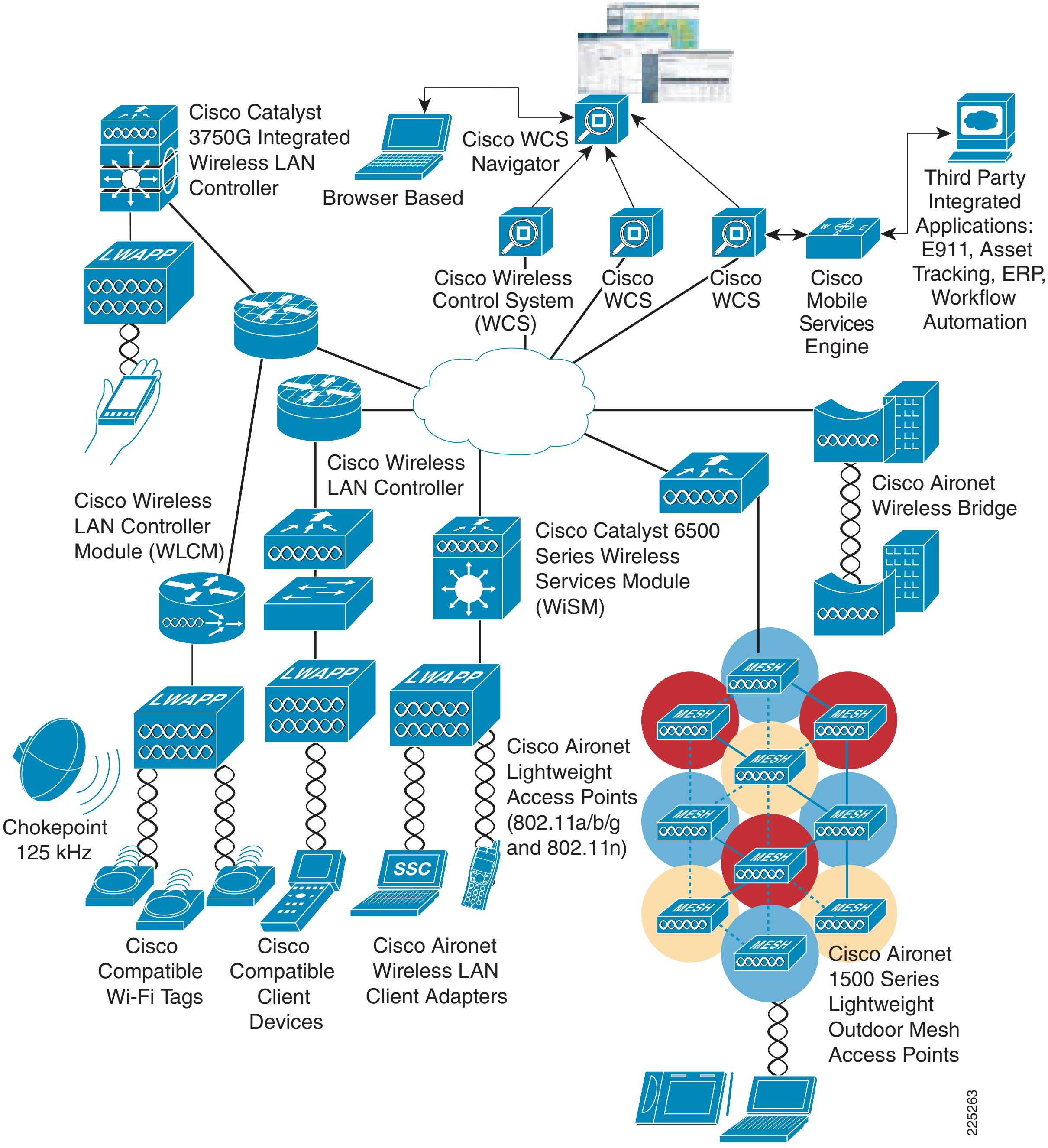
CHAPTER 4

Cisco Unified Wireless Network Architecture—Base Security Features

The Cisco Unified Wireless Network solution builds upon the base security features of 802.11 by augmenting RF, 802.11 and network-based security features where necessary to improve overall security. Although the 802.11 standards address the security of the wireless medium, the Cisco Unified Wireless Network solution addresses end-to-end security of the entire system by using architecture and product security features to protect WLAN endpoints, the WLAN infrastructure, client communication, and the supporting wired network.

Figure 4-1 shows a high level topology of the Cisco Unified Wireless Network Architecture, which includes Lightweight Access Point Protocol (LWAPP) access points (LAPs), mesh LWAPP APs (MAPs), the Wireless Control System (WCS), and the Wireless LAN Controller (WLC); alternate WLC platforms include the Wireless LAN Controller Module (WLCM) or Wireless Services Module (WiSM). The Cisco Access Control Server (ACS) and its Authentication, Authorization, and Accounting (AAA) features complete the solution by providing RADIUS services in support of wireless user authentication and authorization.

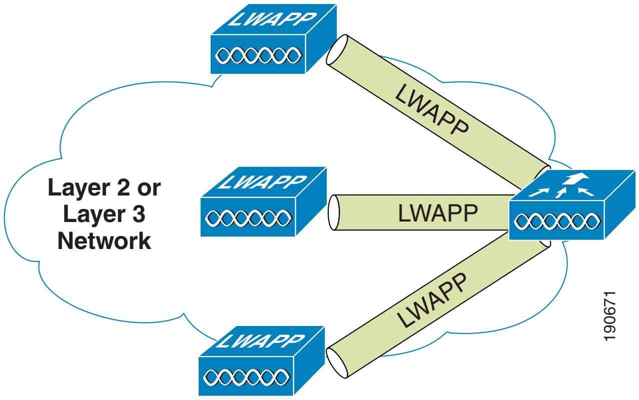
Figure 4-1 Cisco Unified Wireless Network Architecture



Cisco Unified Wireless Network Architecture

Figure 4-2 illustrates one of the primary features of the architecture—how Lightweight Access Point Protocol (LWAPP) access points (LAPs) use the LWAPP protocol to communicate with and tunnel traffic to a WLC.

Figure 4-2 LAP and WLC Connection



LWAPP has three primary functions:

- Control and management of the LAP
- Tunneling of WLAN client traffic to the WLC
- Collection of 802.11 data for the management of the Cisco Unified Wireless System

LWAPP Features

The easier a system is to deploy and manage, the easier it is to manage the security associated with that system. Early implementers of WLAN systems that used "fat" APs (autonomous or intelligent APs) found that the implementation and configuration of such APs was the equivalent of deploying and managing hundreds of individual firewalls, each requiring constant attention to ensure correct firmware, configuration, and safeguarding. Even worse, APs are often deployed in physically unsecured areas where theft of an AP could result in someone accessing its configuration to gain information to aid in some other form of malicious activity.

LWAPP addresses deployment, configuration, and physical security issues by doing the following:

- Removing direct user interaction and management of the AP. Instead, the AP is managed by the WLC through its LWAPP connection. This moves the configuration and firmware functions to the WLC, which can be further centralized through the use of the WCS.
- Having the AP download its configuration from the WLC and be automatically updated when configuration changes occur on the WLC.
- Having the AP synchronize its firmware with its WLC, ensuring that the AP is always running the correct software version
- Storing sensitive configuration data at the WLC and storing only IP address information on the AP. In this way, if the AP is physically compromised, there is no configuration information resident in NVRAM that can be used to perform further malicious activity.
- Mutually authenticating LAPs to WLCs and AES encrypting the LWAPP control channel.

In addition to the improvements in physical security, firmware, and configuration management offered by LWAPP, the tunneling of WLAN traffic in an LWAPP-based architecture improves the ease of deployment without compromising the overall security of the solution. LAPs that support multiple WLAN VLANs can be deployed on access layer switches without requiring dot1q trunking or adding additional client subnets at the access switches. All WLAN client traffic is tunneled to centralized locations (where the WLC resides), making it simpler to implement enterprise-wide WLAN access and security policies.

Cisco Unified Wireless Security Features

The native 802.11 security features combined with the physical security and ease of deployment of the LWAPP architecture improve the overall security of WLAN deployments. In addition to the inherent security benefits offered by the LWAPP protocol described above, the Cisco Unified Wireless solution also includes the following additional security features:

- Enhanced WLAN security options
- ACL and firewall features
- Dynamic Host Configuration Protocol (DHCP) and Address Resolution Protocol (ARP) protection
- Peer-to-peer blocking
- Wireless intrusion detection system (IDS)
- Client exclusion
- Rogue AP detection
- Management frame protection
- Dynamic radio frequency management
- Architecture integration
- IDS integration

Enhanced WLAN Security Options

The Cisco Unified Wireless Network solution supports multiple concurrent WLAN security options. For example, multiple WLANs can be created on a WLC, each with its own WLAN security settings that range from open guest WLAN networks and WEP networks for legacy platforms to combinations of WPA and/or WPA2 security configurations.

