



CHAPTER 3

Cisco Location-Based Services Architecture

This chapter describes the Cisco Location-Based Services (LBS) architecture and has the following main sections:

- [RF Fingerprinting, page 3-1](#)
- [Location-Aware Cisco UWN Architecture, page 3-4](#)
- [Role of the Location Appliance, page 3-7](#)
- [Accuracy and Precision, page 3-12](#)
- [Tracking Clients, Assets and Rogue Devices, page 3-14](#)
- [Cisco Location Control Protocol \(LOCP\), page 3-35](#)

RF Fingerprinting

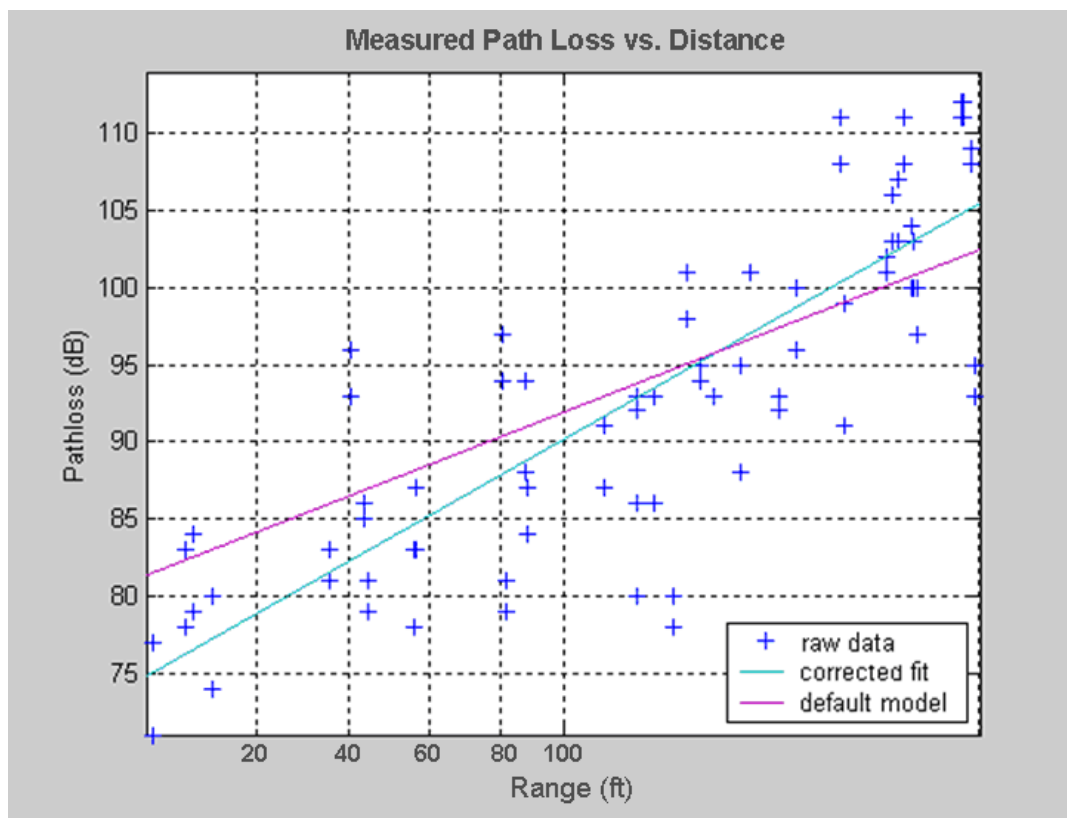
Cisco *RF Fingerprinting* refers to a new and innovative approach that significantly improves the accuracy and precision of traditional signal strength lateration techniques. Cisco RF Fingerprinting offers the simplicity of an RSSI-based lateration approach with the customized calibration capabilities and indoor performance previously available only in location patterning solutions. RF Fingerprinting significantly enhances RSS lateration by using RF propagation models developed from radio propagation data gathered directly from the target environment or environments very similar to it. RF Fingerprinting offers the ability to calibrate an RF model to a particular environment in a fashion similar to (but more expeditious than) that described for location patterning.

In addition to the use of prepackaged propagation models, RF Fingerprinting offers the ability to develop customized models that are based on on-site data collection. This process allows for the overall attenuation characteristics of the actual environment to be taken into consideration during the derivation of both 2.4 GHz and 5 GHz path loss models. For each calibration grid location, the physical location coordinates of the calibration client (provided by the calibration operator) are recorded along with the client RSSI from three or more LWAPP-enabled access points.

The data accumulated during the calibration phase is statistically processed and groomed, then used to build an RF propagation model used to predict tracked device RSSI around each access point, where the path loss exponent, shadow fading standard deviation, and $PL_{1\text{meter}}$ values are calculated from the sample calibration data so as to better reflect specific propagation anomalies present in the environment. This process consists of several computational cycles where the previously-mentioned parameters are calculated for each band. The minimum mean square error (MMSE) estimation technique is used to obtain the *initial* values for the parameters, as shown in [Figure 3-1](#), where the path loss exponent is represented by the slope of the applicable MMSE line of best fit (that is, either default or corrected fit). However, note that in the RF Fingerprinting approach, the selection of a location path loss model does

not end with MMSE. Rather, MMSE is used only as the starting point for the selection of finalized parameters for each band, with the ultimate goal being the optimization of the final path loss model as it pertains to location accuracy. RF Fingerprinting does not rely on good location performance being a by-product of a RF propagation model that simply provides good coverage mapping.

Figure 3-1 MMSE Estimation



To locate a mobile client during the operational phase of RF Fingerprinting, RSS multi-lateration is performed using either a pre-packaged RF model or a customized model created during the calibration phase. This process yields the coordinates of the data point with the highest potential of correctly representing the tracked device's current location. Additional information gleaned from statistical analysis of the distribution of calibration data is then used to further improve location accuracy and precision.

Cisco RF Fingerprinting offers several key advantages over traditional approaches:

- Uses existing LWAPP-enabled Cisco Unified Networking Components—Unlike some other solutions, the location-aware Cisco UWN with RF Fingerprinting provides a Wi-Fi-based RTLS alongside of voice and data services using a combined infrastructure. The Cisco Location Appliance supports location and statistics history and serves as a centralized positioning engine for the simultaneous tracking of up to 2500 devices per appliance. Optional chokepoint triggers can be added to the solution to provide presence and proximity detection if desired, allowing for very granular detection of asset tags, within a range of 25 feet to less than one foot depending on the hardware selected.
- No proprietary client hardware or software required—The location aware Cisco UWN with RF Fingerprinting uses a network-side location model. Because of this, Cisco RF Fingerprinting can provide location tracking for a wide variety of industry-standard Wi-Fi clients (and not just those

