching [2] ☑ Enabled
Learn Client IP Address [6] ☑ Enabled

DHCP Addr. Assignment □ Required

Management Frame Protection (MFP)

Infrastructure MFP Protection ☑ (Global MFP Disabled)
MFP Client Protection [5] Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

NAC

State □ Enabled

Load Balancing and Band Select

Client Load Balancing ☑
Client Band Select ☑

Step 6: Repeat this step on every controller in your location.

Procedure 7 Configure Wireless Mobility

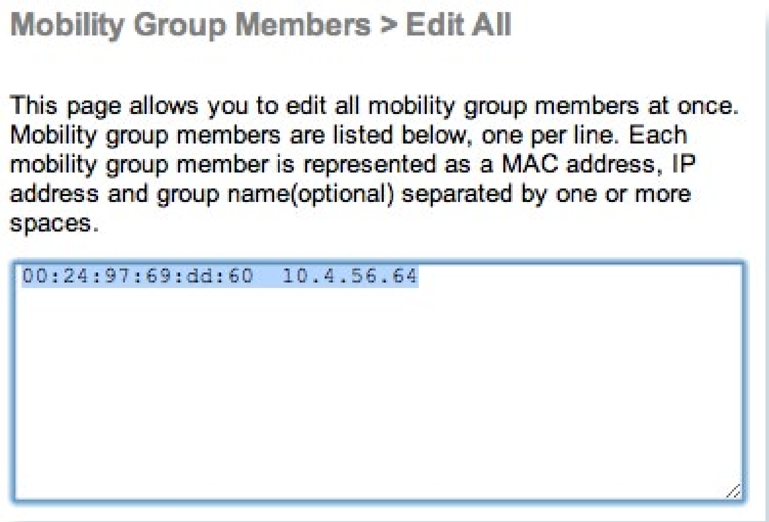
Mobility Groups allow the Wireless LAN Controllers to dynamically share the context and state of client devices, to dynamically share WLC loading information, and to forward data traffic among them, which enables inter-controller wireless LAN roaming and controller redundancy. A Mobility Group can include up to 24 Wireless LAN Controllers of any type. The number of access points supported in a **Mobility Group** is bound by the number of Wireless LAN Controllers and the WLC licensing. From the initial configuration we have completed, each controller now has the Mobility Group name of BN. Now we simply need to allow each controller to know about each other.

Step 1: Capture the Mobility Group Members Identity.

Browse to **Controller** and then select **Mobility Management** to expose and select mobility groups.

Step 2: Click the **Edit All** button to expose the MAC address and IP Address of the controller as shown in Figure 38.

Figure 38. Mobility Groups, Edit All



Mobility Group Members > Edit All

This page allows you to edit all mobility group members at once. Mobility group members are listed below, one per line. Each mobility group member is represented as a MAC address, IP address and group name(optional) separated by one or more spaces.

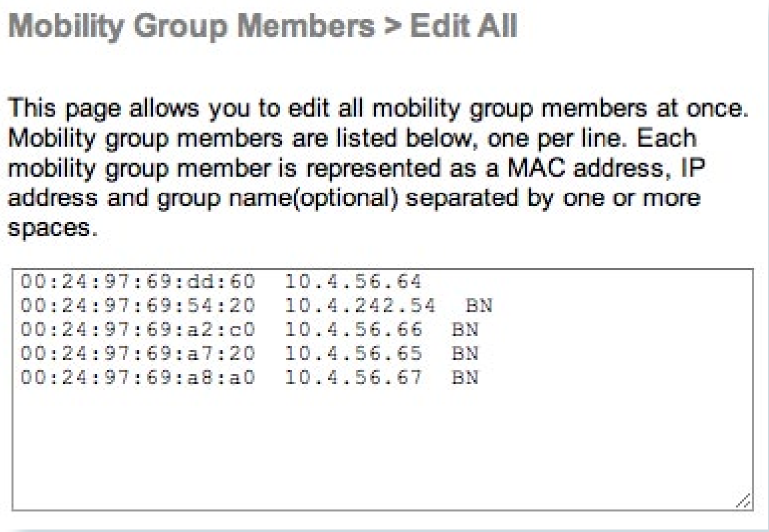
```
00:24:97:69:dd:60  10.4.56.64
```

Step 3: Highlight and copy the mobility group information.

Step 4: Paste this into every controller and click **Apply**.

Step 5: Repeat this process until every controller has every other controllers information as shown in Figure 39.

Figure 39. All Mobility Members



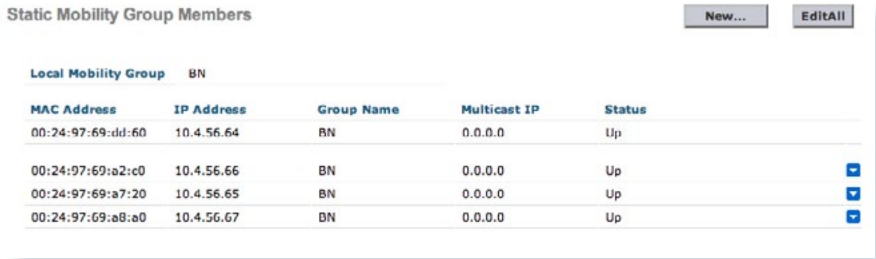
Mobility Group Members > Edit All

This page allows you to edit all mobility group members at once. Mobility group members are listed below, one per line. Each mobility group member is represented as a MAC address, IP address and group name(optional) separated by one or more spaces.

```
00:24:97:69:dd:60  10.4.56.64
00:24:97:69:54:20  10.4.242.54  BN
00:24:97:69:a2:c0  10.4.56.66  BN
00:24:97:69:a7:20  10.4.56.65  BN
00:24:97:69:a8:a0  10.4.56.67  BN
```

Step 6: From the **Controller > Mobility Management > Mobility Groups** page, verify that connectivity is up between all controllers by examining the mobility group information. In the **Status** column, all controllers should be listed as **Up**.

Figure 40. Mobility Group Member Summary



Static Mobility Group Members

Local Mobility Group BN

MAC Address	IP Address	Group Name	Multicast IP	Status
00:24:97:69:dd:60	10.4.56.64	BN	0.0.0.0	Up
00:24:97:69:a2:c0	10.4.56.66	BN	0.0.0.0	Up
00:24:97:69:a7:20	10.4.56.65	BN	0.0.0.0	Up
00:24:97:69:a8:a0	10.4.56.67	BN	0.0.0.0	Up

Procedure 8 Primary Site APs for High Availability

This design utilizes four WLCs; two are primarily for serving Primary Site Access Points, and the other two are primarily for serving Remote Site Access Points. Should disaster strike, any of these four controllers can serve as a resilient service for any of the access points, regardless of itsprimary function.

Any roam, whether it is a Layer 2 or Layer 3, takes resources, but the Catalyst 5508 has more than enough horsepower to handle these client roams. Even so, we are keeping all campus roams at Layer 2. Furthermore, when assigning access points to controllers, it is advisable to split the access points by campus and building to remove as many unnecessary roams as possible.

After deciding which controller will be assigned to each access point, provision the primary site access points for high availability by following these steps:

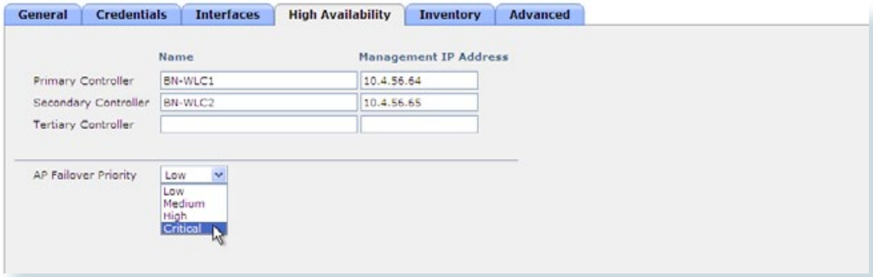
Step 1: Log in to the controller

Step 2: Browse to **Wireless** and select the desired access point.

Step 3: Select the **High Availability** tab

Step 4: From the **AP Failover Priority**, select the appropriate level for this AP and click **Apply**

Figure 41. Configure AP High Availability



	Name	Management IP Address
Primary Controller	BN-WLC1	10.4.56.64
Secondary Controller	BN-WLC2	10.4.56.65
Tertiary Controller		

AP Failover Priority: Low

Tech Tip

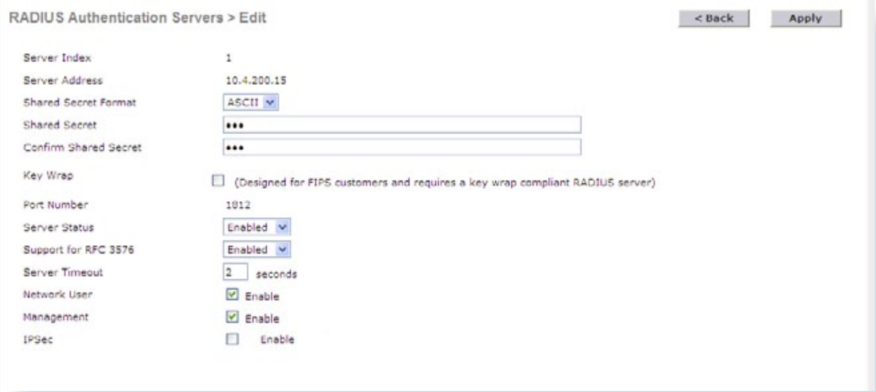
The priority dropdown allows you to decide which AP will be allowed to fail over and which APs will not if a failure occurs and you do not have enough capacity to support every Access Point.

Procedure 9 Cisco Access Control Server (Radius)

Step 1: On each Wireless LAN Controller, browse to **Security** > **Radius** > **Authentication.**

Step 2: Click **New**... and enter the IP address and shared secret. Use the default settings for all other fields.t

Figure 42. Configure Radius Server Details



RADIUS Authentication Servers > Edit

Server Index	1
Server Address	10.4.200.15
Shared Secret Format	ASCII
Shared Secret	•••
Confirm Shared Secret	•••
Key Wrap	□ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Server Timeout	2 seconds
Network User	☑ Enable
Management	☑ Enable
IPSec	□ Enable

Step 3: Click **Apply**.

Step 4: Repeat this step for each controller in the location.

