



Configuring Your WLAN Radio Environment

The following topics provide information about the WLSE radio environment:

- [WLSE Radio Management, page 12-1](#)
- [Configuring Your Network for Radio Management, page 12-5](#)
- [Understanding Radio Management, page 12-8](#)
- [Collecting Radio Location Data, page 12-18](#)

WLSE Radio Management

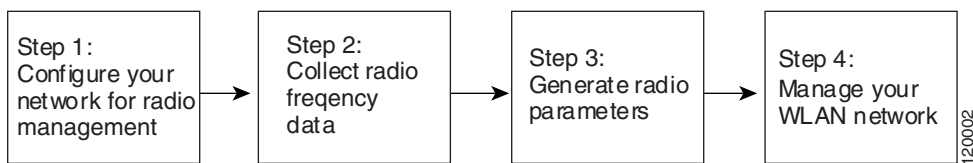
The WLSE simplifies the deployment, expansion, and day-to-day management of your WLAN radio environment. Using radio management, intrusion detection, and site management features, you can:

- Automatically configure network-wide radio parameters during initial deployment and network expansion.
- Detect all neighboring APs and produce path loss data used for rogue location estimations, radio parameter generation, and coverage display data, generate additional data to help provide optimal coverage for the radio parameter generator, and provide configurations for APs based on measurement data collected from client walkabouts and AP radio scans.

- Continuously monitor the radio environment, adjust APs to cover potential areas of lost coverage, alert the WLAN administrator to radio network changes, and feed frame monitoring information to a third-party server for further analysis.
- Detect and report network intrusions, such as rogue APs, interference, ad-hoc networks, excessive management frame transmissions, unregistered clients, and authentication and protection attacks.
- Access a graphical view of the access points (APs) on each floor of your building(s) and view the relative location of unknown or rogue APs.

To set up and manage your WLAN radio environment, use the features provided by the Radio Manager, the Location Manager, and the Intrusion Detection System:

Figure 12-1 Radio Management Setup Overview



Step 1: Configure your network for radio management

All the device information shown under the Radio Manager, Location Manager, and Intrusion Detection Services tabs is polled from the managed devices in your network. The WLSE polls and receives aggregated data from WDS devices and provides intelligent processing of this data. The WLSE can manage multiple subnets, so it can receive radio frequency data from many WDS devices.

The WLSE must register with each WDS in each managed AP subnet to receive radio frequency data. If the WLSE is not registered, *none of the Radio Manager, Location Manager, or Intrusion Detection System functions will work.*

For more information about preparing your network to manage radio devices, see:

- [What is WDS and Why Do I Need It?, page 12-9](#)
- [Configuring Your Network for Radio Management, page 12-5](#)
- [Verifying Radio Management Capability, page 14-35](#)

- The *Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine*. For information about locating this document, see [Finding WLSE Documentation on Cisco.com, page 1-21](#).

Step 2: Collect radio location measurements.

After the access points have been configured for radio management, you can use selections under the Radio Manager and Location Manager tabs to gather radio location measurements. The WLSE uses these measurements to characterize the radio environment and determine the channels and power limits for each 802.11 Basic Service Set (BSS).

To collect this data, you can either:

- Run a wizard that walks you through the data collection process (see [Using the Location Manager Assisted Site Survey Wizard, page 14-22](#)).
- Run the data collection processes separately:
 - a. Run AP Radio Scan—see [Using AP Radio Scans to Collect RM Data, page 14-58](#)
 - b. Run Client Walkabout—see [Using Client Walkabouts to Collect RM Data, page 14-73](#)
 - c. Start Radio Monitoring—see [Using Radio Monitoring to Collect RM Data, page 13-2](#)

For more information about collecting and managing radio location measurements, see:

- [Collecting Radio Location Data, page 12-18](#)
- [Managing RM Data, page 14-106](#)

Step 3: Generate optimal radio parameters values for the APs.

You can use the selections under the Radio Manager or Location Manager tabs to recommend optimal radio transmit power, channel selection, and beacon interval (optional) for each AP, then apply these configuration settings.

