BYOD Network Management and Mobility Services

Revised: March 6, 2014

What’s New: The discussion of how the Cisco Mobility Services Engine (MSE) provides location context awareness for wireless devices has been updated to also discuss how the MSE enhances rogue AP and client detection, Cisco CleanAir interference detection and location, and wireless Intrusion Prevention (wIPS)—all managed through Cisco Prime Infrastructure (PI). A discussion of the benefits of Cisco CleanAir technology has been added to the chapter. Also a discussion around the Wireless Security and Spectrum Intelligence (WSSI) module for the Cisco 3600 Series AP, which provides a dedicated radio for features such as Cisco CleanAir, wIPS, rogue detection, location context awareness, and radio resource management (RRM), has also been added to the chapter.

Network Management for BYOD is separated into five sections:

- **Cisco Mobility Services Engine**—A summary of MSE and all the Cisco wireless technologies that enable MSE’s capabilities.

- **Cisco Prime Infrastructure Overview**—A brief overview that covers the basic capabilities of Cisco Prime Infrastructure. The subsequent sections are focused on specific abilities of Prime Infrastructure directly related to BYOD.

- **User and Device Tracking**—Information from multiple components is consolidated by Cisco Mobility Services Engine and displayed by Prime Infrastructure to identify and track end users and end devices on the network.

- **Interference and Intrusion—Detection and Location**—Information from multiple components is consolidated by Cisco Mobility Services Engine and displayed by Prime Infrastructure to detect, identify, and locate interference devices and intrusion attacks.

- **Template-Based Configuration**—Covers using Cisco Prime Infrastructure as a management tool for configuring and maintaining the BYOD wireless configurations across Cisco Wireless LAN Controllers (WLC).

This document does not cover the basic implementation of Prime Infrastructure and assumes the WLCs are already managed by Prime Infrastructure. For further information on Prime Infrastructure implementation, refer to the Prime Infrastructure Configuration Guide: http://www.cisco.com/en/US/products/ps12239/products_installation_and_configuration_guides_list.html.
Key Acronyms and Terminology

Table 28-1 Acronyms and Terminology

<table>
<thead>
<tr>
<th>Key Term</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prime</td>
<td>Prime refers to Cisco Prime Infrastructure in this document. The Cisco Prime Family includes other products not covered in this document.</td>
</tr>
<tr>
<td>MSE</td>
<td>Mobility Services Engine—Captures and consolidates crucial information about RF spectrum, sources of RF interference, and devices and users on the network.</td>
</tr>
<tr>
<td>wIPS</td>
<td>Wireless Intrusion Prevention System—Protects the network from penetration attacks, rogue wireless devices, and denial-of-service (DoS) attacks to improve security and meet compliance objectives.</td>
</tr>
<tr>
<td>WSSI</td>
<td>Cisco Wireless Security and Spectrum Intelligence Module for the Cisco 3600 series APs that provides always-on security scanning and spectrum intelligence, which helps avoid RF interference. The module also allows MSE to classify security threats faster and provide better location accuracy.</td>
</tr>
<tr>
<td>End Device</td>
<td>Also referred to as Endpoint. Both wired and wireless devices such as Android and Apple tablets and smartphones, wired IP phones, and laptops.</td>
</tr>
<tr>
<td>End User</td>
<td>Also referred to as User. Identified by “username” associated to one or more end devices.</td>
</tr>
<tr>
<td>WLC</td>
<td>Also referred to as Controller. Wireless LAN Controller</td>
</tr>
<tr>
<td>WLAN/SSID</td>
<td>WLAN (Wireless LAN) and SSID have a one-to-one relation and can be thought of as the same thing in this section.</td>
</tr>
</tbody>
</table>

Cisco Mobility Services Engine

Cisco Mobility Service Engine (MSE) is a physical or virtual appliance containing a modular set of applications which deliver the following services.

Cisco Base Location Services

Increase visibility into the network by capturing and consolidating crucial information about RF spectrum, sources of RF interference, and devices and users on the network. Base Location Services also help to enable a comprehensive set of real-time location services (RTLS) and include the Mobility Services API.

Cisco Connected Mobile Experiences

Connected Mobile Experiences (CMX) is a Wi-Fi platform that can enable organizations to deliver customized, location-based mobile services to end users. The CMX license on the MSE includes:

- CMX Connect to provide authentication and onboarding to Wi-Fi networks and a venue-specific, location-based, mobile landing experience.
- CMX Browser Engage to build and measure highly-targeted, location-based, mobile web campaigns.
- CMX Analytics for onsite, online, and social analytics to help organizations gain insight into end-user behavior while inside their venue.

**Cisco Wireless Intrusion Prevention System**

Wireless Intrusion Prevention System (wIPS) protects the network from penetration attacks, rogue wireless devices, and denial-of-service (DoS) attacks to improve security and meet compliance objectives.

**WSSI**

The Cisco Wireless Security and Spectrum Intelligence (WSSI) module, taking advantage of the flexible modular design of the Cisco Aironet® 3600 Series Access Point, delivers unprecedented, always-on security scanning and spectrum intelligence, which helps you avoid RF interference so that you get better coverage and performance on your wireless network.

The WSSI field-upgradeable module is a dedicated radio that off-loads all monitoring and security services from the client/data serving radios to the security monitor module. This not only allows for better client experience but also reduces costs by eliminating the need for dedicated monitor mode access points and the Ethernet infrastructure required to connect those devices into their network.

**Figure 28-1 WSSI Deployment Mode**

The WSSI Module supports the following features concurrently:

- CleanAir technology monitoring for spectrum interference
  
  The WSSI module has CleanAir technology built in to provide insight into the RF layer of the wireless network. In addition CleanAir on the WSSI module provides faster proactive mitigation of RF layer issues by continuously monitoring the Wi-Fi spectrum for interference sources. In addition with the Cisco Mobility Services Engine, better location accuracy for interferers can be achieved.

- Wireless Intrusion Prevention System (wIPS) scanning for network attacks and malicious behavior
With the WSSI module coupled with Mobility Services Engine, there is enhanced level of wIPS threat detection and mitigation. Without the WSSI module the Access Points can still mitigate and detect wIPS threats, however, the WSSI module gives additional ability to classify security threats faster and provide better location accuracy from where the threats are originating from.

- Rogue Detection
  With the WSSI module faster rogue detection and mitigation is possible.

- Location Context-awareness
  Because the WSSI module is constantly scanning the spectrum, location accuracy of clients is enhanced. With higher location accuracy of client location, IT administrators can better diagnose client connectivity issues or use the location information for better Wi-Fi capacity planning, etc.