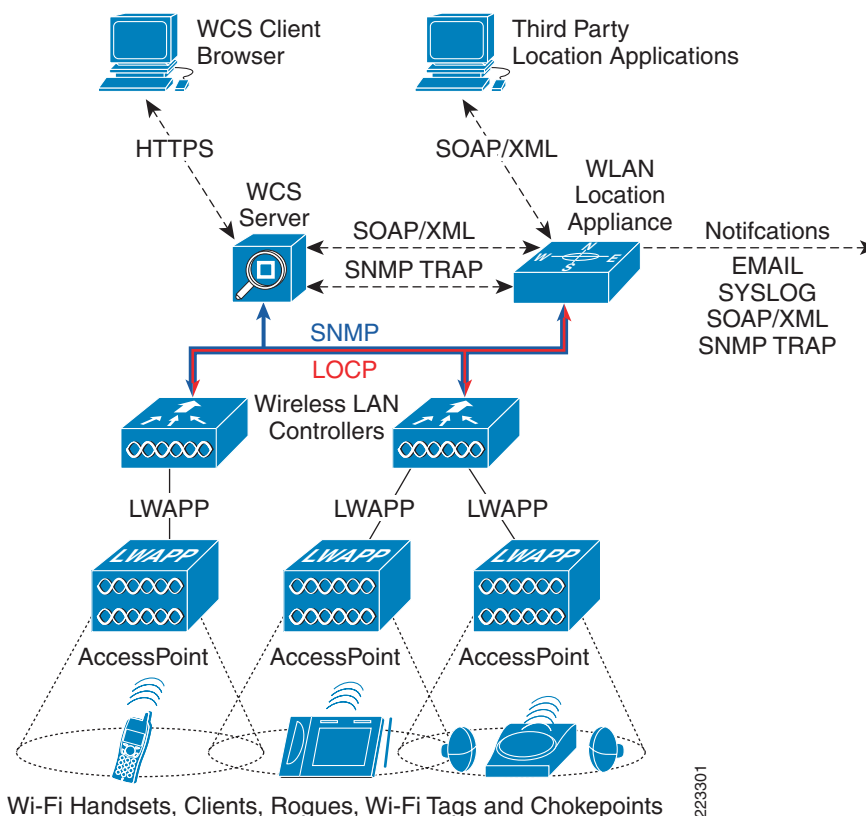
with popular Windows-based operating systems) *without the need to load proprietary client-tracking software or location-enabled wireless drivers in each client*. This includes popular VoIP handsets such as the Cisco 7920 and 7921G, devices for which such proprietary add-on location tracking client software is not available.

- Supports popular Wi-Fi active RFID asset tags—Because the location-aware Cisco UWN implements RF Fingerprinting as a network-side model, there is no dependency on proprietary software being resident in RFID asset tags in order to allow for localization. This enables the location-aware Cisco UWN to interoperate with active RFID asset tags from popular vendors including AeroScout, PanGo Networks, WhereNet, G2 Microsystems and others. Asset tags that support the Cisco Compatible Extensions for Wi-Fi Tags specification can take advantage of advanced features introduced with software Release 4.1, such as the ability to pass tag telemetry and chokepoint information to the Cisco UWN. Cisco makes this specification available to Cisco Technology Development Partners (CTDP) and encourages the development of interoperable active RFID tag hardware in compliance with the specification.
- Better accuracy and precision—Cisco RF Fingerprinting yields significantly better performance than solutions employing pure triangulation or RSS lateration techniques. These techniques typically do not account for effects of attenuation in the environment, making them highly susceptible to reductions in performance. The advantages of Cisco RF Fingerprinting technology start where these traditional approaches leave off. Cisco RF Fingerprinting begins with a significantly better understanding of RF propagation as it relates specifically to the environment in question. With the exception of the calibration phase in location patterning, none of the traditional lateration or angulation approaches discussed thus far take environmental considerations directly into account in this manner. RF Fingerprinting then goes a step further, by applying statistical analysis techniques to the set of collected calibration data. This allows the Cisco Location Appliance to further refine predicted location possibilities for mobile clients, culling out illogical or improbable possibilities and refining accuracy. The net result of these efforts is not only better accuracy but significantly improved precision over traditional solutions.
- Reduced calibration effort—The Cisco RF Fingerprinting technology offers the key advantages of an indoor location patterning solution but with significantly less effort required for system calibration. Although both solutions support on-site calibration, the Cisco RF Fingerprinting approach offers less frequent re-calibration and can operate with a larger inter-access point spacing than location patterning solutions. Cisco RF Fingerprinting can also share RF models among similar types of environments and includes pre-packaged calibration models that can facilitate rapid deployment in typical indoor office environments.

Location-Aware Cisco UWN Architecture

The overall architecture of the location-aware Cisco Unified Wireless Network is shown in [Figure 3-2](#).

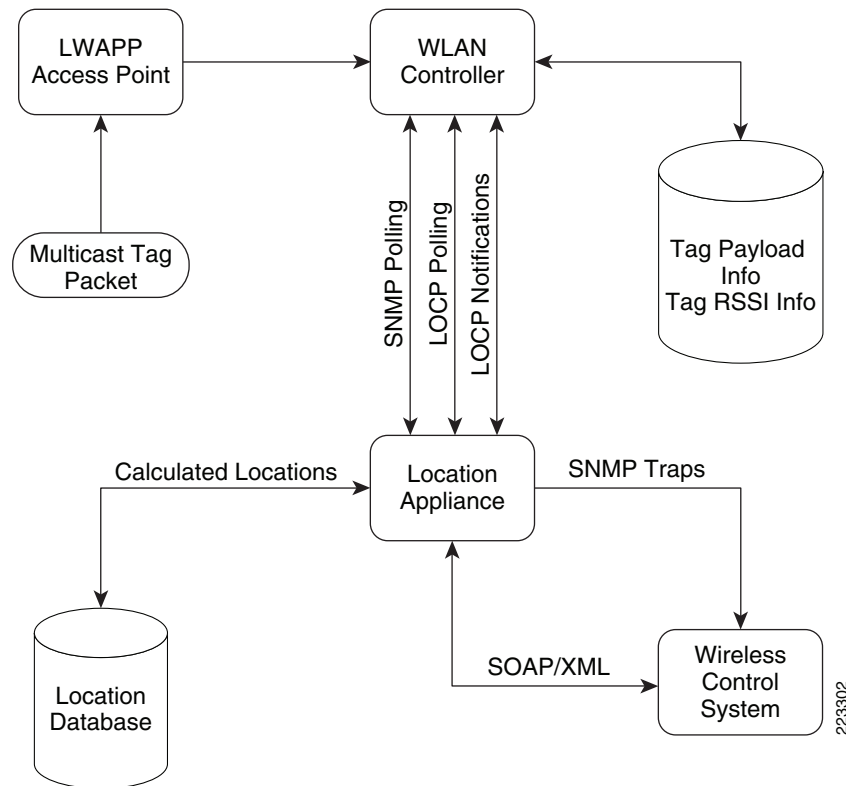
Figure 3-2 *Location-Aware Cisco UWN Architecture*



Access points forward information to WLAN controllers regarding the detected signal strength of any WLAN clients, asset tags, rogue access points, or rogue clients. In normal operation, access points focus their collection activities for this information on their primary channel of operation, going off-channel and scanning the other channels in their regulatory channel set periodically. The collected signal strength information is forwarded to the WLAN controller to which the access point is currently registered, which aggregates the information. The location appliance uses SNMP to poll each controller for the latest signal strength information for each tracked category of device. In the case of a location tracking system deployed without a location appliance, WCS obtains this information from the appropriate controller(s) directly.