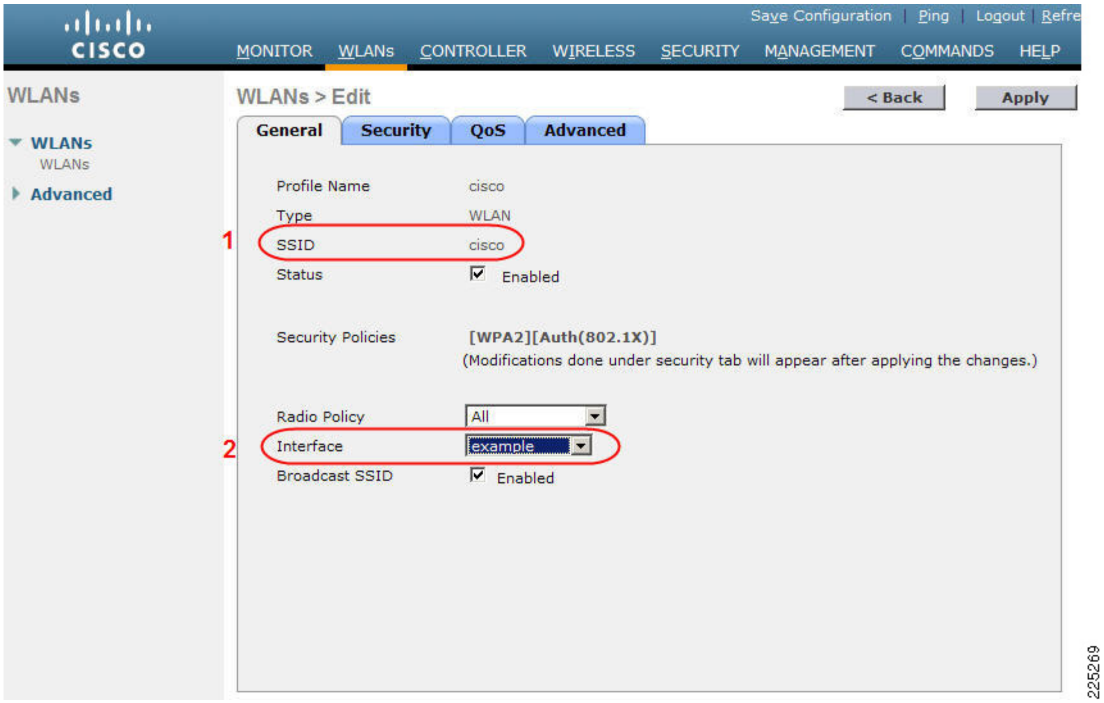
Each WLAN SSID can be mapped to either the same or different dot1q interface on the WLC, or Ethernet over IP (EoIP) tunneled to a different controller through a mobility anchor connection.

If a WLAN client is 802.1X authenticated, the dot1q VLAN assignment can be controlled by the RADIUS attributes passed to the WLC.

Figure 4-3 and Figure 4-4 show a subset of the Unified Wireless WLAN configuration screen. The following three main configuration items appear on this sample screen:

- The WLAN SSID
- The WLC interface to which the WLAN is mapped
- The security method (additional WPA and WPA2 options are on this page, but are not shown)

Figure 4-3 WLAN General Tab


CISCO
Save Configuration | Ping | Logout | Refre
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
< Back
Apply
General
Security
QoS
Advanced
1
2
225269

WLANs > Edit

Profile Name cisco

Type WLAN

SSID cisco

Status ☑ Enabled

Security Policies [WPA2][Auth(802.1X)]

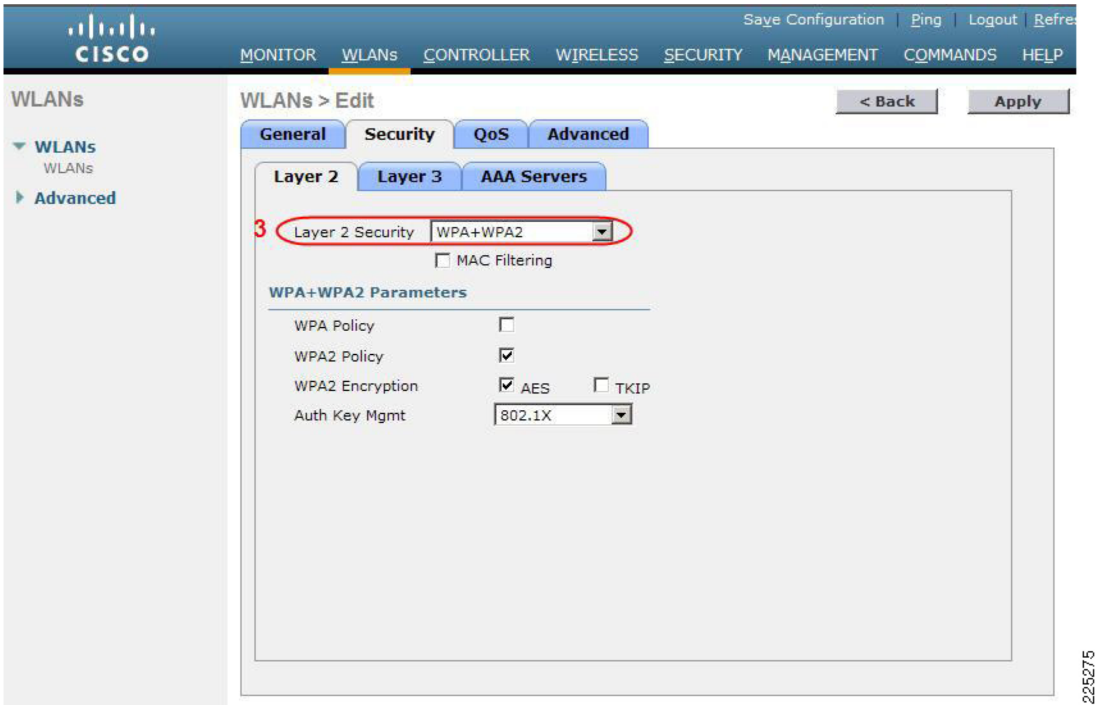
(Modifications done under security tab will appear after applying the changes.)

Radio Policy All

Interface example

Broadcast SSID ☑ Enabled

Figure 4-4 WLAN Layer 2 Security Tab


CISCO
Save Configuration | Ping | Logout | Refre
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
< Back
Apply
General
Security
QoS
Advanced
Layer 2
Layer 3
AAA Servers
3
225275

WLANs > Edit

Layer 2 Security WPA+WPA2

☐ MAC Filtering

WPA+WPA2 Parameters

WPA Policy ☐

WPA2 Policy ☑

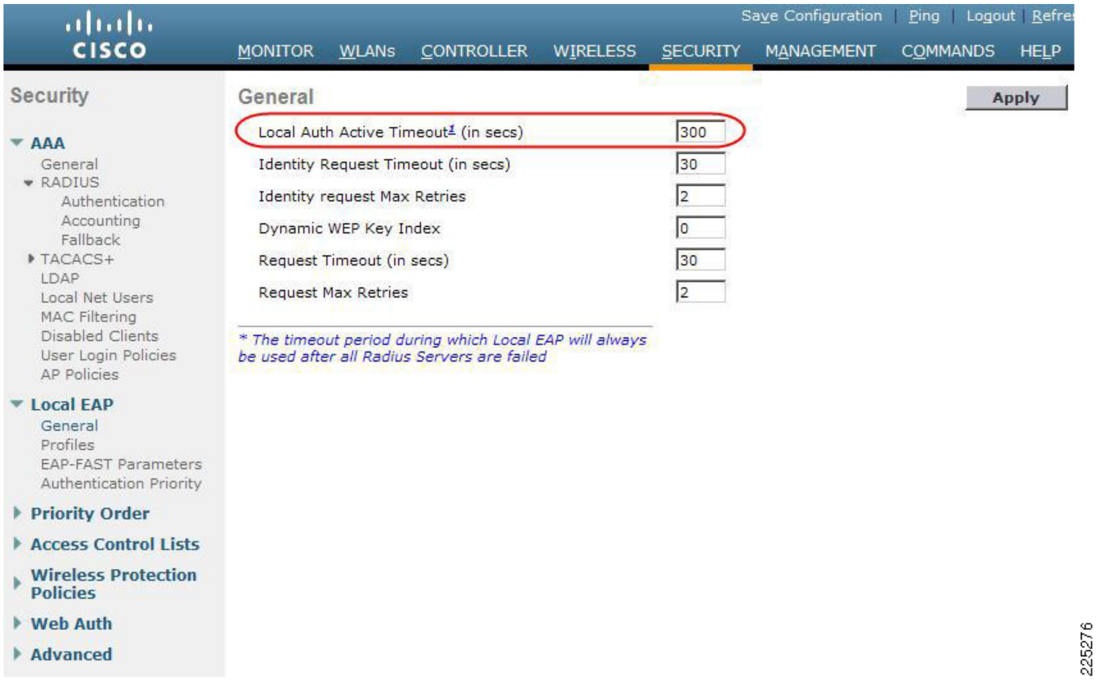
WPA2 Encryption ☑ AES ☐ TKIP

Auth Key Mgmt 802.1X

Local EAP Authentication

The 5.0 WLC code release provides local EAP authentication, which can be used when an external RADIUS server is not available or becomes unavailable. The delay before switching to local authentication is configurable, as shown in Figure 4-5. When RADIUS server availability is restored, the WLC automatically switches back from local authentication to RADIUS server authentication.