- Radio Resource Management
  With constant-on technology, the WSSI module continuously feeds the Radio Resource Management on the network and RF health, enhancing RRM functionalities. In addition because the WSSI module is scanning the entire frequency band, it is constantly aware of various sources of interference and non-Wi-Fi traffic that can impact Wi-Fi traffic. The RRM subsystem can use this data for better channel planning.

CleanAir and wIPS are covered in additional detail in the following sections.

**wIPS**

The Cisco wIPS solution offers a flexible and scalable, 24x7x365-based full time wireless security solution to meet each customer’s needs. Security is a huge factor in today’s BYOD deployments and Cisco wIPS system is designed to meet all layer 1, 2, and 3 security challenges of a BYOD deployment. Using a Cisco solution of a WLC, PI, and MSE with context aware location services, WIPS can locate, mitigate, and contain attacks in campus environments. The various types of attacks that WIPS can support are shown in Figure 28-2.

*Figure 28-2  WIPS Attacks and Cisco Solution*
**On-wire Attacks**

An Access Point in wIPS-optimized mode will perform rogue threat assessment and mitigation using the same logic as current Cisco Unified Wireless Network implementations. This allows a wIPS access point to scan, detect, and contain rogue access points and ad hoc networks. Once discovered, this information regarding rogue wireless devices is reported to PI where rogue alarm aggregation takes place. However with this functionality comes the caveat that if a containment attack is launched using a wIPS mode access point, its ability to perform methodical attack-focused channel scanning is interrupted for the duration of the containment.

**Over-the-Air Attacks**

Cisco Adaptive wireless IPS embeds complete wireless threat detection and mitigation into the wireless network infrastructure to deliver the industry's most comprehensive, accurate, and operationally cost-effective wireless security solution.

**Non-802.11 Threats**

Cisco CleanAir® technology is an effective tool to monitor and manage your network’s RF conditions. The Cisco MSE extends those capabilities.

For a full list of which attacks can be classified by WiPS system, see the following URL:

The basic system components for a Cisco Adaptive wIPS system include:

- Access Points in wIPS monitor mode, in enhanced local mode, or with a wireless security and spectrum intelligence module
- Wireless LAN Controller(s)
- A Mobility Services Engine running the wIPS Service
- A Prime Infrastructure

An integrated wIPS deployment is a system design in which non-wIPS Mode Access Points and wIPS Mode Access Points are intermixed on the same controller(s) and managed by the same Prime Infrastructure. This can be any combination of local mode, FlexConnect mode, enhanced local mode, monitor mode, and 3600 series Access points with the WSSI module. By overlaying wIPS protection and data shares using WSSI on the Access Points, infrastructure costs can be reduced.
**wIPS Deployment Modes**

Beginning with the 7.4 release, Cisco Adaptive Wireless IPS has three options for wIPS mode access points. To better understand the differences between the wIPS mode access points, we discuss each mode.
Figure 28-4  WIPS Operation Modes

Enhanced Local Mode (ELM)

Enhanced local mode (ELM) provides wIPS detection “on-channel”, which means attackers will be detected on the channel that is serving clients. For all other channels, ELM provides best effort wIPS detection. This means that every frame the radio will go “off-channel” for a short period of time. While “off-channel”, if an attack occurs while that channel is scanned, the attack will be detected.

As an example of enhanced local mode on an AP3600, assume the 2.4GHz radio is operating on channel 6. The AP will constantly monitor channel 6 and any attacks on channel 6 will be detected and reported. If an attack occurs on channel 11 while the AP is scanning channel 11 “off-channel”, the attack will be detected.

The features of ELM are:

- Adds wIPS security scanning for 7x24 on-channel scanning (2.4GHz and 5 GHz), with best effort off-channel support.
- The access point is additionally serving clients and with Cisco Aironet 2nd generation (G2) Series Access Points, CleanAir spectrum analysis is enabled on-channel (2.4GHz and 5GHz).
- Adaptive wIPS scanning in the data channel serving local and FlexConnect APs.
- Protection without requiring a separate overlay network.
- Supports PCI compliance for the wireless LANs.
- Full 802.11 and non-802.11 attack detection.
- Adds forensics and reporting capabilities.
- Flexibility to set integrated or dedicated MM APs.
- Pre-processing at APs minimize data backhaul (that is, works over very low bandwidth links).
- Low impact on the Access Point serving client data.
Monitor Mode

Monitor Mode provides wIPS detection “off-channel”, which means the access point will dwell on each channel for an extend period of time, allowing the AP to detect attacks on all channels. The 2.4GHz radio will scan all 2.4GHz channels, while the 5GHz channel scans all 5GHz channels. An additional access point would need to be installed for client access.

Some of the features of Monitor Mode are:

- The Monitor Mode Access Point (MMAP) is dedicated to operate in Monitor Mode and has the option to add wIPS security scanning of all channels (2.4GHz and 5GHz).
- For Cisco Aironet second generation (G2) Series Access Points, CleanAir spectrum analysis is enabled on all channels (2.4GHz and 5GHz).
- MMAPs do not serve clients.

AP3600 with WSSI Module—The Evolution of Wireless Security and Spectrum

A Cisco 3600 series Access point with the WSSI module uses a combination of “on-channel” and “off-channel” operation. This means that the AP3600 2.4GHz and 5GHz internal radios will scan the channel that they are serving clients with and the WSSI module will additionally operate in monitor mode and scan all channels.

Some of the features of the WSSI Module are:

- The industry’s first Access Point enabling the ability to simultaneously “Serve clients, wIPS security scan and analyze the spectrum using CleanAir Technology”.
- Dedicated 2.4GHz and 5GHz radio with its own antennas enabling 7x24 scanning of all wireless channels in the 2.4GHz and 5GHz bands.
- A single Ethernet infrastructure provides simplified operation with fewer devices to manage and optimized return on investment of the AP3600 wireless infrastructure and the Ethernet wired infrastructure.

Additional details on deploying a WiPS solution can be found at: http://www.cisco.com/en/US/docs/wireless/technology/wips/deployment/guide/WiPS_deployment_guide.html

CleanAir

CleanAir technology is supported both on the Cisco Unified Wireless Controllers (CUWN) and the Converged Access platforms (Cisco 5760 wireless LAN controllers and Catalyst 3850 Series switches). While the section below addresses CleanAir technology and CUWN WLCs, the same concepts apply to Converged Access platforms. Readers are encouraged to look at design and deployment guides for both CUWN controllers and Converged Access platforms for CleanAir technology.