A step-by-step flow diagram of this process is provided in [Figure 3-3](#), where the flow of signal strength and tag payload information is shown for active RFID asset tags that communicate via the use of layer two multicasts.

Figure 3-3 Information Flow for Asset Tag RSSI Data



[Figure 3-3](#) summarizes the following events:

-
- Step 1** At each tag transmission interval, the asset tag transmits a multicast frame on each of its configured channels.
 - Step 2** At least three access points detect the asset tag's transmission. It is forwarded to the WLAN controller (WLC) to which the detecting access points are registered.
 - Step 3** The WLC stores the information payload associated with the asset tag in an internal tag information table indexed by the asset tag MAC address. This information payload can contain information such as battery status and tag or asset telemetry.
 - Step 4** For tags detected in the network by access points registered to this WLC, the WLC places the following asset tag information in an internal RSSI table:
 - a. Tag MAC address
 - b. AP MAC address
 - c. AP interface
 - d. RSSI measurement
 - Step 5** The location appliance periodically polls the WLC for the contents of the tag RSSI table using SNMP.

- Step 6** Commencing with software Release 4.1 of the Cisco UWN, the WLC is polled for the contents of the tag information table using the Cisco Location Control Protocol (LOCP).
- Step 7** The location appliance calculates the location of the asset tag using the RSSI information and stores the location information in its database.
- Step 8** The location appliance dispatches any northbound notifications (such as SNMP traps, emails, syslog or SOAP/XML messages based on the updated asset tag location).
- Step 9** Location end users make use of WCS (or a third party location client) to request location information based on floor maps or search criteria. A request for location information is made from the location to the location appliance via a SOAP/XML online query.

Beginning with software Release 4.1 of the location-aware Cisco UWN, LOCP provides for the transmission of asynchronous high-priority messages from the WLAN controller to the location appliance. Included in this category are high-priority tag events such as tag call button alerts, chokepoint proximity and vendor-specific tag payloads.

WCS and the location appliance exchange information (such as calibration maps and network designs) during a process known as *synchronization*. During this process, the partner possessing the more recent information will update the other partner. Synchronization occurs either on-demand or as a scheduled task, the timing of which is determined by the Administration > Scheduled Tasks main menu option under the Cisco Wireless Control System (WCS) main menu bar.

Location information is displayed to the end user using a *location client* application in conjunction with the Cisco Wireless Location Appliance. Typically, this role is fulfilled by the Cisco WCS, which, as will be further explained in subsequent sections of this document. As a location client, Cisco WCS is capable of displaying a wide multitude of information regarding the current and past location of clients, asset tags, rogue access points, and rogue clients.

**Note**

For important information regarding compatibility between versions of WCS and the Cisco Wireless Location Appliance, refer to *Release Notes for Cisco Wireless Location Appliance Release 3.0* at the following URL: http://www.cisco.com/en/US/products/ps6386/prod_release_notes_list.html.

Location client functionality is not limited to WCS. Third-party applications written in accordance with the Cisco Location Appliance Application Programming Interface (API) can also serve as a location client to the Wireless Location Appliance (as shown in [Figure 3-2](#)). The same information contained in the location appliance that is made available to WCS (including vendor-specific information that may have been received from asset tags) is also made available to third-party same location clients via the location appliance API.

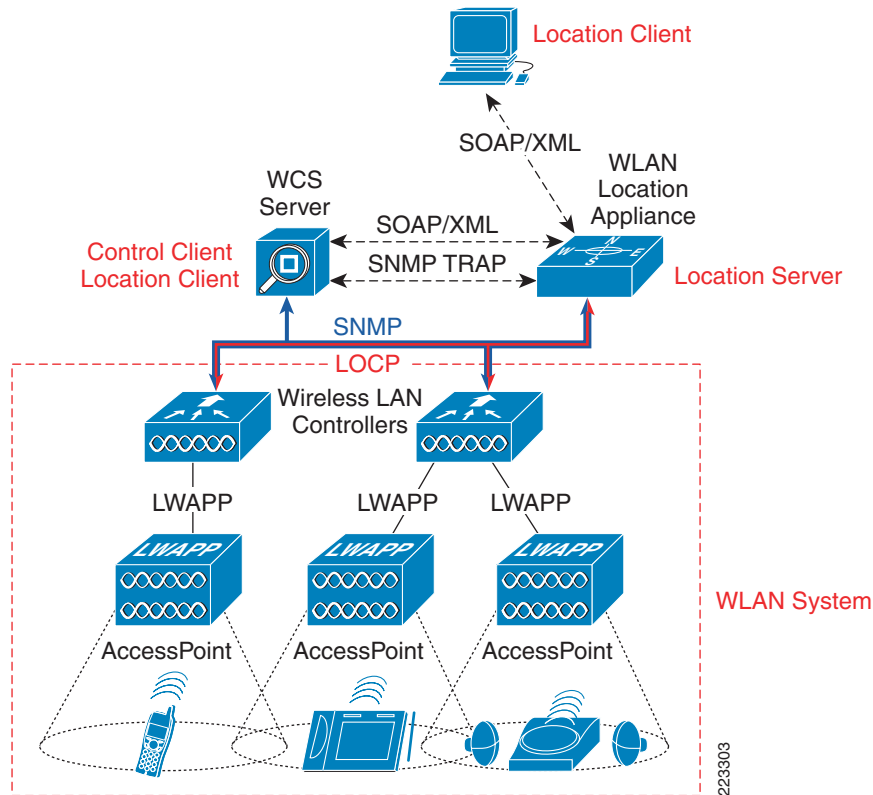
Third-party location clients can synchronize their network designs with the location appliance in a similar fashion to WCS. In this case, the location appliance updates location clients with the latest information regarding network designs and map images. As with WCS, synchronization occurs either on-demand or on a scheduled basis, the timing of which is typically determined by configuration parameters contained within the location client.

The Cisco Location Appliance is also capable of issuing northbound notifications to external systems via email (SMTP), syslog, SNMP traps, or the SOAP/XML protocol. The issuance of these northbound notifications is dependent on the occurrence of one or more of a variety of events, and is discussed in further detail within subsequent sections of this document.

Role of the Location Appliance

The location-aware Cisco UWN can be broken down into four basic component groups, as shown in Figure 3-4.