Wireless Guest Access

In this section we present how to deploy we present how to deploy a guest wireless network that allows visitors with a guest username and password to access the Internet at both the primary site and remote sites.

On the core switches, VLAN 16 was previously defined to trunk guest traffic specifically to the ASA. The VLAN interface on the core switch does not have an IP address because the default gateway for this subnet is the ASA and it does not allow access to the rest of the network. Guest authentication is provided by the WLC. The guest account on the WLC expires after a predetermined length of time (the default is 24 hours), after which a new authentication is needed using a newly created username and password.

Procedure 10 Firewall DMZ Configuration

The firewall DMZ (De-Militarized Zone) is a portion of the network where, typically, traffic to and from other parts of the network is tightly restricted. Agencies place network services in a DMZ for exposure to the Internet; these servers are typically not allowed to initiate connections to the inside network, except for specific circumstances.

The various DMZ networks are connected to the ASAs on the ASAs' GigabitEthernet interface via a VLAN trunk. The DMVPN hub device connects via EtherChannel to a resilient switch stack; the VPN-DMZ VLAN interface on the Cisco ASA is assigned an IP address, which is the default gateway for the VPN-DMZ VLAN subnet. The DMZ switch's VLAN interface does not have an IP address assigned for the VPN-DMZ VLAN.

Procedure Steps:

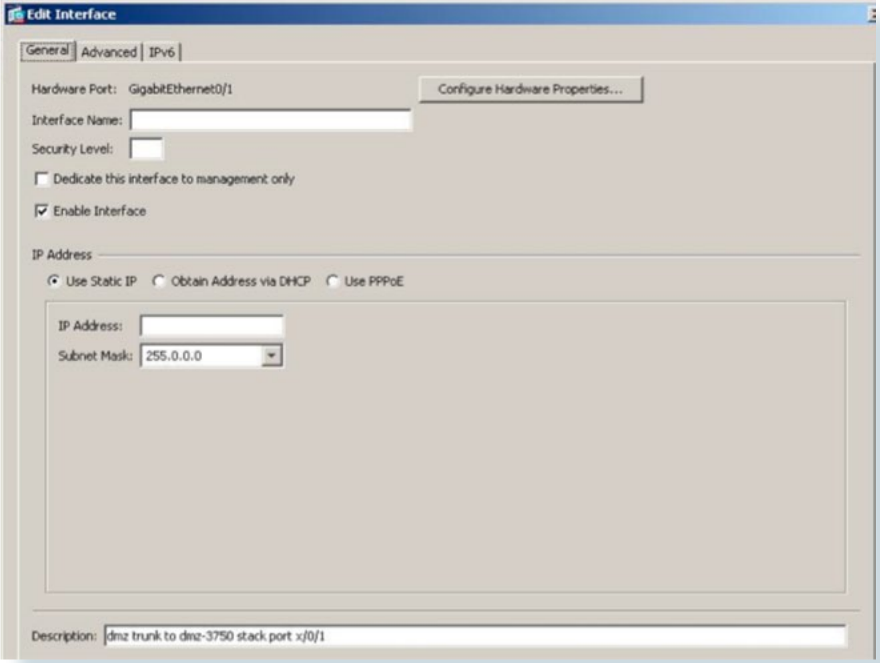
1. Configure the ASA firewall physical interface.
2. Configure the subinterface for the DMZ-Guest

Step 1: Configure the ASA firewall physical interface.

Configure the interface which carries the VLAN trunk for the various DMZs. Values are not assigned for the interface name, security level, or IP address on trunk interfaces. Configuration details are shown in Figure 45.

```
interface GigabitEthernet0/1
  description dmz trunk to dmz-3750 stack port x/0/1
  no nameif
  no security-level
  no ip address
```

Figure 43. Define DMZ Trunk Interface



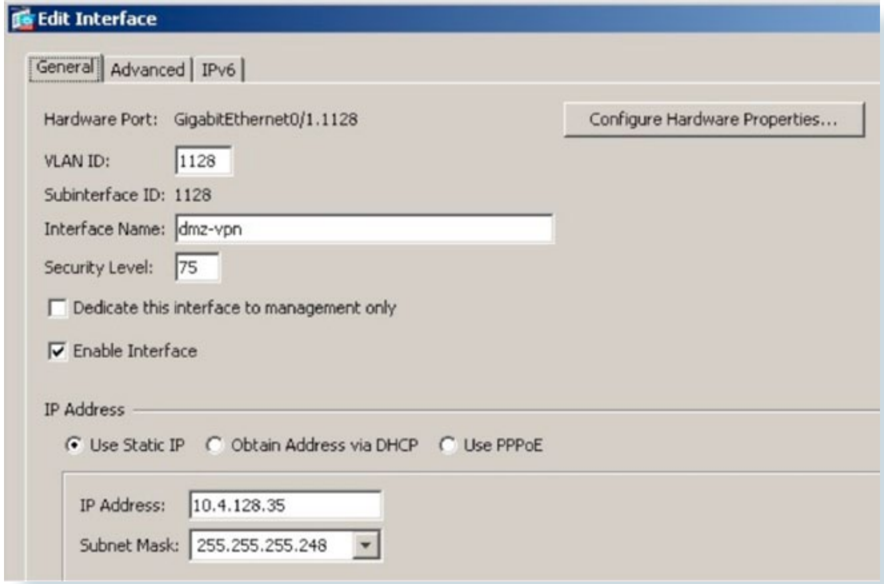
Hardware Port: GigabitEthernet0/1
Interface Name:
Security Level:
□ Dedicate this interface to management only
☑ Enable Interface
● Use Static IP ○ Obtain Address via DHCP ○ Use PPPoE
IP Address:
Subnet Mask: 255.0.0.0
Description: dmz trunk to dmz-3750 stack port x/0/1

Step 2: Configure the DMZ VLAN connectivity on GigabitEthernet 0/1 subinterface.

The DMZ VLAN interface must be assigned an appropriate IP address for the attached subnet, as well as an intuitive interface name to be used for NAT and security policy configuration. The tested design uses the values shown. Figure 44 illustrates the configuration for two VLAN interfaces.

Interface label	IP Address & Netmask	VLAN	Security Level	Name
GigabitEthernet 0/1.1122	10.4.246.1/24	1122	50	dmz-guest-wlc
GigabitEthernet 0/1.1126	192.168.16.1/22	1126	10	dmz-wifi-guest

Figure 44. DMZ Sub-interface Configuration



Hardware Port: GigabitEthernet0/1.1128
VLAN ID: 1128
Subinterface ID: 1128
Interface Name: dmz-vpn
Security Level: 75
□ Dedicate this interface to management only
☑ Enable Interface
● Use Static IP ○ Obtain Address via DHCP ○ Use PPPoE
IP Address: 10.4.128.35
Subnet Mask: 255.255.255.248

```
interface GigabitEthernet0/1.1122
  vlan 1122
  nameif dmz-guest-wlc
  security-level 50
  ip address 10.4.246.1 255.255.255.248
!
interface GigabitEthernet0/1.1126
  vlan 1126
  nameif dmz-wifi-guest
  security-level 10
  ip address 192.168.16.1 255.255.252.0
```

Step 3: On the DMZ switch, define switch ports that connect to the ASAs as trunk ports and add the appropriate VLAN.

Set the distribution layer switch to be the Spanning Tree Root for the Wireless VLANs that you are connecting to the distribution switch.

```
vlan 1122,1126
spanning-tree vlan 1122,1126 root primary
```

If this is the first VLAN to be added to the trunk from the DMZ switch, then use the following set of commands:

```
interface GigabitEthernet1/0/1
  description ASA5540-1 DMZ uplink
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1122, 1126
  switchport mode trunk
  spanning-tree link-type point-to-point
```

If this is an additional VLAN being added to the trunk from the DMZ switch, then use the following set of commands:

```
interface GigabitEthernet1/0/1
switchport trunk allowed vlan add 1122, 1126
```

Procedure 11 Firewall Address Translation Configuration

At this point there is no access from the DMZ-Guest network to the Internet, or from the Internet to the DMZ-Guest network. A last step is required to allow Internet connectivity for the DMZ; the DMZ network uses private network (RFC 1918) addressing that is not Internet routable, so the ASAs must translate the DMZ address to an outside public address. For this configuration, we translate the DMZ-Guest addresses to a public IP address that can be routed on the Internet.

Tech Tip

As you apply the address translation configuration described in this portion of the document, the ASA will apply its default access rule set that permits traffic from higher-security interfaces to lower-security interfaces. Review your expected traffic carefully; if you cannot allow some or all traffic that is allowed by the default rules, you should shut down the various device interfaces until you have completely configured your firewall rule set.

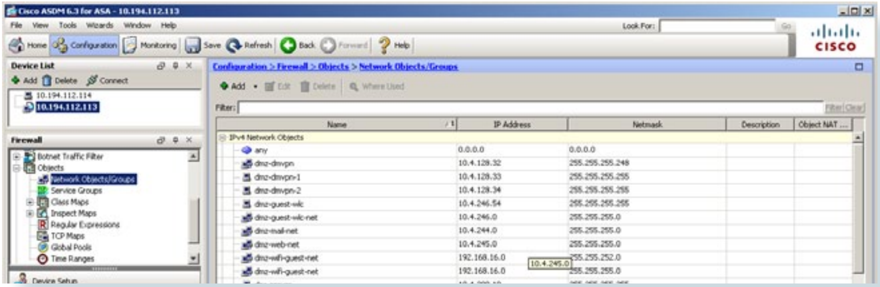
Step 1: Configure name-to-address mappings for DMZ-Guest subnets

These names are used for NAT configuration, as well as Access-Rule definition. Be sure the names that you apply are applicable for all parts of the configuration. Using address-family names and object-groups improves command-line and ASDM usability for the Cisco ASA, as the various IP networks and hosts within your agency are represented as names instead of IP addresses.