Cisco CleanAir technology is the integration of Cisco Spectrum Expert Wi-Fi analysis tools with Cisco access points. Before Cisco CleanAir, operators had to walk around with an instrument to detect signals of interest and physically locate the device that generated them. Cisco CleanAir helps to automate these
tasks within the system management function by adding additional intelligence over Cisco Spectrum Expert, thereby augmenting the overall experience in proactively reclaiming control over the radio spectrum.

The components of a basic Cisco CleanAir solution are the Cisco Wireless LAN Controller and Cisco Aironet 2600 or 3600 Series Access Points. To take advantage of the entire set of Cisco CleanAir features, Cisco Prime Infrastructure can display in real time the data retrieved from CleanAir. Adding Cisco Mobility Services Engine further enhances the available features and provides the history and location of specific interference devices. To get full value from the information that the CleanAir system will supply, the PI and MSE together are key to leveraging a wider efficacy of CleanAir, providing user interfaces for advanced spectrum capabilities like historic charts, tracking interference devices, location services, and impact analysis.

An AP equipped with Cisco CleanAir technology will collect information about non-Wi-Fi interference sources, process it, and forward it to the Wireless LAN Controller (WLC). The WLC is an integral core part of the CleanAir system. The WLC controls and configures CleanAir capable Access Points (AP), collects and processes spectrum data, and provides it to the PI and/or the MSE (Mobility Services Engine). The WLC provides local user interfaces (GUI and CLI) to configure basic CleanAir features and services and display current spectrum information.

The Cisco Prime Infrastructure provides advanced user interfaces for CleanAir including feature enablement and configuration, consolidated display information, historic Air Quality records, and reporting engines. The Cisco MSE is required for location and historic tracking of interference devices and provides coordination and consolidation of interference reports across multiple WLCs.

In the current BYOD CVD, the Mobility Services Engine provides a way to track clients, IT devices, and non-WiFi interference sources in addition to rogues and wiPS threats. The campus BYOD network with the addition of MSE is shown in Figure 28-5.

**Figure 28-5 MSE in Campus BYOD**
Figure 28-6 provides a high-level view of how the MSE enhances Cisco CleanAir technology.

**Figure 28-6  How the MSE Enhances Cisco CleanAir Technology**

1. **Cisco 3600 APs with CleanAir chipset and WSSi modules scan both on and off-channel for interference.**
2. **Interference information from CleanAir aggregated at WLC via Interference Device Reports (IDRs) and Air Quality Index (AQI) reports generated by the APs and sent to WLCs via CAPWAP.**
3. **Interference Device Report (IDR) information sent from WLC to MSE**
4. **MSE can determine the location and provide historic tracking of interference sources, and provide correlation between WLCs**
5. **Network administrator can receive alerts, view location on floor plans, and/or run reports regarding interference sources**

**Figure 28-6 assumes the wireless infrastructure and MSE are already installed and operational with CAS/Basic Location Services enabled.**

- In Step #1 Cisco 3600 Access Points with the CleanAir chipset scan all channels for interference sources. These interference sources could be non-802.11 devices such as Bluetooth, Microwave Ovens, Video Cameras, etc.
- In Step #2 the interference information from CleanAir is aggregated at the wireless controller via Interference Device Reports (IDRs) and Air Quality Index (AQI) reports generated by the Access Points and sent to the wireless controller via CAPWAP. The Interference Device Reports are generated every time a new interferer is either detected or un-detected. In addition IDR reports for existing interferers are sent every 90 seconds to the WLC. Air Quality report on the other hand are sent every 15 minutes to the controller and also contain important information regarding the Air Quality index of the particular channel (or channels). The higher the AQI index, the better and cleaner the RF channel and lower the AQI, the more clogged the RF channel.
- In Step #3 the WLC aggregates Interference Device Report (IDR) from different APs into device clusters. It is possible that several APs on the floor detect the same interference source. The WLC aggregates IDR reports from different APs and makes an intelligent analysis of similar devices and groups them together. The WLC forwards the information onto the MSE via the Network Mobility Services Protocol (NMSP).
- In Step #4 the MSE can then determine the location of and provide historic tracking of interference sources. In addition in a campus environment with multiple WLCs and switches, the MSE provides a secondary level of intelligent analysis on the interference sources and can detect the same
interference sources detected by APs in the same geographical location but connected to different controllers. The MSE to provide a system-wide view (across multiple WLCs) of interference sources.

- In Step #5 the network administrator can receive alerts, view location on floor plans, and run reports regarding interference sources. The network administrator can also use the PI to view reports on channel changes related to CleanAir.

In addition to providing location, interference device reports, and air quality index metrics, the CleanAir system provides the Radio Resource Management RF metrics to mitigate non-WiFi interference threats. This is primarily done through two features—the Persistent Device Avoidance Feature or the Event Driven RRM feature. Both of them are discussed below.

**Persistent Device Avoidance (PDA)**

In a campus environment certain 2.4GHz/5GHz non-Wi-Fi devices are present constantly. They are not intended to harm Wi-Fi networks, but cannot be removed from the premises either (for example, microwave ovens—which cause interference in the 2.4GHz frequency band—in break rooms). The Persistent Device Avoidance feature helps RRM take into consideration these devices when channel planning. The PDA tells the RRM system about all the devices that are consistently present at all times (for example microwave ovens). Using this information, RRM will update channel plans to avoid putting APs on channels near the persistent device channel in the geographical area. This helps in better coverage and channel planning.

**Event Driven RRM (ED-RRM)**

Interference by nature is not predictable and also transient in nature. It is possible to have interference sources that turn on for a short duration of time and shut off after that. Some devices like video cameras can create havoc on Wi-Fi networks by consuming the entire channel by transmitting 100% of the time. The ED-RRM feature helps RRM mitigate such sudden extremely strong source of RF interference. ED-RRM identifies devices with extremely high severity on its channel and alerts the RRM system. The RRM system uses this information to locally change the impacted AP’s channel to a cleaner channel where it can continue to serve clients. If at a future time the severe interference has been located via MSE and removed from the network, the RRM system can automatically re-plan the network to include the impacted channel.

CleanAir can be deployed in both Local Mode and Monitor mode of the AP. Local Mode APs serve clients while also scanning for interference sources. Monitor Mode APs do not serve any clients but strictly act as a scanning AP not just for CleanAir but other features like wIPS, rogue detection, etc. However having an overlay monitor mode APs for CleanAir deployment can be costly and prohibitive. Cisco now offers the Wireless Security and Spectrum Intelligence (WSSI) module for the Cisco 3600 AP. The WSSI module provides a dedicated radio with dedicated antennas which provides continuous scanning across all channels. Simultaneously the 3600 AP also supports data transport for clients via the other two integrated radios within the AP.