Figure 3-4 Components of the Location-Aware Cisco UWN



- Location Client**—The primary role of the location client is to serve as the user interface to the location and asset information contained on the location server. One or more location clients may receive information on a request basis (“pull” mode) or they may assume a listening role awaiting regular transmissions of information from the location server based on pre-defined criteria (“push” mode).
- WCS**—WCS serves as the default location client to the location appliance, providing location display capabilities that can satisfy most IT-centric and network monitoring requirements. The inherent flexibility afforded by the location appliance API allows for third-party location clients to reside in the UWN in a complementary fashion to WCS. These third-party products may provide a very business-focused UI that concentrates on the management of assets and de-emphasizes the details of RFID, localization and network management.
- Control Client**—The control client is capable of administering the location server as well as reading or writing all location and configuration data on the location server. In the location-aware Cisco UWN, the role of control client is performed by the Cisco WCS. The control client’s primary function is to populate the server with information about the physical environment (network designs, floors maps, calibration models, access point locations, etc.) and the network elements that should be monitored. The control client may also have management capabilities over one or more of the location servers deployed in the network.

- *Location Server*—The location server provides general location services for a network or part of a network (its *location domain*), and is primarily responsible for running the algorithms that predict client location. The location server may also provide for the storage of historical location information. A location server can communicate with multiple location or control clients. In the location-aware Cisco UWN, the Cisco Wireless Location Appliance fulfills the role of the location server. The Cisco Location Appliance is also capable of issuing notifications to external systems via email (SMTP), syslog, SNMP traps or the SOAP/XML protocol.
- *Wireless LAN System*—The wireless LAN system is comprised of:
 - Embedded software contained within WLAN controllers that functions as an aggregation point for information regarding station/tag/rogue discovery, device tracking and statistics.
 - The mobile devices (tags, mobile stations, rogue clients and rogue access points) that interact with the wireless network and whose location the location-aware Cisco UWN will monitor.
 - Optional infrastructure components, such as chokepoint triggers, that enhance the functionality available from active RFID tags and allow for increased granularity in the localization of these asset tags.

Although it is possible to access the location appliance directly via a console session, all end-user interaction with the location appliance is typically via WCS or a third-party location client application.

The integration of a Cisco Location Appliance into a Cisco Unified Wireless Network architecture immediately enables location improvements over and above the baseline capabilities of the Cisco UWN such as:

- *Scalability*—Adding a Cisco Location Appliance greatly increases the scalability of the location-aware Cisco UWN from on-demand tracking of a single device to a maximum capacity of 2500 devices (WLAN clients, RFID tags, rogue access points, and rogue clients). To handle situations requiring tracking of more than 2500 devices in the enterprise¹, additional location appliances can be deployed. The design can then be partitioned by assigning specific controllers to each appliance. Each appliance is responsible for tracking up to 2500 devices for the controllers and access points within its location domain, and may be managed by a common WCS.
- *Chokepoint Location*—The addition of a Cisco Location Appliance under software Release 4.1 or subsequent releases allows for the use of optional chokepoint triggers from Cisco technology partners such as AeroScout and WhereNet. These devices can assist in providing very granular asset tag location within a range of less than one foot to over twenty feet.
- *Historical and Statistics Trending*—The appliance records and maintains historical location and statistics information, which is available for viewing via WCS.
- *Location Notifications*—The Cisco Location Appliance can dispatch location-based event notifications via email (SMTP), syslog, SNMP traps, and SOAP/XML directly to specified destinations. These notifications can be triggered if the client or asset:
 - Changes location.
 - Strays beyond a set distance from pre-determined marker locations.
 - Becomes missing or enters/leaves coverage areas.
 - Experiences a change in battery level.
 - Enters the “stimulation zone” of a chokepoint trigger.
 - Experiences one or more priority conditions, such as:
 - Depression of a tag call button.
 - Detachment of a tag from its asset.

1. If tracked devices roam between location domains, the aggregate tracked device capacity may be reduced.

- An attempt at internal tampering.
- SOAP/XML Location Application Programming Interface (API)—The Location Appliance API allows customers and partners to create customized location-based programs that interface with the Cisco Wireless Location Appliance. These programs can be developed to support a variety of unique and innovative applications including real-time location-based data retrieval, telemetry device management, workflow automation, enhanced WLAN security, and people or device tracking. The API provides a mechanism for inserting, retrieving, updating, and removing data from the Cisco Wireless Location Appliance configuration database using a SOAP/XML interface. Developers can access the Cisco Wireless Location Appliance provisioning services and exchange data in XML format. The location appliance API is available to the Cisco development community along with tools to facilitate solution development. Integration support is available via the Cisco Developer Services Program, a subscription-based service.

**Note**

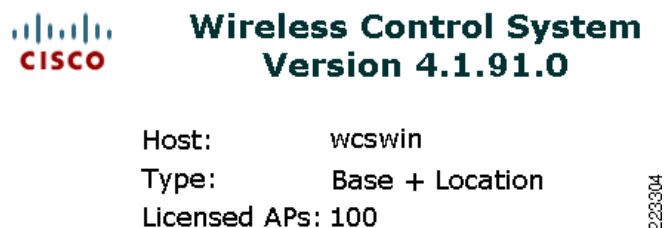
Complete details on the Cisco Developer Service Program may be found at the Cisco Developer Support website, located at the following URL:

http://www.cisco.com/en/US/products/svcs/ps3034/ps5408/ps5418/serv_home.html.

Location Tracking without a Location Appliance

In order to access any RF Fingerprinting-based location tracking features in the Cisco UWN or even to configure the Cisco Wireless Location Appliance, the Cisco WCS must be appropriately licensed for location usage. When a location-licensed version of WCS is used (verified using WCS main menu bar option Help > About the Software, [Figure 3-5](#)), RF Fingerprinting techniques are used to determine non-chokepoint-based location. When a location appliance is not used with a location-licensed version of WCS, RF Fingerprinting techniques are still used to determine location of tracked devices, but only on-demand and only for a single tracked device at a time.

