CHAPTER 4

Medium Enterprise Design Profile (MEDP)—Mobility Design

Mobility Design

The Cisco Medium Enterprise Design Profile is intended to assist enterprises in the design and deployment of advanced network-based solutions within twenty-first century business environments.

At the heart of the Medium Enterprise Design Profile is the network service fabric, which is a collection of products, features, and technologies that provide a robust routing and switching foundation upon which all solutions and services are built. Operating on top of the network service fabric are all the services used within the medium enterprise network to solve business problems.

Today's enterprise worker is dynamic, mobile, and technology-savvy. When at the enterprise site, they move about while equipped with an array of mobility-enabled devices including PDAs, phones, and laptops. Business professionals tend to use state of the art applications and the enterprise network for many aspects of their lives, demanding connectivity, performance and network flexibility wherever they may be located. This connected generation of professionals is untethered from wired networks and typically assume that high-performance, reliable wireless LANs (WLANs) are present at all medium enterprise environments.

The mobility design implemented by a medium enterprise must meet the needs of these mobile workers while also addressing the requirements of guests and visitors. The challenge facing a medium enterprise is to create a robust, end-to-end, mobility-enabled network that supports their requirements at a cost that makes good business sense. Medium enterprises should be equipped with mobility solutions that support the following:

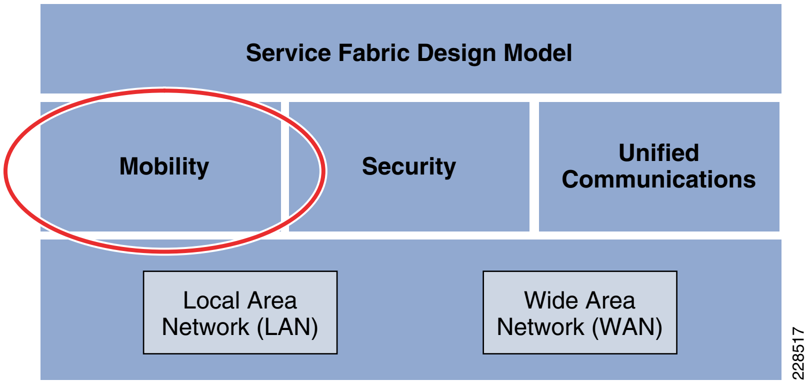
- Secure communications between local and remote sites to support employees, guests and visitors, using mobility-enabled devices and mobile applications
- A scalable design model that can easily accommodate the addition of new local and remote buildings as well as modifications to existing buildings
- Support for bandwidth-intensive, high-speed multimedia applications
- Simplified management tools to facilitate system-wide mobility maintenance
- The use of tools and applications for mobile conferencing, collaboration, and operations
- Effective communication and inter operation with public safety first responders in the event of an emergency.

Medium enterprises must remain competitive and must differentiate themselves from their peers, both for competitive customer marketing purposes as well as to attract and retain the best employee talent. Prospective employees want to be part of medium enterprises that provide services relevant to the way they live, work, and spend their free time. They want to take full advantage of what the medium enterprise has to offer, in ways that serve to enhance both their quality of life and their individual success potential. A medium enterprise with a pervasive, high-speed wireless network not only provides technological leadership and innovation, but enables the deployment of innovative applications that streamline operations, enhance collaboration, and improve productivity.

This mobile enterprise lifestyle helps to drive the need for careful wireless capacity and coverage planning. Keep in mind that traditional offices and conference rooms are by no means the only environments seen within medium enterprises any longer. In fact, high performance, secure wireless technologies can enable “virtual offices” even in non-traditional settings such as leased space in professional buildings, temporary office spaces, and even in employee homes. Administrators need secure access to tools, records, and resources, as well as access to mobile voice capabilities throughout medium enterprise sites. Secure, reliable, and high-performance wireless guest access for contractors, vendors, and other guests of the medium enterprise has become a standard and expected part of modern-day mobile business environments.

To meet these needs, medium enterprises must evolve into mobility-enabled local and remote sites and twenty-first century business centers. In support of this, this chapter discusses design considerations surrounding the requirements, expectations and trade-offs that must be taken into account when integrating mobility into the Cisco Medium Enterprise Design Profile. These design considerations form a critical part of the overall service fabric design model, as shown in Figure 4-1.

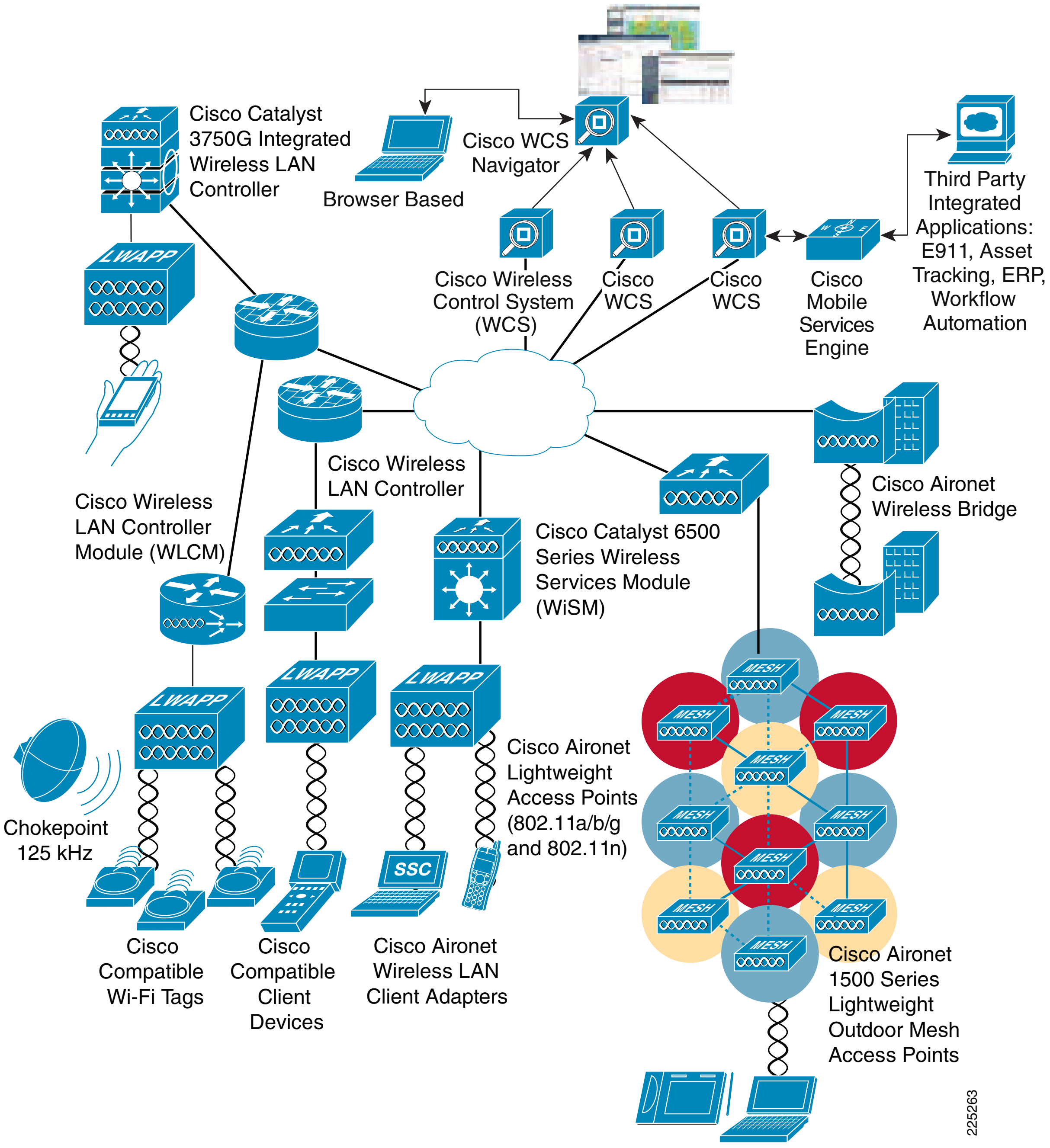
Figure 4-1 Service Fabric Design Model



Given the mobility requirements of medium enterprise professionals, guests, and visitors, wireless LANs have emerged as one of the most effective and high performance means for these mobile users to access the medium enterprise network. The Cisco Unified Wireless Network (Cisco UWN) is a unified solution that addresses the wireless network security, deployment, management, and control aspects of deploying a wireless network. It combines the best elements of wireless and wired networking to deliver secure, scalable wireless networks with a low total cost of ownership.

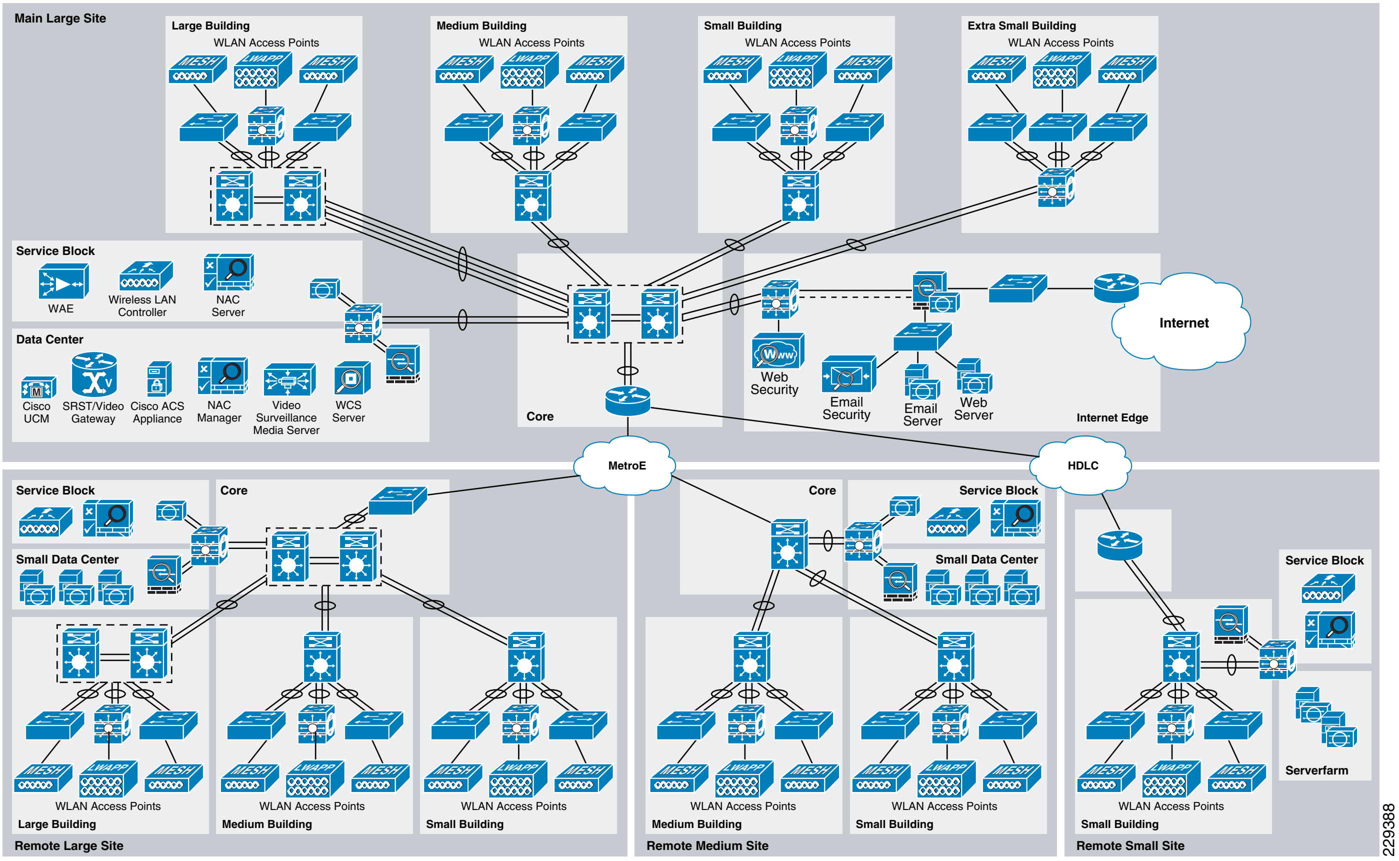
Figure 4-2 shows a high-level topology of the Cisco Unified Network, which includes access points that use the Control and Provisioning of Lightweight Access Points (CAPWAP) protocol, the Cisco Wireless Control System (WCS), and the Cisco Wireless LAN Controller (WLC). In addition to the traditional standalone WLAN controller, alternate hardware platforms include the Cisco ISR router Wireless LAN Controller Module (WLCM) or the Cisco Catalyst 6500 Wireless Services Module (WiSM). The Cisco Access Control Server (ACS) and its Authentication, Authorization, and Accounting (AAA) features complete the solution by providing Remote Authentication Dial-In User Service (RADIUS) services in support of user authentication and authorization.

Figure 4-2 Cisco Unified Wireless Network Overview


Cisco Catalyst 3750G Integrated Wireless LAN Controller
Browser Based
Cisco WCS Navigator
Third Party Integrated Applications: E911, Asset Tracking, ERP, Workflow Automation
Cisco Wireless Control System (WCS)
Cisco WCS
Cisco WCS
Cisco Mobile Services Engine
LWAPP
Cisco Wireless LAN Controller
Cisco Wireless LAN Controller Module (WLCM)
Cisco Aironet Wireless Bridge
Cisco Catalyst 6500 Series Wireless Services Module (WiSM)
LWAPP
LWAPP
LWAPP
MESH
Chokepoint 125 kHz
Cisco Aironet Lightweight Access Points (802.11a/b/g and 802.11n)
SSC
Cisco Compatible Wi-Fi Tags
Cisco Compatible Client Devices
Cisco Aironet Wireless LAN Client Adapters
Cisco Aironet 1500 Series Lightweight Outdoor Mesh Access Points
225263

The Cisco Medium Enterprise Design Profile accommodates a main site and one or more remote sites interconnected over a metro Ethernet or managed WAN service. Each of these sites may contain one or more buildings of various sizes, as shown in Figure 4-3.

Figure 4-3 Medium Enterprise Design Profile Overview



Operating on top of this network are all the services used within the medium enterprise environment such as safety and security systems, voice communications, video surveillance equipment, and so on. The core of these services are deployed and managed at the main (or headquarters) site building, allowing each remote site to reduce the need for separate services to be operated and maintained. These centralized systems and applications are served by a data center at the main site.

As Figure 4-3 shows, the Cisco Medium Enterprise Design Profile uses a centralized approach in which key resources are centrally deployed. The key feature of this integration is the use of one or more WLAN controllers at each site, with the overall WLAN management function (the Cisco WCS) located at the main site. This approach simplifies the deployment and operation of the network, helping to ensure smooth performance, enhance security, enhance network maintainability, maximize network availability, and reduce overall operating costs.

The Cisco Medium Enterprise Design Profile takes into account that cost and limited network administrative resources can, in some cases, be limiting factors for medium enterprises. The topologies and platforms are carefully selected to increase productivity while minimizing the overall cost and complexity of operation. In certain instances, trade-offs are necessary to reach these goals, and this document helps to point out and clarify some of these trade-offs.

The Cisco mobility approach within the Cisco Medium Enterprise Design Profile focuses on the following key areas:

- *Accessibility*

  - Enabling mobile professionals, administrators, guests and visitors to be accessible and productive on the network, regardless of whether they are in a traditional office setting, collaborating in a conference room, having lunch with colleagues within enterprise site dining areas, or simply enjoying a breath of fresh air outside on-site buildings
  - Enabling easy, secure guest access to guests such as prospective customers, future employees, contractors, vendors, and other visitors.
- *Usability*

  In addition to extremely high WLAN transmission speeds made possible by the current generation of IEEE 802.11n technology, latency-sensitive applications (such as IP telephony and video conferencing) are supported over the WLAN using appropriately applied quality-of-service (QoS) classification. This gives preferential treatment to real-time traffic, helping to ensure that video and audio information arrives on time.
- *Security*
  - Segmenting authorized users and blocking unauthorized users
  - Extending the services of the network safely to authorized parties
  - Enforcing security policy compliance on all devices seeking to access network computing resources. Staff enjoy rapid and reliable authentication through IEEE 802.1x and Extensible Authentication Protocol (EAP), with all information sent and received on the WLAN being encrypted.

Note For information on how security design is addressed within the Cisco Medium Enterprise Design Profile, see Chapter 5, "Medium Enterprise Design Profile (MEDP)—Network Security Design."

- *Manageability*

  A relatively small team of network administrators should be able to easily deploy, operate, and manage hundreds of access points that may reside within a multisite medium enterprise. A single, easy-to-understand WLAN management framework provides small, medium, and large sites with the level of WLAN management scalability, reliability, and ease of deployment required in the medium enterprise domain.
- *Reliability*
  - Providing adequate capability to recover from a single-layer fault of a WLAN access component or controller wired link.
  - Ensuring that WLAN accessibility is maintained for employees, administrators, staff, guests, and visitors, in the event of common failures.

Accessibility

This section provides a brief introduction to the fundamental protocol used for communication between access points and WLAN controllers, followed by a discussion of mobility design considerations pertaining to those aspects of the Cisco Medium Enterprise Design Profile relevant to accessibility, such as the following:

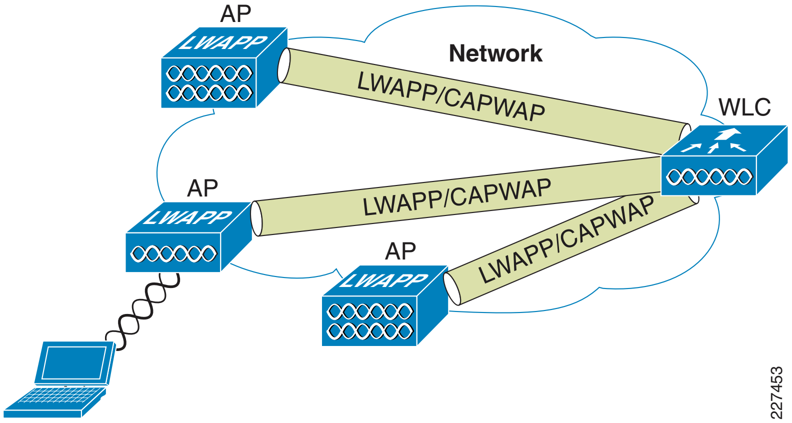
- WLAN controller location
- WLAN controller connectivity

- Access points

The basic mobility components involved with providing WLAN access in the Cisco Medium Enterprise Design Profile consists of WLAN controllers and access points that communicate with each other using the IETF standard CAPWAP protocol. In this arrangement, access points provide the radio connection to wireless clients, and WLAN controllers manage the access points and provide connectivity to the wired network.

Figure 4-4 shows the use of CAPWAP by access points to communicate with and tunnel traffic to a WLAN controller.

Figure 4-4 CAPWAP Access Point to WLC Communication



CAPWAP enables the controller to manage a collection of wireless access points, and has the following three primary functions in the mobility design:

- Control and management of the access point
- Tunneling of WLAN client traffic to the WLAN controller
- Collection of 802.11 data for overall WLAN system management

CAPWAP is also intended to provide WLAN controllers with a standardized mechanism with which to manage radio-frequency ID (RFID) readers and similar devices, as well as enable controllers to interoperate with third-party access points in the future.

In controller software Release 5.2 or later, Cisco lightweight access points use CAPWAP to communicate between the controller and other lightweight access points on the network. Controller software releases before Release 5.2 use the Lightweight Access Point Protocol (LWAPP) for these communications. Note that most CAPWAP-enabled access points are also compatible with the preceding LWAPP protocol. An exception is that the Cisco Aironet 1140 Series Access Point supports only CAPWAP.

The mobility approach in the Cisco Medium Enterprise Design Profile is based on the feature set available in Cisco Wireless LAN Controller software Release 6.0, which uses CAPWAP.

For detailed CAPWAP protocol information, see the following URL: http://www.ietf.org/rfc/rfc5415.txt.

WLAN Controller Location

WLAN deployments are typically categorized into two main categories, *distributed* and *centralized*:

- *Distributed controller*—In this model, WLAN controllers are located throughout the medium enterprise network, typically on a per-building basis, and are responsible for managing the access points resident in a given building. This technique is commonly used to connect controllers to the medium enterprise network using distribution routers located within each building. In the distributed deployment model, the CAPWAP tunnels formed between access points and WLAN controllers are typically fully contained within the confines of the building.
- *Centralized controller*—In this model, WLAN controllers are placed at a centralized location within the enterprise. Because centralized WLAN controllers are typically not located in the same building as the access points they manage, the CAPWAP tunnels formed between them must traverse the site backbone network.

The Cisco Medium Enterprise Design Profile is based on the centralization of WLAN controllers, on a per-site basis, and follows established best practices, such as those contained in Chapter 2 of the *Enterprise Mobility 4.1 Design Guide* at the following URL: http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns820/landing_ent_mob_design.html.

Figure 4-3 shows the planned deployment of WLAN controllers within distinct per-site service blocks, each associated with the main (headquarters), large remote, medium remote, and small remote sites respectively. Service blocks tend to be deployed at locations in the network where high availability routing, switching, and power is present. In addition, these areas tend to be locally or remotely managed by network staff possessing higher skill sets.

Some of the advantages underlying the decision to centralize the deployment of WLAN controllers on a per-site basis include the following:

- *Reduced acquisition and maintenance costs*—By servicing the needs of all wireless users from a central point, the number of WLAN controller hardware platforms deployed can be reduced compared to that required for a distributed, per-building design. Similarly, incremental software licensing costs associated with WLAN controllers are reduced as well. These economies of scale typically increase with the size of the enterprise WLAN.
- *Reduced administrative requirements*—By minimizing the total number of WLAN controllers deployed, the controller management burden imposed on site network administrators is minimized.
- *Cost-effective capacity management*—The use of a centralized WLAN controller model allows the designer the ability to centrally service access points located in multiple building locations and efficiently manage controller capacity.
- *Simplified network management and high availability*—Centralized WLAN controller designs simplify overall network management of controllers, as well as facilitate cost-effective controller high availability approaches. This can protect sites from a loss of WLAN access in the rare event of a controller failure, without the expense of 1:1 controller duplication.
- *Reduced component interaction points*—Centralizing WLAN controllers minimizes the number of integration points that must be managed when interfacing the controller with other devices. When integrating the WLAN controller with the Network Admission Control (NAC) appliance on any given site, for example, only one integration point must be administered.
- *Increased performance and reliability*—Centralized WLAN controller deployments usually lead to highly efficient inter-controller mobility. For large sites, there is also an incremental economy of scale that occurs as the network grows larger. By centralizing WLAN controllers on a per-site basis, CAPWAP tunneling between access points and WLAN controllers is not normally required to traverse WAN links (except during controller fail over), thereby conserving WAN bandwidth and improving performance overall.

Note For additional information on inter-controller mobility and roaming, see the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/ch2_Arch.html#wp1028197.

The choice of WLAN controller for the Cisco Medium Enterprise Design Profile is the Cisco 5508 Wireless Controller, as shown in Figure 4-5.

Figure 4-5 Cisco 5508 Wireless Controller

The Cisco 5508 Wireless Controller is a highly scalable and flexible platform that enables system-wide services for mission-critical wireless in medium to large-sized enterprise environments. Designed for 802.11n performance and maximum scalability, the Cisco 5508 Wireless Controller offers the ability to simultaneously manage from 12 to a maximum of 250 access points per controller. Base access point controller licensing provides the flexibility to purchase only the number of access point licenses required, with the ability to add additional access point licenses in the future when medium enterprise site growth occurs. In sites requiring more than 250 total access points, or load sharing/high availability is required, multiple controllers can be deployed as necessary.