To generate these parameters, you can either:

- Run a wizard that walks you through the parameter generation process
- Run the RM Assisted Configuration procedure

For more information about generating AP radio parameters, see [Generating Radio Parameters, page 14-90](#).

Step 4: Manage your WLAN network.

After you have configured your network for radio management, collected the radio location data, and generated the radio parameters, you are ready to manage your WLAN environment. You can:

- Use the Radio Manager to evaluate AP radio performance, adjust neighboring AP interfaces to cover potential areas of lost coverage, or use dedicated APs as sensors to feed information to a third-party server for further analysis (see [Using the Radio Manager, page 13-1](#)).
- Use a graphical view of the APs on each floor of your building(s) to display the predicted coverage of each AP (see [Managing Your WLAN Radio Environment by Sites, page 14-1](#)).
- Detect network intrusions such as rogue APs, ad-hoc networks, non-802.11 interference, and so on (see [Using the Intrusion Detection System, page 15-1](#)).

Related Topics

- [Configuring Your Network for Radio Management, page 12-5](#)
- [Understanding Radio Management, page 12-8](#)

Configuring Your Network for Radio Management

Before you can use the radio management features provided by WLSE, you must configure your network. If your network is not properly configured, *none of the Radio Manager, Location Manager, or Intrusion Detection System functions will work.*

If you are configuring APs or WLSM devices as WDS devices, you can use the Deployment Wizard (see [Using the Deployment Wizard, page 2-1](#)). The Deployment Wizard replaces many of the manual configuration procedures that are normally required to configure infrastructure access points and WDS devices and to configure the WLSE to discover and manage those devices.

Although you can use the Deployment Wizard to set up most APs, you must use the following manual procedure to configure an external ACS server for AP-WDS-WLSE authentication.

Procedure

- Step 1** Be sure that all APs are managed (discovered, inventoried, and managed—see [Device Discovery and Management, page 4-1](#)).
- Step 2** Configure one or more WDS devices (for more information about WDS, see [What is WDS and Why Do I Need It?, page 12-9](#)):
- **AP-WDS:** You can configure one or more APs in each AP subnet to run WDS. When multiple WDSs exist in the same subnet, one WDS becomes the active WDS and the other WDSs become backups.

For more information about configuring AP-WDS devices, see the “Radio Management Setup—IOS Devices” chapter in *Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine, 2.11*. For information about locating this document, see [Finding WLSE Documentation on Cisco.com, page 1-21](#).
 - **WLSM-WDS:** You can configure a Wireless LAN Services Module (WLSM) device to run WDS. A WLSM device is a module for the Cisco Catalyst 6500 Series switch that provides WDS to the wireless network. For information about configuring WLSM-WDS devices, see the WLSM device documentation.

Step 3 Configure your devices for radio management.

For information about radio management configuration procedures, see the “Radio Management Setup—IOS Devices” chapter in *Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine, 2.11*.

To verify that you have correctly configured the network for radio management, use the **Verify RM Capability** option in the Location Manager (see [Verifying Radio Management Capability, page 14-35](#)).

Step 4 Enable LEAP authentication.



Note All APs must authenticate with a WDS using LEAP. This requirement is separate from the client’s authentication scheme—clients can use a non-LEAP security scheme, but the AP and WLSE must use LEAP to authenticate to the WDS.



Note A WDS can connect to Cisco’s ACS v3.2 as the LEAP Authentication server. You can use the AP/WLSM’s LEAP Local Authentication Server feature if the customer is not using LEAP for any purpose other than to fulfill the requirement on the WLSE/WDS/AP.



Note Do not set a session timeout on the ACS server that is less than 600 seconds. A session timeout of less than 600 seconds can disrupt Radio Manager operations.

For more information about enabling LEAP authentication, see the *Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine, 2.11*. For information about locating this document, see [Finding WLSE Documentation on Cisco.com, page 1-21](#).

Step 5 Configure the WLCCP credentials (see [Enter WLCCP Credentials for Wireless Domain Services, page 4-21](#)).

Step 6 Verify that the active WDS appears under the device tree:

- a. Select **Reports > Device Center**.
- b. Open the **Wireless Domain Services** folder.
- c. Open the **Active WDS** folder.