For more information on configuration and management of CleanAir, see:
ClientLink

With bring your own device (BYOD), a proliferation of client devices has started to penetrate the enterprise wireless landscape. The “proliferation of client devices” generally refers to the various types of wireless clients accessing the network: smartphones, laptops, tablets, etc. Across these clients, different wireless standards are used to access the wireless network: IEEE 802.11a, 802.11g, 802.11n, and the newest standard, 802.11ac. The 802.11ac standard provides an increase in performance for devices. The performance can be further increased if the devices support multiple antennas which allow them to transmit and/or receive one, two, or even three spatial streams. This technology is referred to as Multiple-Input-Multiple-Output (MIMO). However legacy 802.11a/g clients (which do not support MIMO) often hinder the network’s ability to take advantage of the additional performance gains of 802.11ac. With this mixed environment of legacy clients such as 802.11a/g and 802.11n clients with one, two, or three spatial streams, network infrastructures must be able to support a varying combination of different wireless standards.

Cisco ClientLink 2.0 technology specifically focuses on mixed-client networks, optimizing overall network capacity by helping ensure that 802.11a/n and 802.11ac clients operate at the best possible rates, especially when they are near cell boundaries. Cisco ClientLink 2.0 technology helps solve the problems of mixed-client networks by making sure that older 802.11a/n clients operate at the best possible rates. Cisco ClientLink 2.0 improves performance on both the uplink and the downlink, providing a better user experience during web browsing, email, and file downloads. ClientLink 2.0 technology is based on signal processing enhancements to the access point chipset and does not require changes to network parameters.

Cisco Prime Infrastructure Overview

Cisco Prime Infrastructure is an exciting new offering from Cisco aimed at managing wireless and wired infrastructure while consolidating information from multiple components in one place. While allowing management of the infrastructure, Prime Infrastructure gives a single point to discover who is on the network, what devices they are using, where they are, and when. The capabilities of Prime Infrastructure and the other components featured go far beyond the focus of this document. A brief overview of Cisco Prime Infrastructure and supporting components follows.

Prime Infrastructure and Supporting Components

Cisco Prime Infrastructure interacts with many other components to be a central management and monitoring portal. Prime Infrastructure has integration directly with two other appliance-based Cisco products, the Cisco Mobility Services Engine and Identity Services Engine for information consolidation. Prime Infrastructure controls, configures, and monitors all Cisco Wireless LAN Controllers (WLCs), and by extension, all Cisco Access Points on the network. Prime Infrastructure also configures and monitors Cisco Catalyst switches and Cisco routers.
Figure 28-7  Prime Infrastructure Component Interaction Summary

Table 28-2  Prime Infrastructure Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prime Infrastructure</td>
<td>Cisco Prime Infrastructure is the core component that sends information to and consolidates information from the other four component types.</td>
</tr>
<tr>
<td>ISE</td>
<td>Cisco Identity Services Engine is the core component of BYOD for user and device authorization and access to the network. ISE provides user information to Prime Infrastructure.</td>
</tr>
<tr>
<td>WLC</td>
<td>Cisco Wireless LAN Controller is configured, controlled, and monitored by Prime Infrastructure. WLCs provide Prime Infrastructure with a wealth of real-time wireless environment and client device information.</td>
</tr>
<tr>
<td>Switch/Router</td>
<td>Cisco switches and routers are configured, controlled, and monitored by Prime Infrastructure. Wired device information is provided to Prime Infrastructure to be consolidated with wireless device information.</td>
</tr>
<tr>
<td>MSE</td>
<td>Cisco Mobility Services Engine complements Prime Infrastructure with current and historical location, usage, and other information for all devices Prime Infrastructure sees.</td>
</tr>
</tbody>
</table>

The following link has more information about Cisco Prime Infrastructure and the rest of the Cisco Prime family of products: [http://www.cisco.com/go/prime](http://www.cisco.com/go/prime).

User and Device Tracking

The ability to track users and devices on the wired and wireless networks is critical to knowing who is accessing the network, with what they are accessing it, where are they accessing it, and when they accessed it.
Understanding who is accessing the corporate network, what they are using, and where they are connected allows customers to better understand:

- Location and movement of employees and devices on the network
- Suspicious or unauthorized access of the network
- Location of missing or stolen assets, such as in a college campus environment
- Location of unknown devices on the network
- Current utilization of the network

Adding historical logging of when users and devices access the network allows:

- Persistent records of when users and devices accessed the network and their specific locations
- Searchable historical data of user and device access for tracking and troubleshooting issues
- Historical port utilization data

**Components**

Cisco Prime Infrastructure is the central portal for user and device tracking. Prime Infrastructure uses information from multiple places to give a single, consolidated view of current and historical user and device access to the network. Figure 28-9 adds to Figure 28-7 showing how the components cover the Who, What, Where, and When aspects of user and device tracking.
Figure 28-9 Prime Infrastructure Component Interaction Summary for User and Device Tracking

Figure 28-10 shows a more detailed view of how Prime Infrastructure interacts with the rest of the architecture. The five main components needed for User and Device tracking of both wired and wireless users are listed below with brief summaries of each.

Table 28-3 Prime Infrastructure Interaction with Other Infrastructure Components

<table>
<thead>
<tr>
<th>Components</th>
<th>Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Prime—MSE</td>
<td>Prime receives current and historical location information for mobile devices</td>
</tr>
<tr>
<td>2 Prime—ISE</td>
<td>Prime receives user information including username and device MAC and authentication history</td>
</tr>
<tr>
<td>3 Prime—Switch/Router</td>
<td>Prime receives wired device information including port and MAC. Prime sends/receives component configuration.</td>
</tr>
<tr>
<td>4 Prime—WLC</td>
<td>Prime receives wireless user and extensive device information. Prime sends/receives component configuration.</td>
</tr>
<tr>
<td>5 Switch—ISE</td>
<td>RADIUS authentications</td>
</tr>
<tr>
<td>6 WLC—ISE</td>
<td>RADIUS authentications</td>
</tr>
</tbody>
</table>
To locate and track users and devices, Prime Infrastructure pulls information from all of these sources, consolidating it based mainly on common MAC. Prime Infrastructure is device focused and displays detailed reports based on a particular device. Prime Infrastructure also has the ability to show all devices with which a particular user accesses the network, giving the ability to track a particular user across multiple wireless and wired devices.

Locating Users and Devices

There are two basic ways to display information on users and devices. Both options are considered “Search” options, although the abilities to filter and display based on an extensive list of criteria goes far beyond what most would consider a simple search option.