Figure 4-5 Local Auth Timeout



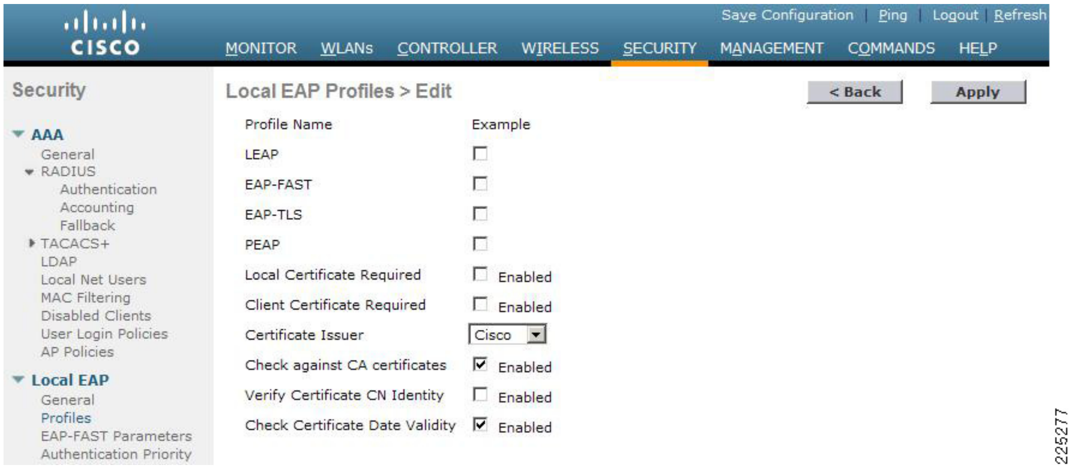
General

Local Auth Active Timeout[1] (in secs)	300
Identity Request Timeout (in secs)	30
Identity request Max Retries	2
Dynamic WEP Key Index	0
Request Timeout (in secs)	30
Request Max Retries	2

* The timeout period during which Local EAP will always be used after all Radius Servers are failed

The EAP types supported locally on the WLC are LEAP, EAP-FAST, and EAP-TLS. Examples of local EAP profiles are shown in Figure 4-6.

Figure 4-6 Local EAP Profiles

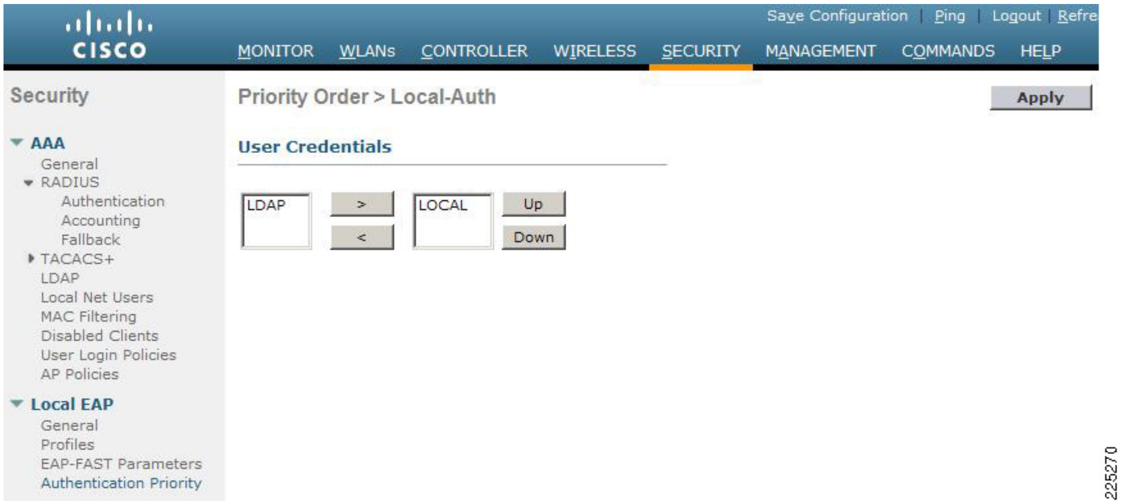


Local EAP Profiles > Edit

Profile Name	Example
LEAP	□
EAP-FAST	□
EAP-TLS	□
PEAP	□
Local Certificate Required	□ Enabled
Client Certificate Required	□ Enabled
Certificate Issuer	Cisco
Check against CA certificates	☑ Enabled
Verify Certificate CN Identity	□ Enabled
Check Certificate Date Validity	☑ Enabled

A WLC supports the use of a local database for authentication data and it can also access an LDAP directory to provide data for EAP-FAST or EAP-TLS authentication. The priority that an LDAP server has over the local authentication database of local net users is configurable, as shown in Figure 4-7.

Figure 4-7 Local EAP Priority



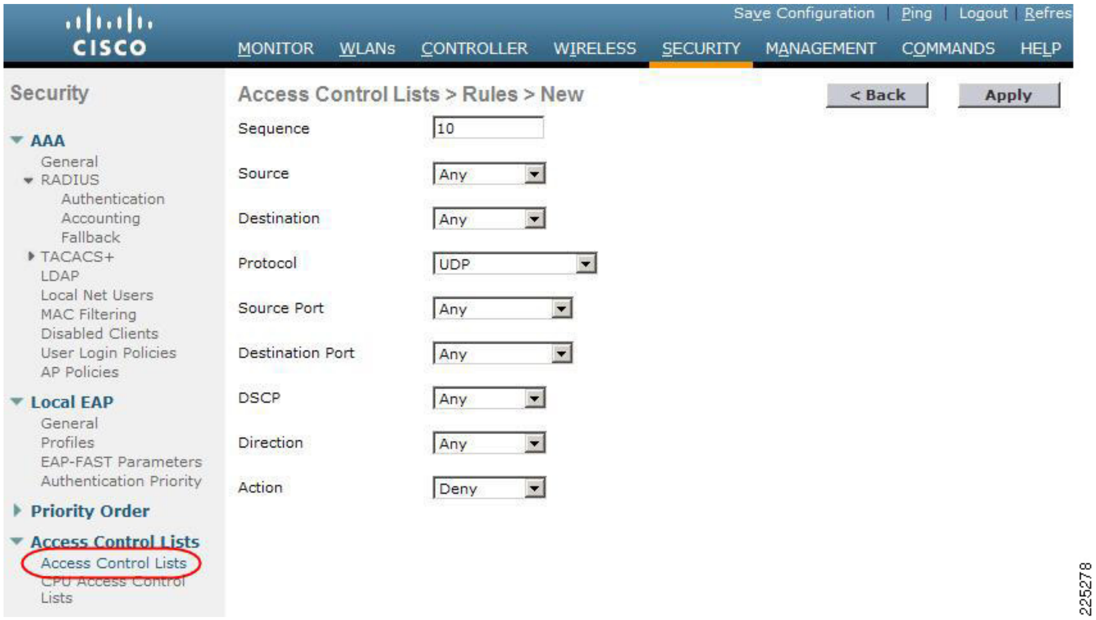
ACL and Firewall Features

The WLC allows access control lists (ACLs) to be defined for any interface configured on the WLC, as well as ACLs to be defined for the CPU of the WLC itself. These ACLs can be used to enforce policy on particular WLANs to limit access to particular addresses and protocols, as well as to provide additional protection to the WLC itself.

Interface ACLs act on WLAN client traffic in and out of the interfaces to which the ACLs are applied. CPU ACLs are independent of interfaces on the WLC and are applied to all traffic to and from the WLC system.

Figure 4-8 shows the ACL configuration page. The ACL can specify source and destination address ranges, protocols, source and destination ports, differentiated services code point (DSCP), and direction in which the ACL is to be applied. An ACL can be created out of a sequence of various rules.

Figure 4-8 ACL Configuration Page



Access Control Lists > Rules > New

Sequence: 10
Source: Any
Destination: Any
Protocol: UDP
Source Port: Any
Destination Port: Any
DSCP: Any
Direction: Any
Action: Deny

DHCP and ARP Protection

The WLC acts as a relay agent for WLAN client DHCP requests. In doing so, the WLC performs a number of checks to protect the DHCP infrastructure. The primary check is to verify that the MAC address included in the DHCP request matches the MAC address of the WLAN client sending the request. This protects against DHCP exhaustion attacks, because a WLAN client can request only an IP address for its own interface. The WLC by default does not forward broadcast messages from WLAN clients back out onto the WLAN, which prevents a WLAN client from acting as a DHCP server and spoofing incorrect DHCP information.