More information on the Cisco 5508 Wireless Controller can be found at the following URL: http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps10315/data_sheet_c78-521631.html.

WLAN Controller Connectivity

This section discusses WLAN controller connectivity, including the following:

- Controller connectivity to the wired network
- Controller connectivity to the wireless devices
- Defining WLANs and Service Set Identifiers (SSIDs)
- WLAN controller mobility groups
- WLAN controller access point groups
- WLAN controller RF groups

Controller Connectivity to the Wired Network

WLAN controllers possess physical entities known as *ports* that connect the controller to its neighboring switch (the Cisco 5508 Wireless Controller supports up to eight Gigabit Ethernet Small Form-Factor Pluggable [SFP] ports). Each physical port on the controller supports, by default, an 802.1Q VLAN trunk, with fixed trunking characteristics.

Note For more information concerning the various types of ports present on Cisco WLAN controllers, see the *Cisco Wireless LAN Controller Configuration Guide, Release 6.0* at the following URL: http://www.cisco.com/en/US/docs/wireless/controller/6.0/configuration/guide/Controller60CG.html.

Interfaces are logical entities found on the controller. An interface may have multiple parameters associated with it, including an IP address, default gateway, primary physical port, optional secondary physical port, VLAN identifier, and Dynamic Host Configuration Protocol (DHCP) server. Each interface is mapped to at least one primary port, and multiple interfaces can be mapped to a single controller port.

Note For more information concerning the various types of interfaces present on Cisco WLAN controllers, see the *Cisco Wireless LAN Controller Configuration Guide, Release 6.0* at the following URL: http://www.cisco.com/en/US/docs/wireless/controller/6.0/configuration/guide/Controller60CG.html.

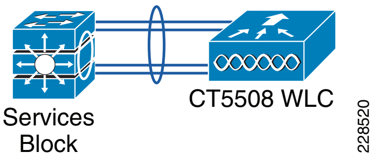
A special type of controller interface is known as the *AP manager interface*. A controller has one or more AP manager interfaces, which are used for all Layer 3 communications between the controller and its joined access points. The IP address of the AP manager interface is used as the tunnel source for CAPWAP packets from the controller to the access point, and as the destination for CAPWAP packets from the access point to the controller. The AP manager interface communicates through a distribution system port by listening across the Layer 3 network for CAPWAP "join" messages generated by access points seeking to communicate with and "join" the controller.

Link aggregation (LAG) is a partial implementation of the 802.3ad port aggregation standard. It bundles all of the controller distribution system ports into a single 802.3ad port channel, thereby reducing the number of IP addresses needed to configure the ports on your controller. When LAG is enabled, the system dynamically manages port redundancy and load balances traffic transparently to the user. LAG bundles all the enabled distribution ports on the WLAN controller into a single EtherChannel interface.

Currently published best practices specify either multiple AP manager interfaces (with individual Ethernet links to one or more switches) or link aggregation (with all links destined for the same switch or switch stack) as the recommended methods of interconnecting WLAN controllers with wired network infrastructure. For more information, see the following URL: http://www.cisco.com/en/US/docs/wireless/controller/6.0/configuration/guide/c60mint.html#wp1277659.

In the Cisco Medium Enterprise Design Profile, the Cisco 5508 Wireless Controllers are interconnected with the modular switches or switch stacks found in the services block using link aggregation and EtherChannel exclusively, as shown in Figure 4-6.

Figure 4-6 WLAN Controller Link Aggregation to Services Block



In this way, one or more centralized WLAN controllers are connected via the services block to the site core. This design can make use of up to eight Gigabit Ethernet connections from the Cisco 5508 Wireless Controller to the services block. These Gigabit Ethernet connections should be distributed among different modular line cards or switch stack members as much as possible, so as to ensure that the failure of a single line card or switch stack failure does not result in total failure of the

WLAN controller connection to the site network. The switch features required to implement this connectivity between the WLAN controller and the services block are the same switch features that would otherwise be used for EtherChannel connectivity between switches in general.

Further discussion of the advantages of using controller link aggregation, as well as the considerations concerning its implementation in the Cisco Medium Enterprise Design Profile can be found in Controller Link Aggregation, page 4-35.

The key advantage of using link aggregation in this fashion instead of multiple AP manager interfaces is design performance, reliability, and simplicity:

- With the Ethernet bundle comprising up to eight Gigabit Ethernet links, link aggregation provides very high traffic bandwidth between the controller and the site network.
- With link aggregation, if any of the controller ports fail, traffic is automatically migrated to one of the other controller ports. As long as at least one controller port is functioning, the system continues to operate, access points remain connected to the network, and wireless clients continue to send and receive data. Terminating on different modules within a single Catalyst modular switch, or different switch stack members (as shown in Figure 4-6), provides redundancy and ensures that connectivity between the services block switch and the controller is maintained in the rare event of a failure.
- Link aggregation also offers simplicity in controller configuration; for example, configuring primary and secondary ports for each interface is not required.

Controller Connectivity to Wireless Devices

This section deals with the design considerations that involve provisioning wireless access for the various user groups that reside within the medium enterprise, such as the administrators, employees, and guests. These considerations include the WLAN controllers deployed in the services blocks, as well as the access points that are located in buildings.

Defining WLANs and SSIDs

In most medium enterprises, various user groups will likely require access to the WLAN for a variety of different purposes. Although usage peaks may occur, it is safe to assume that a large portion of these groups will likely want access to the WLAN at more or less the same time. Thus, in designing for mobility in the Cisco Medium Enterprise Design Profile, the wireless infrastructure must support logical segmentation in such a fashion that a reasonable proportion of all users can be serviced simultaneously and with an appropriate degree of security and performance.

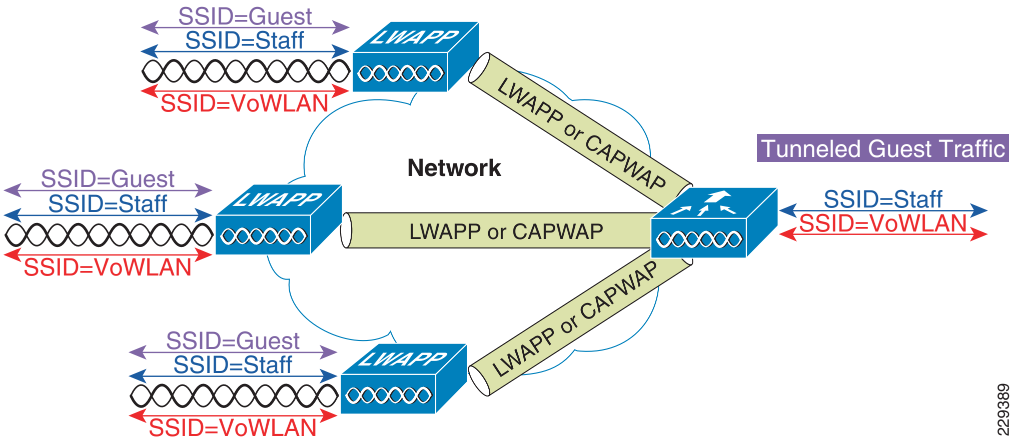
One of the basic building blocks used in the WLAN controller to address this need is the ability to provision logical WLANs, each of which are mapped to different wired network interfaces by the WLAN controller. These WLANs are configured and assigned a unique SSID, which is a sequence of characters that uniquely names a WLAN. For this reason, an SSID is also sometimes referred to simply as a *network name*.

Note Each set of wireless devices communicating directly with each other is called a basic service set (BSS). Several BSSs can be joined together to form one logical WLAN segment, referred to as an extended service set (ESS). An SSID is simply the 1–32 byte alphanumeric name given to each ESS.

To promote ease of administration, the value chosen for the SSID should bear some direct relationship to the intended purpose of the WLAN.

Figure 4-7 provides a high-level illustration of the three logical WLANs that provide mobility within the Cisco Medium Enterprise Design Profile, and how they are mapped to WLAN controller network interfaces or tunneled to another controller. For ease of administration and the support of employees, administrators, guests and visitors that frequent multiple sites, the names chosen for the WLAN SSIDs should be consistent within each site in the medium enterprise system. For example, in Figure 5-7 employee wireless access is made available anywhere there is WLAN RF coverage using the SSID titled "staff".

Figure 4-7 WLAN SSIDs



In the Medium Enterprise Design Profile, the set of WLAN SSIDs provide access to the following WLANs:

- A *secured staff* WLAN network with dynamically generated per-user, per-session encryption keys.

  This WLAN would be used by enterprise employees, administrators and other staff members using managed client devices, such as laptops, PDAs, and so on. The secured staff WLAN is designed to provide secure access and good performance for devices supported by the medium enterprise network administration staff. Devices that are used on the secured staff WLAN are usually procured and deployed by (or with the knowledge and cooperation of) the medium enterprise network administration staff on behalf of full-time and temporary employees. These employees are typically prohibited from bringing their own personal PDAs, laptops, or voice over WLAN (VoWLAN) phones to use on the secured staff WLAN. This allows, for example, a uniform baseline level of authentication and encryption to be deployed for the secured staff WLAN across all such devices. An underlying assumption made here is that only devices supporting compatible authentication and encryption would be considered for deployment at all.

  The characteristics of this WLAN include the following:

  - Wi-Fi Protected Access 2 (WPA2) encryption with 802.1x/EAP authentication, and Cisco Centralized Key Management (Cisco CKM, also referred to as CCKM) for enhanced roaming.

    Most modern WLAN client devices being produced today support this level of authentication and encryption. The addition of Cisco CKM in this case provides for faster roaming by enabling Cisco CKM-equipped clients to securely roam from one access point to another without the need to re-authenticate after the roam completes.

  - Broadcast SSID enabled. Enabling this helps to avoid potential connectivity difficulties with some clients. There is no real disadvantage to enabling broadcast SSID.
  - QoS profile setting of *silver* (best effort delivery).

Note For more details on WLAN QoS, see the references contained at the end of Quality-of-Service, page 4-26.

- Wi-Fi Multimedia (WMM) policy of allowed. This allows devices and applications that can support 802.1e enhanced QoS prioritization to do so. Enabling the use of WMM in this way is also in compliance with the 802.11n.
- Mandatory IP address assignment via DHCP. Eliminating the configuration of static IP addresses helps to mitigate the risk of IP address duplication.
- Radio policy set to allow clients to use either 2.4 GHz or 5 GHz to access this WLAN. This allows clients that can take advantage of benefits of 5 GHz operation (such as increased capacity and reduced interference) to do so.

Note The 802.11b and 802.11g physical layers (PHYs) are applied in the unlicensed 2.4 GHz industrial, scientific, and medical (ISM) frequency band, whereas the 802.11a PHY is applied in the unlicensed 5 GHz ISM band. "Dual-band" 802.11a/bg clients are capable of operating in either 2.4 or 5 GHz frequency bands because they are capable of using any of the three PHYs. Selection between PHYs is typically achieved via software configuration.

Clients using the very high speed 802.11n PHY may be designed to operate in a single band, or they may be 802.11n "dual-band" clients. Unlike the 802.11b, 802.11g, and 802.11a PHYs, simply stating that a client is 802.11n does not precisely indicate what frequency bands the client is capable of operating within.

For more information about the 802.11n PHY and its application to the 2.4 and 5 GHz frequency bands, see the following URL: http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns348/ns767/white_paper_80211n_design_and_deployment_guidelines.html.

- A *secured VoWLAN* network that is optimized for VoWLAN usage by employee staff and administrators using managed VoWLAN client devices.

  As was the case with the secured staff WLAN, this WLAN is designed to provide secure access and good performance when used with VoWLAN devices (such as the Cisco Unified Wireless IP Phone 7925G) that are usually procured, deployed, and managed by (or with the knowledge and cooperation of) the medium enterprise network administration staff. Such procurement is usually conducted on behalf of full-time and temporary employee staff users. To assure proper security and promote effective device management, employee staff users are typically prohibited from bringing their own personal VoWLAN phones and using them on this WLAN. This allows, for example, a baseline level of authentication and encryption to be deployed for this WLAN with the knowledge that the devices using this WLAN will support that level of security. The key differences between this WLAN and the secured staff WLAN include the following:

  - The security policy on this WLAN is WPA with Cisco CKM, which is recommended as a best practice for the Cisco 7921G and 7925G VoWLAN phones.
  - WLAN controller QoS profile setting of *platinum*, which assigns the highest prioritization to voice traffic.
  - WMM policy is *required* (this precludes the use of clients that do not support WMM).

  - Load-based Call Admission Control (CAC) should be specified for this WLAN. This prevents VoWLAN calls from being added to an access point that is unable to accept them without compromising call quality.
  - The radio policy should be set to allow clients to access only this WLAN using 5 GHz. This helps to ensure that all secured voice devices take full advantage of the robust call capacity and reduced co-channel interference characteristics associated with 5 GHz.

  For further information on best practices for voice applications, see the *Voice over Wireless LAN 4.1 Design Guide* at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/vowlan/41dg/vowlan41dg-book.html.

- A *guest access* WLAN that uses web authentication for guest users of the enterprise network.

  Traffic to and from this guest access WLAN is tunneled to the DMZ transparently, with no visibility by, or interaction with, other traffic in the enterprise. The Cisco Medium Enterprise Design Profile uses the Cisco Unified Wireless Network to provide a flexible, easy-to-implement method for deploying wireless guest access by using Ethernet in IP (RFC3378). Ethernet in IP is used to create a tunnel across a Layer 3 topology between two WLAN controller endpoints (known as the *foreign* and *anchor* controllers). The foreign controller is the controller resident in the respective site services block described earlier, whereas the anchor controller is resident within the network DMZ. The benefit of this approach is that no additional protocols or segmentation techniques must be implemented to isolate guest traffic travelling within the tunnel from all other enterprise traffic.

  See Guest Access, page 4-27 for further information regarding considerations surrounding the products and techniques used to provide guest access when designing for mobility in the Cisco Medium Enterprise Design Profile.

  For technical information on Guest Access best practices in wireless networks, see the Guest Access section in the *Enterprise Mobility 4.1 Design Guide* at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/ch10GuAc.html.

  The guest access WLAN must be designed to accommodate the needs of enterprise guests (such as customers, vendors, contractors, prospective employee candidates, and so on) as well as the wide variety of WLAN guest client devices they may bring into the enterprise. Although their numbers will likely be much less compared to that of employees, the WLAN clients brought into the enterprise environment by guest users are typically not managed or directly supported by medium enterprise network administrative staff. Because of the lack of control over the type of device used, mandating the use of 802.1x authentication and WPA or WPA2 encryption does not usually facilitate a practical guest access solution.

  Characteristics of the guest access WLAN include the following:

  - To provide access control and an audit trail, the guest access WLAN authenticates the user via a web portal (web authentication) where all network access, apart from DHCP and Domain Name Service (DNS), is blocked until the user enters a correct user name and password into an authentication web page.
  - The guest access WLAN user is re-directed to a web authentication web page whenever the user attempts to open any web page before successful authentication via the web portal. This authentication web page is provided by an internal WLAN controller web server in the Cisco Medium Enterprise Design Profile. However, there is an option of using a non-controller-based web authentication server, such as the Cisco NAC Appliance. User names and passwords for authentication can reside on a RADIUS AAA server (Cisco ACS).
  - Broadcast SSID is enabled.
  - The guest access WLAN uses a QoS profile setting of *bronze* (less than best effort).
  - WMM policy is set to *allowed*.

- Radio policy should be set such that client access is allowed to use either 2.4 GHz or 5 GHz.

Additional information about the definition of controller WLANs and SSIDs can be found in the *Enterprise Mobility 4.1 Design Guide* at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.html.

WLAN Controller Mobility Groups

A *mobility group* is a group of WLAN controllers that behave as a single virtual WLAN controller, sharing essential end client, access point, and RF information. A given WLAN controller is able to make decisions based on data received from other members of the mobility group, rather than relying solely on the information learned from its own directly connected access points and clients. The WLAN controllers in a mobility group form a mesh of authenticated tunnels between themselves, affording any member controller the ability to efficiently communicate with any other member controller within the group.

Mobility groups are used to help facilitate seamless client roaming between access points that are joined to different WLAN controllers. The primary purpose of a mobility group is to create a virtual WLAN domain (across multiple WLAN controllers) to provide a comprehensive view of a wireless coverage area. Typically, two WLAN controllers should be placed in the same mobility group when an inter-controller roam is possible between access points. If the possibility of a roaming event does not exist, it may not make sense to put the WLAN controllers in the same mobility group.

For example, consider the scenario illustrated in Figure 4-8. Here we see a large and a medium building located within the same medium enterprise site. The buildings are in relatively close proximity to one another, with a small building located on a remote site some distance away from the main site. Assume for the purposes of this example that the access points of each building are joined to a different WLAN controller, with the controllers servicing the large and medium building being located within the main service block at the main site, and the WLAN controller servicing the smaller building located in the remote site. The circular and oval patterns surrounding each building are intended to represent a very simplistic view of hypothetical outdoor RF coverage.

Figure 4-8 Roaming

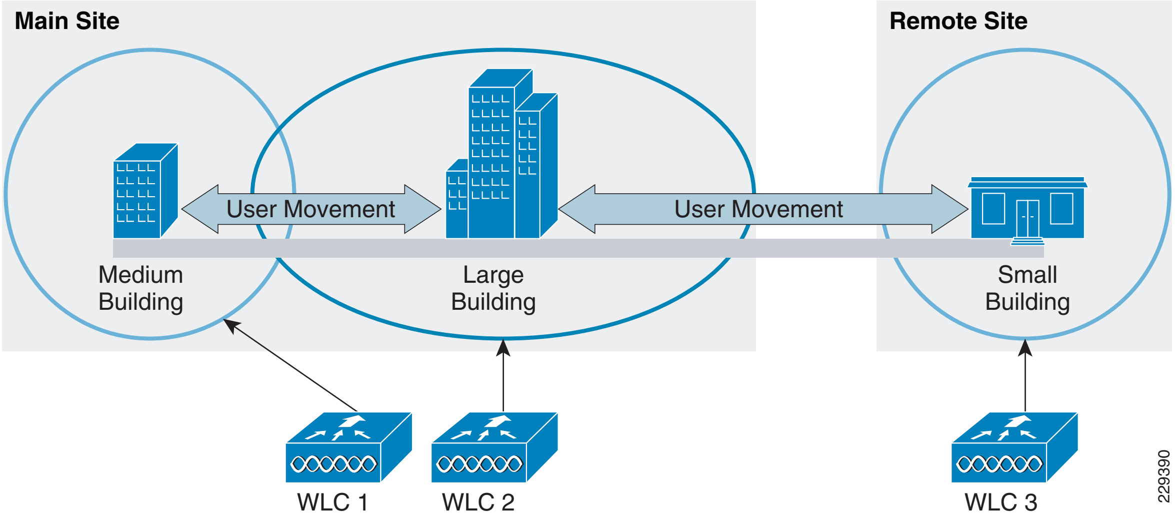


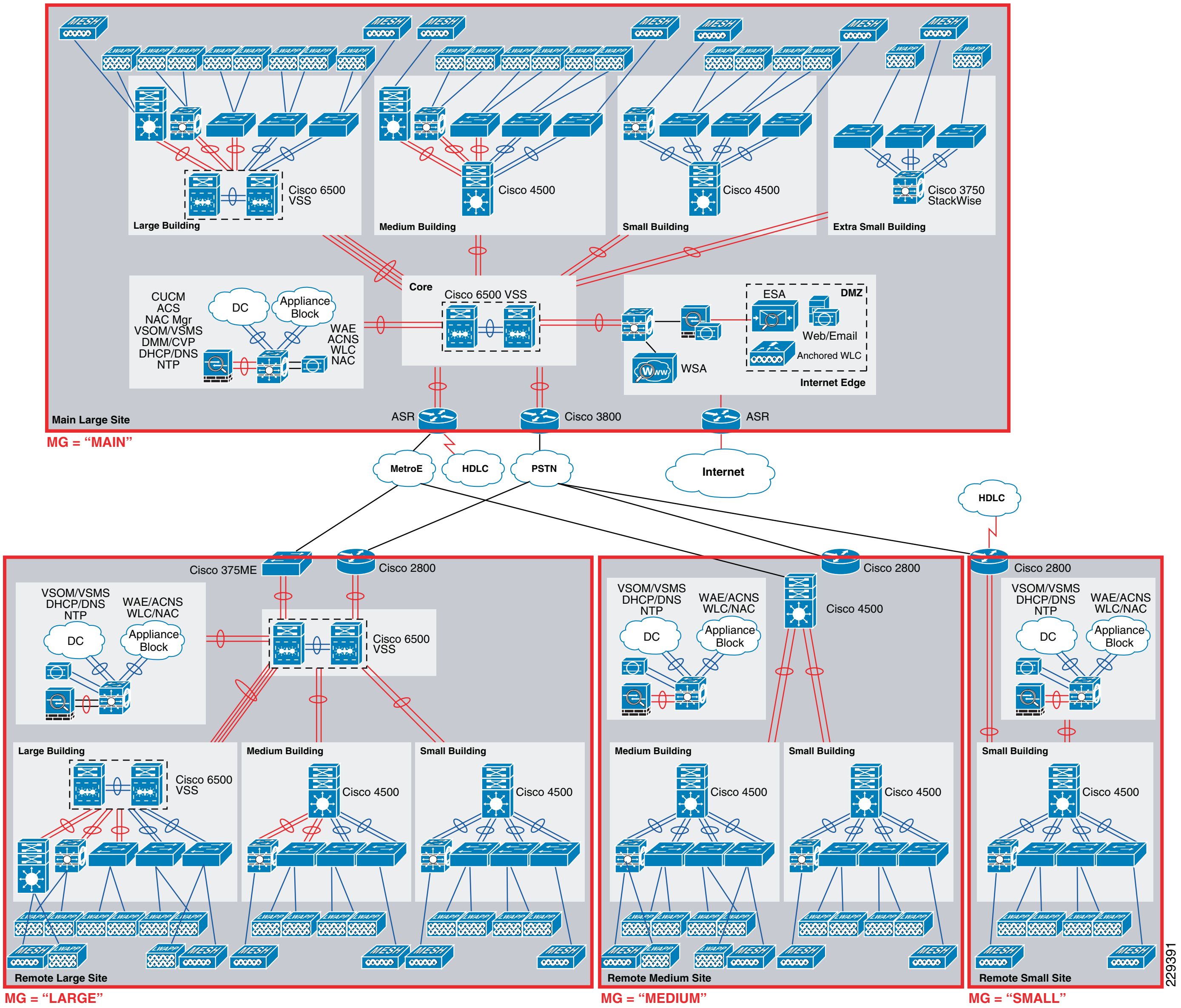
Figure 4-8 shows that there is overlapping RF coverage between the large and medium buildings, but not between the small building and any other building. This is because users must leave the main site and traverse through a part of the town to get to the smaller remote site, and vice versa. Because roaming is clearly possible between the medium and large building, but not between the small building and any other building on any site, only the WLAN controllers servicing the medium and large building are required to be in the same mobility group. The WLAN controller servicing the small building may be configured to be a member of the same mobility group, but it is not mandatory that this be done in this case.

In applying the concept of mobility groups to the Cisco Medium Enterprise Design Profile, consider the following:

- Within a medium enterprise comprised of one or more sites, it is assumed that intra-site roaming is possible between all buildings resident within the same site. Keep in mind that in reality this may not always be the case, as some sites may have collocated buildings with coverage voids between them. However, assuming that intra-site roaming is possible between all buildings allows us to make a design assumption that is generally applicable to both situations. Thus, in our Medium Enterprise Design Profile, all WLAN controllers serving access points deployed on the same site are placed within the same mobility group.
- It is also assumed that in the vast majority of cases, remote sites are sufficiently distant from the main site (as well as from one another) to render inter-site roaming impractical. Allowing of course for the rare exception that two sites may be adjacent to one another, we assume that roaming between buildings located on different sites is very unlikely.