- d. Select the device.
- e. Select **WDS Summary Report**.
- f. Verify that the **WLSE to WDS Authentication Status** column contains the string “KeysSetUpWithWDS” or “Authenticated”.

You can also verify this setting by running the “show wlccp wnm status” command on the active WDS in enable mode. A typical output would look like this:

```
NMS-AP1200-1#show wlccp wnm status
WNM IP Address: 172.16.0.0 Status: SECURITY KEYS SETUP
```

where:

- 172.16.0.0 = IP address of WLSE
- Status = SECURITY KEYS SETUP. This indicates that the active WDS is properly authenticated with WLSE.

Step 7 Verify that the APs are managed and registered with WDS:

- a. Select **Reports > Device Center**.
- b. Open the **Wireless Domain Services** folder.
- c. Open the **Active WDS** folder.
- d. Select the device.
- e. Select **WDS Registered APs**. A list of all the APs that are registered with this WDS is displayed.

You can also verify this setting by running the “show wlccp wds ap” CLI command on the active WDS in enable mode.

Step 8 Configure the ACS server to support fast roaming and simultaneous logins.

For information about configuring the ACS server to support roaming and simultaneous logins, see the ACS server documentation. For other information about configuring the ACS server, see the “Setting Up an ACS Server” chapter in *Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine, 2.11*. For information about locating these documents, see [Finding WLSE Documentation on Cisco.com, page 1-21](#).

Step 9 Configure the AAA server to allow multiple jobs.

For information about configuring the AAA server to multiple logins, see the AAA server documentation. For other information about configuring the AAA server, see the “Setting Up an ACS Server” chapter in *Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine, 2.11*. These documents are also located on Cisco.com.

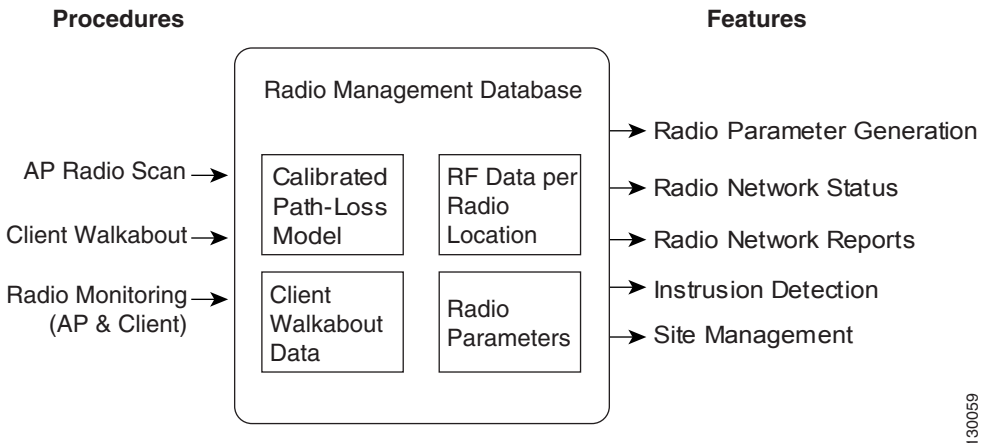
- Step 10** Now you are ready to collect radio location data (see [Collecting Radio Location Data, page 12-18](#)).

Understanding Radio Management

The radio management environment provided by WLSE consists of:

- *Procedures* that gather data about the radio environment.
- The radio frequency *database*, which contains radio data and parameters.
- *Features* that use the information in the database.

Figure 12-2 WLSE Radio Management Environment



The following topics describe how the WLSE implements radio management:

- [What is WDS and Why Do I Need It?, page 12-9](#)

- [Understanding Radio Performance—Coverage and Capacity, page 12-13](#)
- [Understanding Multiple BSSIDs, page 12-17](#)

What is WDS and Why Do I Need It?

The critical software component in the network is a set of IOS features called the Wireless Domain Services (WDS). The following types of devices can supply the WDS:

- An access point configured for WDS
Each WDS access point supports one AP subnet. You can add additional WDS access points for redundancy. The priorities you set on the WDS access points determine which one is the active and which ones are backups.
- A Wireless LAN Services Module (WLSM)
Each WLSM supports multiple AP subnets, as long as all of the subnets are served by the switch on which the WLSM is installed.