Figure 3-5 *WCS Licensed for Location*



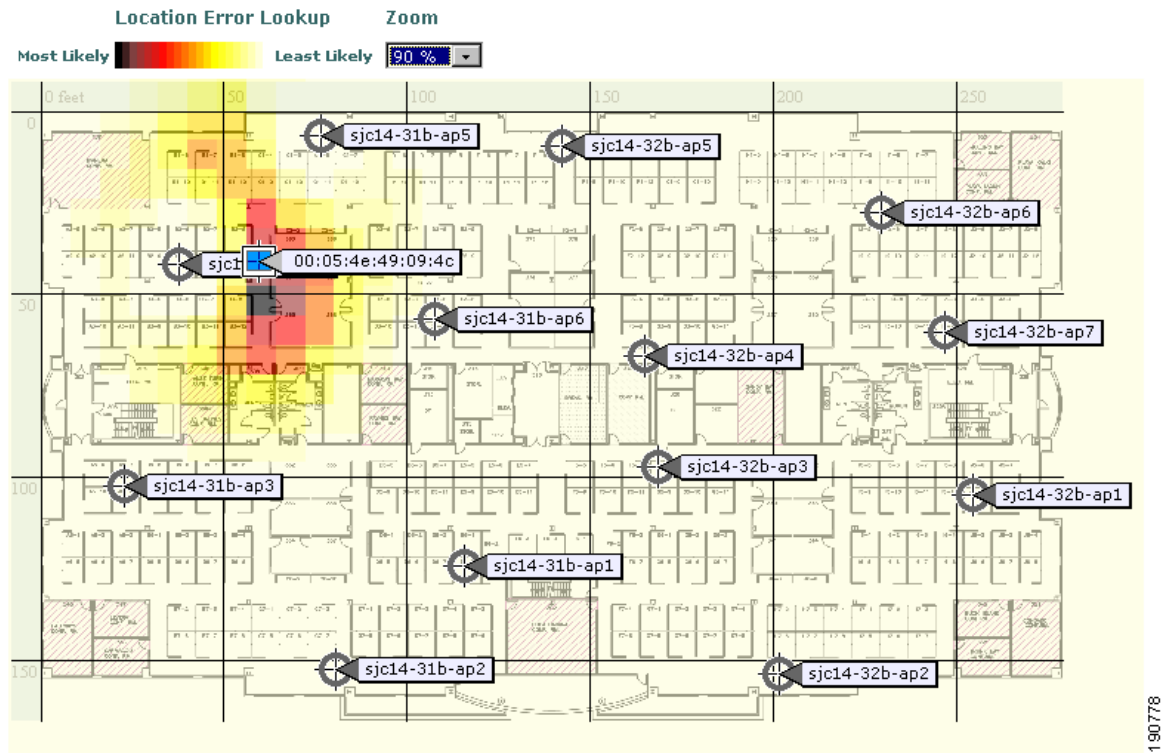
If a location-licensed WCS is used without a location appliance, the following capabilities will be unavailable:

- Ability to configure any Cisco Wireless Location Appliances
- Historical accumulation and playback of location data.
- Tag telemetry and high-priority notifications.
- Chokepoint location.
- The capability to interface to external third-party applications via the SOAP/XML API.
- Simultaneous tracking of multiple devices on a floor map. Location tracking services will be available only as an on-demand service and only for a single device at a time. [Figure 3-6](#) illustrates the use of on-demand localization for a single WLAN client. When using on-demand localization in this manner, it should be noted that colors surrounding the device icon provide an idea of the degree

of location error associated with the icon placement. The darker colors surrounding the icon represent those areas where confidence is high (the probability is higher that the device is physically located where the icon is placed or within this area). The lighter colors represent those areas of lower confidence (the probability is lower that the device is physically located within these areas).

Figure 3-6 On-Demand WLAN Client Localization using WCS with Location License

Maps > Cisco SJ - Site 5 > BLD 14 > 3rd floor



If WCS is licensed for only basic functionality as shown in Figure 3-7, RF Fingerprinting is not employed to determine location. Instead, on-demand location for a single WLAN client or rogue device is performed based on the access point that is detecting the mobile device with the highest signal strength (a derivation of the *nearest access point* concept).

Figure 3-7 WCS Licensed for Only Basic Functions



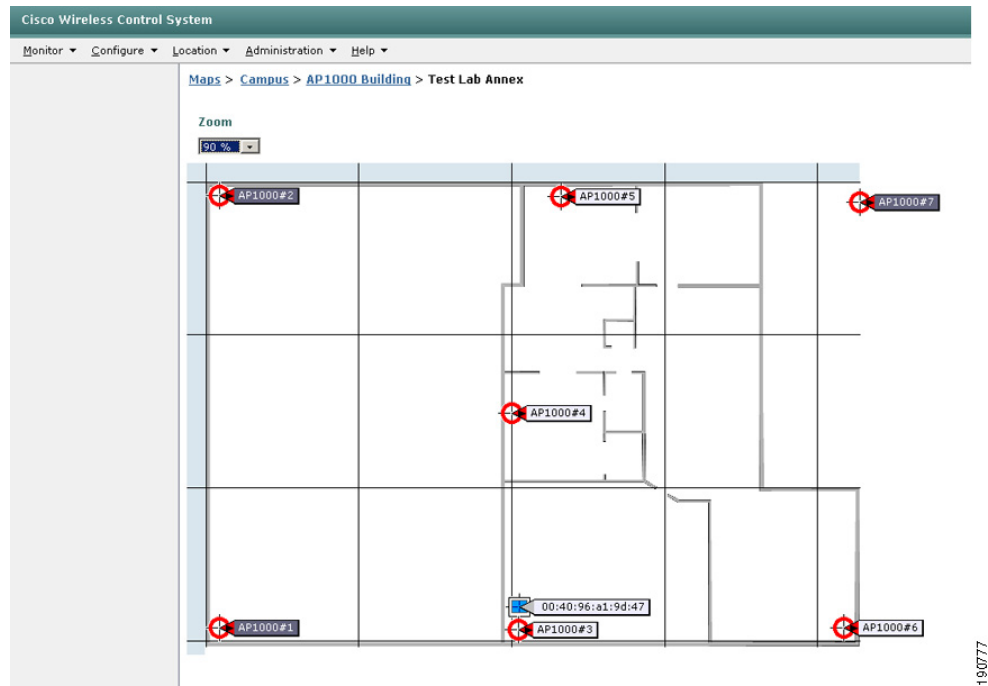
Wireless Control System Version 4.1.91.0

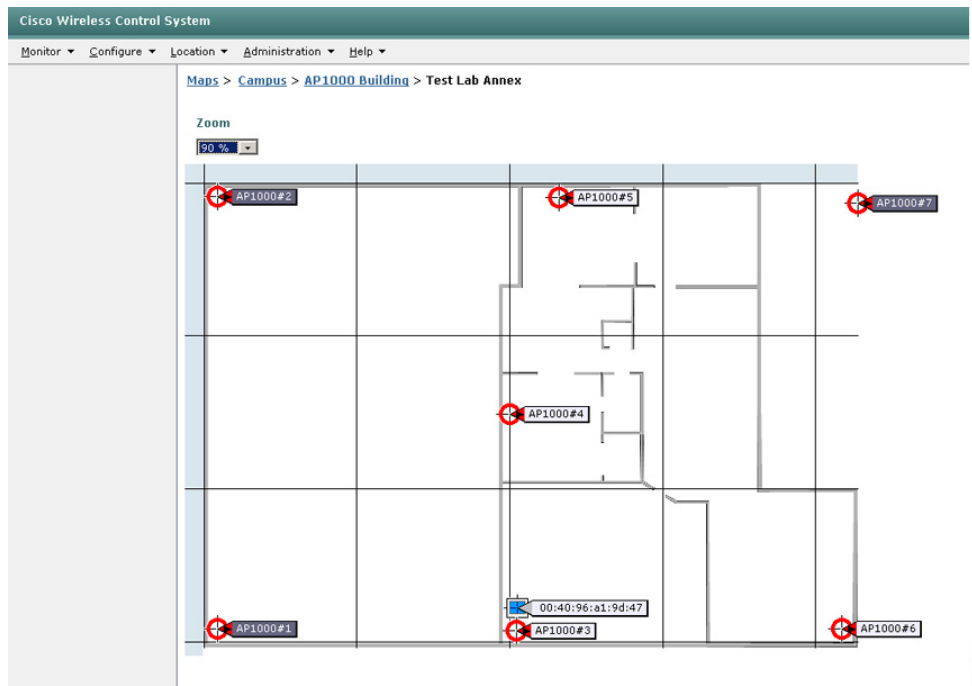
Host: wcswin
Type: Basic
Licensed APs: 50

223305

When using this approach, the tracked device's location is approximated by placing the device icon at the location of the access point detecting it with the highest signal strength, as shown in [Figure 3-8](#). No location probability is displayed in this case.