Figure 4-9 provides a high-level illustration of how mobility group assignment can be handled in the Medium Enterprise Design Profile. Note that *MG* refers to the mobility group name assigned for the site.

Figure 4-9 Medium Enterprise Mobility Groups



The following are some of the key design considerations concerning mobility groups:

- The controllers present at each site are defined as members of a mobility group unique to that site. Each controller in the same mobility group is defined as a peer in the mobility list of all controllers for that mobility group.
- If inter-site roaming between multiple sites is possible, the controllers at each sites should be assigned into the same mobility group and defined as peers in the mobility list of all controllers for that mobility group.
- Because of high-speed WAN/MAN connectivity between sites, access point fail over to a remote backup controller resident at the main site becomes possible. To support this, access points can be configured to fail over to a WLAN controller outside of their mobility group. This is discussed further in Controller Redundancy, page 4-38 and AP Controller Failover, page 4-40.

- A single mobility group can contain a maximum of 72 WLAN controllers. The number of access points supported in a mobility group is bound by the number of controllers and the access point capacity of each controller. Thus, for the Cisco 5508 Wireless Controller, a mobility group can have up to 72 * 250, or 18,000 access points.

The advantage of this mobility group approach is clarity and simplicity in deployment and administration. This is a key point when dealing with medium enterprises that may have limited network administrative staff. By using mobility groups as indicated in Figure 4-9, design simplicity is maintained. Given the large capacity of the Cisco 5508 Wireless Controller, the limitation on the maximum number of controllers per mobility group is not considered to be a significant trade-off.

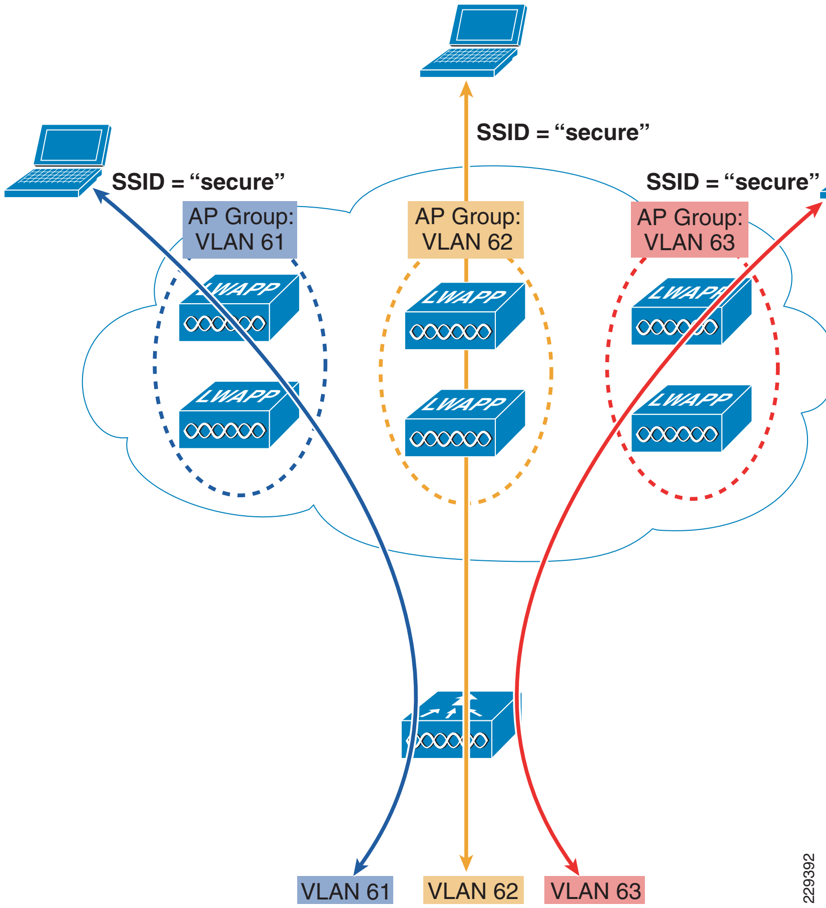
Additional information about WLAN controller mobility groups, including best practice information, can be found in the *Enterprise Mobility 4.1 Design Guide* at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/ch2_Arch.html#wp1028143.

WLAN Controller Access Point Groups

Typically, each WLAN defined on the controller is mapped to a single dynamic interface (as shown earlier for the secure staff, VoWLAN, and guest access WLANs). Consider the case however, where the Cisco 5508 Wireless Controller is deployed and licensed for 250 access points. Assume also that there are 10 users associated to each access point, using the same WLAN and SSID. This would result in 2500 users sharing the single VLAN to which the WLAN is mapped. A potential issue with this approach is that, depending on the particular overall network design, the use of subnets large enough to support 2500 users may not be possible.

To address this issue, the WLAN can be divided into multiple segments using the AP grouping capability of the WLAN controller. AP grouping allows a single WLAN to be supported across multiple dynamic VLAN interfaces on the controller. This is done by assigning a group of access points to an access point group at the WLAN controller, and then mapping the group to a specific dynamic interface. In this way, access points can be grouped logically, such as by building or set of buildings. Figure 4-10 shows the use of AP grouping based on site-specific VLANs.

Figure 4-10 Access Point (AP) Groups



As shown in Figure 4-10, three dynamic interfaces are configured, each mapping to a site-specific VLAN: VLANs 61, 62, and 63. Each site-specific VLAN is mapped to a group of access points that uses the same WLAN/SSID. Each of these access point groups are denoted by an AP Group Name (AP Group VLAN61, VLAN62 or VLAN63). Thus, a staff member associating to the WLAN using an access point that is part of AP group VLAN61 is assigned an IP address from the VLAN 61 IP subnet. Likewise, a staff member associating to the WLAN using an access point that is part of AP group VLAN62 is assigned an IP address from the VLAN 62 IP subnet, and so on. Roaming between the site-specific VLANs is then handled internally by the WLAN controller as a Layer 3 roaming event. As such, the WLAN client maintains its original IP address.

Cisco 5508 Wireless Controllers can contain up to 192 access point group definitions, with up to 16 WLANs defined in each group. Each access point advertises only the enabled WLANs that belong to its access point group. Access points do not advertise disabled WLANs that are contained within its access point group, or WLANs belonging to another access point group.

In implementations of the Cisco Medium Enterprise Design Profile where addressing limitations are present, the use of access point grouping to allow a single WLAN to be supported across multiple dynamic VLAN interfaces on the controller can be extremely beneficial.

WLAN Controller RF Groups

The strategy behind how *RF groups*, otherwise known as *RF domains*, are deployed within the Cisco Medium Enterprise Design Profile represents another important deployment consideration that can affect overall accessibility. An RF group is a cluster of WLAN controllers that collectively coordinate and calculate their dynamic radio resource management (RRM) settings. Grouping WLAN controllers into RF groups in this way allows the dynamic RRM algorithms used by the Cisco Unified Wireless Network to scale beyond a single WLAN controller. In this way, the benefits of Cisco RRM for a given RF group can be extended between floors, buildings, and even across sites.

Note Complete information regarding Cisco Radio Resource Management can be found in the *Cisco Radio Resource Management under Unified Wireless Networks* at the following URL: http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a008072c759.shtml.

If there is any possibility that an access point joined to one WLAN controller may receive RF transmissions from an access point joined to a different WLAN controller, the implementation of system-wide RRM is recommended, to include both controllers and their access points. In this way, RRM can be used to optimize configuration settings to avoid 802.11 interference and contention as much as possible. In this case, both WLAN controllers should be configured with the same RF group name.

In general, simplicity is preferred in the configuration of RF groups within the mobility design. Thus, all WLAN controllers in the Medium Enterprise Design Profile are configured with the same RF group name. Although it is true that geographically disparate WLAN controllers have very little chance of experiencing RF interaction, and thus need not be contained in the same RF domain, for most medium enterprise deployments there is no real disadvantage to doing so. An exception to this would be in extremely large deployments, as the maximum number of controllers that can be defined in a single mobility group is twenty. A clear advantage to this approach is simplicity of configuration and better support of N+1 controller redundancy (see Controller Redundancy, page 4-38 for further details).

A more detailed discussion as well as best practice recommendations regarding the use of RF groups can be found in the *Enterprise Mobility 4.1 Design Guide* at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/ch2_Arch.html#wp1028184.

Access Points

In the Cisco Medium Enterprise Design Profile, it is anticipated that each building requiring WLAN access will be outfitted with dual-band 802.11n access points providing RF coverage in both the 2.4 and 5 GHz bands. It is generally assumed that users will require WLAN access in most building interior areas, plus a 50–75 yard outdoor perimeter area surrounding each building. Of course, it is important to consider that most buildings will almost certainly contain some areas not intended for human entry or occupancy at any time. Similarly, some buildings may possess areas within the aforementioned outdoor perimeter that simply may not be accessible to any users at any time. During your initial mobility design, these vacant areas may not be identified. Therefore, the precise subset of interior and exterior areas requiring WLAN access will likely be better determined instead during the site survey planning process, which is typically an integral part of any wireless network deployment.

Note For more information on site survey planning, see the *Cisco 802.11n Design and Deployment Guidelines* at the following URL: http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns348/ns767/white_paper_80211n_design_and_deployment_guidelines.html.

In most medium enterprises, the vast majority of interior building WLAN access can be provided by the Cisco Aironet 1140 Series 802.11n access point (see Figure 4-11), which delivers pervasive wireless connectivity while blending in seamlessly with the aesthetics of modern-day enterprise environments.

Figure 4-11 Cisco Aironet 1140 Series 802.11n Access Point (AIR-LAP1142N)

To deliver the right mix of style and performance, the Cisco Aironet 1140 Series 802.11n access point contains six integrated omni-directional antenna elements that incorporate the use of three hidden discrete elements for each frequency band. Ideal for indoor environments such as offices, conference rooms, corridors, and so on, the Cisco Aironet 1140 Series 802.11n access point has a visually pleasing metal housing covered by a white plastic shell that blends with the most elegant environments. The Aironet 1140 series 802.11n access point provides the ability to be powered directly from 802.3af power-over-Ethernet (PoE) while sustaining full-performance 802.11n connections on both of its radios simultaneously. In the Cisco Medium Enterprise Design Profile, the model of the Cisco 1140 Series 802.11n access point recommended for most interior building locations is the AIR-LAP1142N.

Note Complete information (including country-specific ordering information) regarding the Cisco Aironet 1140 series 802.11n Access Point can be found at the following URL: http://www.cisco.com/en/US/products/ps10092/index.html

Although the Cisco Aironet 1140 Series 802.11n access point is capable of servicing the bulk of all medium enterprise interior wireless needs, there are some trade-offs to consider in specialized situations. For example, in situations where the results of pre-site survey planning indicate that the use of external antennas are required to best meet specific RF coverage requirements, an access point that provides antenna connectors is necessary. This might include situations where a focused directional antenna pattern is required, or simply one where aesthetic requirements demand that the access point be completely hidden, with only a small antenna footprint exposed to public view. In other cases, perhaps one or more access points will need to be deployed in refrigerated storage, research or even product testing environments where the anticipated operating temperature extremes are not within common norms. Here, extended operating temperature tolerances beyond that of the Cisco Aironet 1140 Series 802.11n access point may be required.

To assist in addressing these and other rare but still significant deployment challenges that may be encountered within medium enterprise sites, the Cisco Aironet 1250 Series 802.11n access point is recommended (see Figure 4-12).

Figure 4-12 Cisco Aironet 1250 Series 802.11n Access Point (AIR-LAP1252AG)

Designed with a next-generation ruggedized modular form factor, the Cisco Aironet 1250 Series 802.11n access point is intended for no-compromise performance in combination with the inherent expand-ability required to address challenging deployment situations. With robust modularized construction and six RP-TNC antenna jacks that allow antennas to be positioned independently of the access point itself, the Cisco Aironet 1250 Series 802.11n access point can be used to address situations requiring focused directional coverage patterns, extended operating temperature capabilities or minimal-footprint installations where it is highly preferable that the access point chassis is totally hidden from view. In the Cisco Medium Enterprise Design Profile, the AIR-LAP1252AG model of the Cisco 1250 Series of access points is recommended for those and other types of demanding deployments.

Note To help discourage theft and vandalism, both the Cisco 1140 as well as 1250 Series 802.11n access points are manufactured with a security slot machined into the access point casing. You can secure either model access point by installing a standard security cable (such as the Kensington Notebook MicroSaver, model number 64068) into the access point security cable slot.

Complete information regarding the Cisco Aironet 1250 series 802.11n access point can be found at the following URL: http://www.cisco.com/en/US/products/ps8382/index.html. Additional information concerning the antenna options available for the Cisco Aironet 1250 Series 802.11n access point can be found at the following URL:
http://www.cisco.com/en/US/prod/collateral/wireless/ps7183/ps469/at_a_glance_c45-513837.pdf

Note that Cisco Aironet 1140 Series 802.11n access points can power both 802.11n radios, at full transmit power running two spatial streams with encryption, while drawing only 15.4 watts of power from an 802.3af PoE Catalyst switch. A tradeoff associated with the use of Cisco Aironet 1250 Series 802.11n access points is that the AP-1250 Series requires slightly more power to reach its peak levels of performance, approximately 18.5 to 20 watts of power from a switch capable of providing enhanced-PoE (ePoE). Keep in mind, however, that if the full performance capability of the Cisco Aironet 1250 series access point is not necessary in your particular deployment, or you wish to support only a single RF band (i.e., either 2.4 GHz or 5 GHz) the Cisco Aironet 1250 Series 802.11n access point can also operate with 15.4 watts from a 802.3af PoE Catalyst switch.

To provide the Cisco Aironet 1250 Series 802.11n access point with 20 watts of input power, Cisco recommends the following power options:

- An ePoE Cisco Catalyst switch or switch blade module (such as the 3560-E, 3750-E, 4500E and 6500E Series.
- The use of a mid-span ePoE injectors (Cisco part number AIR-PWRINJ4). This option allows the Cisco Aironet 1250 series 802.11n access point to deliver full 802.11n performance while connected to any Cisco Catalyst switch. Power is injected directly onto the wire by the AIR-PWRINJ4 mid-span injector without reliance on the power output level of the switch itself.

Although its deployment flexibility is unparalleled within the marketplace, in most medium enterprise installations, the Cisco Aironet 1250 series 802.11n access point is typically only deployed only in those locations where they are necessary to address challenging situations. Other trade offs include a higher total cost per access point because of the added cost of external antennas, a larger footprint, and a heavier mounting weight as compared to the Cisco Aironet 1140 series 802.11n access point.

Note For the Cisco Aironet 1250 Series 802.11n access point, Cisco recommends performing your site survey using the same levels of PoE input power as you expect to use in your final deployment. For example, if you plan to deploy Cisco Aironet 1250 Series 802.11n access points with 15.4 watts of PoE, it is recommended for consistency and accuracy that perform your site survey using the same PoE input power levels.

The following design considerations regarding dual-band access points should be kept in mind when designing networks for dense user environments (for example, large cubicle areas, cafeterias, and employee auditoriums within site buildings):

- *Use the 5 GHz band whenever possible*

  In general, this applies for both 802.11n as well as pre-802.11n wireless clients. The characteristics of 5 GHz operation make it advantageous for most users, and especially 802.11n users, for the following reasons:

  - Despite the maturity of 802.11 wireless LAN technology, the installed base of 5 GHz 802.11a clients generally is not nearly as widespread as 2.4 GHz 802.11b and 802.11g clients. A smaller installed base of users translates into less contention with existing clients and better operation at higher throughput rates.
  - The number of non-802.11 interferers (such as cordless phones and wireless personal networks) operating in the 5 GHz band is still just a fraction of the number found within the 2.4 GHz band.
  - The amount of available bandwidth found in the 5 GHz band is much greater than that of the 2.4 GHz band. In the United States, there are twenty-one 5 GHz non-overlapping channels that can be deployed. This translates into the ability to deploy with density and capacity in mind, and allow background resources such as Cisco RRM to handle channel and power output requirements accordingly.

- *Design and survey for capacity, not just maximum coverage*

  It is a natural tendency to try to squeeze the most coverage from each access point deployed, thereby servicing as much of the site as possible with the lowest total access point investment. When designing networks for high-speed applications, attempting to design for maximum coverage at maximum transmitter output power can be counter-productive, as the maximum coverage footprint is typically attained using lower data rates and degraded signal-to-noise ratios. In addition, such false economies often sacrifice the ability to effectively make use of advanced tools such as Cisco RRM to address anomalies such as "coverage holes" and other deficiencies. Instead, the successful designer should design for capacity and generally aim to have access points installed closer together at lower power output settings. This approach allows for access point transmitter power to be dynamically managed via Cisco RRM. It also allows the practical use of higher data rates, provides RRM with the necessary transmission power "headroom" to allow for the ability to compensate for environmental changes, and facilitates the use of advanced capabilities such as location-based context-aware services.

- *Mount access points or antennas on the ceiling when possible*

Cisco Aironet AP-1140 Series 802.11n access points should be mounted on ceilings only. Ceiling mounting is recommended in general for the types of indoor environments found within medium enterprises, especially for voice applications. In the majority of carpeted indoor environments, ceiling-mounted antennas typically have better signal paths to handheld phones, taking into consideration signal loss because of attenuation of the human head and other obstacles.

Ceiling mounting locations are usually readily available, and more importantly, they place the radiating portion of the antenna in open space, which usually allows for the most efficient signal propagation and reception. Cisco Aironet 1250 Series 802.11n access points can be mounted as deemed necessary during pre-site survey planning or during the actual site survey process. However, ceiling mounting of Cisco Aironet 1250 Series access point antennas is highly recommended, especially when using omni-directional antennas.

- *Avoid mounting on surfaces that are highly reflective to RF*

  Cisco recommends that all antennas be placed one to two wavelengths from surfaces that are highly reflective to RF, such as metal. The separation of one or more wavelengths between the antenna and reflective surfaces allows the access point radio a better opportunity to receive a transmission, and reduces the creation of nulls when the radio transmits. Based on this recommendation, a good general rule of thumb then is to ensure that all access point antennas are mounted at least five to six inches away from any large metal reflective surfaces. Note that although recent technological advances have helped greatly in mitigating problems with reflections, nulls, and multipath, a sensible antenna placement strategy still is very important to ensure a superior deployment.

- *Disable legacy and low speed data rates*

  Clients operating at low data rates (for example, 1, 2, and 5.5 Mbps) consume more airtime when compared to clients transmitting the same data payloads at higher data rates such as 36 Mbps and 54 Mbps. Overall system performance in any given access point cell drops significantly when a large percentage of low data rate frames tend to consume available airtime. By designing for capacity and disabling lower data rates, aggregate system capacity can be increased.

  Unless you are aware of specific reasons why one of the data rates described below are required in your deployment (such as the presence of clients that can transmit or receive *only* at these rates), the following actions are recommended:

  - For 2.4 GHz, disable the 1, 2, 5.5, 6, and 9 Mbps rates.
  - For 5 GHz, disable at a minimum the 6 and 9 Mbps rates.

  A common question concerning 2.4 GHz is why not disable 802.11b entirely? In other words, why not disable the 1, 2, 5.5, and 11 Mbps 2.4 GHz rates altogether? Although this certainly may offer advantages relating to better performance for 802.11g users, this approach may not be entirely practical, especially on guest access WLANs where a visitor might attempt to gain access using a device with embedded legacy radio technology that may not support 802.11g. Because of this, depending on the mix of clients in the environment, it may be wiser to simply disable only the three 802.11b data rates below 11 Mbps. Only if you completely confident that the situation just described is entirely not applicable in your environment should you consider completely disabling all 802.11b data rates.

Additional best practice guidelines for access point and antenna deployments can be found in the following reference documents:

- *Enterprise Mobility 4.1 Design Guide*—
  http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.html
- *Voice Over Wireless LAN 4.1 Design Guide*—
  http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/vowlan/41dg/vowlan41dg-book.html

To provide outdoor WLAN access around the immediate perimeter area of each building, the Cisco Aironet 1520 Series Lightweight Outdoor Access Point is recommended (see Figure 4-13).

Figure 4-13 Cisco Aironet 1520 Series Lightweight Outdoor Access Point

As part of the Cisco Medium Enterprise Design Profile, the Cisco Aironet 1520 Series Lightweight Outdoor Access Point provides an outdoor extension to the enterprise wireless network, with central management provided through WLAN controllers and the Cisco Wireless Control System. A very rugged enclosure allows for deployment outdoors without the need to purchase additional housings or third-party National Electrical Manufacturers Association (NEMA) enclosures to provide protection from extreme weather. The robust, weatherized housing of the Cisco Aironet 1520 Series Lightweight Outdoor Access Point can be painted to adapt to local codes and aesthetics.

Although the Cisco Aironet 1520 Series Lightweight Outdoor Access Point is part of the outdoor mesh series of Cisco access point products, a full outdoor mesh infrastructure is beyond the scope of the Cisco Medium Enterprise Design Profile at this time. Rather, in this design Cisco Aironet 1520 Series Lightweight Outdoor Access Points are deployed only as root access points (RAPs), located outdoors on each building in such a manner that a satisfactory outdoor perimeter area is established. The precise location of these outdoor access points, as well as antenna choices, depends on the characteristics associated with the required coverage area and other particulars, and should be determined during pre-site survey planning.

For readers who wish to augment the recommendations made in this design guide and deploy a full site outdoor mesh configuration, see the *Cisco Aironet 1520, 1130, 1240 Series Wireless Mesh Access Points, Design and Deployment Guide,* Release 6.0 at the following URL: http://www.cisco.com/en/US/docs/wireless/technology/mesh/design/guide/MeshAP_60.html.

In choosing among the various models of Cisco Aironet 1520 Lightweight Outdoor Access Points, readers may also wish to consider whether local, municipal, state or other public safety agencies are currently using or otherwise plan to deploy compatible 4.9 GHz public safety equipment (see note below) in emergency response vehicles. If this is the case, it may be wise to plan ahead in conjunction with on-site and local public safety agencies to accommodate the use of this licensed band for connectivity from properly equipped first responders and emergency vehicles to your WLAN. In the event of a site emergency, the ability to connect to and monitor in-building events, or access key safety and security applications, can significantly enhance the ability of law enforcement and other agencies to locate and combat threats.

Note In 2003, the U.S. Federal Communications Commission (FCC) allocated 50 MHz of spectrum in the 4.9 GHz band to public safety services. Public safety agencies can use this 4.9 GHz band to implement wireless networks with advanced services for the transmission of mission-critical information. Because of the limited number of transmitters and the requirement for licensing, interference on the 4.9 GHz band tends to be below that of other bands, such as 2.4 GHz and 5 GHz. Communications using the 4.9 GHz public safety band must be related to the protection of life, health, or property. Examples include WLANs for incident scene management, mobile data, video surveillance, VoWLAN, fixed point-to-point, and so on.

Even if 4.9 GHz access is not available at your site, public safety agencies may still be able to access the WLAN using standard 2.4 GHz or 5 GHz unlicensed bands. This depends on whether the emergency response vehicles of the agencies in question are equipped to do so, as well as the configuration of their equipment. Keep in mind that when public safety users access WLANs using unlicensed 2.4 GHz and 5 GHz frequencies, they must also contend for access with other unlicensed users of these frequencies, as well as deal with any interference from other sources located within those bands.