The following topics describe these devices types:

- [Understanding WDS Access Points, page 12-9](#)
- [Understanding WLSM WDS Devices, page 12-11](#)

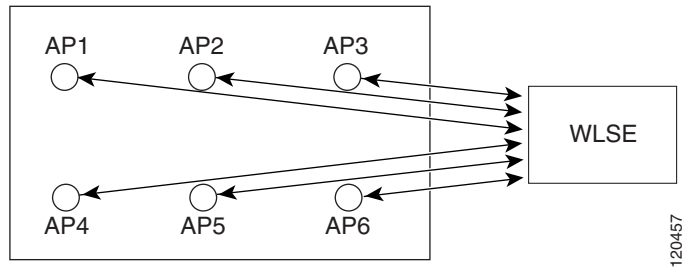
Understanding WDS Access Points

The WDS provides control path technologies that must be active on an AP in each AP subnet; a backup WDS can also be defined in each AP subnet. The WDS provides:

- Fast, secure layer-2 wireless client roaming—The WDS acts as an 802.1x authenticator for wireless clients within the layer-2 network.
- Radio Management (RM) data aggregation—The WLSE provides intelligent processing of aggregated data collected by the WDS access points from other wireless clients in the network. The WLSE can manage multiple subnets, so it can receive radio data from many APs running WDS.

There is no RM data aggregation without a WDS. Without a WDS, the communication between the access points and WLSE looks like this:

Figure 12-3 Basic Network Management Communications



Using this approach, the WLSE can communicate with the APs using only these two methods:

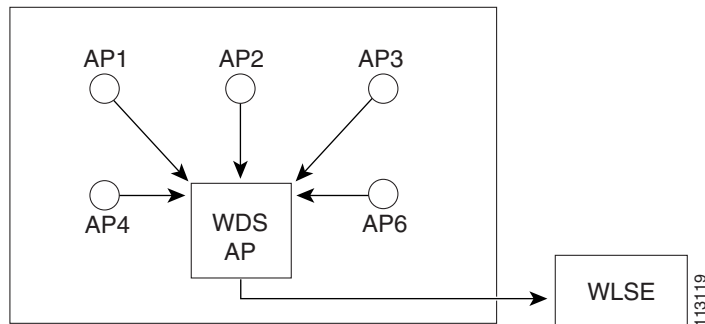
- Primary: SNMP
- Secondary: CLI over telnet or SSH



Caution

The WLSE must register with the WDS in each managed AP subnet to receive Radio Manager data. If the WLSE is not registered, *none of the Radio Manager functions will work.*

After you configure the network for Radio Management tasks (see [Configuring Your Network for Radio Management, page 12-5](#)), the WLSE communicates all Radio Management activities with one or more WDS APs instead of all APs in the network. Each WDS AP collects data from other wireless clients in the network and sends this aggregated data to the WLSE.

Figure 12-4 Additional Radio Management Communications

Understanding WLSM WDS Devices

A Wireless LAN Services Module ([WLSM](#)) device is a module for the Cisco Catalyst 6500 Series switch that provides WDS to the wireless network. Each WLSM supports multiple AP subnets, as long as all of the subnets are served by the switch on which the WLSM is installed.

You can add a second WLSM to serve as a standby. The WLSE authenticates with both the HSRP active and HSRP standby WLSM devices (WLSM uses HSRP to handle redundancies). In the reports, both WLSM devices (HSRP active and HSRP standby) will appear as active WDSs.

If the HSRP active WLSM goes down, the HSRP standby WLSM will communicate with the AP subnets (see [Figure 12-5](#)).