**Figure 28-11   Types of Search**

<table>
<thead>
<tr>
<th>Context Aware Dashboard Search</th>
<th>Standard and Advanced Search</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Simple search of Username, MAC, or IP</td>
<td>• Simple search of Username, MAC, or IP</td>
</tr>
<tr>
<td>• Results for single end user or end device</td>
<td>• Advanced Search based on extensive list of criteria</td>
</tr>
<tr>
<td>• Location focused results</td>
<td>• List of results for all end user and end devices that match criteria</td>
</tr>
<tr>
<td></td>
<td>• Usage focused results</td>
</tr>
</tbody>
</table>

**Context Aware Dashboard Search**

Context Aware search is used to display information on a single device based on current MAC, IP, or Username of the end user of the device. While limited in how you can search and what is displayed, this option does give you a slightly different view of location information compared to the standard search.

The Context Aware Dashboard in Figure 28-12 has a search box titled “Location Assisted Client Troubleshooting”, which is where the search is executed. The search instantly resolves the MAC, IP, or Username to the device and display that device only.
The results shown in Figure 28-13 are common to both types of search and give quite a bit of current information about the device and end user of it, if there is one.

The information in the search results unique to the Context Aware Search is location based. Standard and Advanced Search show “Association History”, which includes location, but not in the same format.

Context Aware Search results give you the ability to easily see exactly where a device was at a given time as well as show historical motion of the device. Using the “Play” feature, the device location is shown being updated on a map for a visual representation of movement, which can be accurate down to several feet in a properly implemented wireless network.
Figure 28-14 shows the location results with a blue square showing current location on the floor plan map adjacent. Pressing “Play” would show the blue square moving as location references were cycled through.

**Figure 28-14  Context Aware Search Location Results**

### Standard and Advanced Search

In addition to searching for clients or devices using the Context Aware Dashboard, Standard and Advanced Search may be performed in the top right corner of the Prime Infrastructure interface, visible at any time. Much more granular searches may be performed using the Advanced Search option shown in Figure 28-15. Search results are more device usage focused with the Standard and Advanced Search, but still contain location information.

**Figure 28-15  Standard and Advanced Search Box**

With Advanced Search, results for many end users or end devices that meet a particular set of criteria may be displayed instead of looking for one particular user or device. Parameters such as physical location, type of user, SSID, and even posture/authentication status may be used. Figure 28-16 shows a subset of criteria available.
Figure 28-16  Advanced Search Criteria

The form above is dynamic, changing as selections are made, which means this image shows only a subset of the criteria available for the “Clients” category, which in this case refers to both end devices and end users.

Additional search criteria and information may be found in the Cisco Prime Infrastructure Configuration Guide:

Figure 28-17 shows the search results list, which contains both wired and wireless users unless one type is filtered out. In this example two devices are shown, the first a wireless device and the second wired.

Figure 28-17  Standard and Advanced Search Results List

An extensive amount of information is available from just the search results screen. The result columns may be customized and results list sorted by any of those columns. Figure 28-18 shows a list of available columns.
Figure 28-19 through Figure 28-24 show examples of basic and extended information shown for individual devices selected from the search list.

Figure 28-19 shows the same basic end user and end device information as the Context Aware Search discussed earlier.
Figure 28-19  General User and Device Details

Client 18:46:17:e5:43:68
Refreshed 2012-May-02, 14:05:55 EST

Client Attributes

<table>
<thead>
<tr>
<th>General</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name: z-ad-user-05</td>
<td>Controller Name: z-wk5508-1</td>
</tr>
<tr>
<td>IP Address: 172.26.152.151</td>
<td>AP Name: Z-AP3502-1</td>
</tr>
<tr>
<td>Vendor: Samsung</td>
<td>AP Type: Cisco AP</td>
</tr>
<tr>
<td>Endpoint Type: Undetermined</td>
<td>AP Blee Radio MAC: 00:25:72:7c:49:90</td>
</tr>
<tr>
<td>Client Type: Regular</td>
<td>Anchor Controller: Data Not Available</td>
</tr>
<tr>
<td>Media Type: Lightweight</td>
<td>Association ID: 2</td>
</tr>
<tr>
<td>Mobility Status: Local</td>
<td>Port: 1</td>
</tr>
<tr>
<td>Hostname: Data Not Available</td>
<td>Interface management:</td>
</tr>
<tr>
<td></td>
<td>SSID: z-ssid-2</td>
</tr>
<tr>
<td></td>
<td>Profile Name: z-ssid-2</td>
</tr>
<tr>
<td></td>
<td>Protocol: 802.11n(5GHz)</td>
</tr>
<tr>
<td></td>
<td>VLAN ID: 0</td>
</tr>
<tr>
<td></td>
<td>AP Mode: local</td>
</tr>
</tbody>
</table>

Security

<table>
<thead>
<tr>
<th>Security Policy Type: WPA2</th>
<th>EAP Type: PEAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>On Network: Yes</td>
<td></td>
</tr>
<tr>
<td>802.11 Authentication: Open System</td>
<td></td>
</tr>
<tr>
<td>Encryption Cipher: CCMP (AES)</td>
<td></td>
</tr>
<tr>
<td>EAP Type: PEAP</td>
<td>EAP Type: PEAP</td>
</tr>
<tr>
<td>AAA Override ACL: Name: none</td>
<td>AAA Override ACL: Name: none</td>
</tr>
<tr>
<td>Redirect URL: none</td>
<td>Redirect URL: none</td>
</tr>
<tr>
<td>ACL Name: none</td>
<td>ACL Name: none</td>
</tr>
<tr>
<td>ACL Applied Status: N/A</td>
<td>ACL Applied Status: N/A</td>
</tr>
<tr>
<td>RADIUS RAC State: RUN</td>
<td>RADIUS RAC State: RUN</td>
</tr>
<tr>
<td>TrustSec Security Group: Data Not Available</td>
<td></td>
</tr>
</tbody>
</table>

Figure 28-20 shows association times, durations, and locations, which is similar but not the same as the location history with the Context Aware Search.