With this in mind, the particular model of outdoor access point recommended for outdoor perimeter building coverage, depending on the inclusion of 4.9 GHz as follows:

- The Cisco Aironet 1524PS (Public Safety) Lightweight Outdoor Access Point includes 4.9 GHz capability and provides flexible and secure outdoor WLAN coverage for both public safety and mobility services. The Cisco Aironet 1524PS Public Safety Lightweight Outdoor Access Point is a multiple-radio access point that complies with the IEEE 802.11a and 802.11b/g standards, as well as 4.9 GHz public safety licensed operation parameters. This access point can support independent data exchanges across all three radios simultaneously. The main trade-off with the Cisco Aironet 1524PS Public Safety Lightweight Outdoor Access Point is the added purchase and deployment cost. However, in environments where public safety agencies are already equipped with compatible 4.9 GHz clients, the added benefits and advantages afforded by the 1524PS are often considered worthwhile. The model of Cisco Aironet 1524PS Public Safety Lightweight Outdoor Access Point recommended in the Cisco Medium Enterprise Design Profile is the AIR-LAP1524PS.
- The Cisco Aironet 1522 Outdoor Lightweight Access Point is a dual-radio, dual-band product that is compliant with IEEE 802.11a (5-GHz) and 802.11b/g standards (2.4-GHz). Designed for demanding environments, the Cisco Aironet 1522 provides high performance device access through improved radio sensitivity and range performance. The trade offs of deploying this model are the lack of 4.9 GHz licensed public safety support in environments where 4.9 GHz is in use among public safety agencies. The model of Cisco Aironet 1522 Lightweight Outdoor Access Point recommended in the Cisco Medium Enterprise Design Profile for deployments without 4.9GHz is the AIR-LAP1522AG.

Cisco offers a wide array of antenna options for the entire range of Cisco Aironet 1520 Series Lightweight Outdoor Access Points. Information on these antenna options can be found in the *Cisco Aironet 1520 Series Lightweight Outdoor Access Point Ordering Guide* at the following URL: http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps8368/product_data_sheet0900aecd8066a157.html.

All models of the Cisco Aironet 1520 Series Lightweight Outdoor Access Point can be powered from a multitude of sources, including PoE, direct DC, or direct AC. The entire range of power input options is described in the *Cisco Aironet 1520 Series Lightweight Outdoor Access Point Ordering Guide*.

Note Although the Cisco Aironet 1520 Series Lightweight Outdoor Access Point can be conveniently powered via PoE, a power injector (Cisco AIR-PWRINJ1500-2) specific to this product line must be used. Do not use any other power injector or Ethernet switch PoE capability (including enhanced PoE switches) in an attempt to directly provide PoE to Cisco Aironet 1520 Series Lightweight Outdoor Access Points. The Cisco Aironet 1520 Series Lightweight Outdoor Access Point is approved for use only with the Cisco AIR-PWRINJ1500-2 power injector. Keep in mind that although the Cisco Aironet 1520 Series Lightweight Outdoor Access Point is intended to be installed exposed to outdoor weather elements, the AIR-PWRINJ1500-2 power injector is approved for indoor installation only.

Some Cisco partners and customers may choose instead to integrate a standard access point into their own weatherproof outdoor enclosure. In this case, it is highly recommended that the Cisco Aironet 1250 Series 802.11n access point be used as the basis for that integration, as its external antenna capabilities would facilitate connection to external antennas via bulkhead connectors. However, integrating a standard indoor access point into a weatherproof outdoor enclosure in this manner has the disadvantage of lacking 4.9 GHz support in areas where public safety agencies are so equipped.

Usability

This section discusses the mobility design considerations pertaining to those aspects of the Cisco Medium Enterprise Design Profile that are relevant to overall usability, such as the following:

- Quality-of-service (QoS)
- Guest access

Quality-of-Service

The WLAN controller should be configured to set the 802.1p marking of frames received and forwarded onto the wired VLAN to reflect the QoS policy used on this WLAN. Therefore, if the WLAN controller is connected to a switch that is configured to trust the class-of-service (CoS) and maintain a translation table between CoS and Differentiated Services Code Point (DSCP), the translation between wireless QoS policy and wired network QoS policy occurs automatically.

In the Cisco Medium Enterprise Design Profile, WLAN traffic is prioritized based on the QoS profiles (platinum, silver, bronze, and so on) applied to each WLAN. However, this does not change the IP QoS classification (DSCP) of the client traffic carried, which means that client traffic leaving WLAN controllers may need to be reclassified based on network policy.

This may be achieved via one of following approaches:

- Applying policy at each of the switch virtual interfaces (SVIs) connecting the WLAN controller to the wired network
- Learning the QoS policy that has already been applied by the wireless networking components, because this should already be in alignment with the overall network policy

In the Cisco Medium Enterprise Design Profile, the plan is to use the latter approach, because it provides both the advantage of initial configuration simplicity as well as ongoing ease of maintenance. This technique requires only that the QoS profiles be maintained on the WLAN controllers themselves, without the need to configure explicit policies on adjacent switches. Switches need to be configured to trust only the QoS of frames forwarded to them by the WLAN controller.

To implement this approach, the WLAN controller should be configured to set the 802.1p marking of packets forwarded onto wired VLANs to reflect the QoS policy used on the specific WLAN from which they were received. Therefore, if the WLAN controller is connected to a switch that is configured to trust CoS and maintain a translation table between CoS and DSCP, the translation between wireless and wired network QoS policy occurs automatically.

For example, assume a packet received originates from a WLAN to which a platinum QoS profile has been assigned. This translates to a DSCP value of EF; therefore, the WLAN controller assigns a CoS value of 5 in the header of the frame that carries this data to the wired switch. Similarly, if the same packet originates from a WLAN assigned a QoS profile of silver, the translated CoS value is 0.

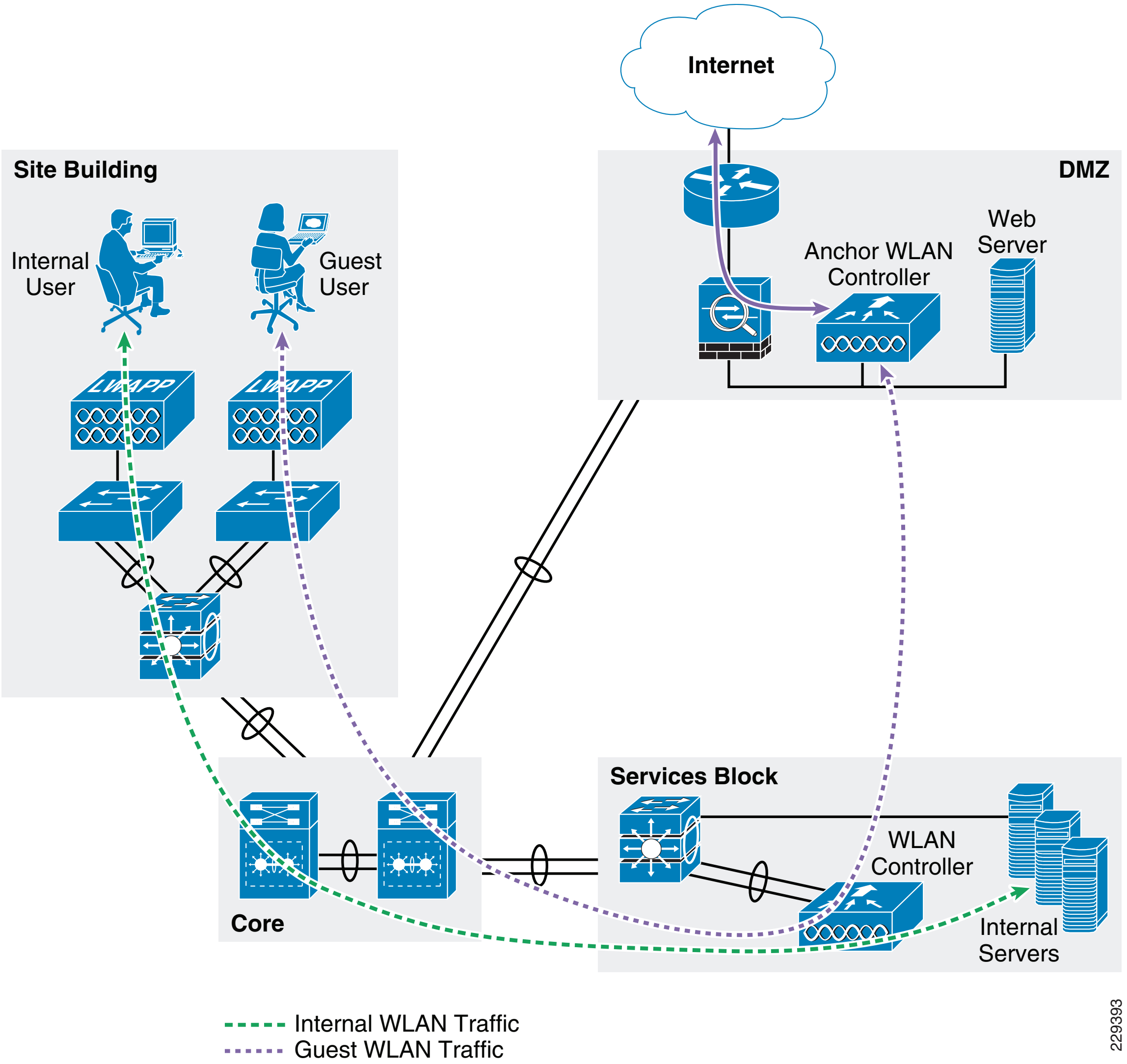
For more information on WLAN QoS, see the following URLs:

- *Voice over Wireless LAN 4.1 Design Guide 4.1*— http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/vowlan/41dg/vowlan41dg-book.html.
- *Enterprise Mobility 4.1 Design Guide*— http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/ch5_QoS.html

Guest Access

The Cisco Medium Enterprise Design Profile uses the Cisco Unified Wireless LAN Guest Access option to offer a flexible, easy-to-implement method for deploying wireless guest access via Ethernet over IP (EoIP), as described in RFC3378. EoIP tunneling is used between two WLAN controller endpoints in the centralized network design. The benefit of this approach is that there are no additional protocols or segmentation techniques necessary to achieve guest traffic isolation in relation to other internal traffic. Figure 4-14 shows a high-level view of guest access using this technique with a centralized WLAN controller design.

Figure 4-14 Guest Access Solution High-Level Overview



As shown in Figure 4-14, a WLAN controller with a specific purpose is located in the main site DMZ, where it is referred to as an anchor controller. The anchor controller is responsible for terminating EoIP tunnels originating from centralized site WLAN controllers, and interfacing the traffic from these controllers to a firewall or border router. As described in earlier sections of this document, the centralized site WLAN controllers are responsible for termination, management, and standard operation of the various WLANs provisioned throughout the enterprise, including one or more guest WLANs. Instead of being switched locally to a corresponding VLAN on the site controller, guest WLANs are instead transported via the EoIP tunnel to the anchor controller in the DMZ.

When an access point receives information from a WLAN client via the guest access WLAN/SSID, these frames are encapsulated using CAPWAP from the access point to the site WLAN controller. When received at the WLAN controller, they are encapsulated in EoIP from there to the anchor controller. After reaching the anchor controller, these frames are de-encapsulated and passed to a firewall or border router via the guest VLAN. The use of EoIP and an anchor WLAN controller in the DMZ allows guest user traffic to be transported and forwarded to the Internet transparently, with no visibility by, or interaction with, other traffic in the enterprise.

Because the anchor controller is responsible for termination of guest WLAN traffic and is positioned within the Internet DMZ, firewall rules must be established to limit communication between the anchor controller and only those controllers authorized to establish EoIP tunnels to them. Such rules might including filtering on source or destination controller addresses, UDP port 16666 for inter-WLAN controller communication, and IP protocol ID 97 (Ethernet over IP) for client traffic. Other rules that might be needed include the following:

- TCP 161 and 162 for SNMP
- UDP 69 for TFTP
- TCP 80 or 443 for HTTP, or HTTPS for GUI access
- TCP 23 or 22 for Telnet, or SSH for command-line interface (CLI) access

The following are other important considerations to keep in mind regarding the use of this guest access solution:

- For the best possible performance, Cisco strongly recommends that the anchor controller be dedicated to supporting EoIP guest access tunneling only. In other words, do not use the anchor controller for any other purpose but EoIP guest access tunneling. In particular, in addition to its guest access role, the anchor controller should not be used to control and manage other access points in the enterprise.
- When deploying a Cisco 5508 Wireless Controller as an anchor controller, keep in mind that because the anchor controller is not going to be used to manage access points, it can be licensed to support only a minimal number of access points. For example, a Cisco CT5508-12 (12 access point-licensed capacity) can function quite well as an anchor controller in the Cisco Medium Enterprise Design Profile, even in networks where hundreds or thousands of access points may be joined to other Cisco 5508 Wireless Controllers.
- Multicast traffic is not supported over guest tunnels, even if multicast is enabled on wireless controllers.
- The mobility group name of the anchor controller should differ from that configured for site controllers. This is done to keep the anchor controllers logically separate from the mobility groups associated with the general wireless deployment.
- The mobility group name for every WLAN controller that establishes EoIP tunnels with the anchor controller must be configured as a mobility group member in the anchor controller configuration.

Finally, although the focus for the Cisco Medium Enterprise Design Profile is on the pure controller-based guest access solution, note that other, equally functional solutions are available that combine what is discussed in this section with the use of an access control platform external to the WLAN controller. For example, the guest access solution topology described in this section can be integrated with the Cisco NAC Appliance. This might be the case, for example, if the medium enterprise has already deployed the Cisco NAC Appliance within their Internet DMZ to support wired guest access services. As shown in Figure 4-15, the wireless guest access topology remains the same, except that in this scenario, the guest VLAN interface on the anchor controller connects to an inside interface on the NAC Appliance, instead of to a firewall or border router.

Figure 4-15 Cisco UWN Guest Access with Anchor WLC and NAC Appliance

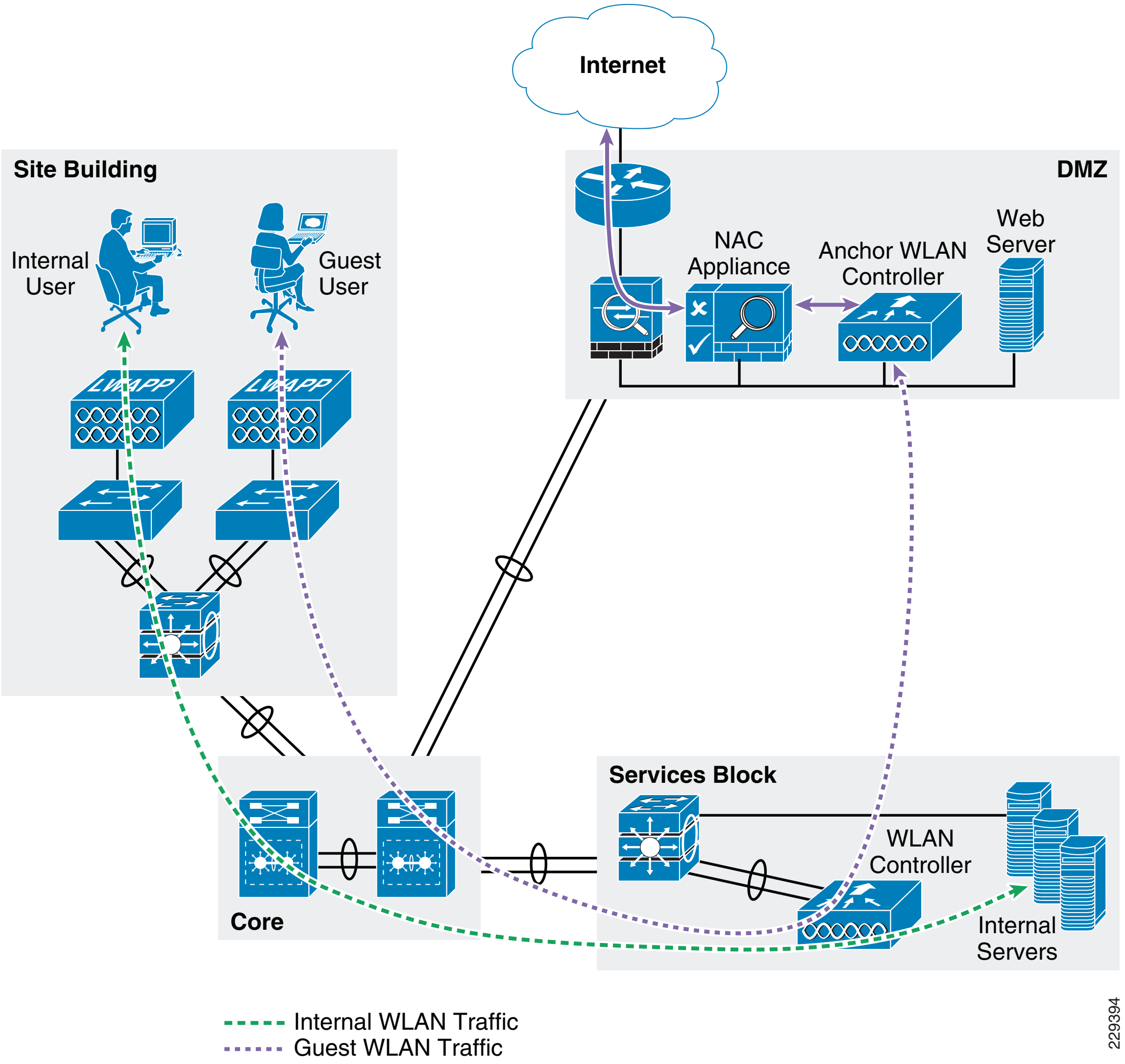
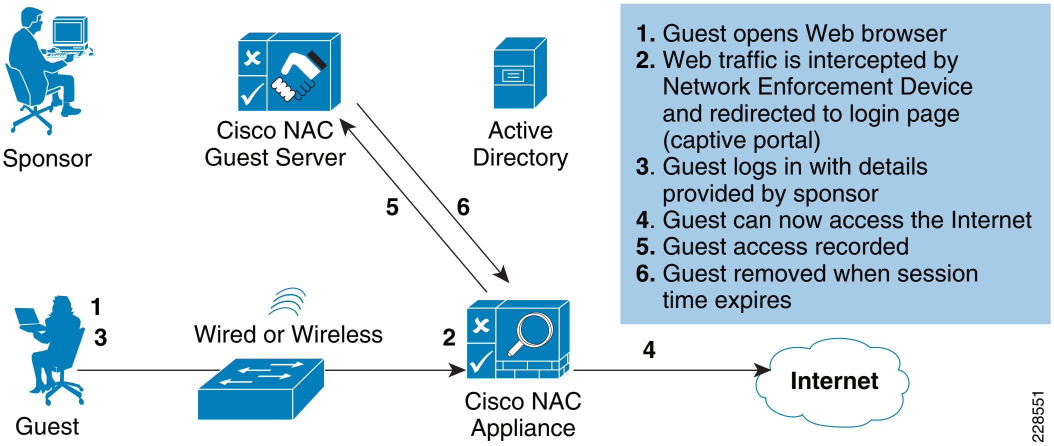


Figure 4-15 shows that the NAC Appliance is responsible for redirection, web authentication, and subsequent access to the Internet. The site and anchor controllers are used only to tunnel guest WLAN traffic across the enterprise into the DMZ, where the NAC appliance is used to actually control guest access. The trade-off here is the added cost of the external access control solution, versus the benefits it affords in relation to your particular deployment.

Note Additional information concerning the design and deployment of the Cisco Unified Wireless Network guest access solution can be found in the *Enterprise Mobility 4.1 Design Guide* at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/ch10GuAc.html#wp999659.

The Cisco NAC Guest Access Server is another member of the Cisco Network Admission Control solution family that can further enhance the utility of your design by assisting network administrators in the provisioning of guest access user accounts. The NAC Guest Access Server facilitates the creation of guest accounts for temporary network access by permitting provisioning by authorized personnel in a simple and secure manner. In addition, the whole process is recorded in a single place and stored for later reporting, including details of the network access activity. Cisco NAC Guest Server integrates with Cisco NAC Appliance through an application programming interface (API), allowing for guest accounts to be controlled via the Guest Server user interface, including creation, editing, suspension, and deletion of accounts. The Cisco NAC Guest Server then controls these accounts on the Cisco NAC Appliance through the API (shown in Figure 4-16). In addition, the Guest Server receives accounting information from the NAC Appliance to enable full reporting.

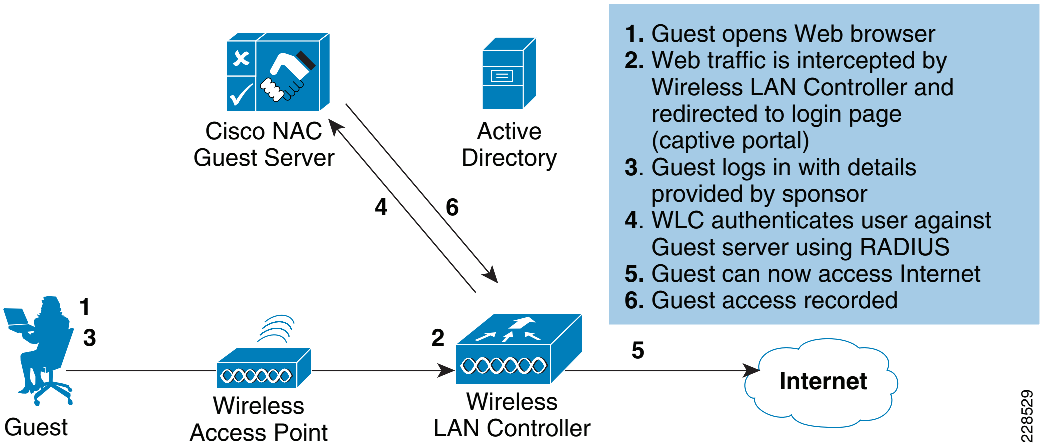
Figure 4-16 ***NAC Guest Server with NAC Appliance and WLAN Controller***



1. Guest opens Web browser
2. Web traffic is intercepted by Network Enforcement Device and redirected to login page (captive portal)
3. Guest logs in with details provided by sponsor
4. Guest can now access the Internet
5. Guest access recorded
6. Guest removed when session time expires

Cisco NAC Guest Server can also integrate directly with Cisco WLAN controllers through the RADIUS protocol, allowing for guest accounts to be controlled via the Guest Server user interface, including the creation, editing, and deletion of guest accounts. In this case, the WLAN controller makes use of the NAC Guest Server to authenticate guest users (shown in Figure 4-17). In addition, the Guest Server receives accounting information from the WLAN controller to enable full reporting.

Figure 4-17 ***NAC Guest Server with WLAN Controller Alone***



1. Guest opens Web browser
2. Web traffic is intercepted by Wireless LAN Controller and redirected to login page (captive portal)
3. Guest logs in with details provided by sponsor
4. WLC authenticates user against Guest server using RADIUS
5. Guest can now access Internet
6. Guest access recorded

Note For more information on the Cisco NAC Guest Server, see the following URL: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5707/ps8418/ps6128/product_data_sheet0900aecd806e98c9.html.

Manageability

As mentioned earlier, each WLAN controller in the Cisco Medium Enterprise Design Profile provides both a CLI as well as a graphical web user interface, which are primarily used for controller configuration and management. These user interfaces provide ready access to the network administrator. However, for a full-featured, centralized complete life cycle mobility management solution that enables network administrators to successfully plan, configure, deploy, monitor, troubleshoot, and report on indoor and outdoor wireless networks, the use of the Cisco Wireless Control System (WCS) is highly recommended (see Figure 4-18).