Figure 3-8 On-Demand Client Localization using WCS with Basic License



**Note**

A WCS server that is not licensed for location usage cannot be used as a location or control client to the Cisco Wireless Location Appliance. Commencing with software Release 4.1 of the Cisco UWN, on-demand location tracking of asset tags is not possible when using a WCS that is not licensed for location use.

Accuracy and Precision

For most users, the performance metric having the most familiarity and significance is *accuracy*, which typically refers to the quality of the information you are receiving. *Location accuracy* refers specifically to the quantifiable error distance between the estimated and the actual location of a tracked device.

In most real-world applications, however, a statement of location accuracy has little value without the ability of the solution to repeatedly and reliably perform at this level. *Precision* is a direct measure reflecting on the reproducibility of the stated location accuracy. Any indication of location accuracy should therefore include an indication of the confidence interval or percentage of successful location detection as well, otherwise known as the *location precision*.

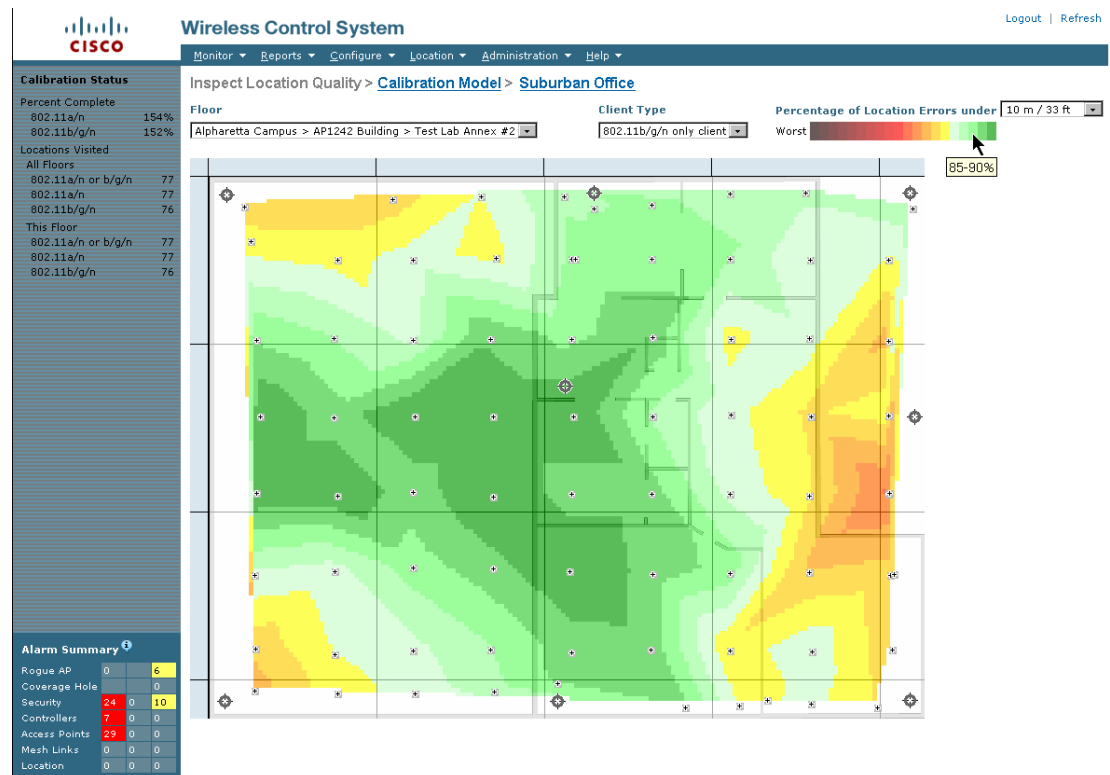
With deployment in accordance with the best practices outlined in this document, the location-aware Cisco UWN is capable of meeting a baseline performance specification of at least 10 meters accuracy with 90 percent precision. When combined with chokepoint location support, this level of performance

can be increased for asset tags possessing chokepoint location capabilities and compatible with the Cisco Compatible Extensions for Wi-Fi Tags specification. Depending on the configured range of the specific chokepoint trigger deployed, a location resolution radius of as little as one foot is possible.

This location appliance's baseline performance level can be achieved by following the best practices along with the use of the design, calibration, and deployment tools described in this and other reference documents. These tools would include predicative, pre-deployment tools such as the *Location Planning* and *Location Readiness* utilities as well as post-deployment tools such as the *Location Inspection* tool.

In order to determine those areas where baseline performance improvements may be necessary, the Location Inspection tool (shown in Figure 3-9), can be used to evaluate what the current, post-calibration levels of accuracy and precision are in the environment. The Location Inspection tool displays (in color coded format) the level of precision at any point from 0 to 5 percent to a maximum of 95 to 100 percent. After viewing the output, the system designer can work with the installation and deployment teams to address any areas requiring remedial attention if necessary.

Figure 3-9 Post-Calibration Location Inspection



Using these tools, the system architect as well as the installation team can not only plan towards the achievement of stated performance goals, but can verify that these targets are indeed being met.

For those interested in a professional service offering that includes the tuning of location performance and much more, Cisco offers a Wireless LAN Location Planning and Design Professional Service. This service offering enlists the skills of trained WLAN engineers to deliver an integrated solution that includes the services Cisco has identified as essential for successful deployment of a secure location-based services solution.

Further information on Cisco Wireless LAN Location Planning and Design Professional Services may be found located at the Cisco Wireless LAN Services website, which is located at the following URL:

http://www.cisco.com/en/US/products/ps8306/serv_home.html

Tracking Clients, Assets and Rogue Devices

This section discusses the mechanics behind the WLAN client probing mechanism and explains how variations in client probing can affect location accuracy. In addition, Cisco Compatible Extensions Location Measurements are explained in detail, along with a close examination of how location for each of the different device categories are displayed by the location client present within WCS.

Client Probing

Fundamentally, the location of WLAN clients is determined based on the RSSI of probe requests detected by access points and forwarded via their registered WLAN controllers to the location appliance. Therefore, the probing behavior of the WLAN and rogue clients in your network can be expected to have a significant impact on the ability of the location appliance to provide accurate location tracking.