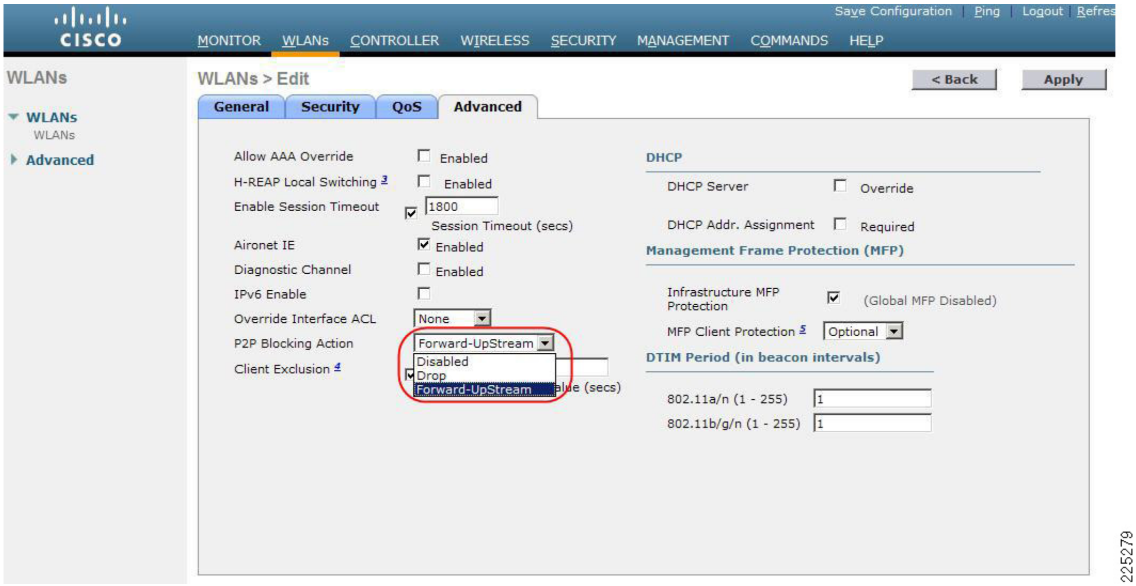
The WLC acts as an ARP proxy for WLAN clients by maintaining the MAC address-IP address associations. This allows the WLC to block duplicate IP address and ARP spoofing attacks. The WLC does not allow direct ARP communication between WLAN clients. This also prevents ARP spoofing attacks directed at WLAN client devices.

Peer-to-Peer Blocking

The WLC can be configured to block communication between clients on the same WLAN. This prevents potential attacks between clients on the same subnet by forcing communication through the router. Figure 4-9 shows the configuration of peer-to-peer blocking on a WLAN.

Note This is a change from the previous code releases where peer to peer blocking was a global setting on the WLC.

Figure 4-9 Peer-to-Peer Blocking



WLANs > Edit

Allow AAA Override □ Enabled

H-REAP Local Switching [3] □ Enabled

Enable Session Timeout ☑ 1800 Session Timeout (secs)

Aironet IE ☑ Enabled

Diagnostic Channel □ Enabled

IPv6 Enable □

Override Interface ACL None

P2P Blocking Action Forward-UpStream (Disabled, Drop, Forward-UpStream)

Client Exclusion [4] ☑ ...alue (secs)

DHCP

DHCP Server □ Override

DHCP Addr. Assignment □ Required

Management Frame Protection (MFP)

Infrastructure MFP Protection ☑ (Global MFP Disabled)

MFP Client Protection [5] Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255) 1

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

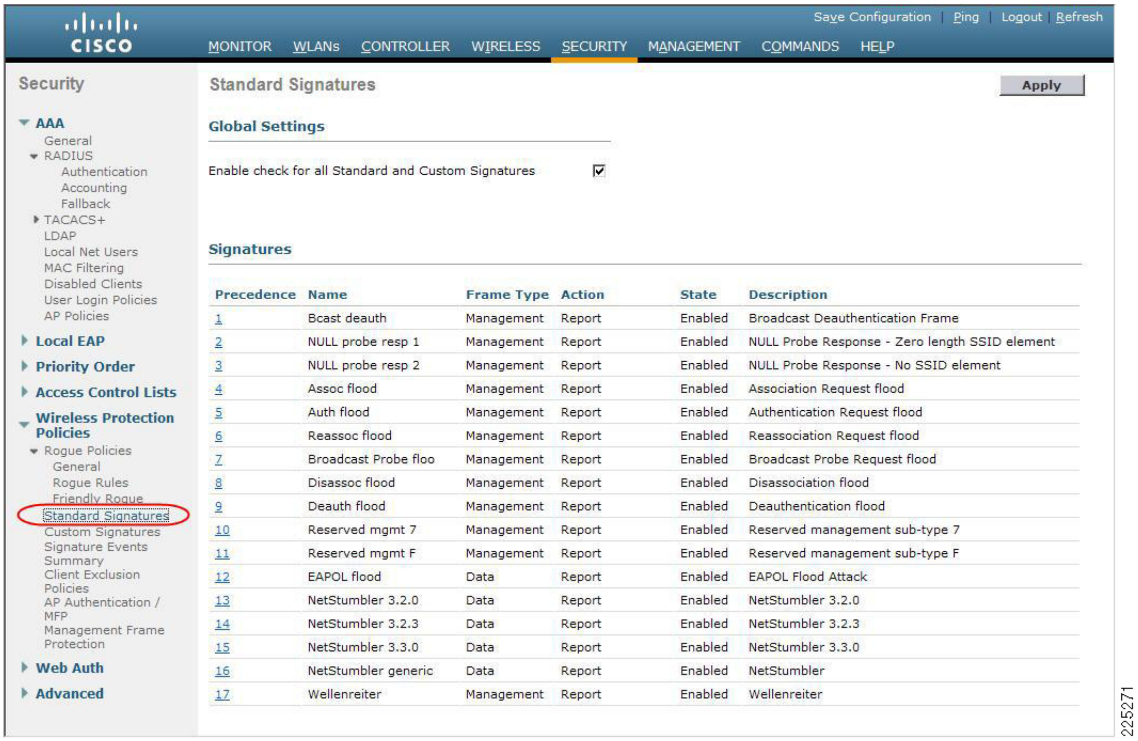
Wireless IDS

The WLC performs WLAN IDS analysis using all the connected APs and reports detected attacks on to WLC as well to the WCS. The Wireless IDS analysis is complementary to any analysis that may otherwise be performed by a wired network IDS system. The embedded Wireless IDS capability of the WLC analyzes 802.11- and WLC-specific information that is not available to a wired network IDS system.

The signature files used on the WLC are included in WLC software releases, but can be updated independently using a separate signature file; custom signatures are displayed in the Custom Signatures window.

Figure 4-10 shows the Standard Signatures window on the WLC.

Figure 4-10 Standard WLAN IDS Signatures



Standard Signatures

Global Settings

Enable check for all Standard and Custom Signatures ☑

Signatures

Precedence	Name	Frame Type	Action	State	Description
1	Bcast deauth	Management	Report	Enabled	Broadcast Deauthentication Frame
2	NULL probe resp 1	Management	Report	Enabled	NULL Probe Response - Zero length SSID element
3	NULL probe resp 2	Management	Report	Enabled	NULL Probe Response - No SSID element
4	Assoc flood	Management	Report	Enabled	Association Request flood
5	Auth flood	Management	Report	Enabled	Authentication Request flood
6	Reassoc flood	Management	Report	Enabled	Reassociation Request flood
7	Broadcast Probe floo	Management	Report	Enabled	Broadcast Probe Request flood
8	Disassoc flood	Management	Report	Enabled	Disassociation flood
9	Deauth flood	Management	Report	Enabled	Deauthentication flood
10	Reserved mgmt 7	Management	Report	Enabled	Reserved management sub-type 7
11	Reserved mgmt F	Management	Report	Enabled	Reserved management sub-type F
12	EAPOL flood	Data	Report	Enabled	EAPOL Flood Attack
13	NetStumbler 3.2.0	Data	Report	Enabled	NetStumbler 3.2.0
14	NetStumbler 3.2.3	Data	Report	Enabled	NetStumbler 3.2.3
15	NetStumbler 3.3.0	Data	Report	Enabled	NetStumbler 3.3.0
16	NetStumbler generic	Data	Report	Enabled	NetStumbler
17	Wellenreiter	Management	Report	Enabled	Wellenreiter

Mobility Services Engine

The Cisco Mobility Services Engine is a platform that is designed to support a variety of services loaded onto the platform as a suite of software.

While any number of services may be delivered on the MSE, an example of services includes Context Aware software, Adaptive Wireless IPS, Mobile Intelligent Roaming, and Secure Client Manager. Each of these services is designed to provide intelligence from the network to help optimize a specific application.

Table 4-1 summarizes the key definitions and functionalities of these services.

Table 4-1 Summary of Mobility Services Software Suite

	Context Aware	Adaptive Wireless IPS	Mobile Intelligent Roaming	Secure Client Manager
Description	Optimize business process with context such as location and telemetry	Mitigate wireless threats with integrated intrusion prevention	Deliver handoff for mobility applications across public and private networks	Simplify device provisioning and management for the wave of new mobile devices

Table 4-1 Summary of Mobility Services Software Suite (continued)