Figure 4-18 Cisco Wireless Control System

The Cisco Wireless Control System allows very effective management of wireless networks supporting high-performance applications and mission-critical solutions. Effective management of these networks helps to simplify network operation and improve the productivity of employees, administrators, guests and site visitors. The comprehensive Cisco WCS platform scales to meet the needs of small, midsize, and large-scale WLANs across local and remote sites. Cisco WCS gives network administrators immediate access to the tools they need when they need them, wherever they may be located within the enterprise.

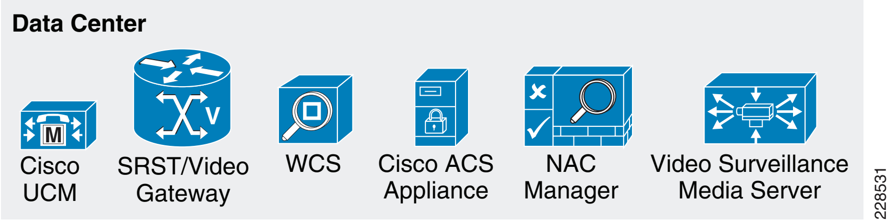
Operational costs are significantly reduced through a simplified and intuitive GUI, with built-in tools delivering improved efficiency and helping to reduce training costs, even as the site network grows incrementally larger. Cisco WCS lowers operational costs by addressing the whole range of mobility management requirements (radio frequency, access points, controllers, mobility services, and so on) using a single unified management platform deployed in a centralized location, and with minimal impact on staffing requirements.

Cisco WCS can scale to manage hundreds of Cisco WLAN controllers, which in turn can manage thousands of Cisco Aironet access points. For installations where network management capabilities are considered mission-critical, WCS also supports a software-based high availability option that provides failover from a primary (active) WCS server to a secondary (standby). Adding mobility services such as context-aware software and adaptive wireless intrusion prevention systems (wIPS) is simplified through Cisco WCS integration with the Cisco Mobility Services Engine (MSE).

Note A detailed description of each management feature and benefit available in the Cisco Wireless Control System is beyond the scope of this chapter, but the information can be found at the following URL: http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps6301/ps6305/product_data_sheet0900aecd802570d0.html.

In the Cisco Medium Enterprise Design Profile, a centralized WCS management server located in the data center block within the main site is used. The data center block was initially shown in Figure 4-3. Figure 4-19 provides greater detail and magnification.

Figure 4-19 WCS Within the Data Center Block



The current upper limit for scaling WCS on a high-end server is up to 3000 Cisco Aironet CAPWAP-based access points, and up to 750 Cisco WLAN controllers. As such, most implementations of the Cisco Medium Enterprise Design Profile are well served by a mobility design using a WCS management server located on the main site.

Note For further information on WCS hardware platforms and requirements, see the following URL: http://www.cisco.com/en/US/docs/wireless/wcs/6.0/configuration/guide/6_0wst.html#wp1061082.

The planning, configuration, deployment, monitoring, reporting, auditing, and troubleshooting made available by WCS are accessible to any authorized medium enterprise network administrator via standard secured web browser access.

Generally speaking, it is anticipated that access to WCS will be restricted to network administrators and their staff located at the main and remote sites, as well as local site administrators for sites where network administrators are not present. However, these groups will most likely not have equivalent resource and functionality access. It is anticipated that resource access will be limited further, based on administrative level and assigned site or sites.

In this design, the ability to query and manage site mobility resources is regulated using the virtual domain feature of WCS, in conjunction with the appropriate assignment of WCS user rights. Thus, although key members of the main site central network administration staff may possess the authority to manage any and all mobility resources located on any site throughout the enterprise, remote site administrators may be limited by the following:

- *Site resource management visibility policy*—This is performed by assigning the network mobility infrastructure components associated with each site to a WCS virtual domain, and assigning the virtual domains to appropriate network administrators. Key members of the central administrative staff are assigned to the WCS root domain, granting them overall authority to view and configure all mobility infrastructure resources, on any site, via their WCS management consoles. However, personnel responsible for local site network administration are restricted to the discrete mobility infrastructure components associated with the virtual domain representing their local site. These infrastructure components include WLAN controllers, access points, configuration templates, WCS events, reports, alarms, WLAN clients, and so on.
- *Site resource management access policy*—Although the visibility of a resource is determined by WCS virtual domain assignment, the subset of acceptable actions that are allowed against any visible resources are further regulated by the assignment of appropriate WCS user and group rights, which allow policies to be applied that further limit what actions each may be allowed against any visible resources.

Via the WCS GUI interface, virtual domains (as well as WCS user rights) can be assigned at the WCS server or using an external security manager such as Cisco Secure ACS.

Note Further information regarding how WCS virtual domains may be used to limit individual site network administrator access to segments of the mobility network outside of their scope of responsibility, while still providing for overall "root" administrator control of the entire wireless network, may be found at the following URL: http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps6301/ps6305/brochure_c02-474335.html.

Guest access credentials can be created and managed centrally using the Cisco WCS. A network administrator can create a limited privilege account within WCS that permits "lobby ambassador" access for the purpose of creating guest credentials. With such an account, the only function a lobby ambassador is permitted is to create and assign guest user credentials to controllers that have web-policy configured WLANs. In the rare event that a centralized WCS management system is not available because of a server failure, a network administrator can establish a local administrator account on the anchor WLAN controller, with lobby ambassador privileges, as a backup means of managing the guest access solution.

The use of a centralized WCS management server in the Cisco Medium Enterprise Design Profile provides key advantages such as reduced initial deployment cost and ease of maintaining server resources in a centralized location, coupled with good performance across modern high-speed LANs and WANs. Of course, as with any design choice, certain trade offs exist, such as the following:

- *WCS server failure*

  In the Cisco Medium Enterprise Design Profile, the centralized mobility network management services provided by WCS are not regarded as being mission-critical for the majority of medium enterprise deployments. Thus, in the rare event of a WCS server failure, it is assumed that direct WLAN controller management work a rounds (such as that described earlier for guest access management) are an acceptable cost compromise. Any downtime realized because of a WCS server failure, although undoubtedly very inconvenient, would in most cases not be viewed as entirely catastrophic. This being the case, the Cisco Medium Enterprise Design Profile does not at this time provide for the added cost of a secondary WCS management server in an N+1 software-based high-availability arrangement. However, deployments where WCS management services are critical to the mission of the medium enterprise should instead consider modifying the design to include the services of a secondary WCS management platform configured for N+1 software-based high-availability.

  Note For more information on WCS high availability configurations, see the following URL: http://www.cisco.com/en/US/docs/wireless/wcs/6.0/configuration/guide/6_0admin.html#wp1132580.

- *Unrecoverable WAN failure*

  A catastrophic, unrecoverable WAN failure can interrupt management traffic between WCS and the WLAN controllers that are located on remote sites. One way to protect against this is to distribute the WCS management server function out further into the network, and centralize WCS management on a per-site basis. However, this increases the cost of WCS deployment significantly, requiring one WCS management server per site, and preferably a Cisco WCS Navigator management aggregation platform located at the main site. Because it is believed that the centralized mobility network management services provided by WCS are not regarded as mission-critical to the majority of medium enterprises, these decentralized management options are not included in the Cisco Medium

Enterprise Design Profile at this time. Instead, it is assumed that in this type of a rare occurrence, the aforementioned ability to minimally manage WLAN controllers directly will suffice, should any network management intervention be required in such circumstances.

Note For more information on WCS Navigator, see the following URL: http://www.cisco.com/en/US/products/ps7305/index.html.

Reliability

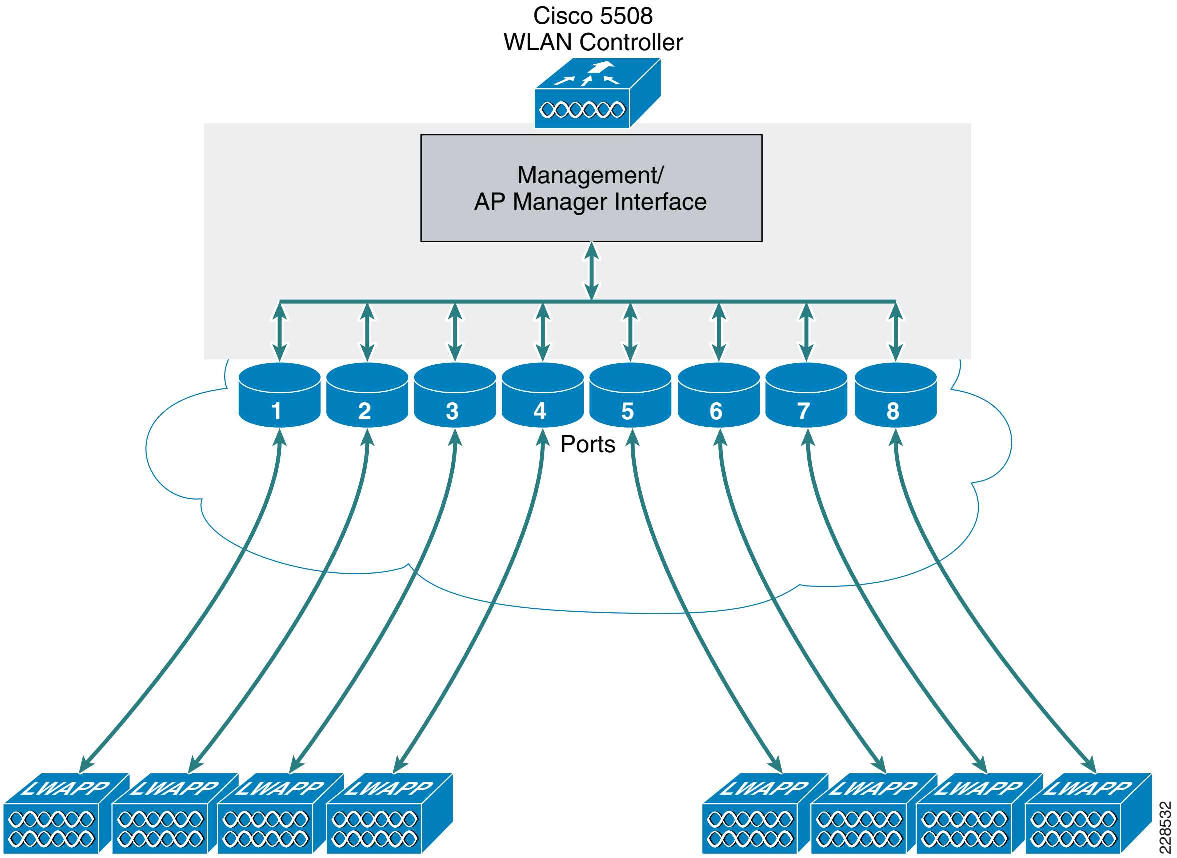
This section discusses the mobility design considerations pertaining to those aspects of the Cisco Medium Enterprise Design Profile relevant to overall reliability, and includes the following:

- Controller link aggregation
- Controller redundancy
- AP controller failover

Controller Link Aggregation

An important capability used to enhance the reliability of WLAN controller interconnection to the wired network is *link aggregation* (*LAG*). As mentioned earlier, LAG is a partial implementation of the 802.3ad port aggregation standard. It bundles all the controller distribution system ports into a single 802.3ad port channel, thereby reducing the number of IP addresses needed to make use of all controller wired ports. When LAG is enabled, the system dynamically manages port redundancy and load balances access points across each port, without interaction from the network administrator. With the Cisco 5508 Wireless Controller and the release 6.0 software used in the Cisco Medium Enterprise Design Profile, all eight ports can be bundled together into a single Gigabit EtherChannel interface. LAG is effective in distributing access point traffic across all controller ports, as shown in Figure 4-20. This can be especially important with high capacity controllers licensed for many access points, such as the Cisco CT5508-250.

Figure 4-20 LAG in the Cisco 5508 WLC



LAG simplifies controller configuration and improves the overall solution reliability. If any of the controller ports fail, traffic is automatically migrated to one of the remaining ports. As long as at least one controller port is functioning, the system continues to operate, access points remain connected to the network, and wireless clients continue to send and receive data.

The Gigabit Ethernet connections comprising the LAG (up to eight on the Cisco 5508 Wireless Controller) should be distributed among different modular line cards or switch stack members in the services block to the greatest degree possible. This is done to ensure that the failure of a single line card or switch stack member does not result in total failure of the WLAN controller interconnection to the network.

For example, if there are four switch stack members in the services block and LAG is configured using all eight WLAN controller interfaces, the Gigabit Ethernet links from the services switch block to the WLAN controller should be distributed two per services block switch stack member. In this way, if any switch stack member fails, six other Gigabit Ethernet links to the WLAN controller remain ready, active, and available to pass data.

The switch features required to implement this connectivity between the WLAN controller and the services block are the same switch features that are otherwise generally used for EtherChannel connectivity between switches.

When using a Cisco 5508 Wireless Controller with link aggregation enabled, it is important to keep the following considerations in mind:

- When the port channel is configured as “on” at both ends of the link, it does not matter if the Cisco Catalyst switch is configured for either Link Aggregation Control Protocol (LACP) or Cisco proprietary Port Aggregation Protocol (PAgP), because no channel negotiation occurs between the controller and the switch.

The recommended load balancing method for Cisco Catalyst switches is by use of the CLI command **src-dest-ip**.

- You cannot configure the controller ports into separate link aggregation groups. Only one link aggregation group is supported per controller. Therefore, you can connect a controller in link aggregation mode to only one neighbor switch device (note that this can be a switch stack with multiple member switches).
- When you enable link aggregation or make any changes to the link aggregation configuration, you must immediately reboot the controller.
- When you enable link aggregation, only one AP manager interface is needed because only one logical port is needed. The in-band management interface of the Cisco 5508 Wireless Controller can also serve as the AP manager interface.
- When you enable link aggregation, all Cisco 5508 Wireless Controller distribution ports participate in link aggregation by default. Therefore, you must configure link aggregation for all the connected ports in the neighbor switch that have been outfitted with small form-factor plug-in (SFP) modules.
- When you enable link aggregation, only one functional physical distribution port is needed for the controller to pass client traffic. Although Cisco 5508 Wireless Controllers have no restrictions on the number of access points per port, Cisco recommends that if more than 100 access points are connected to the controller, make sure that at least two or more Gigabit Ethernet interfaces are used to connect the controller to the services block.
- As mentioned previously, there are eight SFP interfaces on the Cisco 5508 Wireless Controller. These may be fully deployed to take full advantage of multi layer site design guidelines regarding the oversubscription of access layer uplinks. By doing so, it is relatively straightforward to design a solution that delivers access layer uplinks from the WLAN controller with an oversubscription rate of between 8:1 and 20:1 (Note that these oversubscription rates are not unique to wireless products and are equivalent with what is typically seen in wired networks as well.)

  Table 4-1 provides information for the Cisco 5508 Wireless Controller deployed with its maximum complement of 250 access points.

Table 4-1 Cisco 5508 Wireless Controller Oversubscription Rates

Throughput per AP (Mbps)	Cisco 5508 Wireless Controller Oversubscription Rate (8 Gbps)
25	1:1
50	2:1
100	4:1
150	5:1
200	7:1
250	8:1

Table 4-1 shows that even if designing for peak 802.11n throughput of 250 Mbps per access point, oversubscription is not expected to exceed site design guidelines of 8:1 when using all the available controller interfaces with LAG.

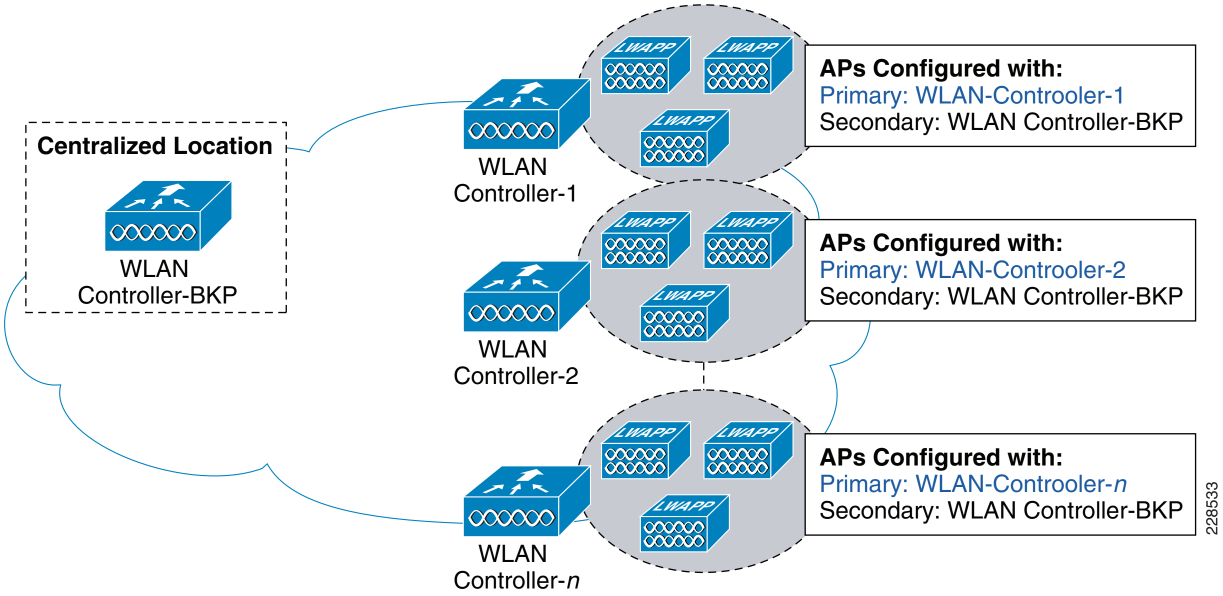
Note For more information concerning WLAN controller link aggregation, see *Deploying Cisco 440X Series Wireless LAN Controllers* at the following URL: http://www.cisco.com/en/US/docs/wireless/technology/controller/deployment/guide/dep.html#wp1062211.

Controller Redundancy

The ability of the solution to recover from a reasonable degree of component failure is important in ensuring the reliability of any WLAN networking solution. This is especially important when there are many users that may rely on a centralized component, such as a WLAN controller, for access into the network. An easy solution is to have a "hot" standby secondary controller always at the ready for each primary controller in active service (otherwise known as 1:1 controller redundancy). Although this offers the highest degree of protection from any number of failed primary controllers, it is also the most costly approach.

In the Cisco Medium Enterprise Design Profile, unforeseen controller failures are avoided using an "N+1" controller redundancy model, in which the redundant WLAN controller is placed in a central location and acts as a backup for multiple active WLAN controllers. Each access point is configured with the name or IP address of its primary WLAN controller, but is also configured with the name or IP address of the redundant controller as its secondary WLAN controller. The N+1 controller redundancy approach is based on the assumption that the probability of more than one primary WLAN controller failure occurring simultaneously is very low. Thus, by allowing one centralized redundant controller to serve as the backup for many primary controllers, high availability controller redundancy can be provided at a much lower cost than in a traditional 1:1 redundancy arrangement. Figure 4-21 provides a general illustration of the principle of N+1 controller redundancy.

Figure 4-21 General N+1 WLAN Controller Redundancy


Centralized Location
WLAN Controller-BKP
WLAN Controller-1
WLAN Controller-2
WLAN Controller-n
LWAPP
APs Configured with:
Primary: WLAN-Controoler-1
Secondary: WLAN Controller-BKP
APs Configured with:
Primary: WLAN-Controoler-2
Secondary: WLAN Controller-BKP
APs Configured with:
Primary: WLAN-Controoler-n
Secondary: WLAN Controller-BKP
228533

The main tradeoff associated with the N+1 redundancy approach is that the redundant controller may become oversubscribed if multiple primary controllers fail simultaneously. In reality, experience indicates that the probability of multiple controller failures is low, especially at geographically separate site locations. However, when designing an N+1 redundant controller solution, you should assess the risk of multiple controller failures in your environment as well as the potential consequences of an oversubscribed backup controller. In situations where there is reluctance to assume even this generally small degree of risk, other controller redundancy approaches are available that can provide increasingly greater degrees of protection, albeit with associated increases in complexity and equipment investment.

Note For more details on controller redundancy, see *Deploying Cisco 440X Series Wireless LAN Controllers* at the following URL: http://www.cisco.com/en/US/docs/wireless/technology/controller/deployment/guide/dep.html#wp1060810.

The configuration of N+1 redundancy in any mobility design depends greatly on the licensed capacity of the controllers used and the number of access points involved. In some cases, configuration is rather straightforward, emulating what is shown in Figure 4-21 by having the access points of the main site as well as all remote sites address a common redundant controller located in the main site services block. In other cases, there may be sufficient capacity on the primary controllers located on the main site themselves to accommodate the access point and user load of a single failed controller on any of the remote sites. This approach requires that main site controllers be licensed for a greater number of access points than necessary for the support of the main site alone. Additional licensing of existing controllers is performed in place of providing a dedicated additional controller platform at the main site for system-wide redundancy. In this case, the available capacity of the primary main site WLAN controllers allow them to act as the secondary destination for the access associated with the largest remote site. Thus, in this particular case, the need to deploy hardware at the main site explicitly for the purposes of controller redundancy may be avoided.

For example, assume that the main site shown in Figure 4-3 contains a total of 250 combined access points across all main site buildings, and the largest of the remote sites also contains 250 combined access points across all remote site buildings. In this case, if the main site services block is equipped with two Cisco CT5508-250 WLAN controllers (the “-250” signifies that this particular Cisco 5508 Wireless Controller is licensed for 250 access points), the access point load of the main site alone can be split equally between the two controllers (125 access points on each controller). This leaves ample capacity in the main site for one of the following scenarios to occur:

- Either of the main site controllers may fail and allow up to 125 joined access points to migrate (fail over) to the other controller in the pair. This results in the remaining functional controller bearing the full load of 250 access points.
- Any remote site controller may fail and allow its joined access points to migrate (fail over) to the main site controllers. In the case of a failure of the largest remote site, this results in each of the main site controllers operating at their full licensed capacity.

Further information regarding WLAN controller redundancy may be found in the following documents:

- *Deploying Cisco 440X Series Wireless LAN Controllers*— http://www.cisco.com/en/US/docs/wireless/technology/controller/deployment/guide/dep.html#wp1060810
- *Enterprise Mobility 4.1 Design Guide*— http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.html

AP Controller Failover

The Cisco Unified Wireless Network provides for multiple failover options that can allow access points to determine which WLAN controller to migrate in the event of a controller failure, based on pre-configured priorities. When an access point goes through its discovery process, it learns about all the WLAN controllers in its mobility group. The access point can prioritize which controller it attempts to join based on its high availability configuration, or choose a WLAN controller based on loading.

In the Cisco Medium Enterprise Design Profile, a high-speed WAN/MAN is present between sites, thus making access point fail over to a remote WLAN controller feasible, as described in the previous section. To accomplish this in the Cisco Medium Enterprise Design Profile, access points can be configured to fail over to a WLAN controller that is outside their mobility group. In this scenario, the remote WLAN controller is not in the mobility group that is learned during the AP discovery process, and the IP address of the remote WLAN controller must be provided in the HA configuration.

For this to be effective, however, a common WLAN SSID naming policy for key WLANs must be implemented to ensure that WLAN clients do not have to be re configured in the event of an access point fail over to the main site backup controller.