Because consistent and regular probing of the network is so important to good WLAN client location fidelity, it is important to understand the mechanics of the process. The process begins with clients issuing probe requests in order to discover the existence of 802.11 networks in their immediate vicinity. An unassociated client may be seen to generate probe requests quite regularly, while clients that are currently associated to a network will typically be seen to issue probe requests less often. Associated clients periodically check their environment for potential access points and networks that they can roam to through a process called *scanning*. In *active scanning*, the client will issue probe requests to solicit probe responses from any access points in its vicinity. From these responses the client forms a list of potential access point roam candidates. Clients may, however, adopt a listen-only approach and simply note the beacons and probe responses they receive from access points around them, without actually soliciting these responses themselves (*passive scanning*). Clients that use passive scanning to determine potential access point roam candidates do not issue probe requests, hence passive scanning in and of itself does little to promote improved location fidelity. It is not unusual to see some clients use a combination of both techniques.

Since the location-aware Cisco UWN uses client probe requests to determine client location, it logically follows that the more consistent the client is in transmitting probe responses, the better the ability of the system will be to provide accurate location tracking of that client. For example, location accuracy can be degraded if a client:

- Refrains from active scanning for long periods
- Does not transmit probe requests across all channels in use
- Does not transmit probe requests for all configured SSIDs
- Transmits probe requests at power levels that deviate abnormally from that expected by the RTLS

IEEE 802.11 standards leave such areas open for interpretation, which does not lead to consistent probing behavior across vendors. This can have both good and not so good connotations from the standpoint of WLAN client location fidelity in the Cisco UWN. While some clients perform active scans and issue probe quite regularly, others may be seen to probe quite minimally.

Cisco Compatible Extensions Location Measurements

The impact of variations in client probing may be greatly reduced by standardizing on clients that are compliant with the Cisco Compatible Extensions for WLAN Devices specification at version 2 or greater. Compatible clients that support the S36 Radio Measurement Requests¹ introduced in Cisco Compatible Extensions for WLAN Devices specification version 2 will perform active scanning and probe all configured SSIDs upon command. Support of this capability enables clients to participate in

features such as Cisco Compatible Extensions Location Measurement. When this feature is enabled, registered lightweight access points broadcast Radio Measurement Request frames to their associated clients (via each enabled SSID and radio interface) at a configurable interval from 60 (default) to 32,400 seconds (see [Figure 3-10](#)).

Each Radio Measurement Request contains a beacon request that elicits compatible clients to respond by transmitting probe requests on the channels specified within the Radio Measurement Request. The consistency inherent to this mechanism helps enhance location accuracy for clients so equipped. Note that in software Release 4.1, DFS channels are not included in Radio Measurement Requests.

Using the WCS or controller GUI, Cisco Compatible Extensions Location Measurement can be enabled or disabled per radio interface type (such as 802.11bg or 802.11a) on each WLAN controller. It can also be enabled or disabled globally across controllers using WCS templates. In some cases, more granular control over the Cisco Compatible Extensions Location measurement parameter may be desired, such as when performing testing in specific areas. To support such cases, the WLAN controller CLI allows the Cisco Compatible Extensions Location Measurement feature to be applied to only specific access points if desired. For more information on configuring the Cisco Compatible Extensions Location Measurement using the WLAN controller CLI, refer to the *Cisco WLAN Controller Configuration Guide* at the following URL:

http://www.cisco.com/en/US/products/ps6366/products_configuration_guide_chapter09186a008082d6c5.html#wp1121089.

1. This is one of the features contained in the *RF Scanning and Reporting* category of Cisco Compatible Extensions for WLAN Devices. A complete list of Cisco Compatible Extensions features are found at the following URL:
http://www.cisco.com/web/partners/pr46/pr147/program_additional_information_new_release_features.html

Figure 3-10 Enabling CCX Location Measurement Using WCS Controller Template**10.1.56.18 > 802.11b/g Parameters**

General		Data Rates	
802.11b/g Network Status	<input checked="" type="checkbox"/> Enabled	1 Mbps	Mandatory
802.11g Support	<input checked="" type="checkbox"/> Enabled	2 Mbps	Mandatory
Beacon Period	100	5.5 Mbps	Mandatory
DTIM Period (beacon intervals)	1	6 Mbps	Supported
Fragmentation Threshold (bytes)	2346	9 Mbps	Supported
Short Preamble *	<input checked="" type="checkbox"/> Enabled	11 Mbps	Mandatory
Pico Cell Mode	<input type="checkbox"/> Enable	12 Mbps	Supported
Template Applied	802.11bConfig_166	18 Mbps	Supported
		24 Mbps	Supported
		36 Mbps	Supported
		48 Mbps	Supported
		54 Mbps	Supported

802.11b/g Power Status		Noise/Interference/Rogue Monitoring Channels	
Dynamic Assignment	Automatic	Channel List	DCA Channels
Current Tx Level	5	CCX Location Measurement Mode <input checked="" type="checkbox"/> Enabled Interval (seconds) 60 **	
Control Interval sec	600		
Dynamic Tx Power Control	<input checked="" type="checkbox"/> Enabled		

802.11b/g Channel Status	
Assignment Mode	Automatic
Update Interval sec	600
Avoid Foreign AP Interference	<input checked="" type="checkbox"/> Enabled
Avoid Cisco AP load	<input type="checkbox"/> Enabled
Avoid non 802.11 Noise	<input checked="" type="checkbox"/> Enabled
Signal Strength Contribution	<input checked="" type="checkbox"/> Enabled

* Controller must be rebooted for new value to take an effect

Save **Audit**

190542

If the Cisco Compatible Extensions Location Measurement parameter is enabled, Radio Measurement Requests will be broadcast to all associated WLAN clients, regardless of their capability to support Cisco Compatible Extensions. Clients that do not support S36 Radio Measurement Requests (such as those supporting Cisco Compatible Extensions version 1 or those not compatible with the Cisco Compatible Extensions for WLAN Devices specification at all) will ignore any Radio Measurement Requests that are received.