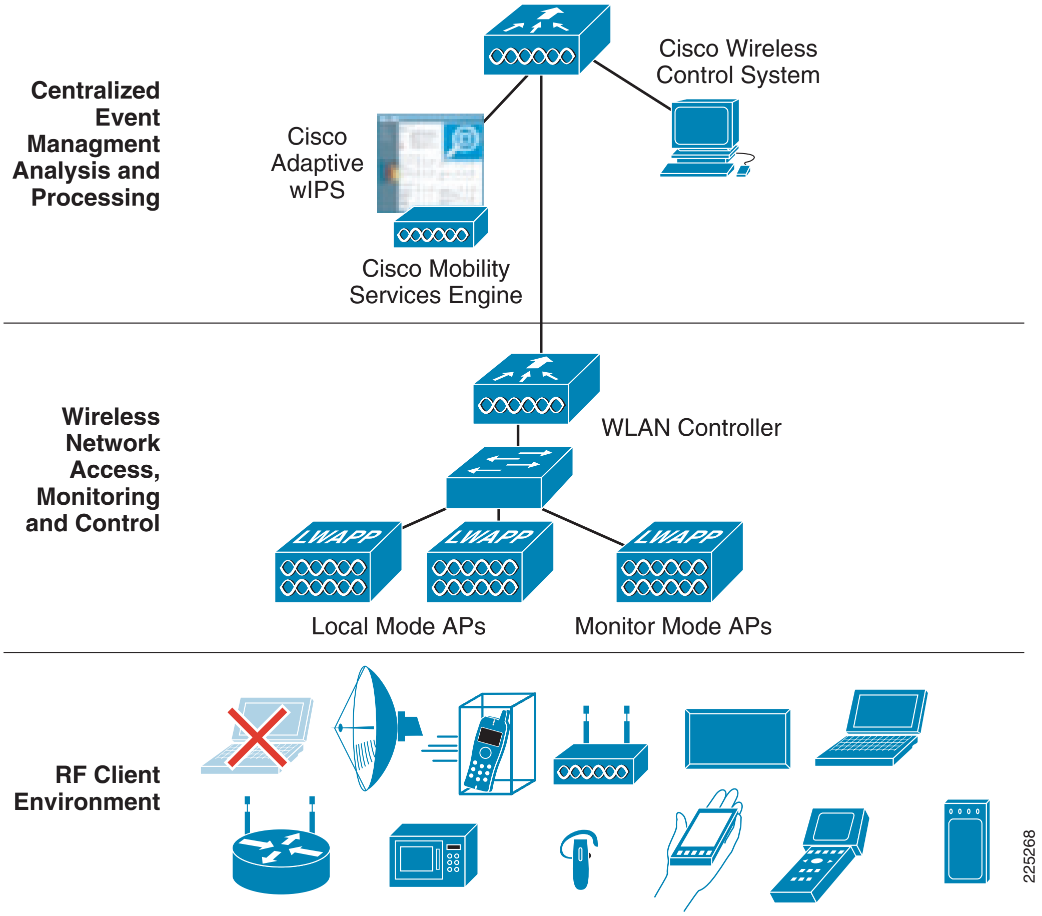
	Context Aware	Adaptive Wireless IPS	Mobile Intelligent Roaming	Secure Client Manager
Applications	Asset Tracking Condition Monitoring	Regulatory Compliance—PCI, HIPAA, SOX	Dual Mode Voice and Data Applications	Secure Connectivity
Primary Industries	Health care Manufacturing	Retail Financial Services Health care	Enterprise Health care Education	Retail Health care Enterprise

Adaptive Wireless IPS

Adaptive Wireless IPS offers protection above that offered by the WLC Wireless IPS, by using the power and position of the Mobility Services Engine, to analyze WLAN data from all sources in within the Cisco Unified Wireless Network.

The Cisco Mobility Services Engine provides analysis processing performance and scalability, storage capacity for historical reporting and forensics, and integration capabilities for services such as location or contact aware asset tracking and client security management. As the mobile business network expands, the Cisco Adaptive Wireless IPS solution provides monitoring and analysis of the growing number of new devices and spectrum uses to ensure ongoing protection of critical business information. Figure 4-11 shows the components that make up the Cisco Adaptive Wireless IPS Solution.

Figure 4-11 Components of the Cisco Adaptive Wireless IPS Solution

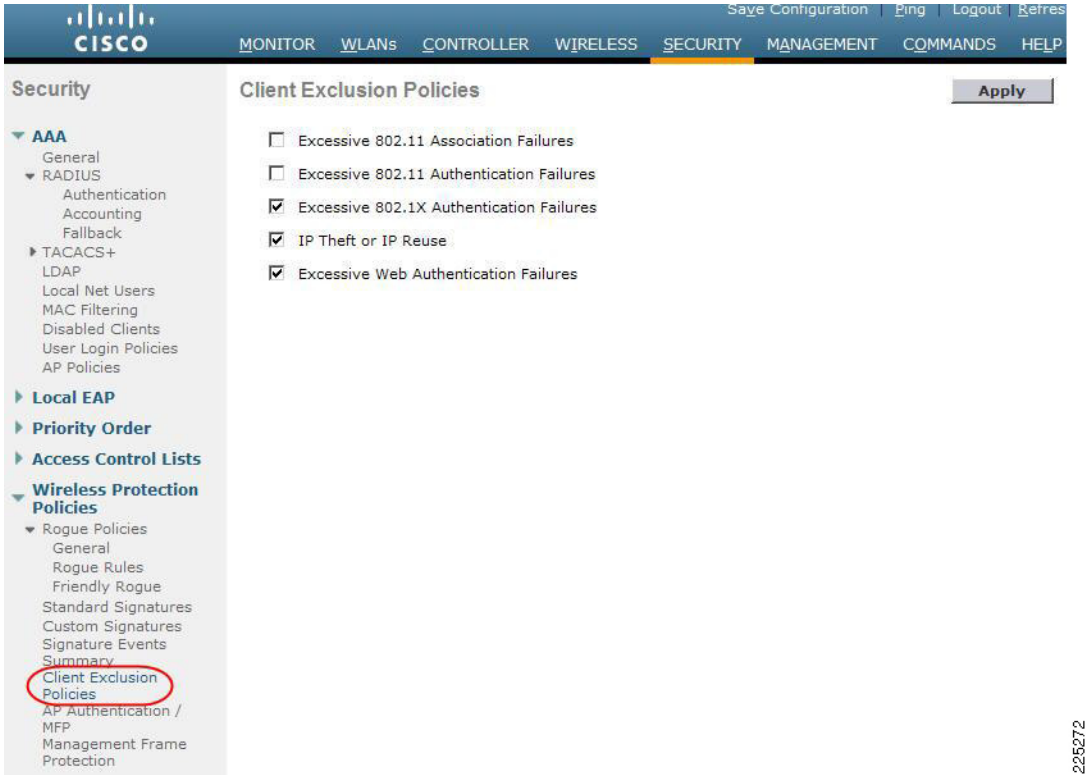

Centralized Event Managment Analysis and Processing
Cisco Adaptive wIPS
Cisco Wireless Control System
Cisco Mobility Services Engine
Wireless Network Access, Monitoring and Control
WLAN Controller
LWAPP
LWAPP
LWAPP
Local Mode APs
Monitor Mode APs
RF Client Environment
225268

Client Exclusion

In addition to Wireless IDS, the WLC is able to take additional steps to protect the WLAN infrastructure and WLAN clients. The WLC is able to implement policies that exclude WLAN clients whose behavior is considered threatening or inappropriate. Figure 4-12 shows the Exclusion Policies window, containing the following currently supported client exclusion policies:

- Excessive 802.11 association failures—Possible faulty client or DoS attack
- Excessive 802.11 authentication failures—Possible faulty client or DoS attack
- Excessive 802.1X authentication failures—Possible faulty client or DoS attack
- External policy server failures—Network-based IPS server identified client for exclusion
- IP theft or IP reuse—Possible faulty client or DoS attack
- Excessive web authentication failures—Possible DoS or password-cracking attack

Figure 4-12 Client Exclusion Policies



Client Exclusion Policies

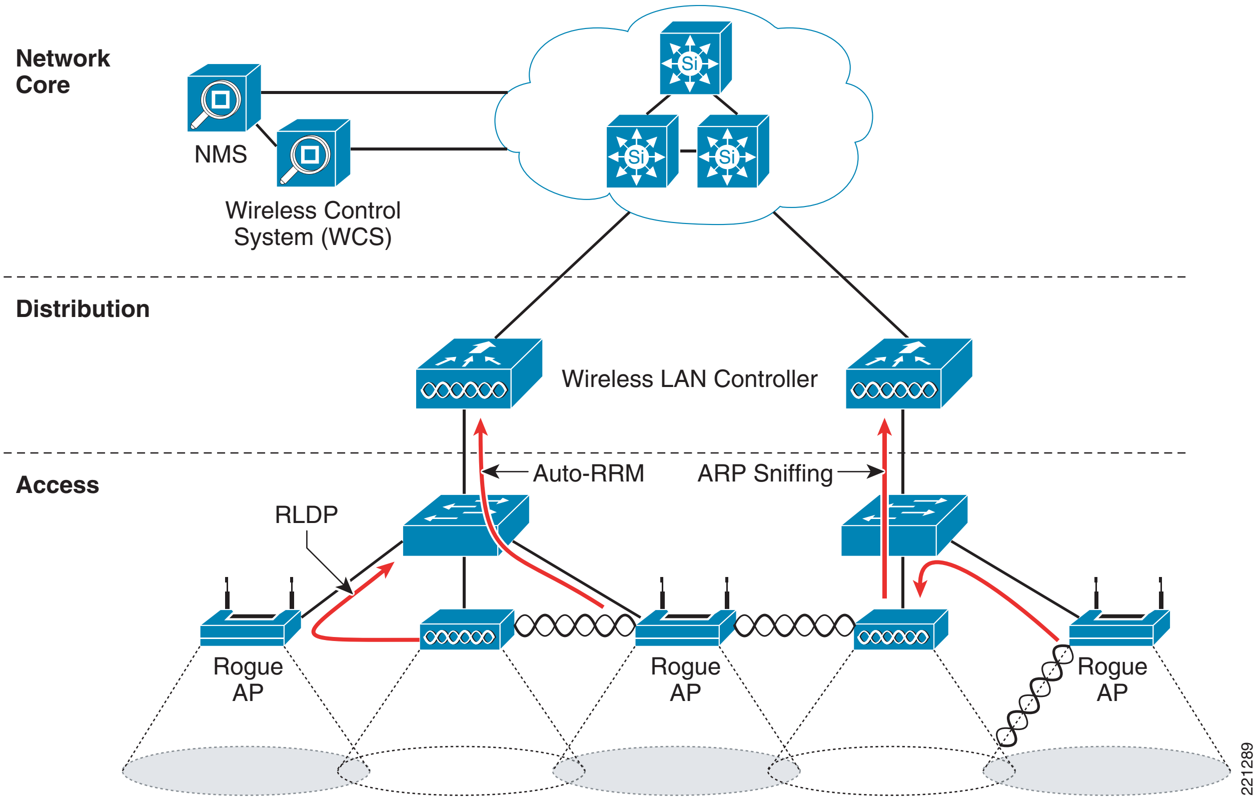
□ Excessive 802.11 Association Failures
□ Excessive 802.11 Authentication Failures
☑ Excessive 802.1X Authentication Failures
☑ IP Theft or IP Reuse
☑ Excessive Web Authentication Failures