Figure 28-20  Device Association History

<table>
<thead>
<tr>
<th>Association Time</th>
<th>Controller Name</th>
<th>Duration</th>
<th>User Name</th>
<th>IP Address</th>
<th>IP Address Type</th>
<th>AP Name</th>
<th>SSID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012-May-10, 15:13:00 EST</td>
<td>z-wk5508-1</td>
<td>5 min 0 sec</td>
<td>z-ad-user-03</td>
<td>172.26.152.135</td>
<td>Dual-Stack</td>
<td>Z-AP3502-1</td>
<td>z-ssid-1</td>
</tr>
<tr>
<td>2012-May-10, 15:18:00 EST</td>
<td>z-wk5508-1</td>
<td>2 hrs 50 min 1 sec</td>
<td>z-ad-user-03</td>
<td>172.26.152.155</td>
<td>Dual-Stack</td>
<td>Z-AP3502-1</td>
<td>z-ssid-1</td>
</tr>
<tr>
<td>2012-May-10, 18:08:01 EST</td>
<td>z-wk5508-1</td>
<td>3 days 18 hrs 15 min 46 sec</td>
<td>z-ad-user-03</td>
<td>172.26.152.155</td>
<td>Dual-Stack</td>
<td>Z-AP3502-1</td>
<td>z-ssid-1</td>
</tr>
<tr>
<td>2012-May-14, 12:43:48 EST</td>
<td>z-wk5508-1</td>
<td>12 hrs 15 min 5 sec</td>
<td>z-ad-user-03</td>
<td>172.26.152.135</td>
<td>Dual-Stack</td>
<td>Z-AP3502-1</td>
<td>z-ssid-1</td>
</tr>
</tbody>
</table>

Figure 28-21 is pulled directly from ISE and shows recent authentication successes and failures.
**Figure 28-21**  **Device Authentication History**

Identity Services Engine

<table>
<thead>
<tr>
<th>Last Time</th>
<th>Between Dates</th>
<th>And Dates</th>
<th>Status</th>
<th>Failure Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 Hours</td>
<td>/03/2012</td>
<td>/03/2012</td>
<td></td>
<td>None</td>
</tr>
</tbody>
</table>

Authentication Records

<table>
<thead>
<tr>
<th>Date</th>
<th>Status</th>
<th>Failure Reason</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 03, 2012 01:10 AM</td>
<td>Authentication Passed</td>
<td>None</td>
<td>14:39:17</td>
</tr>
<tr>
<td>May 03, 2012 01:20 PM</td>
<td>Authentication Passed</td>
<td>None</td>
<td>14:39:17</td>
</tr>
<tr>
<td>May 03, 2012 01:31 PM</td>
<td>Authentication Passed</td>
<td>None</td>
<td>14:39:17</td>
</tr>
<tr>
<td>May 03, 2012 06:45 AM</td>
<td>Authentication Passed</td>
<td>None</td>
<td>14:39:17</td>
</tr>
<tr>
<td>May 03, 2012 08:55 AM</td>
<td>Authentication Passed</td>
<td>None</td>
<td>14:39:17</td>
</tr>
<tr>
<td>May 03, 2012 09:07 AM</td>
<td>Authentication Passed</td>
<td>None</td>
<td>14:39:17</td>
</tr>
<tr>
<td>May 03, 2012 09:17 AM</td>
<td>Authentication Passed</td>
<td>None</td>
<td>14:39:17</td>
</tr>
</tbody>
</table>

**Figure 28-22** shows signal quality for various, changeable time frames in graph format.
Figure 28-22  Device Signal Quality and Usage History

- **Client RSSI History**

- **Client SNR History**

- **Bytes Sent and Received (kbps)**

- **Packets Sent and Received (per sec.)**
Figure 28-23 shows the device in its current location, along with any additional information chosen. In this example, only heat map and AP location is selected, but many other items are available for display, such as interfering devices and other clients.

**Figure 28-23  Floor Plan Heat Map with APs and Client Device**

![Floor Plan Heat Map with APs and Client Device](image)

Figure 28-24 shows details of any device shown on the heat map.

**Figure 28-24  Device Detail Pop-up from Heat Map**

![Device Detail Pop-up from Heat Map](image)

**Interference and Intrusion—Detection and Location**

Through the Cisco Prime Infrastructure (PI) interface, interference sources and attackers can be easily identified and located. Prime Infrastructure works with Cisco Mobility Services Engine (MSE) to retrieve, consolidate, and provide useable interferer and attacker device detail and location data.
Interference Detection and Location

Cisco Mobility Services Engine (MSE) processes data from multiple components to locate and track interference sources. Cisco Prime Infrastructure (PI) displays interference device history and location information from MSE including graphical representation on floor maps to show precise location.

Locating interference sources is critical to both optimal wireless performance and network security. Interference sources range from non-wifi devices that create noise in frequencies used by the corporate wifi network, to non-corporate wifi devices that may both reduce corporate wifi performance as well as be a security risk. A rogue AP, for example, is both a security risk as well as a possible source of performance degradation for the corporate wifi network.

Figure 28-25 is the Interferer display filter showing all interferer types displayed by Prime Infrastructure. The default is to show all interferers.

Figure 28-25 Prime Infrastructure Interferer Display Filter

Figure 28-26 is an example of a floor map with three types of possible interferers detected and displayed. Displayed are two non-wifi devices, a WiMAX and Bluetooth device depicted by small lightning bolts. A Rogue AP, which is classified separately within Prime Infrastructure, is also shown as the skull and crossbones on the map.
Selecting interference devices on the map displays summary information about the device. Figure 28-27 and Figure 28-28 shown an example of the summary information provided when selecting the WiMAX device and Rogue AP shown above.
Detailed information may then be accessed via the “Details” link within the summary display.

**wIPS Intrusion Detection and Location**

Cisco Mobility Services Engine (MSE) processes wIPS data from the wireless controllers to locate and track malicious intrusion attacks. Before the MSE has access to this information, wIPS monitoring must be enabled in the wireless network. The use of Cisco 3600 series APs with WSSI modules installed greatly enhances wIPS monitoring capability. Information regarding WSSI modules and the types of wIPS implementations is detailed earlier in this chapter.

Cisco Prime Infrastructure displays wIPS intrusion location and history information from MSE including graphical representation on floor maps to show precise locations. In addition to detecting and location malicious attacks, Prime Infrastructure provides information about possible security issues detected throughout the network. Figure 28-29 is an example of portions of the Security Overview screen in Prime Infrastructure.
Figure 28-29  Security Overview—Top Security Issues

- Telnet is enabled on the controller (1)
- "MFP Client Protection" is set to "Optional" for WLAN (1)
- SNMP v1/v2 is configured with default community strings on the controller (1)
- WLAN interface is set to "management" interface (1)
- "Protection Type" is set to "None" on the controller (1)

Footnotes:
Security index is calculated as part of 'Configuration Sync' background task. 
Last execution time: 2013-Nov-06, 14:00:05 EST
Specific wIPS attack information summarized in Figure 28-30 may be selected for more detail. wIPS attacks may be viewed on a floor map, providing the physical location of the attacker based on triangulated data from the APs. Figure 28-31 shows an individual attack detected and located by MSE.
wIPS attack details may be accessed directly from the floor map by selecting the attack icon, displaying the summary as shown in Figure 28-31. Detailed information of the attack may then be accessed via the “wIPS Attack Details” link within the summary display. An example of detailed attack information is shown in Figure 28-32.
This detailed information is accessible via attack and alarm reporting as well, allowing linking back into the floor maps from the attack details to show precise location. Various types of notifications, such as auto generated email, may be enabled to allow immediate notification of specific types of attacks within the network.