Navigate to Configuration > Firewall > Objects > Network Objects/Groups

```
names
name 10.4.246.0 dmz-guest-wlc-net
name 10.4.246.54 dmz-guest-wlc
name 192.168.16.0 dmz-wifi-guest-net
```

Figure 45. Configure Network Object Names



Configuration > Firewall > Objects > Network Objects/Groups

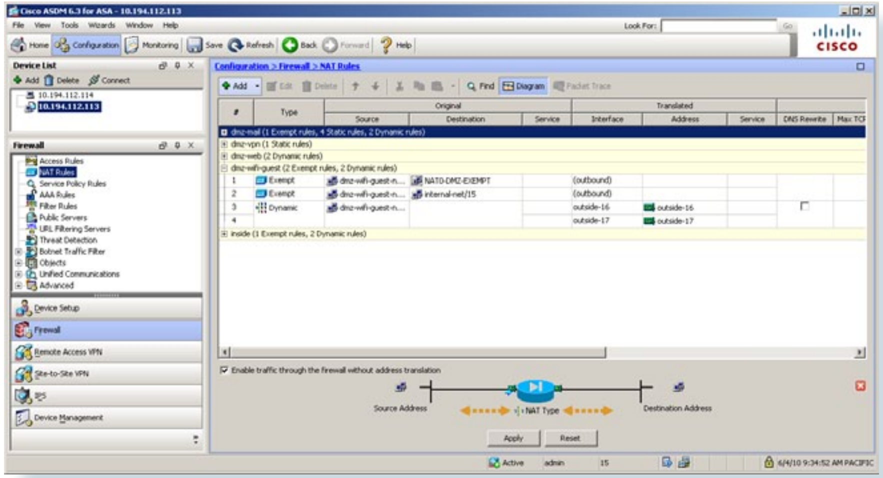
Name	IP Address	Netmask	Description	Object NAT ...
IPv4 Network Objects				
any	0.0.0.0	0.0.0.0		
dmz-dmvpn	10.4.128.32	255.255.255.248		
dmz-dmvpn-1	10.4.128.33	255.255.255.255		
dmz-dmvpn-2	10.4.128.34	255.255.255.255		
dmz-guest-wlc	10.4.246.54	255.255.255.255		
dmz-guest-wlc-net	10.4.246.0	255.255.255.0		
dmz-mail-net	10.4.244.0	255.255.255.0		
dmz-web-net	10.4.245.0	255.255.255.0		
dmz-wifi-guest-net	192.168.16.0	255.255.252.0		
dmz-wifi-guest-net	192.168.16.0	255.255.255.0		

Step 2: Configure the Dynamic NAT rule that is used for the guest Wi-Fi network in Configuration > Firewall > NAT Rules :

An internet configuration that uses only one outside interface will have one 'global' configuration line.

```
global (outside) 1 interface
nat (dmz-wifi-guest) 0 access-list WIFI-GUEST_NAT0_OUTBOUND
nat (dmz-wifi-guest) 1 dmz-wifi-guest-net 255.255.252.0
```

Figure 46. Define dynamic NAT for Internet Edge-5K



Configuration > Firewall > NAT Rules

#	Type	Original Source	Original Destination	Original Service	Translated Interface	Translated Address	Translated Service	DNS Rewrite	Max TCP
dmz-mail (1 Exempt rules, 4 Static rules, 2 Dynamic rules)									
dmz-vpn (1 Static rules)									
dmz-web (2 Dynamic rules)									
dmz-wifi-guest (2 Exempt rules, 2 Dynamic rules)									
1	Exempt	dmz-wifi-guest-n...	NAT0-DMZ-EXEMPT		(outbound)				
2	Exempt	dmz-wifi-guest-n...	internal-net/15		(outbound)				
3	Dynamic	dmz-wifi-guest-n...			outside-16	outside-16		□	
4					outside-17	outside-17			
inside (1 Exempt rules, 2 Dynamic rules)									

☑ Enable traffic through the firewall without address translation

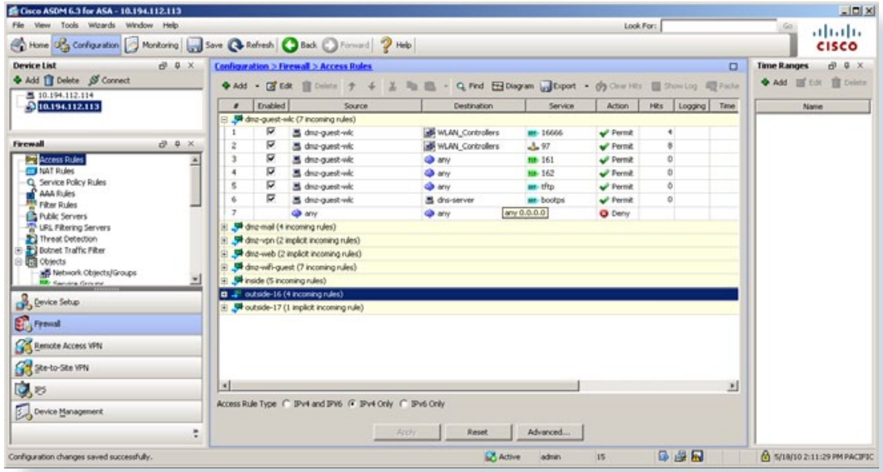
Procedure 12 Configure Firewall Policy for Wireless Guest

Security policy configuration is fairly arbitrary to suit the policy and management requirements of an agency. Thus, examples here should be used as a basis for your network's security requirements.

The Internet does not originate any connections into the guest WLC DMZ; the Guest WLC only needs to send traffic to and receive traffic from the network's other Wireless LAN Controllers.

Step 1: Define the security policy that allows the Guest WLC to reach the Internal WLCs and the internal DHCP servers.

Figure 47. DMZ-Guest WLC Policy Configuration



Configuration > Firewall > Access Rules

#	Enabled	Source	Destination	Service	Action	Hits	Logging	Time
dmz-guest-wlc (7 incoming rules)								
1	☑	dmz-guest-wlc	WLAN_Controllers	16666	Permit	4		
2	☑	dmz-guest-wlc	WLAN_Controllers	97	Permit	8		
3	☑	dmz-guest-wlc	any	161	Permit	0		
4	☑	dmz-guest-wlc	any	162	Permit	0		
5	☑	dmz-guest-wlc	any	tftp	Permit	0		
6	☑	dmz-guest-wlc	dns-server	bootps	Permit	0		
7		any	any		Deny			
dmz-mail (4 incoming rules)								
dmz-vpn (2 implicit incoming rules)								
dmz-web (2 implicit incoming rules)								
dmz-wifi-guest (7 incoming rules)								
inside (5 incoming rules)								
outside-16 (4 incoming rules)								
outside-17 (1 implicit incoming rule)								

Access Rule Type ○ IPv4 and IPv6 ● IPv4 Only ○ IPv6 Only

Configuration changes saved successfully.

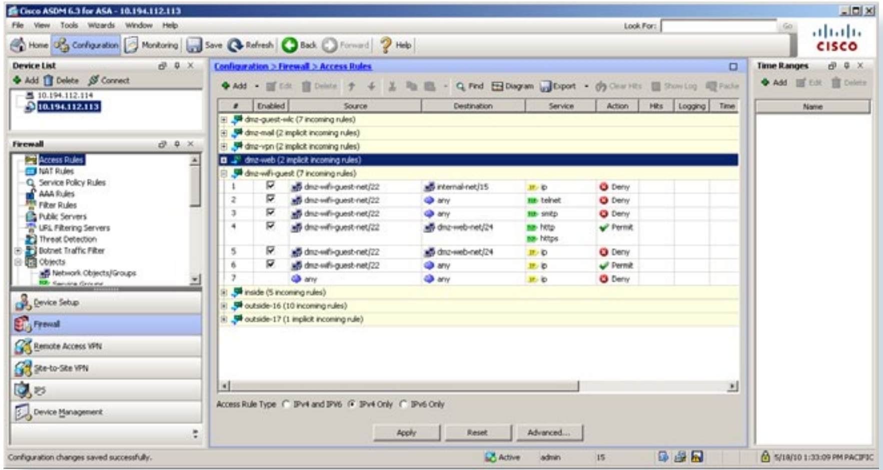
```
object-group network WLAN_Controllers
  network-object host 10.4.56.64
  network-object host 10.4.56.65
  network-object host 10.4.56.66
  network-object host 10.4.56.67
  network-object host 10.4.56.68
access-list DMZ-GUEST-WLC_ACCESS_IN remark For Guest WLC @ 
10.4.246.54
access-list DMZ-GUEST-WLC_ACCESS_IN extended permit udp host 
dmz-guest-wlc object-group WLAN_Controllers eq 16666 
access-list DMZ-GUEST-WLC_ACCESS_IN extended permit 97 host 
dmz-guest-wlc object-group WLAN_Controllers 
```

```
access-list DMZ-GUEST-WLC_ACCESS_IN extended permit tcp host 
dmz-guest-wlc any eq 161
access-list DMZ-GUEST-WLC_ACCESS_IN extended permit tcp host 
dmz-guest-wlc any eq 162
access-list DMZ-GUEST-WLC_ACCESS_IN extended permit udp host 
dmz-guest-wlc any eq tftp
access-list DMZ-GUEST-WLC_ACCESS_IN extended permit udp host 
dmz-guest-wlc eq bootpc host dns-server eq bootps
access-group DMZ-GUEST-WLC_ACCESS_IN in interface dmz-guest-
wlc
dhcprelay server dns-server inside
dhcprelay enable dmz-wifi-guest
dhcprelay timeout 60
```

Step 2: Configure a similar policy to prevent guest wireless users from gaining access to the internal network, to restrict guest access to the HTTP and HTTPS services in the DMZ, to block all guest WiFi SMTP, and to allow other IP access:

If guest-wireless users will have access to your network (or other remote-access services on the Internet) with remote-access VPN, be sure the guest-wireless DMZ policy does not interfere with the cryptographic traffic that remote-access VPN typically employs.