Rogue AP

The Cisco Unified Wireless Networking solution provides a complete rogue AP solution, shown in Figure 4-13, which provides the following:

- Air/RF detection—Detection of rogue devices by observing/sniffing beacons and 802.11 probe responses
- Rogue AP location—Use of the detected RF characteristics and known properties of the managed RF network to locate the rogue device
- Wire detection—A mechanism for tracking/correlating the rogue device to the wired network
- Rogue AP isolation—A mechanism to prevent client connection to a rogue AP

Figure 4-13 Unified Wireless Rogue AP Detection



Air/RF Detection

There are two AP RF detection deployment models:

- Standard AP deployment
- Monitor mode AP deployment

Both deployment models support RF detection and are not limited to rogue APs, but can also capture information upon detection of ad hoc clients and rogue clients (the users of rogue APs). In monitor mode, the AP is dedicated to scanning the RF channels, but does not pass client data.

When searching for rogue APs, a unified wireless AP goes off channel for 50 ms to listen for rogue clients, monitor for noise, and channel interference (the channels to be scanned are configured in the global WLAN network parameters for 802.11a and 802.11b/g). Any detected rogue clients and/or access points are sent to the controller, which gathers the following information:

- Rogue AP MAC address
- Rogue AP name
- Rogue connected client(s) MAC address
- Whether the frames are protected with WPA or WEP
- The preamble
- Signal-to-noise ratio (SNR)
- Received signal strength indication (RSSI)

The WLC then waits to label this as a rogue client or AP, until it has been reported by another AP or until it completes another cycle. The same AP again moves to the same channel to monitor for rogue access points/clients, noise, and interference. If the same clients and/or access points are detected, they are listed as a rogue on the WLC. The WLC now begins to determine whether this rogue is attached to the local network or is simply a neighboring AP. In either case, an AP that is not part of the managed local WLAN is considered a rogue.

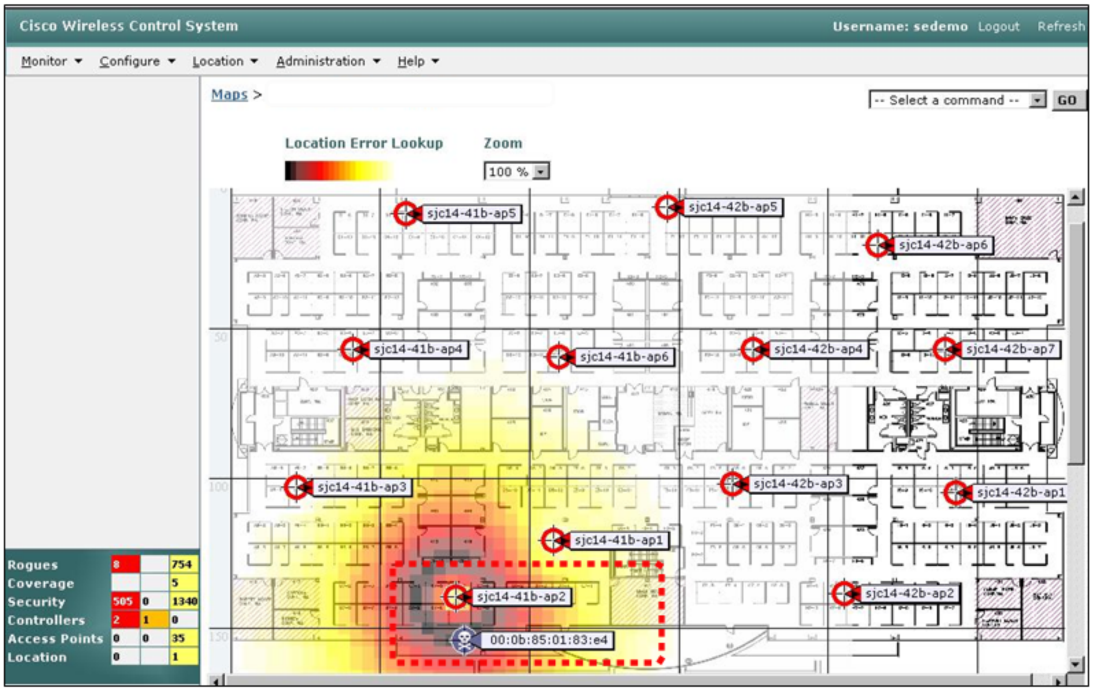
In monitor mode, the AP does not carry user traffic but spends all its time scanning channels. This mode of deployment is most common when a customer does not want to support WLAN services in a particular area, but wants to monitor that area for rogue APs and rogue clients.

Location

The location features of the WCS can be used to provide a floor plan indicating the approximate location of a rogue AP. An example of this is shown in Figure 4-14. The floor plan shows the location of all legitimate APs and highlights the location of a rogue AP using the skull-and-crossbones icon.

For more information on the Cisco Unified Wireless Location features, see http://www.cisco.com/en/US/products/ps6386/index.html.

Figure 4-14 Rogue AP Mapping



Rogues	8		754
Coverage			5
Security	505	0	1340
Controllers	2	1	0
Access Points	0	0	35
Location	0		1

221290

Note Need to update with new WCS page.

Wire Detection

Situations may exist where the WCS rogue location features described above are not effective, such as in branch offices that contain only a few APs or where accurate floor plan information may not be available. In those cases, the Cisco Unified Wireless solution offers two other “wire”-based detection options:

- Rogue detector AP
- Rogue Location Discovery Protocol (RLDP)

If an AP is configured as a rogue detector, its radio is turned off and its role is to listen on the wired network for MAC addresses of clients associated to rogue APs; that is, rogue clients. The rogue detector listens for ARP packets that include these rogue client MAC addresses. When it detects one of these ARPs, it reports this to the WLC, providing verification that the rogue AP is attached to the same network as the Cisco Unified Wireless Network. To be effective at capturing ARP information, the rogue AP detector should be connected to all available broadcast domains using a Switched Port Analyzer (SPAN) port because this maximizes the likelihood of detection. Multiple rogue AP detector APs may be deployed to capture the various aggregated broadcast domains that exist on a typical network.

If a rogue client resides behind a wireless router (a common home WLAN device), their ARP requests are not seen on the wired network, so an alternative to the rogue detector AP method is needed. Additionally, rogue detector APs may not be practical for some deployments because of the large number of broadcast domains to be monitored (such as in the main campus network).

The RLDP option can aid in these situations. In this case, a standard LAP, upon detecting a rogue AP, can attempt to associate with the rogue AP as a client and send a test packet to the controller, which requires the AP to stop being an active AP and to go into client mode. This action confirms that the rogue AP in question is actually on the network, and provides IP address information that indicates its logical location in the network. Given the difficulties in establishing the location data in branch offices and the likelihood of their being located in multi-tenant buildings, rogue AP detector and RLDP are useful tools that augment location-based rogue AP detection.

Rogue AP Containment

Rogue AP-connected clients, or rogue ad hoc connected clients, may be contained by sending 802.11 de-authentication packets from local APs. This should be done only after steps have been taken to ensure that the AP is truly a rogue AP, because it is illegal to do this to a legitimate AP in a neighboring WLAN. This is the reason why Cisco removed the automatic rogue AP containment feature from this solution.