Best practice considerations regarding to AP controller failover include the following:

- After access points initially discover a WLAN controller, access points should be manually assigned to primary and secondary controllers. By doing this, AP assignment and WLAN redundancy behavior is deterministic.
- A common WLAN SSID naming policy is necessary to ensure that WLAN clients do not have to be re configured in the event of an access point fail over to a central backup controller. The SSID used to access a particular WLAN throughout the multisite medium enterprise should be the same, regardless of the controller.
- WLAN controllers have a configurable parameter known as *AP Fallback* that causes access points to return to their primary controllers after a failover event, after the primary controller comes back online. This feature is enabled by default. However, leaving this parameter at the default value can have some unintended consequences. When an access point “falls back” to its primary controller, there is a brief window of time, usually approximately 30 seconds or so, during which service to wireless clients is interrupted because the access points are busy re-joining the primary controller. In addition, if connectivity to the primary WLAN controller becomes unstable for some reason, the access point might “flap” between the primary controller and the backup. For this reason, it is preferable to disable AP Fallback and, in the rare event of a controller failure, move the access points back to the primary controller in a controlled fashion during a scheduled service window.

Note For more information and best practices regarding AP controller failover, see the *Enterprise Mobility 4.1 Design Guide* at the following URL:
http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.html.

Wireless LAN Controller Configuration

The core component of the Cisco Unified Wireless architecture is the WLAN Controller (WLAN controller) that provides the interface between the “split-MAC” wireless network and the wired network. That is, the WLAN controller is the Layer-2 connection point between WLAN client traffic and the wired network, making the WLAN controller an aggregation and control point for WLAN traffic. In addition, the WLAN controller is the primary control point of AP and RF management.

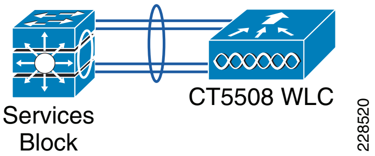
The reference design used for testing WLAN services in the Medium Enterprise Design Profile mobility design uses the following four WLAN controllers:

- Two WLAN controllers (cr23-5508-1, cr23-5508-2) for the main site
- One WLAN controller (cr14-5508-1) for a remote site
- One anchor WLAN controller (cr11-5508-wlc) for guest services

WLAN Controller and Wired Network Connections

The WLAN controllers in the main site are centralized for that site and connected to a 3750E stack in services block connected to the site core, as shown in Figure 4-22. These WLAN controllers provide WLAN services for the entire site, as well as fail over support for APs in remote sites, in the event of WLAN controller outage at that location. The number of WLAN controllers for the main site is driven by the number of APs deployed and the type of fail over support required. In this example, two WLAN controllers are used to illustrate the basic configuration requirements.

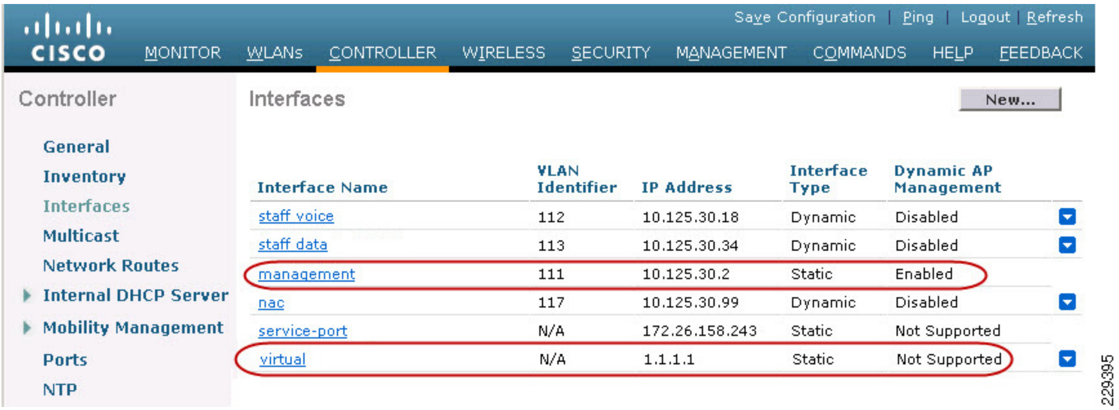
Figure 4-22 Services Block WLAN Controller Connection



The two main site WLAN controllers share the VLAN and subnet configuration, differing only in their IP addressing. Figure 4-23 and Figure 4-24 show the interface summary on the two WLAN controllers. The two key interfaces are highlighted, that is the management and virtual interfaces. The management interface is used as the interface for in-band communication with the WLAN controller, including CAPWAP tunnel termination (there is no AP-manager interface), and the virtual interface is used to support mobility.

Note Although the 1.1.1.1 address has been used in example mobility configurations, the 1.0.0.0/8 address range has now been assigned, and it is best that customers use a private address that would not be a valid address within their own network.

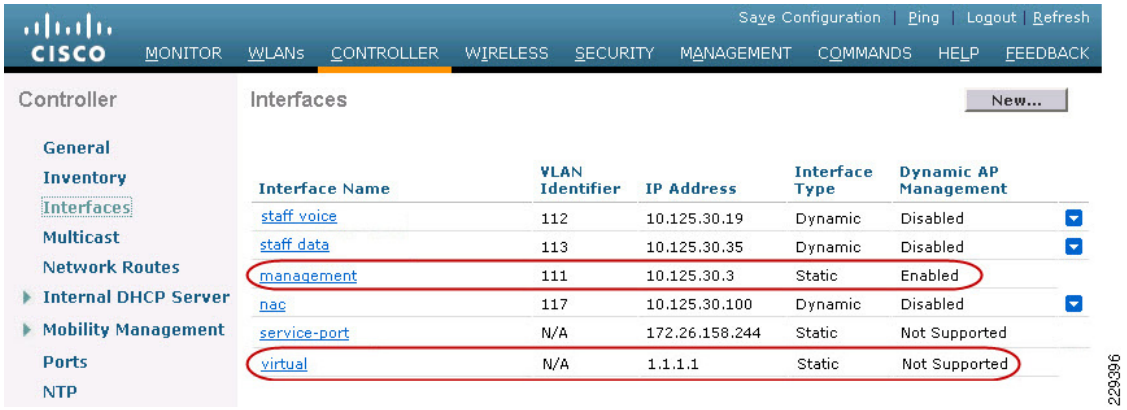
Figure 4-23 cr23-5508-1 Interfaces



Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
staff voice	112	10.125.30.18	Dynamic	Disabled
staff data	113	10.125.30.34	Dynamic	Disabled
management	111	10.125.30.2	Static	Enabled
nac	117	10.125.30.99	Dynamic	Disabled
service-port	N/A	172.26.158.243	Static	Not Supported
virtual	N/A	1.1.1.1	Static	Not Supported

Figure 4-24 cr23-5508-2 Interfaces

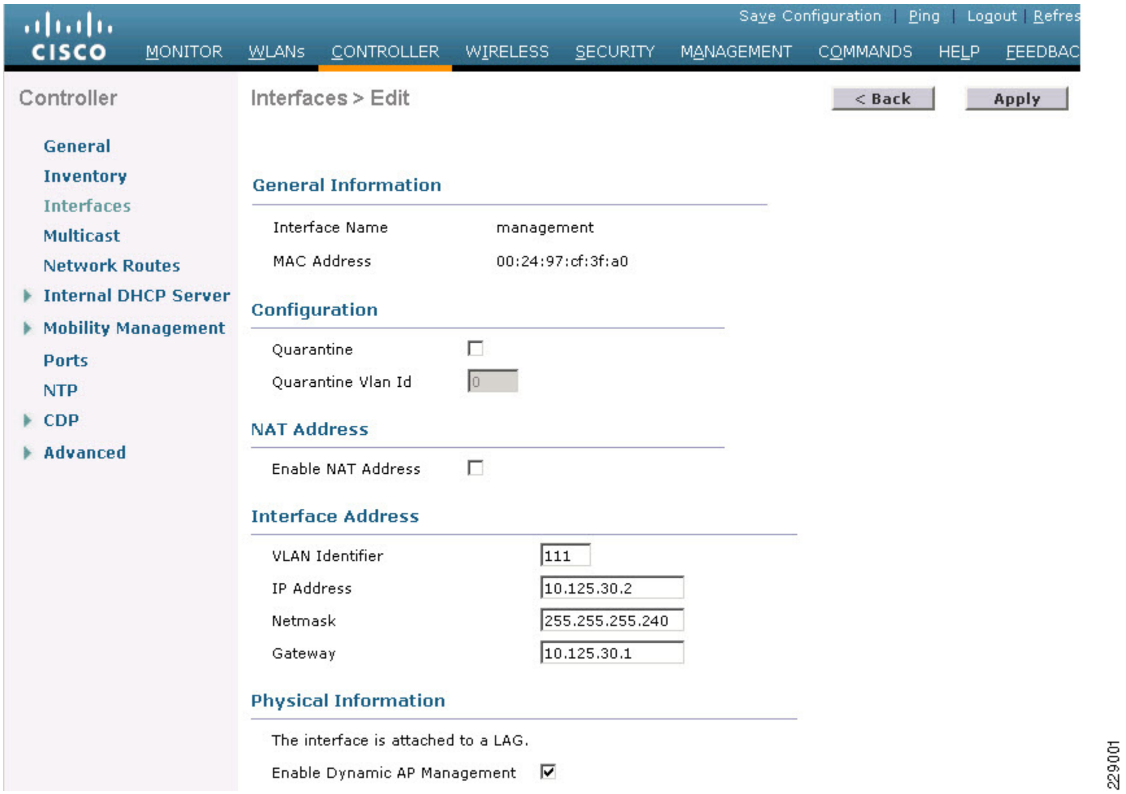


Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
staff voice	112	10.125.30.19	Dynamic	Disabled
staff data	113	10.125.30.35	Dynamic	Disabled
management	111	10.125.30.3	Static	Enabled
nac	117	10.125.30.100	Dynamic	Disabled
service-port	N/A	172.26.158.244	Static	Not Supported
virtual	N/A	1.1.1.1	Static	Not Supported

Figure 4-25 shows the management interface of WLAN controller cr23-5508-1. Note that Link Aggregation (LAG) is enabled on all the WLAN controllers used in the Medium Enterprise Design Profile mobility design.

Figure 4-25 cr23-5508-1 Management Interface



Interfaces > Edit

General Information

Interface Name management
MAC Address 00:24:97:cf:3f:a0

Configuration

Quarantine □
Quarantine Vlan Id 0

NAT Address

Enable NAT Address □

Interface Address

VLAN Identifier 111
IP Address 10.125.30.2
Netmask 255.255.255.240
Gateway 10.125.30.1

Physical Information

The interface is attached to a LAG.
Enable Dynamic AP Management ☑

Example 4-1 and Example 4-2 show examples of the switch configuration for the 3750 stack switch connecting the main WLAN controllers to the wired network.

Example 4-1 Example of WLAN Controller 3750 Stack Port Channel Configuration

```
interface Port-channel11
```

```
 description cr23-5508-1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 801
 switchport trunk allowed vlan 111-115,117,313,317
 switchport mode trunk
 switchport nonegotiate
 load-interval 30
 carrier-delay msec 0
 hold-queue 2000 in
 hold-queue 2000 out
end
```

Example 4-2 Example of WLAN Controller 3750 Stack Interface Configuration

```
interface GigabitEthernet1/0/10
 description Connected to cr23-5508-1 port Gi0/0/1 via CG#11
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 801
 switchport trunk allowed vlan 111-115,117,313,317
 switchport mode trunk
 switchport nonegotiate
 load-interval 30
 carrier-delay msec 0
 udld port
 mls qos trust cos
 channel-group 11 mode on
 hold-queue 2000 in
 hold-queue 2000 out
end

interface GigabitEthernet2/0/10
 description Connected to cr23-5508-1 port Gi0/0/2 via CG#11
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 801
 switchport trunk allowed vlan 111-115,117,313,317
 switchport mode trunk
 switchport nonegotiate
 load-interval 30
 carrier-delay msec 0
 udld port
 mls qos trust cos
 channel-group 11 mode on
 hold-queue 2000 in
 hold-queue 2000 out
end
```

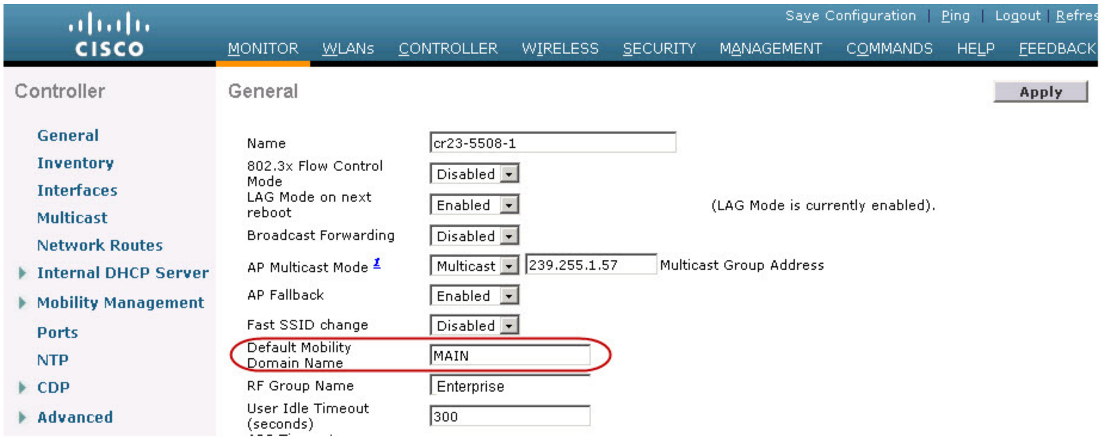
Remote Site

The remote site WLAN controller and wired network connection is the same as that used in the main site. In other words, WLAN controller is connected to a 3750E stack that acts as a services block for the remote site. The configuration is the same; therefore, the details are not duplicated here.

Mobility Groups

The primary purpose of a Mobility Group in the Cisco Unified Wireless Network (CUWN) is to share client information between WLAN controllers. This helps to ensure seamless mobility when clients roam between APs that are connected to WLAN controllers within the same Mobility Group. The default Mobility Group Name is created in the Controller General configuration page, as shown in Figure 4-26.

Figure 4-26 cr23-5508-1 Mobility Group Definition



General

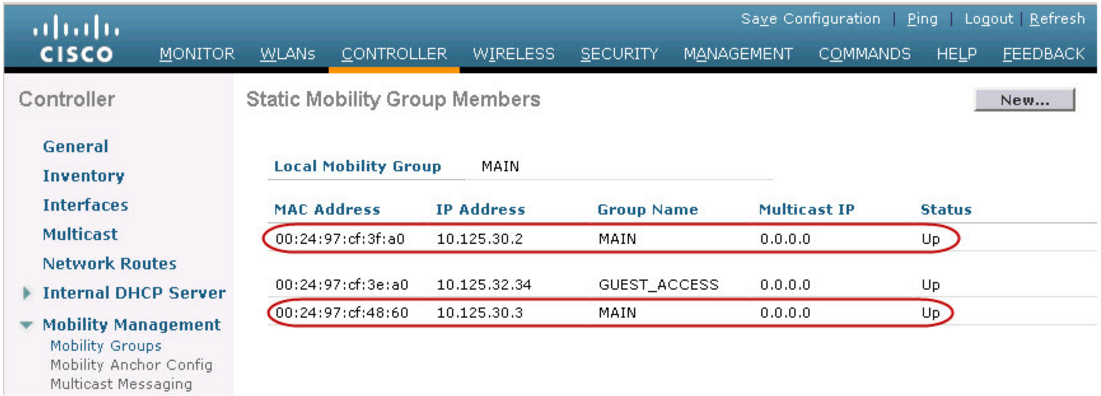
Name	cr23-5508-1	
802.3x Flow Control Mode	Disabled	
LAG Mode on next reboot	Enabled	(LAG Mode is currently enabled).
Broadcast Forwarding	Disabled	
AP Multicast Mode [1]	Multicast 239.255.1.57	Multicast Group Address
AP Fallback	Enabled	
Fast SSID change	Disabled	
Default Mobility Domain Name	MAIN	
RF Group Name	Enterprise	
User Idle Timeout (seconds)	300	

The default Mobility Domain Name is automatically entered in the Mobility Group membership for that controller, along with the necessary IP address and MAC address information for that controller. The IP address and MAC address information of other controllers in that Mobility Group must be entered manually.

Figure 4-27 and Figure 4-28 show the Mobility Group membership information for both main site WLAN controllers. It can be seen that the Mobility Group membership has two main members for the two WLAN controllers that are providing WLAN access within the main site. These WLAN controllers are also members of another Mobility Group GUEST_ACCESS. This Mobility Group has been configured to provide guest access tunneling and is discussed later in this chapter.

The remote site WLAN controller Mobility Group membership configuration uses a different mobility group name, and does not include either of the main site WLAN controllers. The reason for it not including either of the main site WLAN controllers is because it is not expecting to support seamless roaming between the remote site and main site. There is no point of providing seamless roaming between controllers when there is no seamless WLAN coverage between APs connected to those controllers. Because this design includes supporting guest access tunneling for users at the remote site, the GUEST_ACCESS mobility group-member information also appears on the remote site WLAN controller.

Figure 4-27 cr23-5508-1 Mobility Group Members

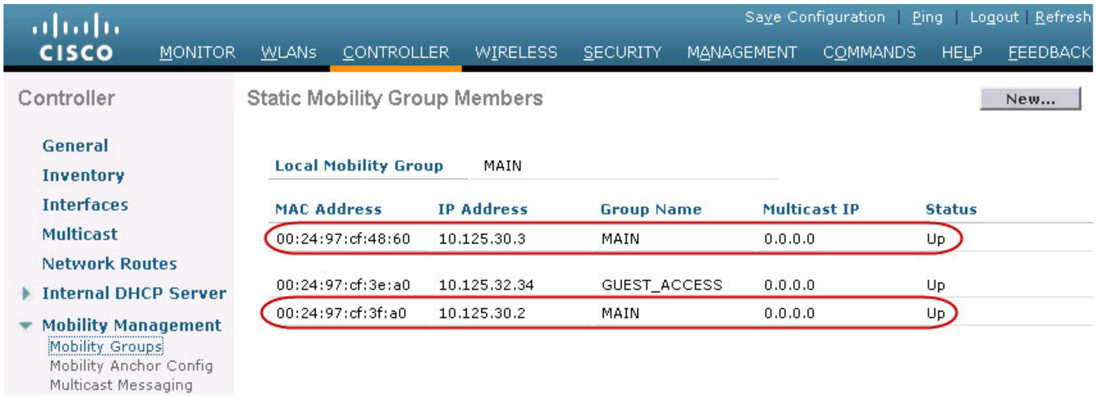


Static Mobility Group Members

Local Mobility Group MAIN

MAC Address	IP Address	Group Name	Multicast IP	Status
00:24:97:cf:3f:a0	10.125.30.2	MAIN	0.0.0.0	Up
00:24:97:cf:3e:a0	10.125.32.34	GUEST_ACCESS	0.0.0.0	Up
00:24:97:cf:48:60	10.125.30.3	MAIN	0.0.0.0	Up

Figure 4-28 cr23-5508-2 Mobility Group Members



Static Mobility Group Members

Local Mobility Group MAIN

MAC Address	IP Address	Group Name	Multicast IP	Status
00:24:97:cf:48:60	10.125.30.3	MAIN	0.0.0.0	Up
00:24:97:cf:3e:a0	10.125.32.34	GUEST_ACCESS	0.0.0.0	Up
00:24:97:cf:3f:a0	10.125.30.2	MAIN	0.0.0.0	Up

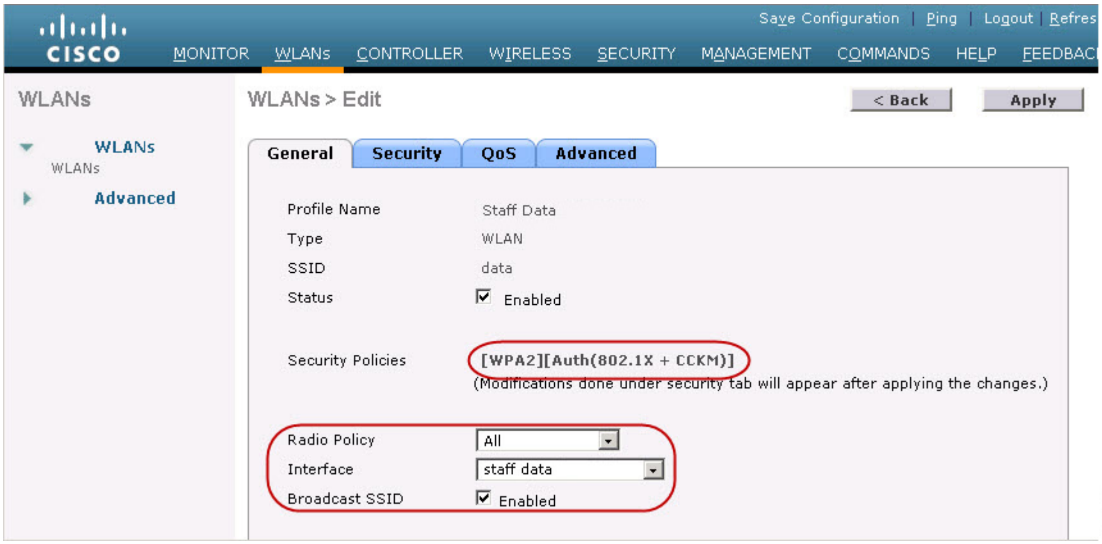
229004

WLAN Configuration

Staff Data WLAN

Figure 4-29 shows the general WLAN configuration for the staff data WLAN network. The key point to note on this tab is the security policy that has been set under the security tab, and the WLAN controller interface that the WLAN has been mapped to. The security configuration recommended is to use WPA2 with 802.1X+CCKM. Most WLAN clients should now support WPA2, and CCKM has been added to 802.1X as it provides faster roaming for WLAN clients that support CCKM, while using the AAA features of 802.1X to secure the WLAN connection.

Figure 4-29 Staff Data WLAN



WLANs > Edit

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

229398

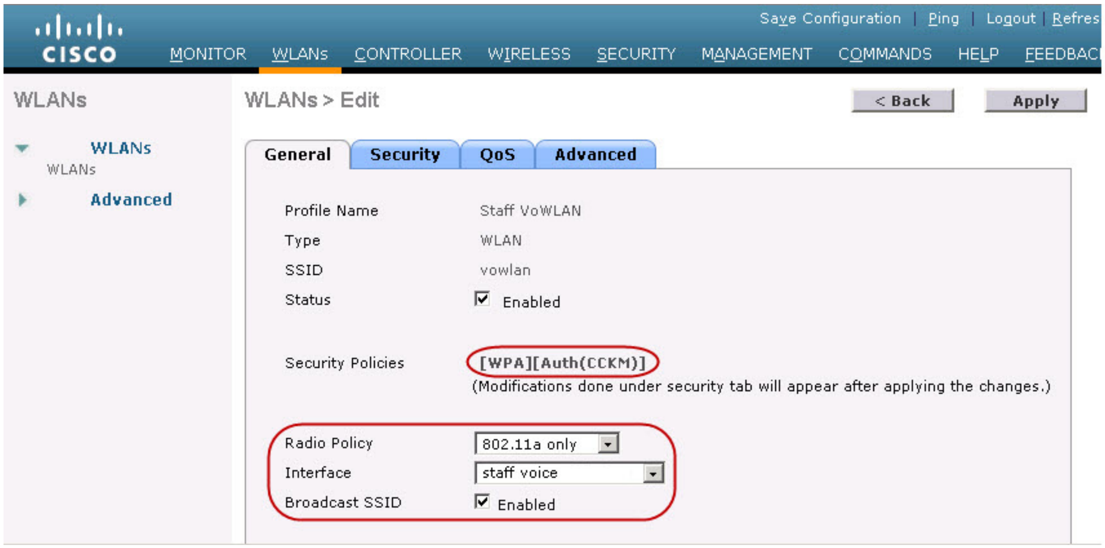
Apart from setting DHCP as required in the advanced settings, the remainder of the WLAN configuration uses default settings. Unless static IP address are needed, obtaining IP addresses using DHCP is recommended as a best practice.