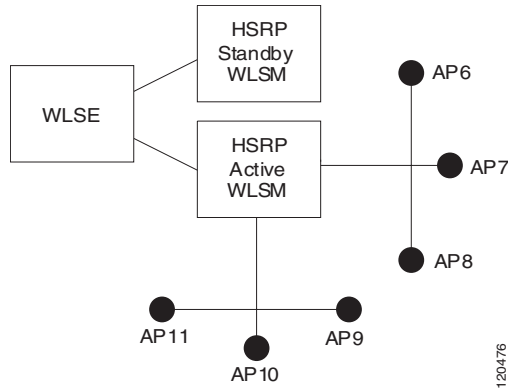
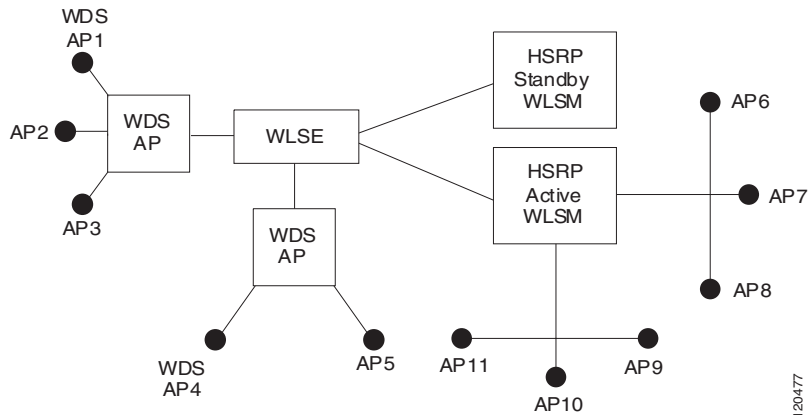
Figure 12-5 WLSE-WLSM Communications

Figure 12-6 illustrates a network that uses both AP and WLSM WDS devices to manage the access points in the network. In this example, additional access points have been identified as backup AP-WDS devices (AP1 and AP4), and an additional HSRP-based WLSM-WDS device has been added to as a standby for the active WLSM-WDS.

Figure 12-6 Sample Network Using AP-WDS and WLSM-WDS Devices

Understanding Radio Performance—Coverage and Capacity

The Radio Manager:

- Quantifies the performance within a region

Each region is defined by the rough degree of contention and packet collisions experienced by clients in the region due to traffic outside of the BSS.

The inter-BSS contention and collision translates into performance degradation, which the Radio Manager estimates for all potential clients within the region. Contention and collisions from managed APs *and* rogue and friendly APs are used in the performance evaluation.



Note All relevant APs are used in the performance evaluation regardless of building or floor placement.

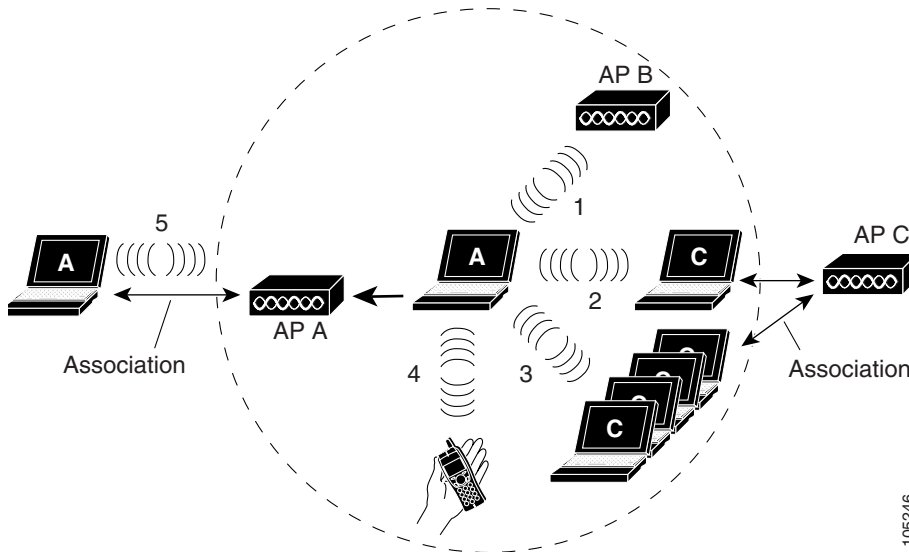
- Takes the region sizes into account to assure coverage over the region

The types and sizes of performance regions determine the expected maximum, minimum, and average performance of a particular domain.