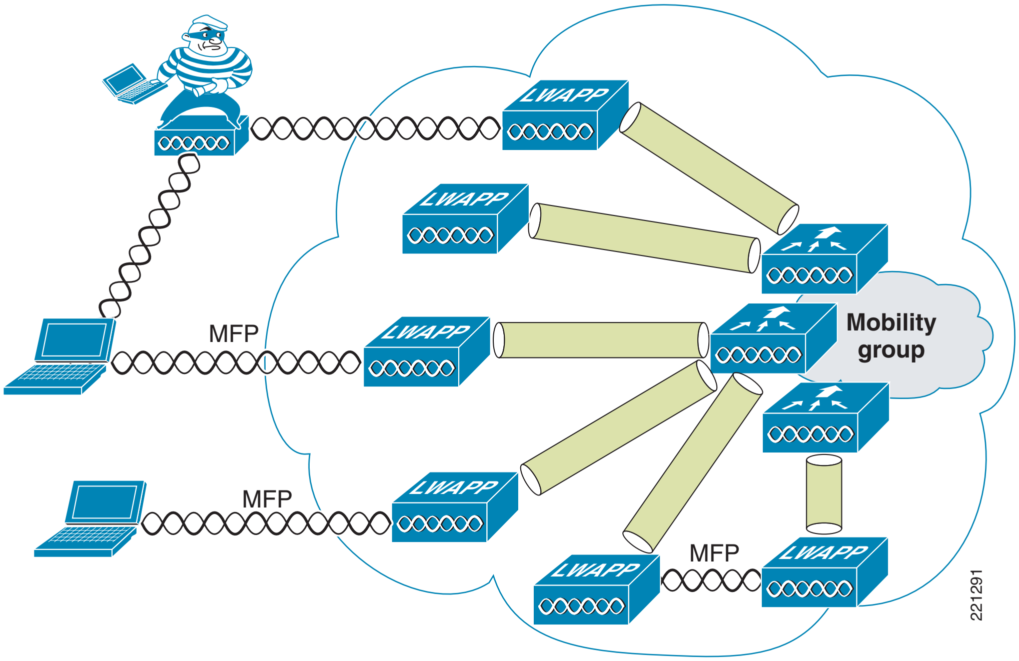
To determine whether rogue AP clients are also clients on the enterprise WLAN, the client MAC address can be compared with MAC addresses collected by the AAA during 802.1X authentication. This allows the identification of possible WLAN clients that may have been compromised or users that are not following security policies.

Management Frame Protection

One of the challenges in 802.11 has been that management frames are sent in the clear with no encryption or message integrity checking, and are therefore vulnerable to spoofing attacks. The spoofing of WLAN management frames can be used to attack the WLAN network. To address this, Cisco created a digital signature mechanism to insert a message integrity check (MIC) to 802.11 management frames. This allows the legitimate members of a WLAN deployment to be identified and therefore allows the identification of rogue infrastructure, and spoofed frames, through their lack of valid MICs.

The MIC that is used in management frame protection (MFP) is not a simple CRC hashing of the message, but also includes a digital signature component. The MIC component of MFP ensures that a frame has not been tampered with and the digital signature component ensures that the MIC could have only been produced by a valid member of the WLAN domain. The digital signature key used in MFP is shared among all controllers in a mobility group; different mobility groups have different keys. This allows the validation of all WLAN management frames processed by the WLCs in that mobility group. (see Figure 4-15).

Figure 4-15 Management Frame Protection



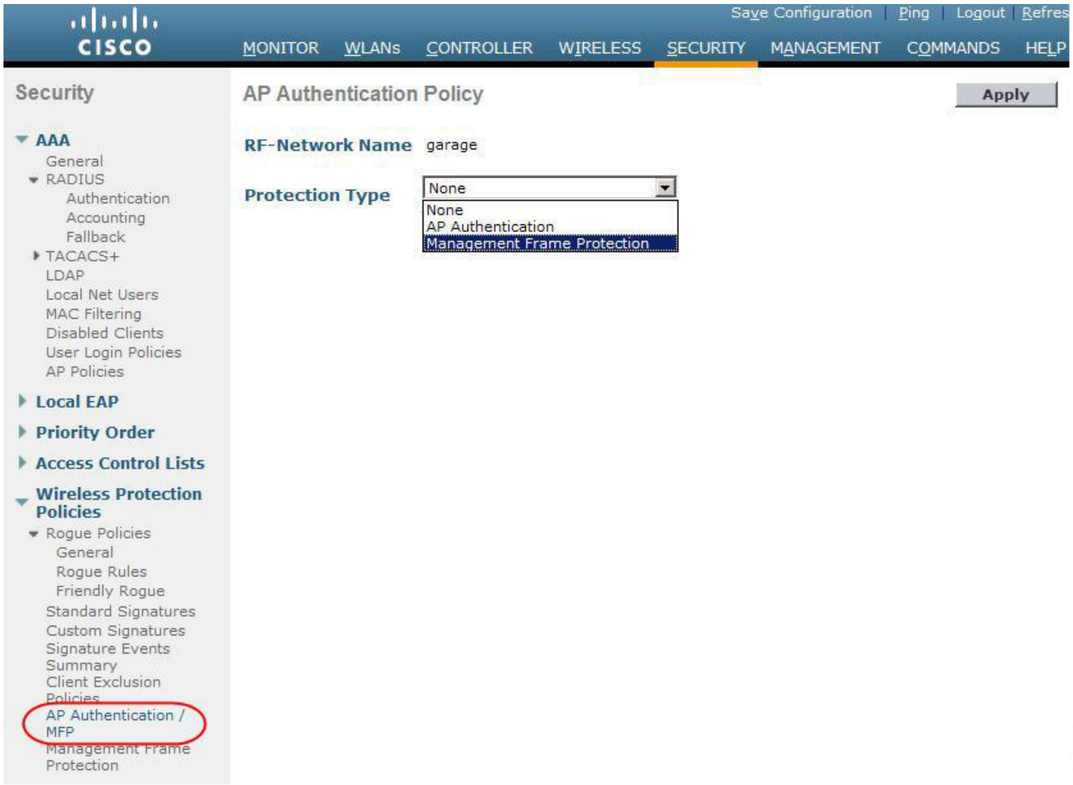
Both infrastructure-side and client MFP are currently possible, but client MFP requires CCXv5 WLAN clients to be able to learn the mobility group MFP key and can therefore detect and reject invalid frames. MFP provides the following benefits:

- Authenticates 802.11 management frames generated by the WLAN network infrastructure
- Allows detection of malicious rogues that spoof a valid AP MAC or SSID to avoid detection as a rogue AP, or as part of a man-in-the-middle attack
- Increases the effectiveness of the rogue AP and WLAN IDS signature detection of the solution
- Provides protection of client devices with CCX v5

Two steps enable MFP:

- Enabling it on the WLC (see Figure 4-16)
- Enabling it on the WLANs in the mobility group (see Figure 4-17)

Figure 4-16 Enabling MFP on the Controller



AP Authentication Policy

RF-Network Name garage

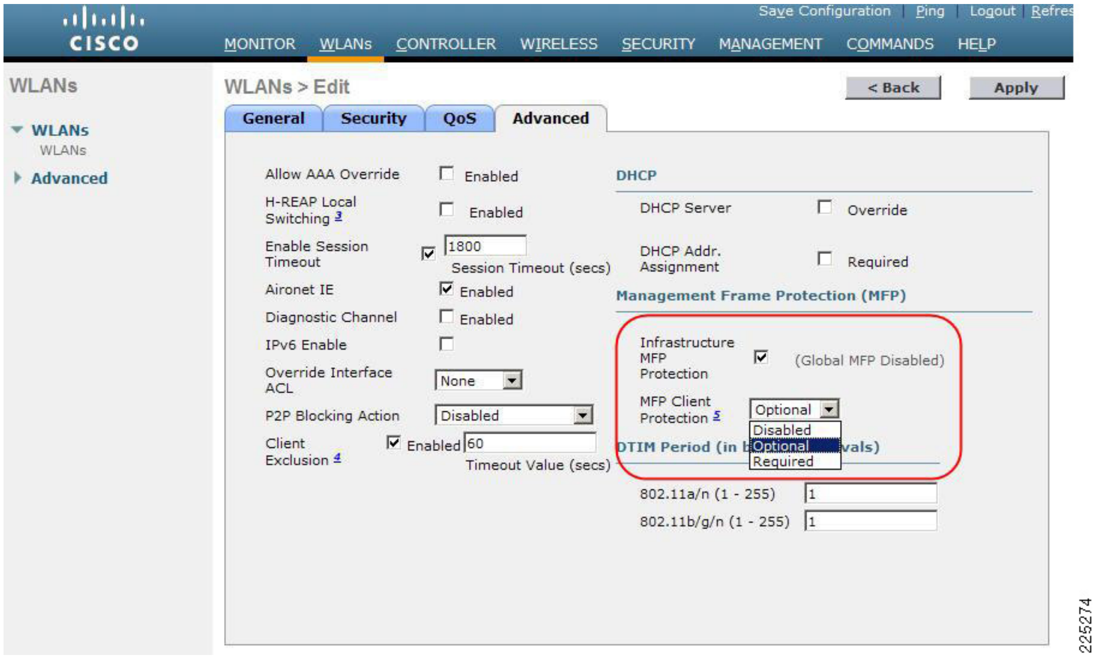
Protection Type None

Client Management Frame Protection

CCXv5 WLAN clients support MFP. This is enabled on a per-WLAN basis, as is shown in Figure 4-17.

The method of providing MFP for WLAN clients is fundamentally the same as that used for APs, which is to use a MIC in the management frames. This allows trusted management frames to be identified by the client. The WLAN client is passed the cryptographic keys for the MIC as part of the WPA2 authentication process. Client MFP is available only for WPA2. If WPA and WPA clients share the same WLAN, client MFP must be set to “optional”.