Figure 48. DMZ-Guest Internet Access Policy Configuration



Configuration > Firewall > Access Rules

#	Enabled	Source	Destination	Service	Action	Hits	Logging	Time
dmz-guest-wlc (7 incoming rules)								
dmz-mail (2 implicit incoming rules)								
dmz-vpn (2 implicit incoming rules)								
dmz-web (2 implicit incoming rules)								
dmz-wifi-guest (7 incoming rules)								
1	☑	dmz-wifi-guest-net/22	internal-net/15	ip	Deny			
2	☑	dmz-wifi-guest-net/22	any	telnet	Deny			
3	☑	dmz-wifi-guest-net/22	any	smtp	Deny			
4	☑	dmz-wifi-guest-net/22	dmz-web-net/24	http https	Permit			
5	☑	dmz-wifi-guest-net/22	dmz-web-net/24	ip	Deny			
6	☑	dmz-wifi-guest-net/22	any	ip	Permit			
7		any	any	ip	Deny			
inside (5 incoming rules)								
outside-16 (10 incoming rules)								
outside-17 (1 implicit incoming rule)								

Access Rule Type ○ IPv4 and IPv6 ● IPv4 Only ○ IPv6 Only

Configuration changes saved successfully.

```
object-group service DM_INLINE_TCP_1 tcp
  port-object eq www
  port-object eq https
interface access-list dmz-wifi-guest_access_in extended deny 
ip dmz-wifi-guest-net 255.255.252.0 internal-net 255.254.0.0 
access-list dmz-wifi-guest_access_in extended deny tcp dmz-
wifi-guest-net 255.255.252.0 any eq telnet 
access-list dmz-wifi-guest_access_in extended deny tcp dmz-
wifi-guest-net 255.255.252.0 any eq smtp 
access-list dmz-wifi-guest_access_in extended permit tcp dmz-
wifi-guest-net 255.255.252.0 dmz-web-net 255.255.255.0 object-
group DM_INLINE_TCP_1 
access-list dmz-wifi-guest_access_in extended deny ip dmz-
wifi-guest-net 255.255.252.0 dmz-web-net 255.255.255.0 
access-list dmz-wifi-guest_access_in extended permit ip dmz-
wifi-guest-net 255.255.252.0 any
access-group dmz-wifi-guest_access_in in interface dmz-wifi-
guest
```

Configure the DMZ switch for WLC Connectivity

The switch in the DMZ should be set up for a Layer 2 port channel to connect both the control and client traffic. Two VLANs are used for the port channel: VLAN 1122 is for Wireless LAN Controller traffic and VLAN 1126 is for Wireless Guest traffic. Guest traffic can only go to the Internet through the permitted agency web server

Procedure 13 DMZ Switch Configuration

After all the Wireless LAN Controllers are physically installed and powered up, configure an EtherChannel between each controller and the LAN distribution switch.

The VLANs used in the following configuration examples are:

- Guest WLC Management: VLAN 1122, IP: 10.4.246.0/24
- Guest Data Network: VLAN 1126, IP 10.4.52.0/22

Step 1: Configure Layer 2.

Step 2: EtherChannel Member Interface Configuration

This design uses Layer 2 EtherChannels to connect Wireless LAN Controllers to the distribution switch. Connect the WLC EtherChannel uplinks to separate devices in the distribution layer virtual switch or stack, and in the case of the Cisco Catalyst 4507R-E distribution layer switch, connect to separate redundant line cards for additional resiliency.

On the distribution switch, the physical interfaces that are members of a Layer 2 EtherChannel are configured prior to configuring the logical port-channel interface. Doing the configuration in this order 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.

Configure two or more physical interfaces to be members of the EtherChannel. It is best if they are added in multiples of two.

```
interface range [interface type] [port 1], [interface type] 
[port 2]
  channel-group [number] mode on
```

Step 3: Trunk Configuration

An 802.1Q trunk is used for the connection to the access layer which allows the distribution switch to provide the Layer 3 services to all the VLANs defined on the access layer switch. The VLANs allowed on the trunk are pruned to only the VLANs that are active on the access switch. .

```
interface [interface type] [number]
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1122,1126
  switchport mode trunk
  no shutdown
```

Procedure 14 Guest Wireless LAN Controller Configuration

As previously seen with the Wireless LAN Controllers, we use CLI commands for the initial configuration, and then complete the remainder of the configuration using the Graphical User Interface (GUI) through a web browser. For this deployment, we use the following information to configure Wireless guest access:

```
VLAN 1122
IP address 10.4.246.54
Netmask 255.255.255.0
Gateway 10.4.246.1
Primary DHCP server 10.4.200.10
SSID guest
```

After the initial hardware boot process is complete, you see the following information displayed on the screen:

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
Would you like to terminate autoinstall? [yes]:no
```

Step1: Enter a system name.

```
System Name [Cisco_7e:8e:73] (31 characters max): BN-GUEST
```

Step 2: Enter an administrator username and password.

Tech Tip

Do not use the username below. When you enter the passwords, the characters echo back as "*" symbols.

```
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Re-enter Administrative Password     : *****
```

Step 3: Use DHCP for the service port Interface address.

```
Service Interface IP address Configuration [none] [DHCP]: DHCP
```

Step 4: Enable Link Aggregation.

```
Enable Link Aggregation (LAG) [yes][NO]: YES
```

Step 5: Enter the IP address and subnet mask for the management interface (that is, IP address 10.4.56.64, netmask 255.255.255.0, default gateway 10.4.56.1, and VLAN 156).

```
Management Interface IP Address: 10.4.246.54
Management Interface Netmask: 255.255.255.0
Management interface Default Router: 10.4.246.1
```

Tech Tip

Every interface is tagged. We do not use the untagged VLAN or native VLAN to the Layer 2 port channel for any interface.

```
Management Interface VLAN Identifier (0 = untagged): 1122
```

Step 6: Enter the default DHCP server for clients.

Tech Tip

In this deployment guide, 10.4.200.10 is the IP address of the DHCP server in the server farm.

```
Management Interface DHCP Server IP Address: 10.4.200.10
```

Step 7: The virtual interface is used by the WLC for Mobility DHCP relay and inter-controller communication (i.e. 1.1.1.1)

```
Virtual Gateway IP Address: 1.1.1.1
```

Step 8: Enter the name to be used as the default mobility and RF group (that is, BN).

Tech Tip

Use something other than **default** for the building or campus name.

```
Mobility/RF Group Name: BN
```

Step 9: Enter **guest** as the initial SSID, or enter the guest SSID you wish to use as you can later leverage this name for the guest WLAN.

```
Network Name (SSID): guest
```

Step 10: Enter **no** to make clients use DHCP IP addresses, as you do not want users to be able to assign their own address when connecting to your network. This type of addressing works much the same way as DHCP snooping.

```
Allow Static IP Addresses {YES][no]: NO
```

Step 11: Enter **no** to configure RADIUS because we configure it later through the GUI.

```
Configure a RADIUS Server now? [YES][no]: NO
```

The default WLAN security policy requires a RADIUS server.

Step 12: Enter the correct country code for the country you are deploying in.

```
Enter Country Code list (enter 'help' for a list of countries) 
[US]: US
```

Step 13: Enter **yes** to enable all wireless networks. 802.11a is typically used for wireless Voice traffic, while 802.11g/g/n is typically used for data.

```
Enable 802.11b network [YES][no]: YES
Enable 802.11a network [YES][no]: YES
Enable 802.11g network [YES][no]: YES
```

Step 14: Enter **yes** to enable the WCL radio resource management (RRM) auto RF feature. This important and unique feature of the Cisco Wireless LAN controller can help you keep your network up and operational.

```
Enable Auto-RF [YES][no]: YES
```

Step 15: Configure NTP at a later time. We skip the NTP configuration section by entering the current date and time because there is no way to ensure an NTP server is reachable until the entire network is configured and network connectivity is established.

```
Configure a NTP server now? [YES][no]: NO
Enter the date in MM/DD/YY format: 02/16/10
Enter the time in HH:MM:SS format: 10:10:50
```

Step 16: Enter **yes** to save the configuration. If you enter **no**, the system restarts from Step 1 and guides you through this same process without saving what you have already configured.

```
Configuration correct? If yes, system will save it and reset 
[yes][NO]: YES
Configuration saved!
```

Procedure 15 Create Wireless Guest Interface

The wireless guest interface can be used to connect to the DMZ of the ASA 5540 security appliance to allow guest wireless traffic only to and from the Internet. All traffic, regardless of the controller that the guest initially connects to, is automatically anchored to this guest access controller and appears on the new interface. With this architecture we have now deviated from the 10.x.y.z to more easily identify guest traffic from internal traffic in our network.

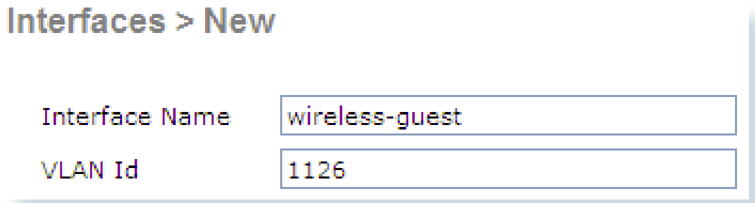
For this deployment, we use the following information to configure the Wireless guest interface:

```
VLAN 1126 (Guest WLC), or VLAN 0 (Primary Site WLCs)
Netmask 255.255.252.0
Gateway 192.168.16.1 (ASA 5540 DMZ interface on VLAN 1126)
Primary DHCP server 10.4.200.10
```

Step 1: Use your browser and the GUI of the WLC to create the new interface on the BN Guest Controller.

From the **Controller > Interfaces** page, click **New...**. Enter an interface name such as wireless-guest and the VLAN ID 1126 if it is the guest WLC; otherwise, enter the VLAN ID 0 and click **Apply**.

Figure 49. New Guest Interface



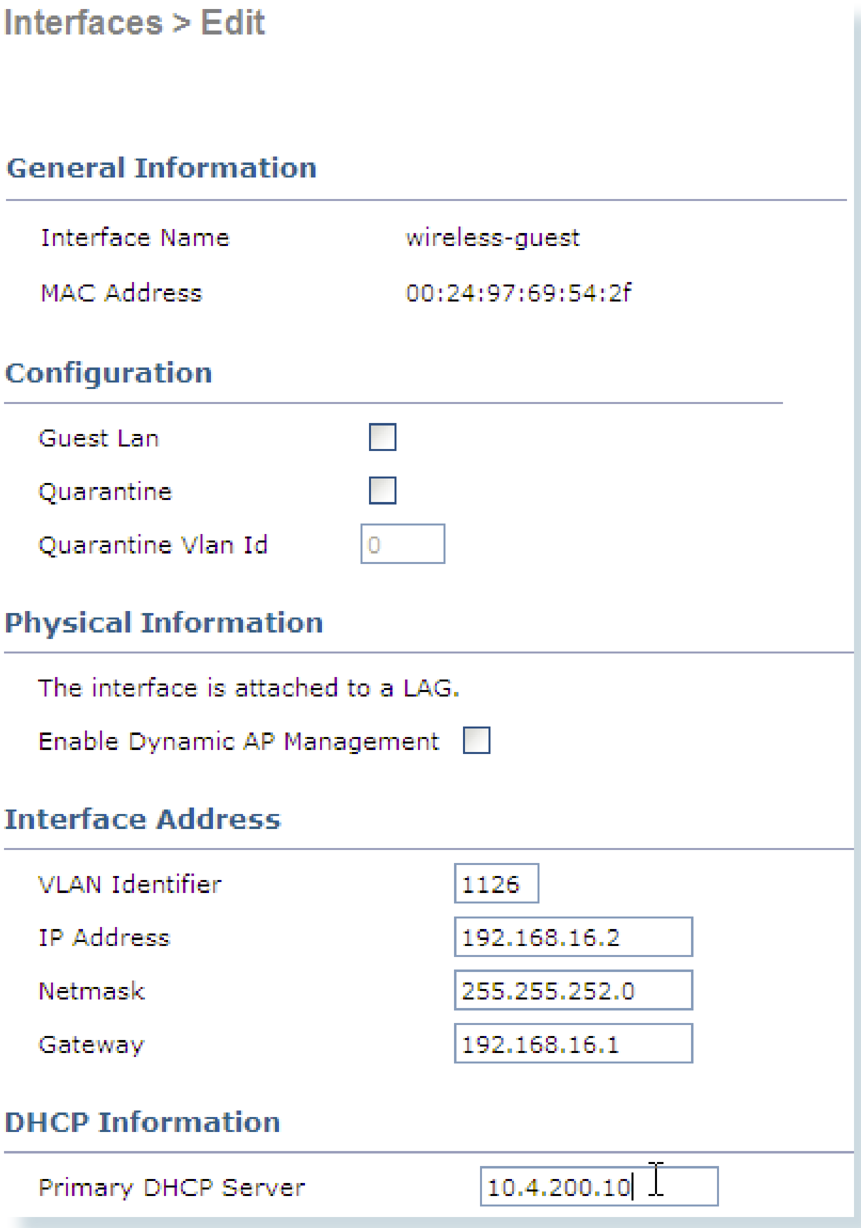
Interfaces > New

Interface Name	wireless-guest
VLAN Id	1126

Step 2: Enter all necessary information for this interface as described previously.

Controller	Guest Interface IP Address
BN-GUEST	192.168.16.2 255.255.252.0
BN-WLC1	192.168.16.3 255.255.252.0
BN-WLC2	192.168.16.4 255.255.252.0
BN-WLC3	192.168.16.5 255.255.252.0
BN-WLC4	192.168.16.6 255.255.252.0

Figure 50. Guest Interface Details



Interfaces > Edit

General Information

Interface Name	wireless-guest
MAC Address	00:24:97:69:54:2f

Configuration

Guest Lan	□
Quarantine	□
Quarantine Vlan Id	0

Physical Information

The interface is attached to a LAG.

Enable Dynamic AP Management □

Interface Address

VLAN Identifier	1126
IP Address	192.168.16.2
Netmask	255.255.252.0
Gateway	192.168.16.1

DHCP Information

Primary DHCP Server	10.4.200.10

Procedure 16 Add Guest Anchor to BN Mobility Group

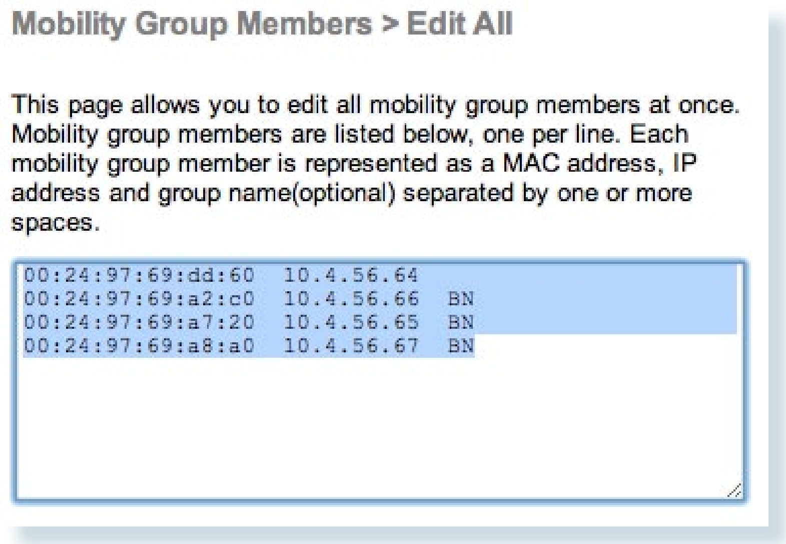
Previously we added all the primary site controllers to each mobility group table. With the Guest Access Controller up and running, we now need to add the Guest Access LAN Controller to each primary site controller and add every primary site controller to the Guest Access WLC.

Step 1: On any primary site controller, log in and select CONTROLLER > Mobility Management > Mobility Groups

Step 2: Click EditAll.

Step 3: Copy Mobility Members.

Figure 51. Capture All Controllers



Mobility Group Members > Edit All

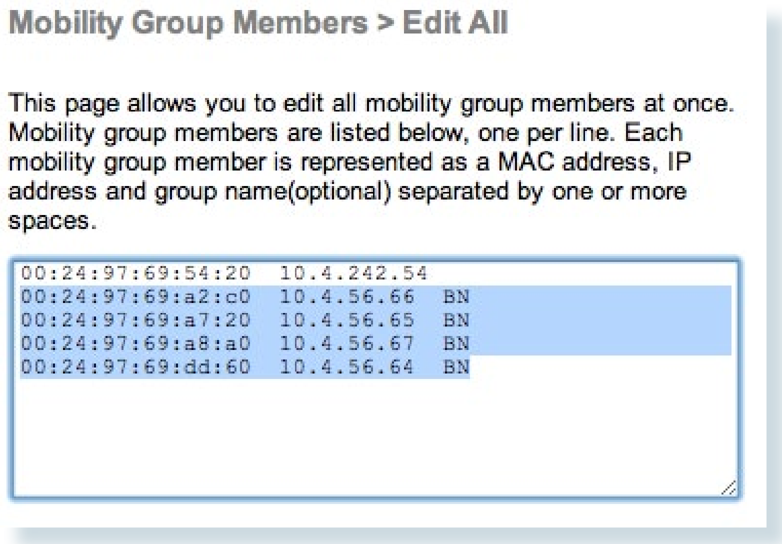
This page allows you to edit all mobility group members at once. Mobility group members are listed below, one per line. Each mobility group member is represented as a MAC address, IP address and group name(optional) separated by one or more spaces.

```
00:24:97:69:dd:60  10.4.56.64
00:24:97:69:a2:c0  10.4.56.66   BN
00:24:97:69:a7:20  10.4.56.65   BN
00:24:97:69:a8:a0  10.4.56.67   BN
```

Step 4: On the guest controller, open Mobility groups by logging into the guest access controller, select CONTROLLER > Mobility Management > Mobility Groups.

Step 5: Click EditAll button and paste list into field after the first line as shown below.

Figure 52. Add All Foreign Controllers



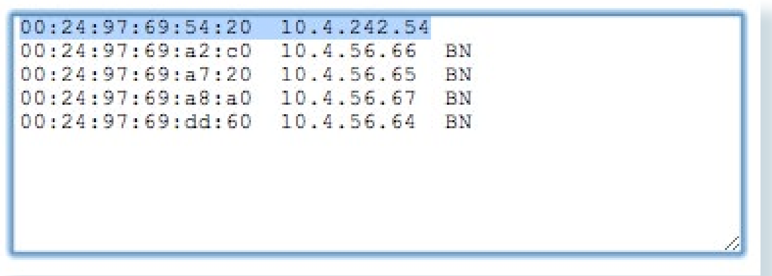
Mobility Group Members > Edit All

This page allows you to edit all mobility group members at once. Mobility group members are listed below, one per line. Each mobility group member is represented as a MAC address, IP address and group name(optional) separated by one or more spaces.

```
00:24:97:69:54:20  10.4.242.54
00:24:97:69:a2:c0  10.4.56.66   BN
00:24:97:69:a7:20  10.4.56.65   BN
00:24:97:69:a8:a0  10.4.56.67   BN
00:24:97:69:dd:60  10.4.56.64   BN
```

Step 6: Copy the Guest Access Controller MAC address and IP address from the first line of this mobility list as shown in Figure 53.

Figure 53. Add Guest WLC to all other Controllers