Staff Voice WLAN

Figure 4-30 shows the general WLAN configuration for the Staff VoWLAN network. The key point to note on this tab is the security policy that has been set under the security tab, and the WLAN controller interface that the WLAN has been mapped to. The security configuration recommended is to use WPA with CCKM. The VoWLAN clients (7921 and 7925) support WPA and CCKM. CCKM provides optimal roaming performance for voice calls, and the level of security provided by Enterprise WPA is sufficient for VoWLAN traffic. The radio policy of this WLAN is to use the 5GHz (802.11a) band for VoWLAN support, in order to ensure optimal VoWLAN capacity and performance.

The QoS requirements for the WLAN are that it be set for the platinum profile and that WMM be required. Apart from the QoS differences, the remainder of the WLAN configuration is the same as the "Staff Data WLAN" section on page 4-45.

Figure 4-30 Staff Voice WLAN



Profile Name Staff VoWLAN
Type WLAN
SSID vowlan
Status ☑ Enabled

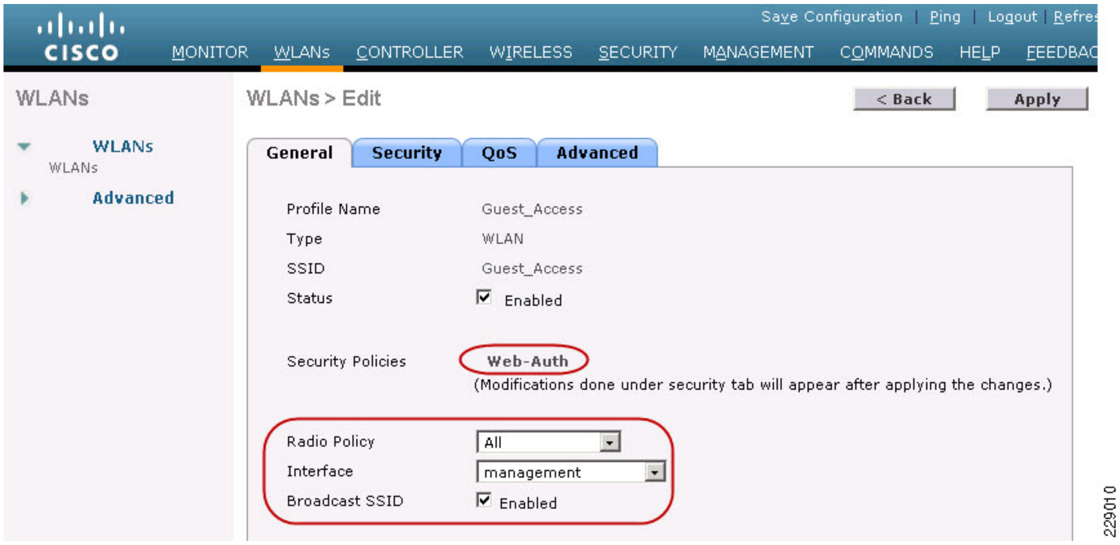
Security Policies [WPA][Auth(CCKM)]
(Modifications done under security tab will appear after applying the changes.)

Radio Policy 802.11a only
Interface staff voice
Broadcast SSID ☑ Enabled

Guest Access WLAN

Although the configuration for the Guest WLAN indicates that it has been assigned to the management interface, the true interface used by the Guest WLAN is on the anchor WLAN controller that is located in the DMZ. The WLAN client traffic from the Guest WLAN is tunneled by the WLAN controller to the anchor WLAN.

Figure 4-31 Guest WLAN


CISCO
Save Configuration | Ping | Logout | Refres
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBAC
WLANs
WLANs
WLANs
Advanced
< Back
Apply
General
Security
QoS
Advanced
229010

WLANs > Edit

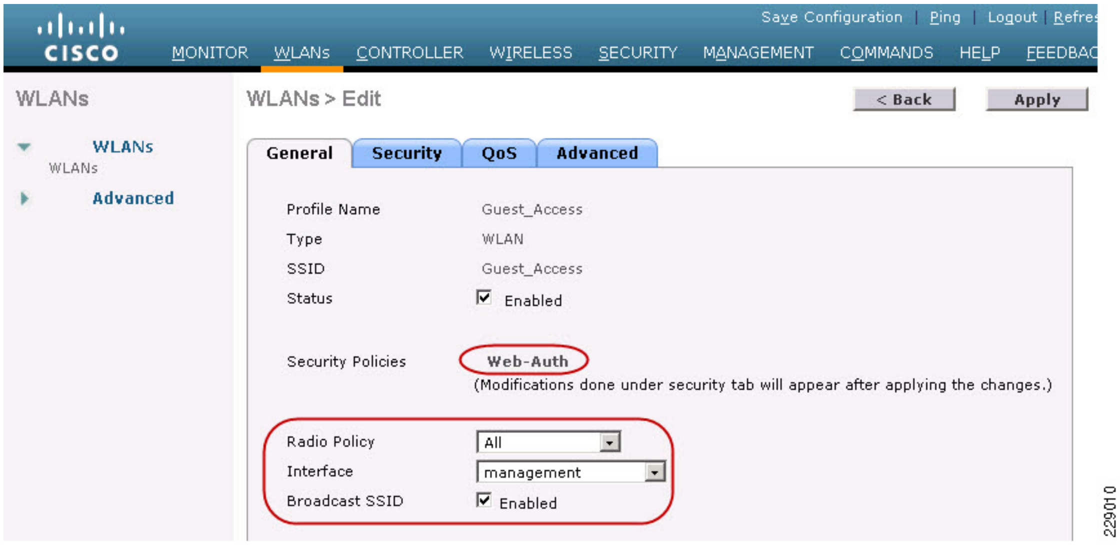
Profile Name Guest_Access
Type WLAN
SSID Guest_Access
Status ☑ Enabled

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

Radio Policy All
Interface management
Broadcast SSID ☑ Enabled

Figure 4-32 and Figure 4-33 show the first steps in configuring Guest Access Tunneling for the WLAN, namely, the creation of a mobility anchor for the Guest WLAN. The address chosen for the mobility anchor is the management address of the anchor WLAN controller that is located in the DMZ.

Figure 4-32 WLAN Mobility Anchor Selection


CISCO
Save Configuration | Ping | Logout | Refres
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBAC
WLANs
WLANs
WLANs
Advanced
< Back
Apply
General
Security
QoS
Advanced
229010

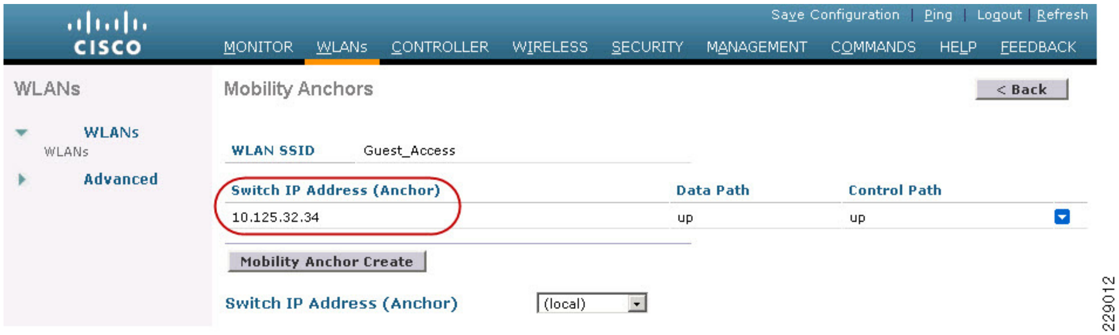
WLANs > Edit

Profile Name Guest_Access
Type WLAN
SSID Guest_Access
Status ☑ Enabled

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

Radio Policy All
Interface management
Broadcast SSID ☑ Enabled

Figure 4-33 Mobility Anchor Selection



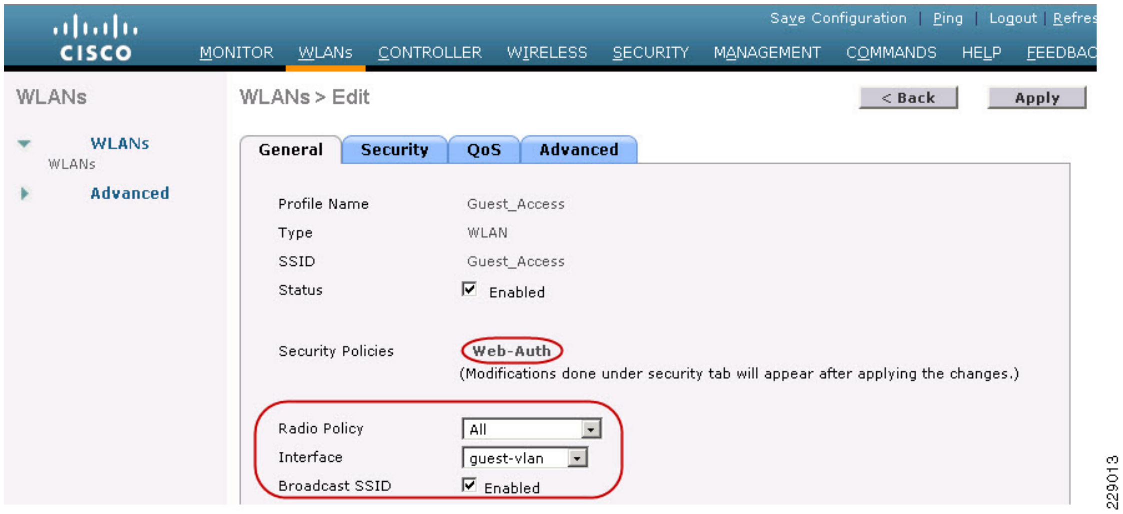
WLAN SSID Guest_Access

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

Switch IP Address (Anchor) (local)

Figure 4-34 shows the DMZ anchor Guest WLAN configuration. The WLAN configuration must be exactly the same as the home controller, except that it has a real local interface, and shown in Figure 4-34 and Figure 4-35.

Figure 4-34 Anchor Guest WLAN

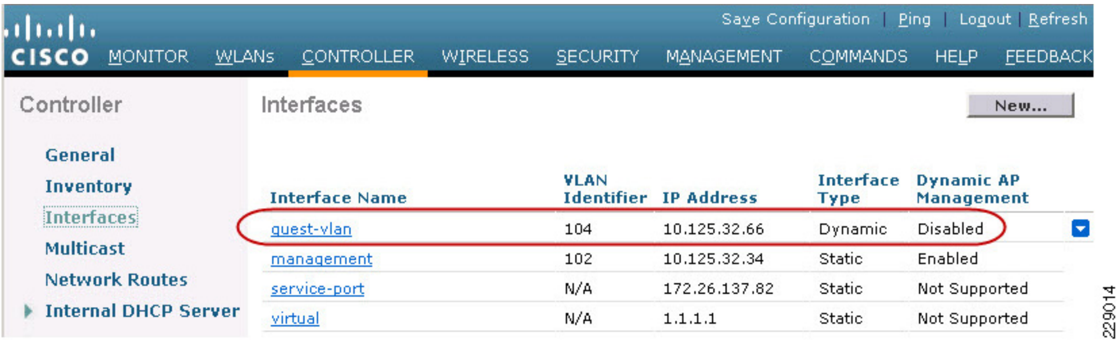


Profile Name Guest_Access
Type WLAN
SSID Guest_Access
Status ☑ Enabled

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

Radio Policy All
Interface guest-vlan
Broadcast SSID ☑ Enabled

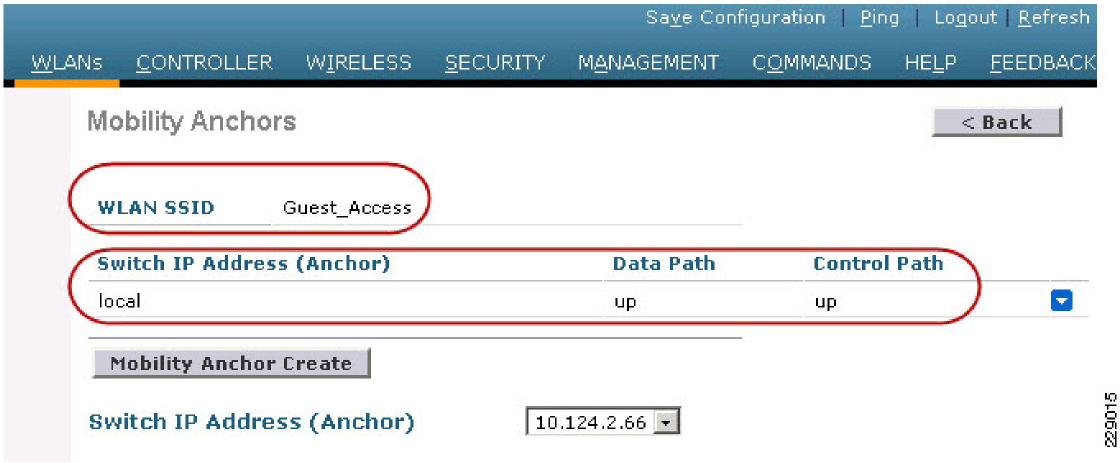
Figure 4-35 Anchor WLAN Controller Interfaces



Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
guest-vlan	104	10.125.32.66	Dynamic	Disabled
management	102	10.125.32.34	Static	Enabled
service-port	N/A	172.26.137.82	Static	Not Supported
virtual	N/A	1.1.1.1	Static	Not Supported

The WLAN on the DMZ anchor WLAN controller must also be configured with a mobility anchor, but in this case the Mobility Anchor is its own local management address, as shown in Figure 4-36.

Figure 4-36 Anchor Guest WLAN Mobility Anchor


Save Configuration | Ping | Logout | Refresh
WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
< Back
Mobility Anchor Create
229015

Mobility Anchors

WLAN SSID Guest_Access

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

Switch IP Address (Anchor) 10.124.2.66

WLAN QoS

The Cisco Unified Wireless Network (CUWN) prioritizes traffic based on the QoS profiles applied to each WLAN, but it does not change the IP QoS classification (DSCP) of the client traffic. This means that client traffic leaving the CUWN may need to be reclassified based on the network QoS policy. There are two ways to achieve this reclassification:

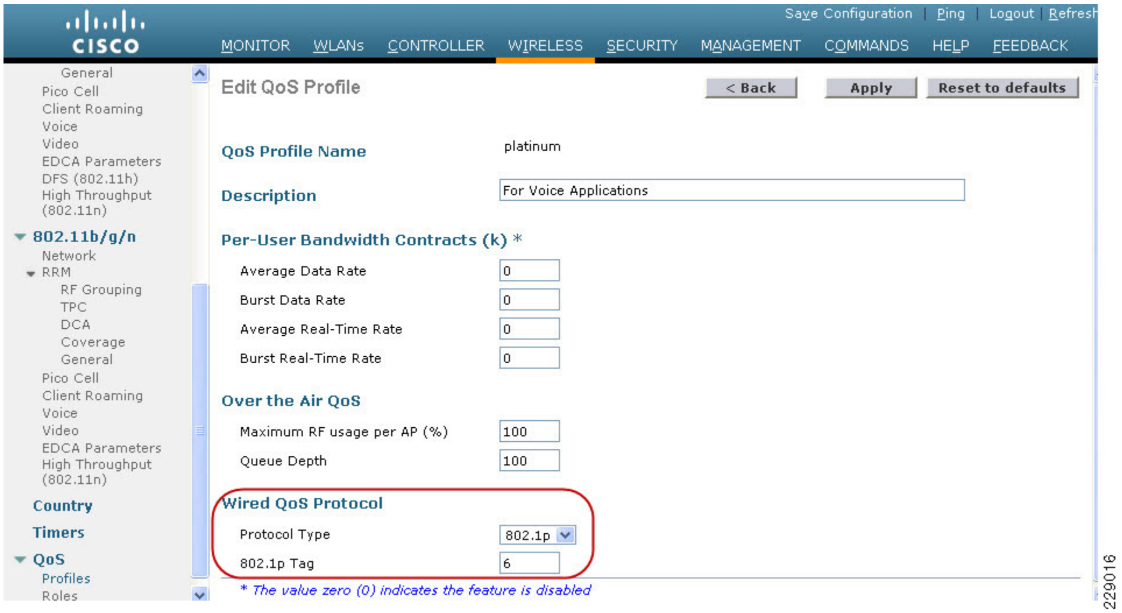
1. Applying policy at each of the network SVIs that connect the WLAN controller to the network.
2. Learning the QoS policy that was applied within the CUWN, because this should be aligned with the network policy.

The latter method is preferable as it requires less configuration and less policy maintenance (the policy only needs to be maintained on WLAN controllers and not on the connected switches as well). To achieve this, each of the four QoS profiles (platinum, gold, silver and bronze) on the WLAN controller must have its Wired QoS Protocol Type set to 802.1p. All other QoS profile settings can remain at the defaults (an example is shown in Figure 4-37). This procedure configures the WLAN controller to set the 802.1p marking of the frames sent from the WLAN controller to reflect QoS policy for that WLAN. For example, if the IP packet was from a platinum WLAN and had a DSCP value of EF, the WLAN controller would use a CoS of 5 in the frame header. If the same packet had been on a silver WLAN, the CoS value assigned would be 0. Therefore, as long as the WLAN controller is connected to a switch network that is configured to trust CoS and maintain a translation table between CoS and DSCP for its network, the translation between CUWN policy and network policy will occur automatically.

For more information on WLAN QoS refer to the *Voice over WLAN Design Guide* at the following URL:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/vowlan/41dg/vowlan41dg-book.html

Figure 4-37 Wired QoS Protocol Configuration



Edit QoS Profile

QoS Profile Name: platinum

Description: For Voice Applications

Per-User Bandwidth Contracts (k) *

Average Data Rate: 0

Burst Data Rate: 0

Average Real-Time Rate: 0

Burst Real-Time Rate: 0

Over the Air QoS

Maximum RF usage per AP (%): 100

Queue Depth: 100

Wired QoS Protocol

Protocol Type: 802.1p

802.1p Tag: 6

* The value zero (0) indicates the feature is disabled

Access Point Configuration

The configuration and software management of Cisco Unified Wireless Network access points is determined by the WLAN controller they ultimately join. Therefore, establishing the connection between APs and the correct WLAN controller is a key component of the design.

The CUWN provides many different options to allow APs to discover the correct WLAN controller (DHCP, DNS, over the air, or static configuration). These are detailed in the *Deploying Cisco 440X Series Wireless LAN Controllers* document at the following URL:

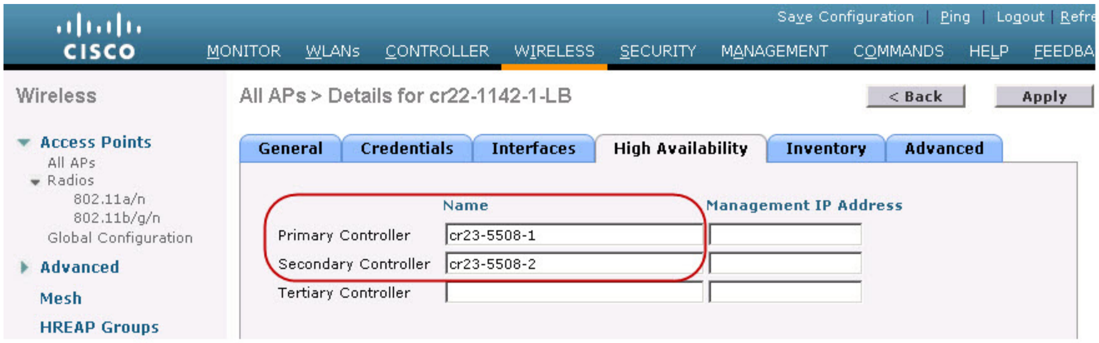
http://www.cisco.com/en/US/partner/docs/wireless/technology/controller/deployment/guide/dep.html

For the purposes of testing in this design, the APs used DHCP to discover a WLAN controller appropriate for their location. The configuration of DHCP for APs is discussed in the *DHCP OPTION 43 for Lightweight Cisco Aironet Access Points Configuration Example* document at the following URL:

http://www.cisco.com/en/US/partner/tech/tk722/tk809/technologies_configuration_example09186a00808714fe.shtml

Once an AP is in communication with a WLAN controller that has been defined using a discovery mechanism, it learns about all of the WLAN controllers in the default mobility group of the discovered WLAN controller. An AP can be configured for preferred primary, secondary, and tertiary WLAN controllers within that mobility group. Figure 4-38 shows an example of this where the AP is configured with its preferred WLAN controller (primary controller), and its preferred fail over WLAN controller (secondary controller).

Figure 4-38 AP Controller Preferences


Save Configuration | Ping | Logout | Refre
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBA
Wireless
Access Points
All APs
Radios
802.11a/n
802.11b/g/n
Global Configuration
Advanced
Mesh
HREAP Groups
< Back
Apply
General Credentials Interfaces High Availability Inventory Advanced
229017

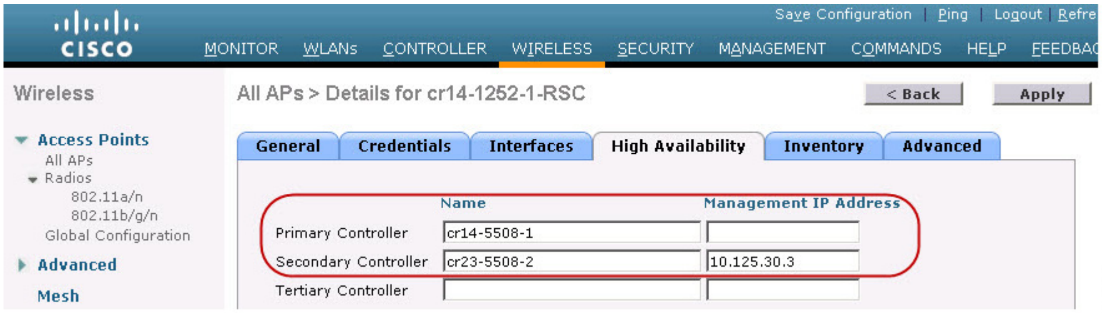
All APs > Details for cr22-1142-1-LB

	Name	Management IP Address
Primary Controller	cr23-5508-1	
Secondary Controller	cr23-5508-2	
Tertiary Controller		

The configuration of access point WLAN controller preference will determine the fail over models for the WLAN deployment. For example, all the APs on the site could be configured to prefer one WLAN controller as primary, with the other WLAN controller used solely as a back-up controller. An alternative configuration would be to spread the AP load across both WLAN controllers, on a per building basis, thereby ensuring that all controllers are actively engaged in passing traffic. The advantage of this approach is that a developing controller failure would potentially be discovered more readily if both controllers were always actively carrying some degree of traffic load, rather than with one of them sitting idle.

In situations where the APs are expected to fail over to a WLAN controller outside of its primary WLAN controllers mobility group, the AP must be configured with the IP address and name of that fail over WLAN controller, rather than just the WLAN controller name. An example of this configuration, from the remote site, is shown in Figure 4-39.