Figure 4-17 Enabling MFP per WLAN


Save Configuration | Ping | Logout | Refres
cisco
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
< Back
Apply
General
Security
QoS
Advanced
225274

WLANs > Edit

Allow AAA Override □ Enabled
H-REAP Local Switching [3] □ Enabled
Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE ☑ Enabled
Diagnostic Channel □ Enabled
IPv6 Enable □
Override Interface ACL None
P2P Blocking Action Disabled
Client Exclusion [4] ☑ Enabled 60 Timeout Value (secs)

DHCP

DHCP Server □ Override
DHCP Addr. Assignment □ Required

Management Frame Protection (MFP)

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

- Disabled
- Optional
- Required

DTIM Period (in beacon intervals)

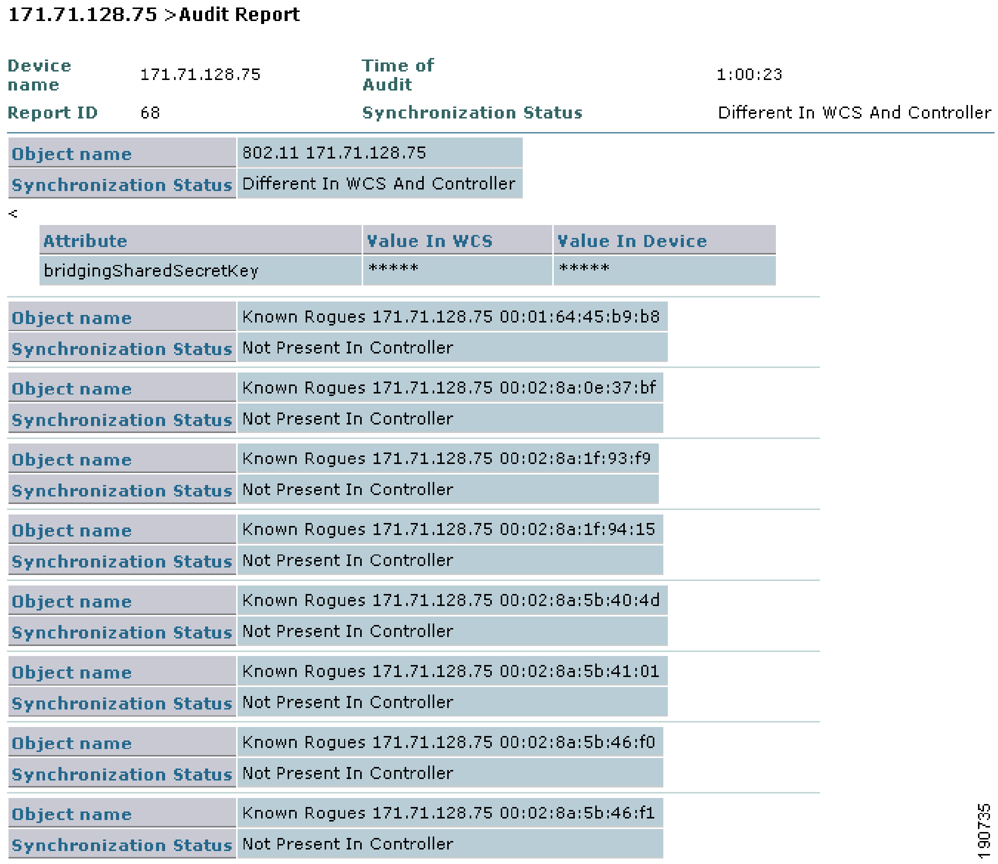
802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

WCS Security Features

Configuration Verification

The WCS can provide on-demand or regularly-scheduled configuration audit reports, which compare the complete current running configuration of a WLC and its registered access points with that of a known valid configuration stored in the WCS databases. Any exceptions between the current running configuration and the stored database configuration are noted and brought to the attention of the network administrator via screen reports (see Figure 4-18).

Figure 4-18 Audit Report Example



171.71.128.75 >Audit Report

Device name	171.71.128.75	Time of Audit	1:00:23
Report ID	68	Synchronization Status	Different In WCS And Controller

Object name	802.11 171.71.128.75
Synchronization Status	Different In WCS And Controller

<

Attribute	Value In WCS	Value In Device
bridgingSharedSecretKey	*****	*****

Object name	Known Rogues 171.71.128.75 00:01:64:45:b9:b8
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:0e:37:bf
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:1f:93:f9
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:1f:94:15
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:5b:40:4d
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:5b:41:01
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:5b:46:f0
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:5b:46:f1
Synchronization Status	Not Present In Controller

Note Need to update.

Alarms

Apart from the alarms that can be generated directly from a WLC and sent to an enterprise network management system (NMS), the WCS can also send alarm notifications. The primary difference between alarm notification methods, apart from the type of alarm sent by the various components, is that the WLC uses Simple Network Management Protocol (SNMP) traps to send alarms, while the WCS relies on Simple Mail Transfer Protocol (SMTP) e-mail to send an alarm message. Standard steps should be taken to protect the e-mail servers to ensure that this cannot be used as a DoS attack on the e-mail system.

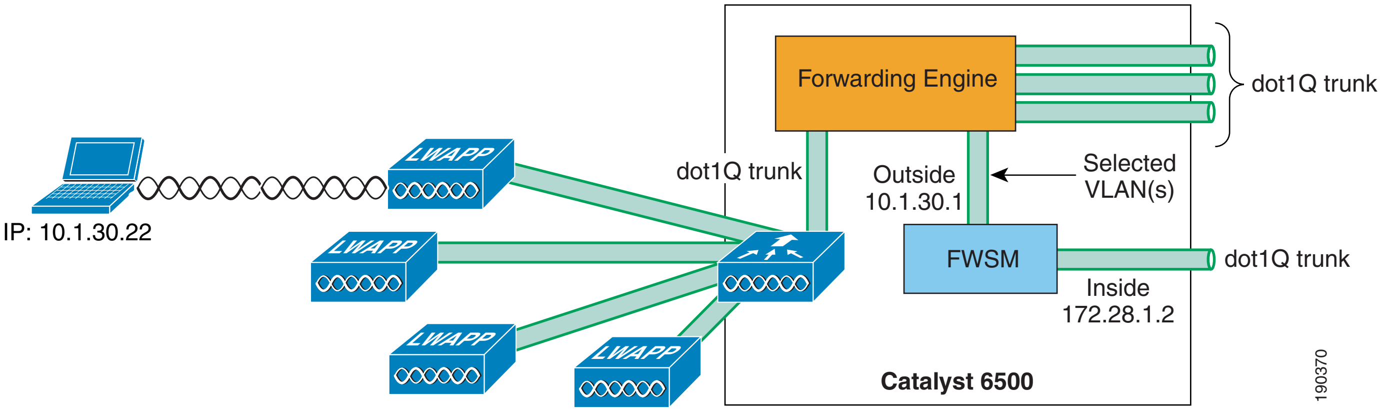
Architecture Integration

Cisco provides a wide variety of security services that are either integrated into Cisco IOS, integrated into service/network modules, or offered as standalone appliances. The Cisco Unified Wireless Network architecture eases the integration of these security services into the solution because it provides a Layer 2 connection between the WLAN clients and the upstream wired network. This means that appliances or modules that operate by being “inline” with client traffic can be easily inserted between the WLAN clients and the core network. For example, a Cisco Wireless LAN Services Module (WLSM)-based deployment required the implementation of VRF-Lite on the Cisco 6500 to enable WLAN client traffic to flow through a Cisco Firewall Service Module (FWSM), whereas a Cisco Unified WLAN deployment using a Wireless Services Module (WiSM) can simply map the (WLAN) client VLAN directly to the FWSM. The only WLAN controllers in the Cisco Unified Wireless portfolio not able to directly map Layer 2 WLAN traffic to a physical interface are ISR-based WLC modules. The ISR WLAN module does have access to all the IOS and IPS features available on the ISR, and therefore requires that IP traffic from the WLAN clients can be directed in and out specific ISR interfaces using IOS VRF features on the router.

Figure 4-19 shows an example of architectural integration between a WiSM and the FWSM module. In this example, the WLAN client is on the same subnet as the outside firewall interface. No routing policy or VRF configuration is required to ensure that WLAN client traffic in both directions goes through the firewall.

A Cisco Network Admission Control (NAC) appliance can be implemented in combination with a WLAN deployment to ensure that end devices connecting to the network meet enterprise policies for compliance with latest security software requirements and operating system patches. Like the FWSM module discussed above, the Cisco NAC appliance (formerly Cisco Clean Access) can also be integrated into a Unified Wireless architecture at Layer 2, thereby permitting strict control over which wireless user VLANs are subject to NAC policy enforcement.

Figure 4-19 Firewall Module Integration Example



In addition to the integration of the Cisco Unified Wireless Network at the networking layers, additional integration is provided at the management and control layers of the Cisco Security solutions. Integration between the Cisco Unified Wireless Network and:

- Cisco NAC appliance
- Cisco IPS
- Cisco CS MARS

Are all discussed in further detail in the following chapters of this design guide, as well as chapters discussion integration of Cisco Firewall solutions and the Cisco Security Agent.

References

- Deploying Cisco 440X Series Wireless LAN Controllers— http://www.cisco.com/en/US/products/ps6366/prod_technical_reference09186a00806cfa96.html

- Cisco Wireless LAN Controller Configuration Guide, Release 5.0— http://www.cisco.com/en/US/products/ps6366/products_configuration_guide_book09186a008082d572.html
- Cisco Wireless Control System Configuration Guide, Release 5.0— http://www.cisco.com/en/US/products/ps6305/products_configuration_guide_book09186a008082d824.html