AP/Client Relationships

The Radio Manager acquires knowledge of the WLAN radio environment from measurements obtained from Cisco APs and Cisco clients. [Figure 12-7](#) illustrates the relationships between three APs and their clients.

Figure 12-7 AP/Client Relationships



In this example, the measuring client and one other client are associated with AP A, but neither client detects the other AP's signal. AP B is close enough to be detected by the measuring client, and AP C is out of range, but the measuring client does detect some of AP C's associated clients. [Table 12-1](#) describes these relationships in more detail.

Table 12-1 AP/Client Relationships

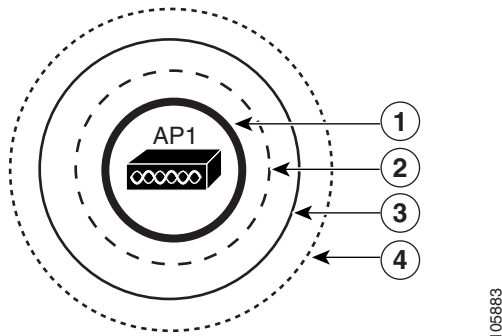
Item	Description
1	The measuring client identifies access point B as a source of 802.11 contention.
2	The measuring client detects contention from a client in another BSS and identifies access point C as the BSS access point.
3	The measuring client reports significant contention due to clients in another BSS. Access point C is identified as the BSS access point.
4	The measuring client indicates intermittent non-802.11 interference and describes the statistics of its received strength.

Table 12-1 AP/Client Relationships (continued)

Item	Description
5	The measuring client identifies another client in its BSS that appears to be hidden from it.

Radio Performance Regions

Radio performance regions within a BSS depend on the placement and transmit power of other co-channel APs. The transmit power of a BSS defines a set of RF reception rings around its AP (see [Figure 12-8](#)).

Figure 12-8 RF Reception Rings

1	Planned BSS coverage	3	Uplink may be decodable
2	Downlink RF influence	4	Uplink RF influence

Two rings correspond to the downlink:

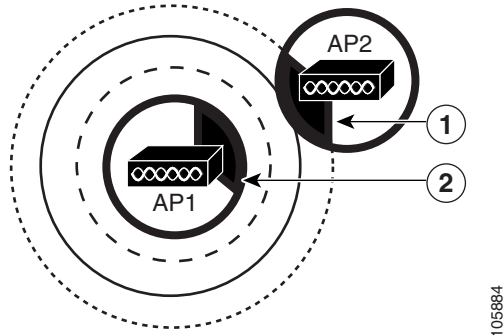
- The **planned BSS coverage ring** (1) corresponds to the area in which clients can reliably receive the downlink signal.
- The **downlink RF influence ring** (2) corresponds to the area in which reception is difficult, but the downlink signal may still contend or collide with a downlink from another AP on the same channel.

Two similar rings correspond with areas of reception and the RF influence emanating from a client positioned at the edge of the BSS coverage ring. The significant ring, the **uplink RF influence ring** (4), corresponds to the signal that originates from a client sending packets up to its AP.

Uplink Contention Regions

In [Figure 12-9](#), AP1 and AP2 share the same channel. AP2 is examined as the BSS of interest, while AP1 is the cochannel neighbor. The highlighted performance region corresponds with an area in which BSS2 clients must contend with traffic from BSS1. The source of contention is shown as a set of clients in BSS1 near the edge of their planned coverage ring. This is known as uplink contention because it delays uplink traffic from clients to their AP.

Figure 12-9 Sample Performance Region



1	BSS2 performance region: AP2 clients that experience contention from AP1's clients
2	Source of contention: AP1 clients that cause the contention.

If AP2 has neighbors sharing the same channel on all sides, then similar uplink contention regions are defined in the direction of each neighboring AP. If any of these neighbors is closer than the one shown in [Figure 12-9](#) or uses a higher power limit, then the uplink contention region is larger than shown in the figure. If clients of the neighboring BSSs are close enough to be detected by AP2, then AP2 experiences downlink contention due to the clients' traffic.