```
00:24:97:69:54:20  10.4.242.54
00:24:97:69:a2:c0  10.4.56.66   BN
00:24:97:69:a7:20  10.4.56.65   BN
00:24:97:69:a8:a0  10.4.56.67   BN
00:24:97:69:dd:60  10.4.56.64   BN
```

Step 7: On each primary site controller, open Mobility groups by logging into the controller, and selecting CONTROLLER > Mobility Management > Mobility Groups

Step 8: Click EditAll and paste the list into the field after the first line, as show in Figure 52.

Verify that all mobility groups are up by checking each controller:

Set Up Auto Anchor on the Primary Site Wireless LAN Controllers

Now that you have Mobility enabled, the required pool of addresses in place, the firewall and your web authentication page set up, it is time to tunnel your traffic. The concept behind guest tunneling is to create what is known as an Auto Anchor which works much the same way as a Layer 3 roam between controllers. The main difference is that when a client connects to the guest SSID, the client is automatically anchored to the controller in the DMZ. The guest clients traffic is tunneled in an IP-IP tunnel from the controller that the AP is connected to, to the anchor controller where it is given an IP for the DMZ and redirected to the internal web authentication page. The client will not be authorized to connect with any IP protocol until they present credentials to this authentication page.

Procedure 17 Configure Auto-Anchor for Guest

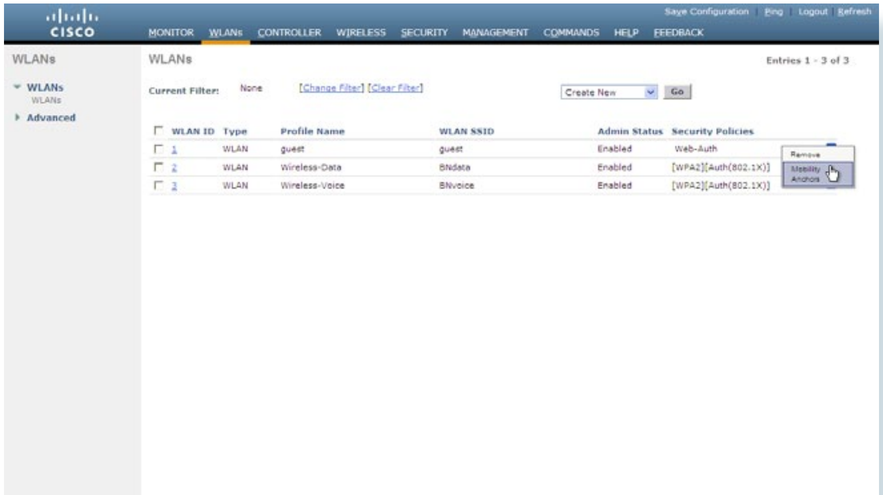
Step 1: Log in to controller.

Step 2: Browse to WLANs.

Step 3: Mouse over blue drop-down list next to your guest WLAN.

Step 4: Select **Mobility Anchors.**

Figure 54. Select Mobility Anchor



WLANs

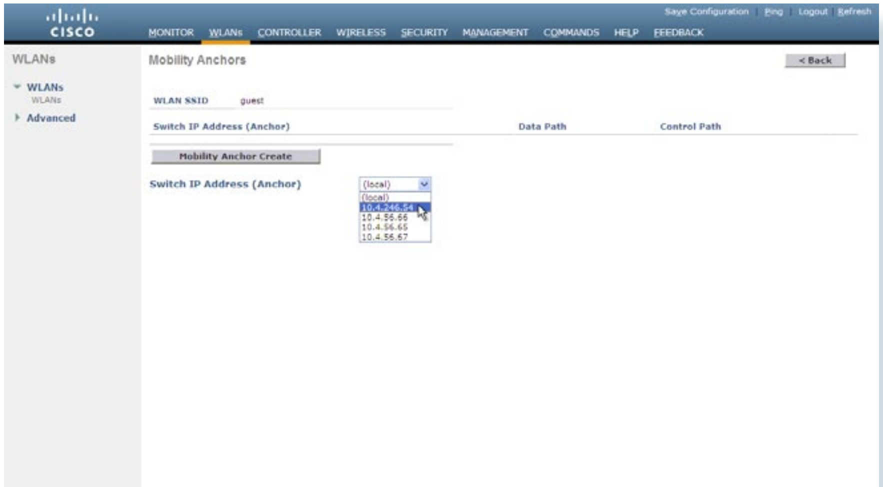
Entries 1 - 3 of 3

Current Filter: None [Change Filter] [Clear Filter]

	WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
□	1	WLAN	guest	guest	Enabled	Web-Auth
□	2	WLAN	Wireless-Data	BNdata	Enabled	[WPA2][Auth(802.1X)]
□	3	WLAN	Wireless-Voice	BNvoice	Enabled	[WPA2][Auth(802.1X)]

Step 5: Select the Guest Anchor Controller from the drop-down list.

Figure 55. Create Mobility to Guest Anchor Controller



Mobility Anchors

WLAN SSID guest

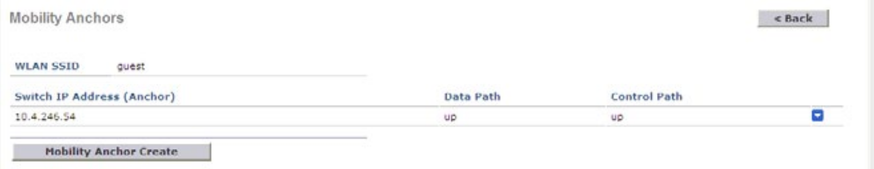
Switch IP Address (Anchor)	Data Path	Control Path

Switch IP Address (Anchor) (local)

(local)
10.4.246.54
10.4.56.66
10.4.56.65
10.4.56.67

Step 6: Click the **Mobility Anchor Create** button.

Figure 56. Guest Anchor Complete



Mobility Anchors

WLAN SSID guest

Switch IP Address (Anchor)	Data Path	Control Path
10.4.246.54	up	up

Step 7: Repeat Step 1 through 6 on every controller.

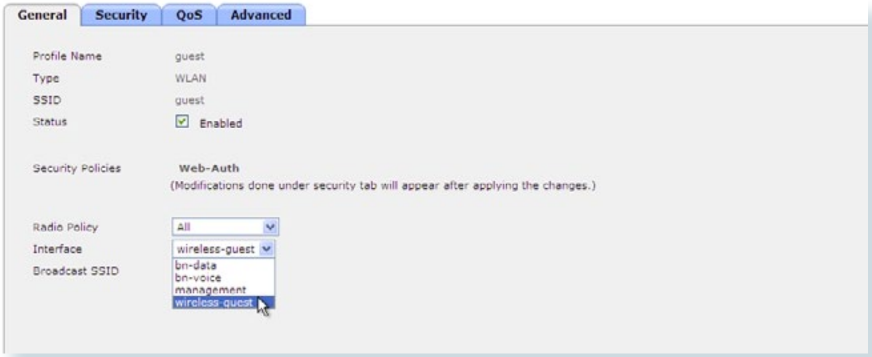
Procedure 18 Guest WLAN for Web Authentication

Step 1: Browse to **WLANs.**

Step 2: Select the **WLAN ID** for the guest WLAN.

Step 3: From the **General** tab, change the interface from management to guest.

Figure 57. Change Interface Anchoring



Profile Name guest
Type WLAN
SSID guest
Status ☑ Enabled

Security Policies **Web-Auth**
(Modifications done under security tab will appear after applying the changes.)

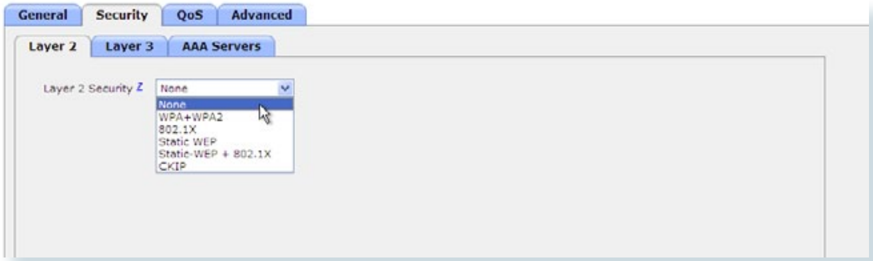
Radio Policy All
Interface wireless-guest
Broadcast SSID

bn-data
bn-voice
management
wireless-guest

Step 4: Select the **Security** Tab.

Step 5: Change **Layer 2 Security** to **None.**

Figure 58. Change Configuration Options



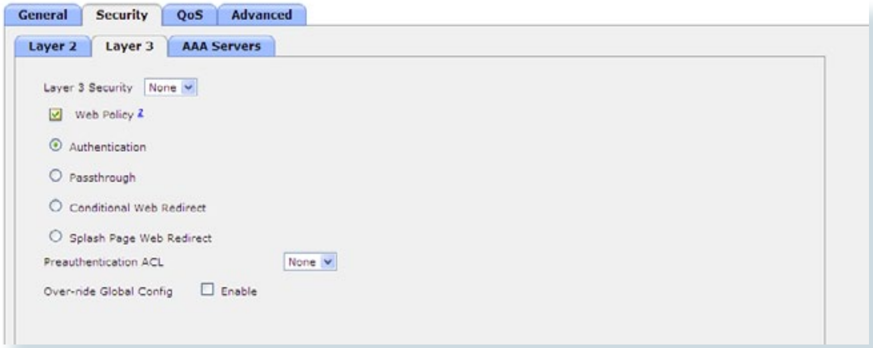
Layer 2 Security None

None
WPA+WPA2
802.1X
Static WEP
Static-WEP + 802.1X
CKIP

Step 6: From the Security tab, select Layer 3.

Step 7: Check the checkbox next to **Web Policy.**

Figure 59. Check WebAuth with Security for WLAN



Layer 3 Security None

☑ Web Policy

● Authentication

○ Passthrough

○ Conditional Web Redirect

○ Splash Page Web Redirect

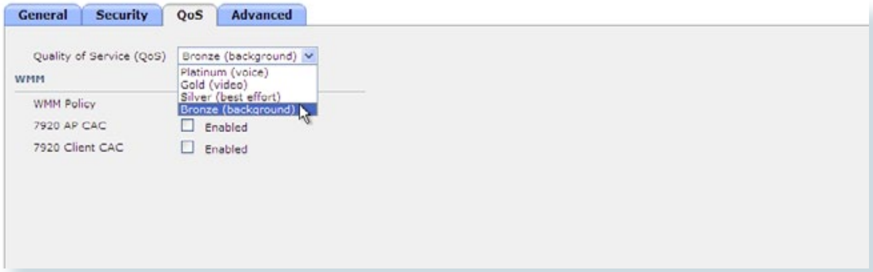
Preauthentication ACL None

Over-ride Global Config □ Enable

Step 8: Select the **QoS** tab.

Step 9: From the drop-down list for **Quality of Service (QoS)** select **Bronze (background).**

Figure 60. Quality of Service for Guest



Quality of Service (QoS) Bronze (background)

Platinum (voice)
Gold (video)
Silver (best effort)
Bronze (background)

WMM

WMM Policy
7920 AP CAC □ Enabled
7920 Client CAC □ Enabled

Step 10: Click **Apply**.

Step 11: Repeat Steps 1 through 10 on every contoller

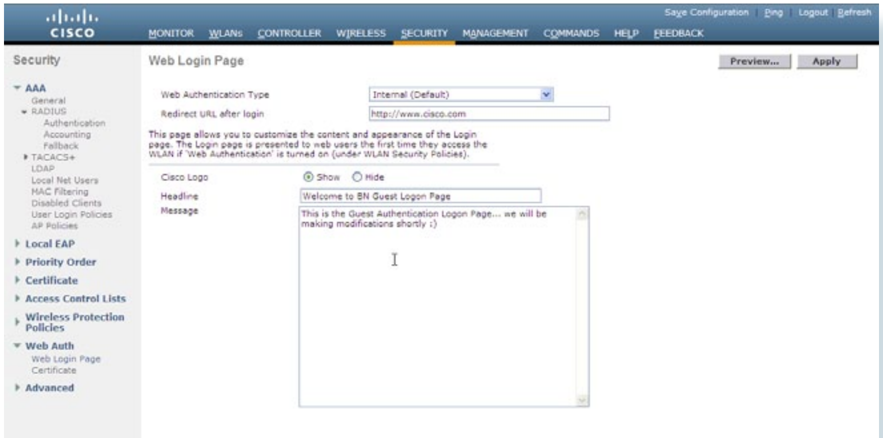
Procedure 19 Guest Wireless LAN Controller Login Page

When your agency guests log in, the first thing they will see is the guest login page. This login page is created using the following steps.

Step 1: Select **Security>Web Auth>Web Login Page**

Step 2: Modify the Web Login Page to reflect what you would like your guest users to view as they attempt to supply guest access credentials.

Figure 61. Guest Login Page Creation



Web Login Page

Web Authentication Type: Internal (Default)

Redirect URL after login: http://www.cisco.com

This page allows you to customize the content and appearance of the Login page. The Login page is presented to web users the first time they access the WLAN if 'Web Authentication' is turned on (under WLAN Security Policies).

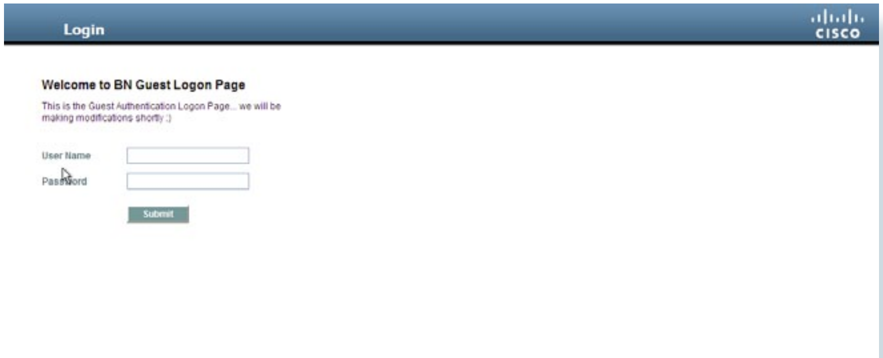
Cisco Logo: ● Show ○ Hide

Headline: Welcome to BN Guest Logon Page

Message: This is the Guest Authentication Logon Page... we will be making modifications shortly :)

By clicking the **Preview** button, you can view what they will see.