**Template-Based Configuration**

This section covers the use of Cisco Prime Infrastructure to deploy and maintain configurations to Cisco Wireless LAN Controllers (WLCs) matching the BYOD configurations referenced in this document.

Cisco Prime Infrastructure has the ability to control configuration of Cisco Wireless LAN Controllers (WLCs) directly or through the use of templates. One template will not configure the entire controller. Templates are separated out to granularly cover each feature of the controller. Templates exist for just about every small feature that can be implemented on the controllers and many portions of the templates can be modified during deployment to accommodate unique settings in WLCs. Templates can be configured for a common configuration across all WLCs as well as be implemented across a sub-set of WLCs or individual WLCs.

---

**Note**

Each WLAN has exactly one SSID and the two terms may be thought of as being the same thing for simplicity in understanding this content: **WLAN = SSID**.
Template-based configuration has a number of advantages compared to individual configuration of WLCs:

- **Consistent Configuration of WLCs**
- **Multiple Templates for Variations of Deployment**
- **Rapid Deployment of New or Replacement Components**
- **Staged Rollout of Configuration Changes with Rapid Rollback**

### Consistent Configuration of WLCs

Inconsistencies in configuration can easily occur when configuring multiple WLCs through their local web-based administrative interfaces. Inconsistencies can have far reaching negative impact on WLAN functionality, security, and performance.

Inconsistencies in even the order of configuration can sometimes have serious impacts. For example, configuring multiple WLANs in different orders on different controllers will cause the WLAN IDs (an integer that uniquely identifies each WLAN) to be inconsistent. WLAN IDs are used by ISE to determine how the client should be treated. Inconsistent WLAN IDs may result in a client attaching to a particular SSID and being assigned access as if they were attached to a different SSID.

One important note here, however, is that Prime Infrastructure will have the controller auto-assign the WLAN ID. If the base configuration of the controllers starts in an inconsistent state, such as a WLAN existing on one controller that does not exist on another, the WLAN IDs will be set inconsistently when applied from Prime Infrastructure. Checks should be done to ensure the WLAN IDs are consistent across all controllers.

### Multiple Templates for Variations of Deployment

Variations in deployment may be required for some features of WLCs based on model or location in the network. If a WLC is being used for dedicated guest access, its configuration for certain features would differ from other WLCs on the network, requiring some variation of templates.

Prime Infrastructure supports multiple templates for the same feature, allowing templates to be created with variation for WLCs. Templates may be applied to all WLCs or individually selected WLCs at the time of application.

### Rapid Deployment of New or Replacement Components

By creating templates for WLC configuration, new and replacement WLCs may be rapidly configured from the latest templates, reducing time to deploy and eliminating errors from misconfigurations.

### Staged Rollout of Configuration Changes with Rapid Rollback

Multiple templates for a specific feature can be created allowing an altered configuration to co-exist with the current configuration in template form. The new configuration template can then be tested on one or more WLCs with ease of rollback to the previous configuration template should issues arise.
Note

The acronym WLC (Wireless LAN Controller) is frequently used in this document while some of the interfaces shown use the common term “Controller”. In this document “WLC” and “Controller” refer to the same thing: **WLC = Controller**.

**Template Creation and Implementation**

Template creation and implementation is a fairly straightforward process in Prime Infrastructure with a few caveats. The templates and configurations that follow are specific to the BYOD solution in this document and are but a tiny subset of the many settings and features that are needed for implementing an enterprise wireless network.

This section assumes the WLCs are already managed by Prime Infrastructure. For further information on Prime Infrastructure implementation, refer to the Prime Infrastructure Configuration Guide: http://www.cisco.com/en/US/products/ps12239/products_installation_and_configuration_guides_list.html.

**Template Creation**

Template creation for WLC configuration may be handled in one of three ways:

1. Create new templates directly in Prime Infrastructure.
2. Configure a WLC through Prime Infrastructure and then create templates from that configuration.
3. Configure a WLC through the local WLC web interface and then create templates from that configuration.

The following material focuses on option 2, configuring a WLC through Prime Infrastructure followed by creation of templates to configure additional WLCs and make changes to the original WLC. This approach would seem the most logical since it incorporates option 3 as well if the WLC were already configured.

This approach would also be appealing to someone wanting to learn the interface and operation of Prime Infrastructure and the WLC at the same time, using a separate WLC to create the configurations and templates to be deployed in production at a future date. For base template creation, functional trials, and understanding of the solution, most of the features covered in this document may be deployed using a relatively inexpensive Cisco 2504 with the base license and a single AP. Two key features the 2504 lacks as part of the BYOD solution are the ability to act as a DMZ Guest WLC and the ability to rate limit traffic. Both of those features are covered in Chapter 21, “BYOD Guest Wireless Access.” All other features and abilities in the BYOD solution are supported on this platform.

Due to the extensiveness of configuration for a FlexConnect environment, not every step is shown for the initial configuration. Using the Prime Infrastructure interface instead of the WLC interface directly should be fairly straightforward. Minor differences in location of options and features in the Prime Infrastructure interface are shown.

Using option 2 from above (Configure a WLC through Prime Infrastructure and then create templates from that configuration) the following steps are used. If beginning with a WLC that was directly configured, just skip steps 1 and 3.

- **Step 1**—Configure Base Network Connectivity on the New WLC
- **Step 2**—Add the WLC as a Managed Device to Prime Infrastructure
- **Step 3**—Using Prime Infrastructure, Directly Configure the WLC
• Step 4—Create Templates from the Configured WLC
• Step 5—Deploy Templates on One or More WLCs

Step 1—Configure Base Network Connectivity on the New WLC
This step should be completed with documentation for the WLC you are implementing. Documentation for all Cisco WLCs can be found at: http://www.cisco.com/web/tsweb/redirects/mm/support/wireless.html.

Step 2—Add the WLC as a Managed Device to Prime Infrastructure
In Prime Infrastructure, use the Device Work Center and manually add the device, as shown in Figure 28-33.