The BSS may also contain regions in which a client receives traffic that has collided with packets from another station. This occurs when the intended source and interfering source do not detect each other. This happens when:

- Stations in the same BSS are hidden from each other.

This situation can be remedied by blocking out time for an access point using RTS/CTS (request-to-send, clear-to-send) commands.

- A client in a neighboring BSS is within range of the client of interest but is not detected by the latter client's AP.

This situation is an inter-BSS interference problem that could exist in any dense WLAN and *cannot* be remedied with RTS/CTS. One goal of the Radio Manager is to minimize this occurrence with good radio configurations.

Understanding Multiple BSSIDs

The Base Service Set Identifier (BSSID) is typically the MAC address of the radio. WLSE also supports multiple BSSIDs (MBSSID) on a single radio (AP). MBSSIDs address several issues:

- Passive client scanning support for multiple SSIDs
- Multiple unencrypted multicast streams
- Segregation of unencrypted and encrypted broadcast streams
- Encrypted multicast streams to not cause decrypt errors at the client
- Support for existing clients (no changes allowed on the client)

To a *client*, an MBSSID AP appears to be several distinct co-located APs. An MBSSID AP transmits a beacon for each BSSID/SSID, which makes all of the SSIDs visible for passive scanning. The distinct VLAN multicast streams are easily separated using the BSSID, which allows multiple unencrypted multicast streams and eliminates the decryption errors that occur with encryption separation.

To the *WLSE*, the MBSSID AP appears to be one AP. Each radio that is configured with MBSSID will appear as one radio with multiple VLANs, and each distinct MAC address associated with the VLAN is considered a synonym of the real radio's MAC address.

Support for multiple BSSIDs does not imply full virtual AP capability and functionality. For example:

- All BSSIDs are synchronized to the same clock.
- All BSSIDs have the same transmit power.
- All BSSIDs use the same set of transmit data rates.
- The MAC address allocation is dynamically assigned by the radio.

Collecting Radio Location Data

Radio location measurements characterize the radio environment and provide the information other Radio Manager features require to determine the channels and power limits for each Basic Service Set (BSS). To gather these measurements:

1. **Perform an AP Radio Scan.** The AP Radio Scan procedure (see [page 12-19](#)) detects all neighboring APs and produces path loss data used for rogue location estimations, radio parameter generation data, and coverage display data.

**Note**

If you do not run AP Radio Scan, the Coverage Display in the Location Manager will be computed using the default pass loss model. Because no path loss measurement data has been collected, the coverage views could be distorted.

2. **Perform a Client Walkabout** (optional, but recommended—see [Using Client Walkabouts to Collect RM Data, page 14-73](#)). The additional data generated by a client walkabout helps provide optimal coverage for the radio parameter generator.

If you do not perform a client walkabout, you *must* enter a floor plan that includes the distances between APs (see [Adding Floors to Location Manager, page 14-11](#)).

3. **Enable Radio Monitoring.** Radio Monitoring (see [Using Radio Monitoring to Collect RM Data, page 13-2](#)) periodically gathers RF statistics, identifies specific signal sources, and is your primary means of detecting rogue access points.

**Note**

If you never enable Radio Monitoring or run AP Radio Scan, no unknown radios (rogue or friendly) will be detected. If you run AP Radio Scan but do not enable Radio Monitoring, some unknown radios will be detected, but not as many as would be detected if Radio Monitoring was running. Self healing also relies on the data generated by Radio Monitoring and AP Radio Scan.

You can also use the Assisted Site Survey wizard, which is part of Location Manager, to walk you through the process of determining the optimal radio transmit power and channel selection. This wizard interface steps you through AP radio scan, client walkabout, and radio parameter generation (see [Using the Location Manager Assisted Site Survey Wizard, page 14-22](#)).

Related Topics

- [Configuring Your Network for Radio Management, page 12-5](#)
- [Viewing Current Path Loss Results, page 11-22](#)
- [Viewing Historical Path Loss Results, page 11-24](#)
- [Viewing Current Channel Load Results, page 11-25](#)
- [Viewing Historical Channel Load Results, page 11-27](#)
- [Managing RM Data, page 14-106](#)
- [Understanding Radio Management, page 12-8](#)