Figure 62. Guest Login Page



Welcome to BN Guest Logon Page

This is the Guest Authentication Logon Page... we will be making modifications shortly :)

Step 3: Click **Apply.**

Procedure 20 Create the Lobby Admin User Account

The Lobby Administrator will be the first person to interact with your agency guests. Traditionally it has been the lobby administrator/greeter that performs this function. The lobby administrator can create individual guest user accounts and passwords that last for one to several days, depending upon the length of stay for each guest.

Step 1: Log in to Guest Anchor Controller.

Step 2: Select **Management > Local Management Users.**

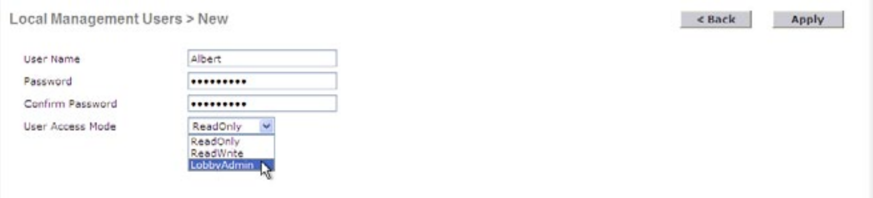
Step 3: Click **New...**

Step 4: Create a username, such as Albert.

Step 5: Create a password.

Step 6: From the drop-down list select **LobbyAdmin.**

Figure 63. Create Lobby Administrator Account



Local Management Users > New

User Name: Albert

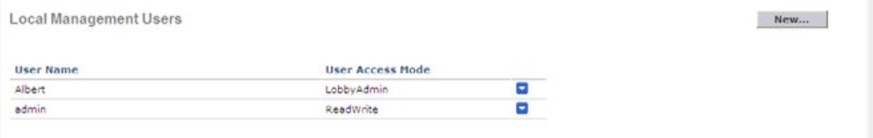
Password: •••••••••

Confirm Password: •••••••••

User Access Mode: ReadOnly

Step 7: Click **Apply.**

Figure 64. All Local Users on Guest WLC



Local Management Users

User Name	User Access Mode
Albert	LobbyAdmin
admin	ReadWrite

Remote Site Wireless

Each remote site will have a site-specific Data and Voice WLAN that will be the same as the WLANs we configured for the primary site, but with one fundamental difference.

At the headquarters, the wireless users traffic is transported over CAPWAP using the wired data VLAN to the WLC where it is then switched out over the link aggregation group (LAG) ports, which is an 802.1Q trunking port channel into the resilient core as illustrated at the beginning of this module. If wireless traffic at the remote sites worked the same way, then the traffic between two devices within the remote site would then be transported via CAPWAP over the WAN to the companies WLC where it would be trunked into the core, to be routed back across the WAN to its destination. This traffic routing is problematic for Unified Communications because as a wireless IP phone making a call out of the remote site gateway would traverse the WAN twice, when it reality, it did not need to leave the remote site at all. To resolve this, the Voice and Data WLAN will be locally switched while the guest WLAN would still be centrally switched: only the management, control and guest traffic will be transported via CAPWAP to the WLC at the primary site. This mode of operation is enabled by switching the AP from local mode to H-REAP mode from the **Wireless** > **AP** menu.

Another benefit of H-REAP is that the AP can operate autonomously should it lose contact with the WLC due to a WAN outage, for example. This ability to operate autonomously, however, would require additional configuration as the wireless authentication is carried out using services located across the WAN at the primary site and is outside the scope of this deployment guide.

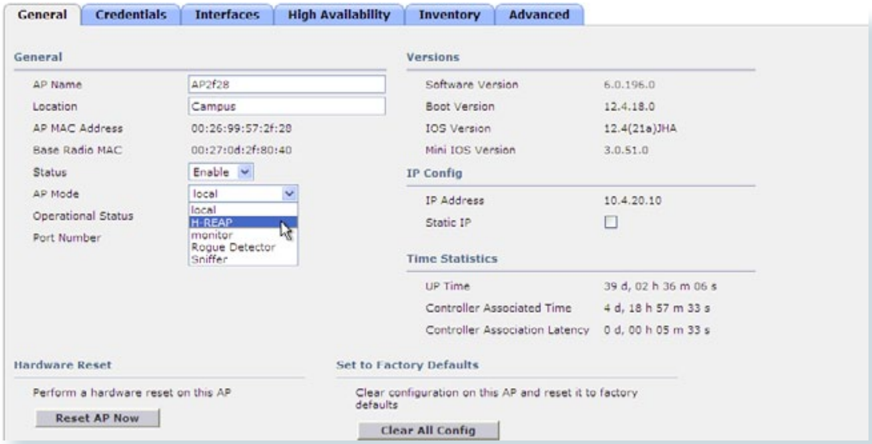
Procedure 21 Provisioning the Remote Site Access-Points

Cisco recommends, but does not require that you pre-provision your remote site access points before deployment. Pre-provisioning gives you a greater opportunity for success and should any issues arise, troubleshooting these issues will be easier.

When your remote site Access Points are connected to your network and you have an IP address and the ability to resolve it for the cisco-lwapp-controller, then the access points can join the primary controller.

Step 1: Select each remote site AP and change the mode as indicated in the Figure 65.

Figure 65. Change Access Point Operating Mode



General

AP Name	AP2f28
Location	Campus
AP MAC Address	00:26:99:57:2f:28
Base Radio MAC	00:27:0d:2f:80:40
Status	Enable
AP Mode	local
Operational Status	
Port Number	

AP Mode: local, H-REAP, monitor, Rogue Detector, Sniffer

Versions

Software Version	6.0.196.0
Boot Version	12.4.18.0
IOS Version	12.4(21a)JHA
Mini IOS Version	3.0.51.0

IP Config

IP Address	10.4.20.10
Static IP	□

Time Statistics

UP Time	39 d, 02 h 36 m 06 s
Controller Associated Time	4 d, 18 h 57 m 33 s
Controller Association Latency	0 d, 00 h 05 m 33 s

Hardware Reset

Perform a hardware reset on this AP

Set to Factory Defaults

Clear configuration on this AP and reset it to factory defaults

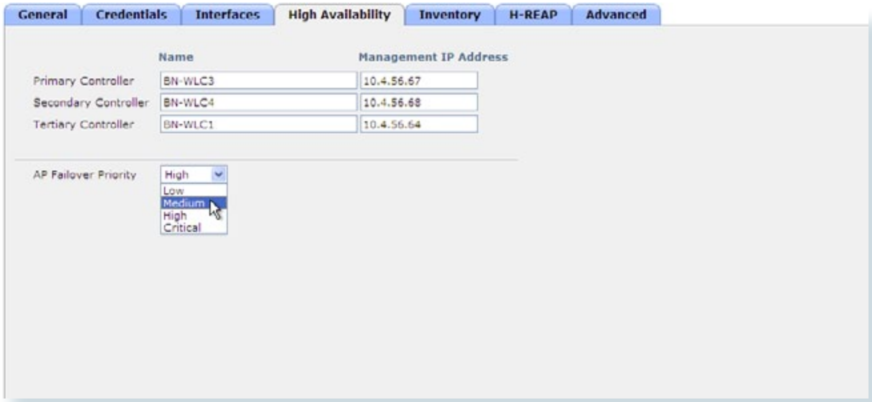
Step 2: Click Apply and the AP will reset and after registering with the WLC, will have an additional H-REAP tab.

Step 3: From Wireless Select the new remote site AP.

Step 4: Select the High Availibility Tab.

Step 5: Enter the primary and secondary controller name and IP addresses.

Figure 66. Configure Remote Site AP High Availability



	Name	Management IP Address
Primary Controller	BN-WLC3	10.4.56.67
Secondary Controller	BN-WLC4	10.4.56.68
Tertiary Controller	BN-WLC1	10.4.56.64

AP Failover Priority: High

Low, Medium, High, Critical

Step 6: Repeat Steps 1 through 5 for each remote site AP.

Procedure 22 Map Voice and Data on Each AP

The switch interface that is connected to the AP should be a trunking interface with the the native VLAN mapped to the access VLAN so that the AP can receive a DHCP address and route traffic through to the primary site WLC.

Step 1: In interface configuration mode on the remote site switch, enter the following commands:

```
interface GigabitEthernet0/23
  description Remote Site H-REAP Access Point
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 64
  switchport trunk allowed vlan 64,65,70
  switchport mode trunk
  spanning-tree portfast trunk
```

Tech Tip

All remote sites use the same VLAN configuration as it is independent of all other configurations; however, different IP broadcast domains exist to maintain proper routing. The VLAN configuration applies to every remote site in this design, which simplifies these configuration tasks.

Step 2: Connect a pre-configured remote site Access Point and allow it to re-register to the primary Controller as configured earlier.

Step 3: Select the remote site AP.

Step 4: Select the **H-REAP** tab.

Step 5: Check the box for **VLAN Support** and click **Apply**.

Step 6: Select the same AP again.

Step 7: Select the **H-REAP** Tab.

Step 8: Enter 64 for the Native VLAN ID value.

Step 9: Click the VLAN Mapping box.

Step 10: Enter VLAN 65 for Data and VLAN 70.

Step 11: Click **Apply.**

Step 12: Repeat for each remote site AP.

Tech Tip

You cannot assign the guest WLAN because it was not originally set up as a locally switched WLAN.

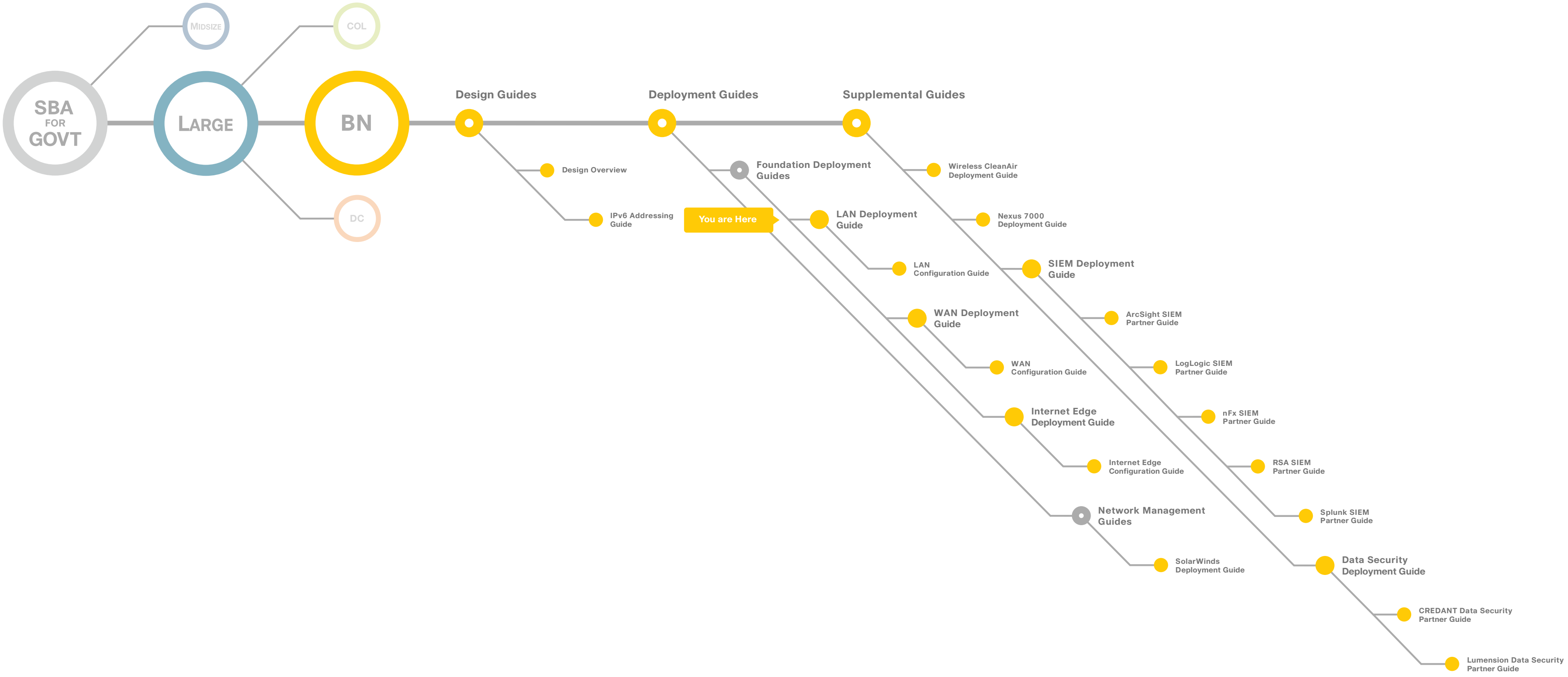
Guest wireless configuration is complete.

Appendix A:
Large Agencies LAN Deployment Product List

Functional Area	Product	Part Numbers	Software Version
Access Layer for PC, phones, APs, other devices	Catalyst 2960S Stackable Ethernet 10/100/1000 port with PoE+ and Stack Module	WS-C2960S-24PD-L Catalyst 2960S 24 GigE PoE+, 2 x 10G SFP+ LAN Base WS-C2960S-48FPD-L Catalyst 2960S 48 GigE PoE +, 2 x 10G SFP+ LAN Base WS-C2960S-24PS-L Catalyst 2960S 24 GigE PoE+, 4 x SFP LAN Base WS-C2960S-48FPS-L Catalyst 2960S 48 GigE PoE+, 4 x SFP LAN Base C2960S-STACK= Catalyst 2960S Flexstack Stack Module	12.2-53.SE2
Access Layer for PC, phones, APs, other devices	Catalyst 3560X Ethernet 10/100/1000 ports with PoE+ and Uplink Module	WS-C3560X-24P-S Catalyst 3750 24 10/100/1000T PoE + and IPB Image WS-C3560X-48PF-S Catalyst 3750 48 10/100/1000T Full PoE + and IPB Image C3KX-NM-1G Catalyst 3750X 1Gig SFP Uplink Module C3KX-NM-10G Catalyst 3750X 10Gig SFP+ Uplink Module	12.2-53.SE2
Access Layer for PC, phones, APs, other devices	Catalyst 3750X Stackable Ethernet 10/100/1000 ports with PoE+ and Uplink Module	WS-C3750X-24P-S Catalyst 3750 24 10/100/1000T PoE + and IPB Image WS-C3750X-48PF-S Catalyst 3750 48 10/100/1000T Full PoE + and IPB Image C3KX-NM-1G Catalyst 3750X 1Gig SFP Uplink Module C3KX-NM-10G Catalyst 3750X 10Gig SFP+ Uplink Module	12.2-53.SE2

Functional Area	Product	Part Numbers	Software Version
Access Layer for PC, phones, APs, other devices	Catalyst 4507RE Dual Supervisors Dual Power Supplies	WS-C4507R-E Catalyst 4500 E-Series 7-Slot Chassis WS-X45-SUP6L-E Catalyst 4500 E-Series Sup 6L-E, 2x10GE(X2) with Twin Gig WS-X4648-RJ45V+E 4500 E-Series 48-Port PoE+ Ready 10/100/1000(RJ45)	12.2-53.SG1
Distribution Layer	Catalyst 3750G Stackable 12 Port SFP	WS-C3750G-12S-S Catalyst 3750 12 SFP + IPS Image	12.2-53.SE1
Distribution Layer	Catalyst 4507RE Dual Supervisors Dual Power Supplies	WS-C4507R-E Catalyst 4500 E-Series 7-Slot Chassis WS-X45-SUP6-E Catalyst 4500 E-Series Sup 6-E, 2x10GE(X2) with Twin Gig WS-X4624-SFP-E Catalyst 4500 E-Series 24-Port GE (SFP) WS-X4606-X2-E Catalyst 4500 E-Series 6-Port 10GbE (X2)	12.2-53.SG1
Distribution Layer	Catalyst 6500 VSS	WS-C6506-E Catalyst 6500 E-Series 6-Slot Chassis VS-S720-10G-3C Catalyst 6500 VSS Supervisor 720 with 2 ports 10GbE WS-X6724-SFP Catalyst 6500 24-port GigE Mod (SFP) WS-X6716-10G-3C Catalyst 6500 16 port 10 Gigabit Ethernet w/ DFC3C (X2)	12.2(33) SXI3 with the IP Services Feature Set
Core Layer	Catalyst 6500	WS-C6506-E Catalyst 6500 E-Series 6-Slot Chassis VS-S720-10G-3C Catalyst 6500 VSS Supervisor 720 with 2 ports 10GbE WS-X6724-SFP Catalyst 6500 24-port GigE Mod (SFP) WS-X6716-10G-3C Catalyst 6500 16 port 10 Gigabit Ethernet w/ DFC3C (X2)	12.2(33) SXI3 with the IP Services Feature Set
Wireless LAN	5508 Wireless LAN Controller	AIR-CT5508-100-K9 5508 Wireless LAN Controller with 100 AP license	6.0.196.0
Wireless LAN	1142 Wireless AP	AIR-LAP1142N-A-K9 802.11a/g/n Fixed Unified AP	6.0.196.0

Appendix B: SBA for Large Agencies Document System


SBA FOR GOVT
MIDSIZE
LARGE
COL
BN
DC
Design Guides
Deployment Guides
Supplemental Guides
Design Overview
IPv6 Addressing Guide
You are Here
Foundation Deployment Guides
LAN Deployment Guide
LAN Configuration Guide
WAN Deployment Guide
WAN Configuration Guide
Internet Edge Deployment Guide
Internet Edge Configuration Guide
Network Management Guides
SolarWinds Deployment Guide
Wireless CleanAir Deployment Guide
Nexus 7000 Deployment Guide
SIEM Deployment Guide
ArcSight SIEM Partner Guide
LogLogic SIEM Partner Guide
nFx SIEM Partner Guide
RSA SIEM Partner Guide
Splunk SIEM Partner Guide
Data Security Deployment Guide
CREDANT Data Security Partner Guide
Lumension Data Security Partner 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.**

C07-641088-00 12/10