Figure 28-33 Device Work Center—Add a Device

You do not need to specify the WLC type as Prime Infrastructure will determine it during the synchronization process. Alternatively, the WLC may be added through the discovery process, which is not shown.

After the WLC is added it will synchronize any existing configuration with Prime Infrastructure. This process should take only a couple of minutes and show a Device Status of “Managed” in the Device Work Center. It will also be placed in the appropriate Device Type folder, which can be expanded on the left side of the Device Work Center screen shown in Figure 28-33.
Step 3—Using Prime Infrastructure, Directly Configure the WLC

The WLC may now be directly configured in the Device Work Center, similar to being on the web-based interface of the WLC itself, by selecting the WLC and then the Configuration tab in the section below. The configuration interface is very similar, but not exactly the same. Figure 28-34 shows how the WLC interface main categories map to the Prime Infrastructure categories.

Figure 28-34   Mapping of WLC Interface Categories to Prime Infrastructure Categories

Be aware that one significant feature, AAA Override, is in a different location.

The feature AAA Override is shown in the Advanced tab of the WLAN settings when configuring through the WLC interface. This same feature is in the Security tab of the WLAN settings when configuring through Prime Infrastructure, as shown in Figure 28-35.
Take note of the WLAN ID caveat at the end of this section as it is important to both the creation of WLANs initially as well as template-based deployment of WLANs.

**Step 4—Create Templates from the Configured WLC**

Creating templates from a configured WLC is a fairly simple process. An automated process creates templates of everything in the WLC that can have a template created. To accomplish this, go to the device in Device Work Center, the same place as the last step. Select the configured WLC and choose Configure and then Discover Templates from Controller, as shown in Figure 28-36.

**Figure 28-36 Discover Templates from Controller**

After the template discovery process completes, the templates are found in the Configuration Templates section in the Design section from the top menu, as shown in Figure 28-37.

**Figure 28-37 Configuration Templates**
The newly discovered templates will be shown under **My Templates**, then **Discovered Templates** as shown in **Figure 28-38**.

**Figure 28-38   Discovered Templates**

![Discovered Templates](image)

There will be many templates shown in this section, but only a small number of them are really needed. Before any customization or deployment of templates occurs, it is highly recommended to organize the needed templates into a custom folder. First, create a new folder by placing the mouse pointer next to **My Templates**, which pops up a box. Click **Add Folder**, as shown in **Figure 28-39**.

**Figure 28-39   Add Folder**

![Add Folder](image)

After creating the folder, in this case named BYOD Templates, place the pointer next to each of the desired templates, one at a time, and click **Move to Folder**, moving them to the newly created folder, as shown in .
Once complete, all the desired templates will show up in the new folder, ready for editing and deployment, as shown in Figure 28-41.

**Figure 28-41**  BYOD Templates

Step 5—Deploy Templates on One or More WLCs

It is fairly straightforward to deploy standard templates with no unique settings. Deploying templates that require unique configurations, such as FlexConnect Groups, is more involved.

A FlexConnect Group has specific APs associated with it, which will be different from WLC to WLC. A simple static template would not be particularly useful and the deployment must accommodate customization. The following template deployment is of a FlexConnect Group, showing the most complex type of deployment as an example.

At the bottom of every template is a button to deploy it, shown in Figure 28-42, which when clicked shows the deployment screen.
When a FlexConnect Group template is launched, the target WLCs must be chosen. In this example two WLCs of different types are selected, as shown in Figure 28-43.

When selected, you see the Value Assignment screen, shown in Figure 28-44. This section allows you to assign values and resources to each WLC independently. In this example APs may be added to the FlexConnect Group separately for each WLC. The APs are added by clicking Add AP on the far right of the screen (not shown) which will bring up a list of all APs that are visible to Prime Infrastructure.

After completion of customization, the template can be deployed immediately or scheduled.

Caveat 1—WLAN ID

WLAN ID is used by ISE in determining what SSID (WLAN) clients are using to connect to the network. This ID is unique to each WLAN on each controller, so ensuring each WLAN has the same WLAN ID on each controller is essential for proper operation and security.

Ensuring this can become complex for large enterprise customers with multiple WLCs. Take note of the following:

- Prime Infrastructure cannot set the WLAN ID and lets the WLC assign the WLAN ID.
- WLCs with existing WLANs increment to the next available integer.
- Creating a WLAN using the WLC web interface directly allows the WLAN ID to be chosen.
- WLAN IDs cannot be changed once the WLAN is created.
The following simple example shows the issue:

- WLC A has no WLANs defined.
- WLC B has WLAN “Special-SSID” with WLAN ID 1.

Using Prime Infrastructure to create a new WLAN, “Employee-SSID”, across all WLCs results in it being assigned WLAN ID 1 on WLC A and WLAN ID 2 on WLC B.

- WLC A
  - WLAN “Employee-SSID” WLAN ID 1
- WLC B
  - WLAN “Special-SSID” WLAN ID 1
  - WLAN “Employee-SSID” WLAN ID 2

To avoid this potentially serious mismatch, it is essential to audit existing WLCs for WLANs and prepare the WLCs for template-based WLAN configuration. Using only Prime Infrastructure and not the WLC interface, the following summarized steps (followed by detailed steps) prevent WLAN ID inconsistencies.

**Detailed Steps for Ensuring WLAN ID Consistency**

1. Add all WLCs to Prime Infrastructure and synchronize their configurations.
2. Using Prime Infrastructure, look at the WLANs on each WLC to determine the highest WLAN ID in existence, as shown in the example in Figure 28-45. In this example, two WLANs exist on a particular WLC.

**Figure 28-45  WLAN ID List**

3. Create disabled dummy WLAN templates and apply to WLCs to bring them all up to the same highest WLAN ID.

   The dummy WLAN settings are irrelevant as long as they are created in the “disabled” state. In this example, two dummy WLAN templates must be created and applied to all WLCs with no WLANs.

   As an alternative to creating the dummy WLANs, the existing WLANs may be deleted and re-created with higher WLAN IDs manually set directly on the WLC. Deletion and re-creation is the only method currently available for changing the WLAN ID. Changing the WLAN ID on an existing WLAN is not possible.
4. Create the new WLAN templates for BYOD configurations and apply to all WLCs.
5. Check WLCs to ensure WLAN IDs are consistently assigned across all WLCs.
6. After WLAN templates are applied, dummy WLANs may be deleted if desired.

**Note**
When adding a new WLC to the network, dummy WLAN templates must be applied to them before applying BYOD WLAN templates. Since the WLAN ID is assigned sequentially, BYOD WLAN templates must always be applied in the same order.