Figure 4-39 AP Failover to a WLAN Controller Outside the Mobility Group


Save Configuration | Ping | Logout | Refre
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBAC
Wireless
Access Points
All APs
Radios
802.11a/n
802.11b/g/n
Global Configuration
Advanced
Mesh
< Back
Apply
General Credentials Interfaces High Availability Inventory Advanced
229018

All APs > Details for cr14-1252-1-RSC

	Name	Management IP Address
Primary Controller	cr14-5508-1	
Secondary Controller	cr23-5508-2	10.125.30.3
Tertiary Controller		

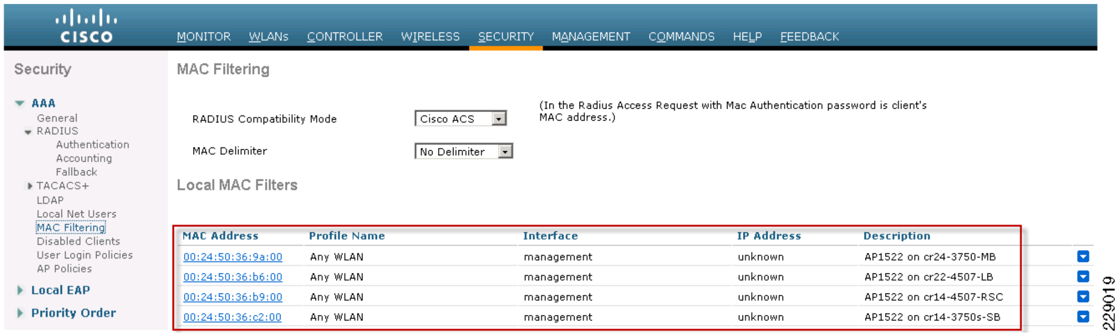
AP 1520 Configuration

AP1520 access points require somewhat further configuration over and above what has been shown in the preceding paragraphs. By default, AP1520 access points are configured for outdoor mesh operation, and in order to use these access points to provide outdoor coverage as root access points, some basic configuration changes must be implemented.

Adding the AP1520 MAC Address to the WLAN Controller

AP1520 series access points will not join a WLAN controller unless the MAC address of the access point has been defined to the WLAN controller. This can be done by adding the BVI MAC of the access point (this is the MAC address printed on a label on the outside of the access point) via the **Security > AAA > MAC Filtering** GUI panel, as shown in Figure 4-40.

Figure 4-40 Adding the AP1520 MAC Address to the WLAN Controller



MAC Filtering

RADIUS Compatibility Mode: Cisco ACS

(In the Radius Access Request with Mac Authentication password is client's MAC address.)

MAC Delimiter: No Delimiter

Local MAC Filters

MAC Address	Profile Name	Interface	IP Address	Description
00:24:50:36:9a:00	Any WLAN	management	unknown	AP1522 on cr24-3750-MB
00:24:50:36:b6:00	Any WLAN	management	unknown	AP1522 on cr22-4507-LB
00:24:50:36:b9:00	Any WLAN	management	unknown	AP1522 on cr14-4507-RSC
00:24:50:36:c2:00	Any WLAN	management	unknown	AP1522 on cr14-3750s-SB

Note that MAC addresses must be defined to all WLAN controllers that an AP1520 access point may join. This includes not only WLAN controllers defined as primary controllers, but any WLAN controllers that are defined as secondary or tertiary as well.

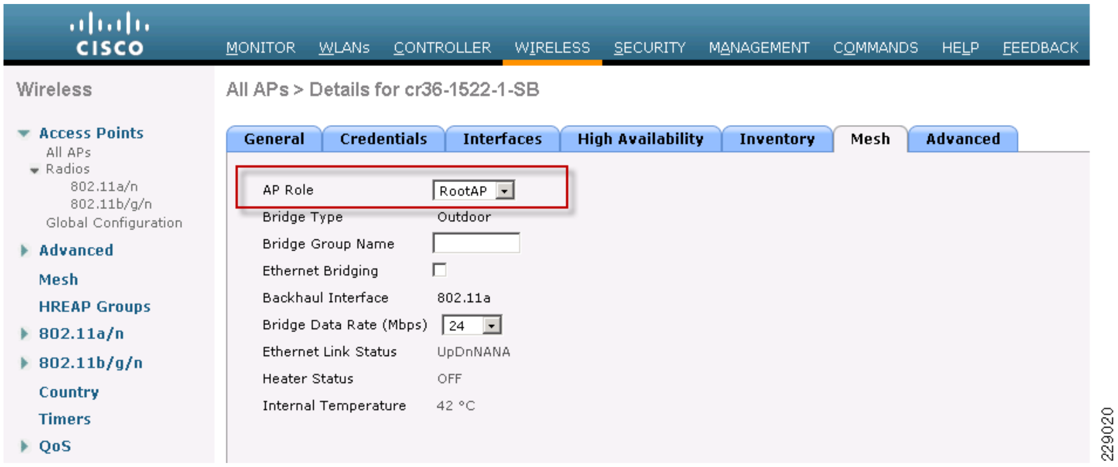
You can also validate the MAC addresses of AP1520 access points externally using Cisco ACS. For complete details on how to do this, refer to the *Cisco Wireless Mesh Access Points Design and Deployment Guide*, Release 6.0 at the following URL:
http://www.cisco.com/en/US/docs/wireless/technology/mesh/design/guide/MeshAP_60.html#wp1194149

Configuring the AP1520 as a Root Access Point (RAP)

AP1520 series access points are shipped with a default outdoor Mesh Access Point (MAP) configuration. In the Medium Enterprise Design Profile mobility design, the AP1520 series access point is used as an outdoor root access point (RAP)[1]. In order to reconfigure the AP1520 to be a RAP, once the access point has joined the controller, the AP role is changed to “RootAP” in the **Wireless > Access Points > All APs > Details > Mesh** configuration panel on the WLAN controller, as shown in Figure 4-41. None of the other parameters need to be changed on this screen.

[1] MAPs and RAPs are explained in much more detail in the *Cisco Wireless Mesh Access Points Design and Deployment Guide*, Release 6.0 at the following URL:
http://www.cisco.com/en/US/docs/wireless/technology/mesh/design/guide/MeshAP_60.html#wp1194149

Figure 4-41 Setting the AP Role



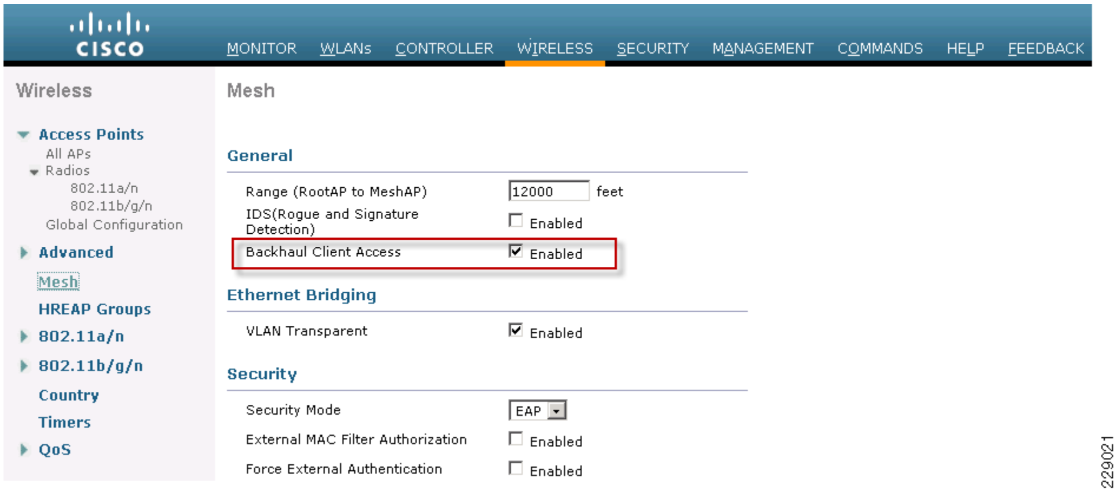
All APs > Details for cr36-1522-1-SB

AP Role: RootAP
Bridge Type: Outdoor
Bridge Group Name:
Ethernet Bridging: □
Backhaul Interface: 802.11a
Bridge Data Rate (Mbps): 24
Ethernet Link Status: UpDnNANA
Heater Status: OFF
Internal Temperature: 42 °C

5 GHz Backhaul Client Access

By default, the 5 GHz radio interface on the AP1522 is enabled only as a back haul interface, and will not allow any 5 GHz clients to associate. In order to enable the use of this interface for 5 GHz client traffic, it must be enabled using the Back haul Client Access check box on the WLAN controller's **Wireless > Mesh** configuration panel, as shown in Figure 4-42. Enabling this once on the WLAN controller enables back haul client access for all AP1520 series access points that join this controller.

Figure 4-42 Enabling Backhaul Client Access



Mesh

General
Range (RootAP to MeshAP): 12000 feet
IDS(Rogue and Signature Detection): □ Enabled
Backhaul Client Access: ☑ Enabled

Ethernet Bridging
VLAN Transparent: ☑ Enabled

Security
Security Mode: EAP
External MAC Filter Authorization: □ Enabled
Force External Authentication: □ Enabled

Primary Backhaul Scanning

Under normal circumstances, an AP1520 configured as a root AP (RAP) communicates with the WLAN controller via its wired Ethernet interface. However, if the Ethernet port is "down" on a RAP, or a RAP fails to connect to a controller when its Ethernet port is "up", the AP1520 will attempt to use the 5 GHz radio interface as the primary backhaul for 15 minutes. Failing to find another AP1520 neighbor or failing to connect to a WLAN controller via the 5 GHz interface causes the AP1520 to begin to scan for reassignment of the primary backhaul, beginning with the Ethernet interface.

In most cases we did not find this behavior to cause any issues in our validation and we recommend that it be left as is. We found this behavior beneficial in that should a switch port for an AP 1520 series access point go down, the connected AP1520 can establish a connection to another AP1520 in the same building or at an adjacent building using the 5 GHz backhaul. This can be especially useful if the neighbor AP1520 is attached to the wired network via a different Ethernet switch. Within 15 minutes of the failed Ethernet port being repaired, the AP1520 should revert back to operation over the Ethernet connection.

If you do not wish to allow primary backhaul scanning, you may either:

- Disable the use of 5 GHz entirely on the AP1520 series access point. In this case, backhaul operation will not occur over any wireless medium (2.4 GHz is never used for backhaul purposes by the AP1520). This is an acceptable alternative if there is no need to support 5 GHz clients within the outdoor perimeter of the buildings where AP1520s are installed.
- Use AP 1250 access points installed within traditional weatherproof outdoor NEMA-rated enclosures (supplied by Cisco partners) to provide outdoor coverage.

WCS Configuration

Configuring WCS to allow basic management of WLAN controllers for each site in the Medium Enterprise Design Profile mobility design is a relatively straightforward process. After installing WCS in the main site, each WLAN controller must be added to WCS, as described in the *Cisco Wireless Control System Configuration Guide* at the following URL:

http://www.cisco.com/en/US/docs/wireless/wcs/6.0/configuration/guide/6_0ctrlcfg.html#wp1041451

Once the WLAN controllers are properly defined and reachable from WCS, the network administrator can begin to use the multitude of configuration, monitoring, and reporting options available under the WCS to begin to manage not only the WLAN controllers themselves, but the access points and devices that connect through them. These capabilities are far too numerous to be described here, but a comprehensive description of these capabilities and how to enable them can be found in the *Cisco Wireless Control System Configuration Guide*, at the above URL.

WCS Users and User Groups

By default, WCS provides for a single root user, which allows access to all WCS functions. The password for this root user should be protected and only known by those who are responsible for the overall Medium Enterprise Design Profile mobility design and with a real need to know (for example, those personnel responsible for the actual installation, maintenance, and detailed administration of WCS). For these users and others who require routine administrative access to WCS, alternate user credentials should be created, with administrative access granted and privileges assigned as necessary via the use of appropriate WCS user groups settings. Chapter 7 of the *Cisco Wireless Control System Configuration Guide*, Release 6.0 (http://www.cisco.com/en/US/docs/wireless/wcs/6.0/configuration/guide/6_0manag.html) provides comprehensive instructions for configuring users and group privileges on the WCS server. This chapter also contains a complete listing of the user groups available in WCS as well as the privileges contained in each group.

Common sense should be used when assigning user privileges. For example, while only a very small set of key technical personnel should have access to the actual WCS root user ID and password, you may wish to assign the ability to make WCS configuration changes to a somewhat larger audience. This larger group can be assigned as WCS “admin” users or assigned to the “superuser” group. Most users who are only interested in viewing the information available to them on WCS will not need more than the ability to simply monitor network activity in WCS. For these users, the privileges accorded to them by the WCS System Monitoring or Monitor Lite user groups may be all that is required, depending upon the specific WCS monitoring functions you wish to grant those users.

WCS Virtual Domains

While WCS user groups define the WCS functionality users have been granted, WCS virtual domains allow the network administrator logically partition the WCS management domain and limit management access. In this way, the group of resources that the WCS functionality assigned to a user group may be exercised against is restricted. A WCS virtual domain consists of a set of assigned devices and maps, and restricts a user's scope to only information that is relevant to those devices and maps. Through an assigned virtual domain, users are only able to use WCS functionality against a predefined subset of the devices managed by WCS.

Users can be assigned one or more virtual domains; however, only one assigned virtual domain may be active for a user at WCS login. The user can change the current virtual domain in use by selecting a different permitted virtual domain using the WCS Virtual Domain drop-down menu.

The WCS virtual domain can be used to limit the user's ability to even view certain resources inside the WCS that are not contained in their active assigned virtual domain. For example, the site manager for a medium enterprise may have the ability to view and report on certain characteristics of wireless assets for his site due to his WCS user account being assigned to an appropriate user group permitting this level of WCS functionality. However, the virtual domain that this site manager is assigned to may only allow such functionality to be exercised against these assets if they are located within his site. Thus, if the site manager for site “A” attempted to use WCS to discover or manage wireless infrastructure located in site “B”, his assigned virtual domain might not allow the ability to manage or even view resources on site “B”.

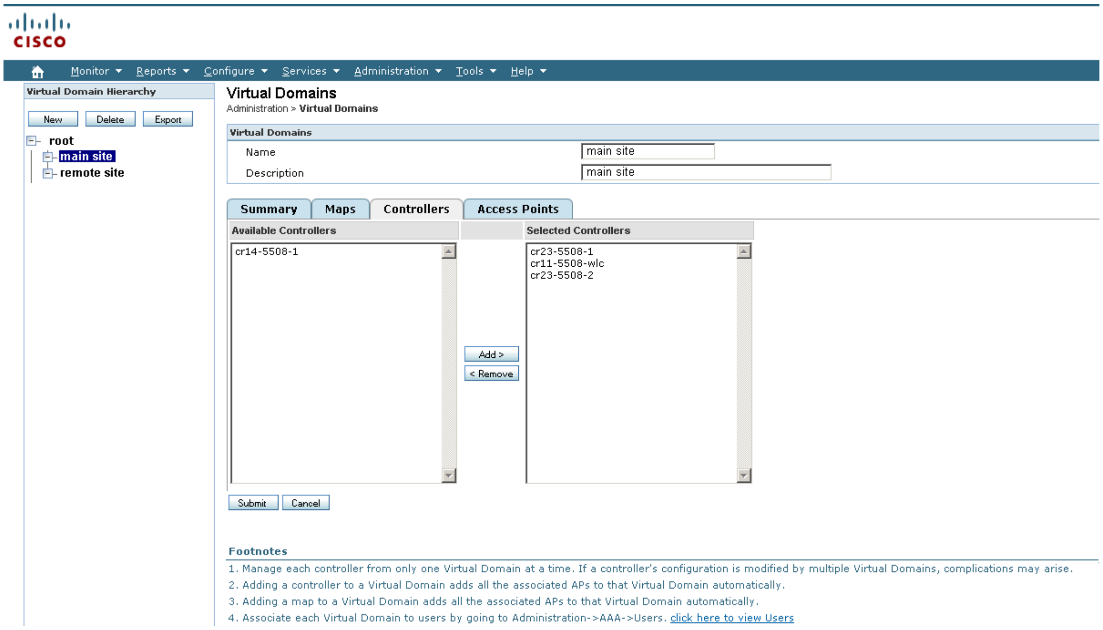
Administrative personnel with system-wide responsibilities, on the other hand, could be assigned a virtual domain that includes all resources in the system (i.e., all sites), and could exercise the functionality assigned to them by their WCS user group against any of these resources. In this way, WCS virtual domain assignment can be useful in prevent unnecessary inter-site WCS traffic, especially traffic whose nature might be based more upon curiosity rather than actual need.

Note WCS user groups assign what actions a user can take against a resource, whereas WCS virtual domains determine what resources those user-group actions can be applied towards.

There are two basic steps necessary to enable the use of virtual domains within WCS:

1. A virtual domain must be created, and we must assign the resources we wish to include in the virtual domain. Figure 4-43 provides an illustration of how controller resources were assigned during lab testing for the “main site” virtual domain.

Figure 4-43 Assigning WLAN Controller Resources to the Main Site Virtual Domain



Virtual Domains
Administration > Virtual Domains

Virtual Domains

Name: main site
Description: main site

Available Controllers	Selected Controllers
cr14-5508-1	cr23-5508-1 cr11-5508-wlc cr23-5508-2

Footnotes

1. Manage each controller from only one Virtual Domain at a time. If a controller's configuration is modified by multiple Virtual Domains, complications may arise.
2. Adding a controller to a Virtual Domain adds all the associated APs to that Virtual Domain automatically.
3. Adding a map to a Virtual Domain adds all the associated APs to that Virtual Domain automatically.
4. Associate each Virtual Domain to users by going to Administration->AAA->Users. click here to view Users

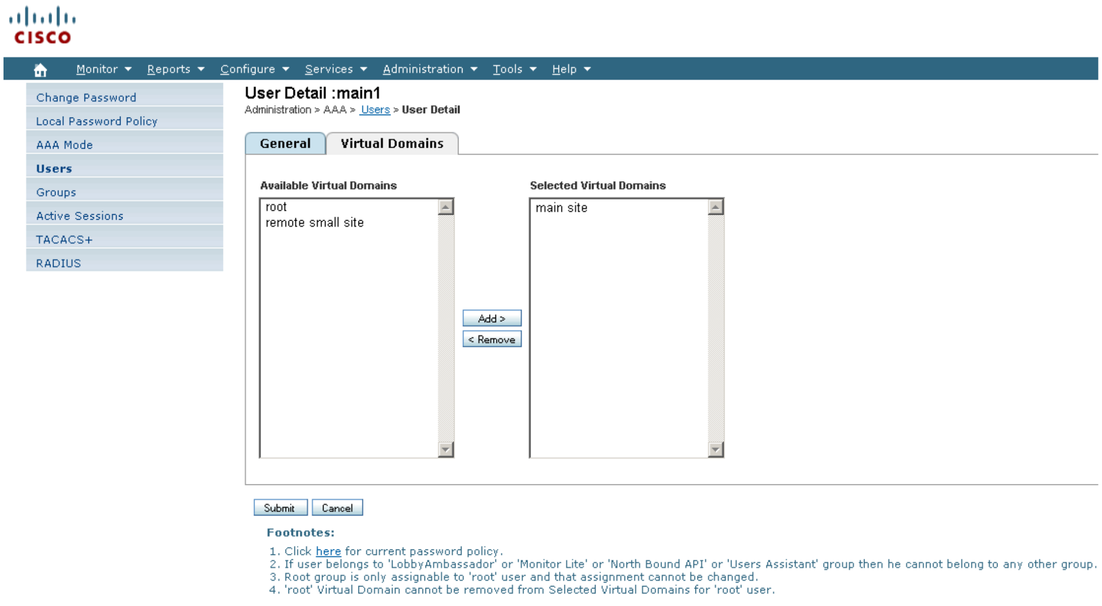
The process for creating and assigning network resources to the virtual domain is detailed in "Chapter 20, "Virtual Domains" of the *WCS Configuration Guide,* Release 6.0, found at the following URL:

http://www.cisco.com/en/US/docs/wireless/wcs/6.0/configuration/guide/6_0virtual.html#wp1040002

2. The virtual domain must be assigned to the user. The process for assigning the main site virtual domain to the "main1" user is shown in Figure 4-44. This process is detailed in a step-by-step fashion in "Chapter 7, Managing WCS User Accounts" at the following URL:

http://www.cisco.com/en/US/docs/wireless/wcs/6.0/configuration/guide/6_0manag.html#wp1097733

Figure 4-44 Assigning the Virtual Domain to a User



User Detail :main1
Administration > AAA > Users > User Detail

Available Virtual Domains	Selected Virtual Domains
root remote small site	main site

Footnotes:

1. Click here for current password policy.
2. If user belongs to 'LobbyAmbassador' or 'Monitor Lite' or 'North Bound API' or 'Users Assistant' group then he cannot belong to any other group.
3. Root group is only assignable to 'root' user and that assignment cannot be changed.
4. 'root' Virtual Domain cannot be removed from Selected Virtual Domains for 'root' user.

Note It is important to note that in Release 6.0, non-root WCS virtual domain users cannot access WCS functions listed under the **Services > Mobility Services** main menu. This includes wired-switch and device location. Refer to Understanding Virtual Domains as a User, WCS Configuration Guide 6.0 http://www.cisco.com/en/US/docs/wireless/wcs/6.0/configuration/guide/6_0virtual.html#wp1120787 for a complete list of WCS functions that are not available in non-root virtual domains.

Additional information on creating WCS users, user groups, and virtual domains can be found in the "Context-Aware Service Design" chapter of the *Cisco Service Ready Architecture for Schools Design Guide* at the following URL*:*
http://cisco.com/en/US/docs/solutions/Enterprise/Education/SchoolsSRA_DG/SchoolsSRA_chap6.html#wp1054537

Reference Documents

A cornerstone of a successful design relies on the knowledge of established best practices. Thus, it is highly recommended that you become familiar with the following general best practice deployment recommendations for Cisco Unified Wireless Networks:

- *Enterprise Mobility Design Guide 4.1*
  http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.html
- *Cisco 802.11n Design and Deployment Guidelines*
  http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns348/ns767/white_paper_80211n_design_and_deployment_guidelines.html
- *Voice over Wireless LAN 4.1 Design Guide*
  http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/vowlan/41dg/vowlan41dg-book.html
- *Cisco Radio Resource Management*
  http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a008072c759.shtml
- *Cisco Wireless Mesh Access Point Design and Deployment Guide*, Release 6.0
  http://www.cisco.com/en/US/docs/wireless/technology/mesh/design/guide/MeshAP_60.html

A successful deployment also involves strong knowledge of how to set key infrastructure configuration procedures. The following documents provide comprehensive configuration guidance and should be referenced as needed:

- *Cisco Wireless LAN Controller Configuration Guide*, Release 6.0
  http://www.cisco.com/en/US/docs/wireless/controller/6.0/configuration/guide/Controller60CG.html
- *Cisco Wireless Control System Configuration Guide*, Release 6.0
  http://www.cisco.com/en/US/docs/wireless/wcs/6.0/configuration/guide/WCS60cg.html

Additional product information on the Cisco wireless infrastructure discussed in this chapter can be found at the following locations:

- *Cisco 5508 Wireless Controller*
http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps10315/data_sheet_c78-521631.html
- *Cisco 1140 Series 802.11n Access Point*
http://www.cisco.com/en/US/products/ps10092/index.html
- *Cisco 1250 Series 802.11n Access Point*
http://www.cisco.com/en/US/products/ps8382/index.html
- *Cisco 1250 Series Antenna Options*
http://www.cisco.com/en/US/prod/collateral/wireless/ps7183/ps469/at_a_glance_c45-513837.pdf
- *Cisco Aironet 1520 Lightweight Outdoor Access Point Ordering Guide*
http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps8368/product_data_sheet0900aecd8066a157.html
- *Cisco Wireless Control System (WCS)*
http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps6301/ps6305/product_data_sheet0900aecd802570d0.html
- *Cisco Wireless Control System Virtual Domains*
http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps6301/ps6305/brochure_c02-474335.html
- *Cisco Wireless Control System Navigator*
http://www.cisco.com/en/US/products/ps7305/index.html