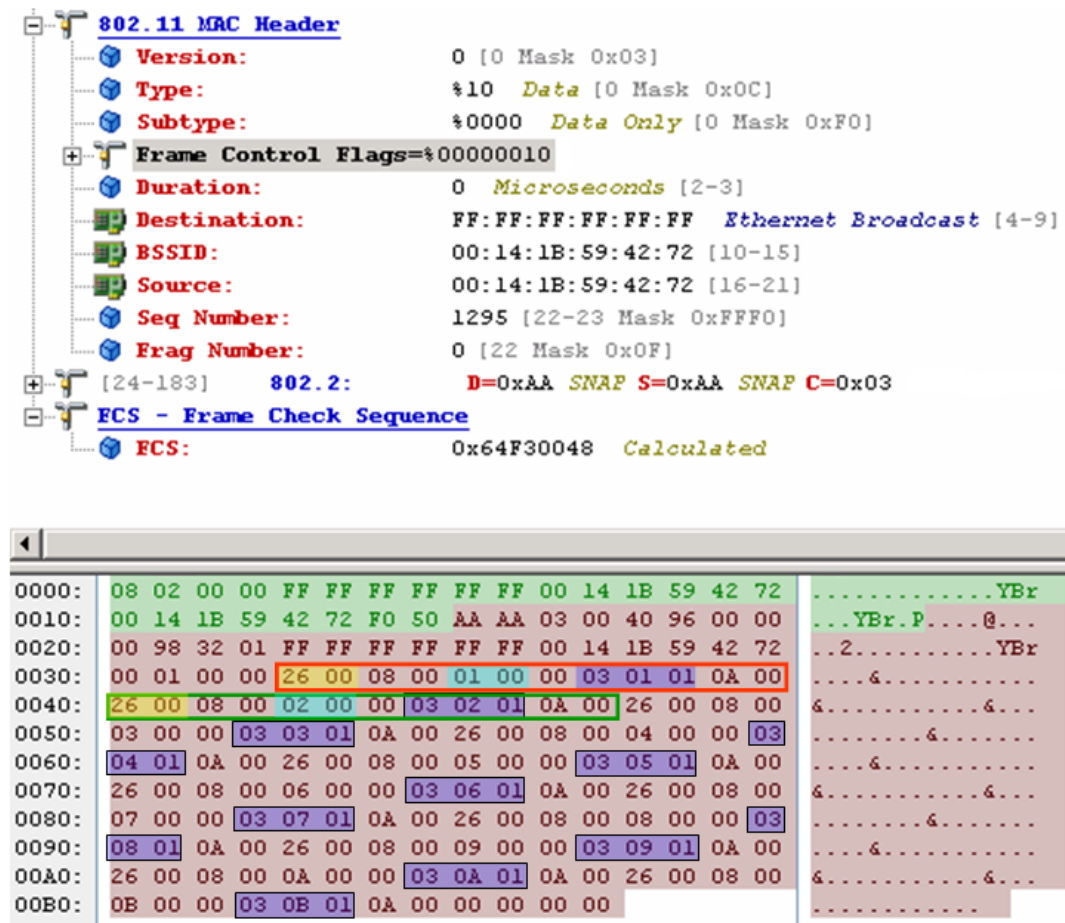
**Note**

When using clients equipped with the Intel® PRO/Wireless 3945ABG Network Connection or the Intel® PRO/Wireless 2915ABG Network Connection adapter, it is important to note that the default “Personal Security” settings of the Intel ProSet Configuration Utility do not include compatibility with the Cisco Compatible Extensions specification. When using this default “personal” level of wireless security (which is not intended for enterprise use), clients equipped with the Intel 3945ABG or 2915ABG client adapters will not support S36 broadcast radio measurement requests and are not compliant with the Cisco Compatible Extensions specification for WLAN devices. In order to enable compatibility with the Cisco Compatible Extensions specification and the support of S36 radio

measurement requests, the Intel ProSet client supplicant must be used to reconfigure the client for “Enterprise Security” and enable Cisco Compatible Extensions. [Figure 5-42 on page 5-60](#) and [Figure 5-43 on page 5-61](#) illustrate how this is performed.

An example of a Radio Measurement Request can be seen in [Figure 3-11](#). This request is seen to emanate from an access point with a 802.11b/g interface MAC address of 00:14:1B:59:42:72.

Figure 3-11 Broadcast Radio Measurement Request



[Figure 3-11](#) provides several key pieces of information that supports our understanding of the effect of Radio Measurement Requests on WLAN clients. We see in [Figure 3-11](#) that the frame broadcast to the associated clients actually contains multiple Radio Measurement Request Elements, the first of which is highlighted within the red rectangle beginning at hex offset 0x0034. Looking closer into the Radio Measure Request Element we see the following¹:

- The element ID of 0x2600 appears at hex offset 0x0034, identifying that what follows is a Measurement Request Element (shown in yellow).
- The measurement token of 0x01 appears at offset 0x0038. This is a non-zero hex value that is unique amongst the Measurement Request Elements in a particular Measurement Request frame.

1. Fields in the radio information elements follow the 802.11 convention of sending the least significant byte first.

- At HEX offset 0x003B, we see the first of several Radio Measurement Request Element detail fields (the first three bytes of each shown highlighted within blue rectangles). Upon closer examination, we can see that each detail field contains:
 - The Measurement Type Definition of 0x03, indicating that this is a Beacon Request. This measurement type requests that the receiving client station perform active or passive scanning (see the Scan Mode Definition field below), and forward the results of those scans upstream to the UWN when it has completed. When performing an active scan, the client device transmits probe request frames that solicit probe responses from receiving access points. In contrast, a passive mode scan requests that 802.11 client devices simply listen for beacon or probe response frames but does not require active solicitation.
 - The Channel Number that the Beacon Request should apply to. This is the second octet of the measurement request detail field and can be seen at hex offset 0x003C with a value of 0x01.
 - The Scan Mode Definition of 0x01, the third octet of the management request detail field. This can be seen at hex offset 0x003D. A Scan Mode Definition of 0x01 indicates that an active scan should be performed. From a strict location fidelity perspective, a passive scan would do little to enhance client location fidelity (since no probe requests are generated). Therefore, when CCX Location Measurement is enabled on the controller, the Scan Mode Definition will always be set to request that active scanning be performed.

Taking all three Radio Measurement Detail fields into consideration, we see that this Radio Measurement Request Element contains a Beacon Request for an active scan to be performed on Channel one.

Note that there are eleven Measurement Request Element fields contained in the Radio Measurement Request. [Figure 3-11](#) highlights only two of them, the first contained within a red rectangle and the second within a green rectangle. This is understandable given that this Radio Measurement Request is being issued on a 802.11b/g radio interface that is operating in the North American regulatory domain with eleven available channels. In the subsequent measurement requests (indicated by the green rectangle), the Channel Number field (seen at hex offset 0x44) is sequentially incremented by 1 from that of the initial measurement request. This continues in the Measurement Request Element fields that follow until the value of 0xB (11) is reached.

802.11bg clients compliant with the Cisco Compatible Extensions for WLAN Devices specification version 2 or greater and supporting S36 Radio Measurement Requests receive the frame shown in [Figure 3-11](#) and will perform an active scan of the specified channels as part of the radio measurement process. When the probe requests are received by access points in the vicinity of such clients, they forward (via their registered controller) signal strength measurements to the location appliance that is used to localize the client. In addition, clients also collect the RSSI information of all probe responses received during the measurement duration, and forward this to the Cisco UWN in a Radio Measurement Report frame.

As per the Cisco Compatible Extensions for WLAN Devices specification version 2, WLAN clients supporting S36 Radio Measurement Requests should:

- Perform radio measurements on the channel over which the Measurement Request was received without significantly degrading performance.
- Perform measurements on non-serving channels while temporarily buffering outgoing traffic.
- Respond to each Radio Measurement Request frame accepted with a Radio Measurement Report frame.
- Disregard any measurement requests that would significantly degrade performance of the client device.
- Support active scanning.

WLAN Clients

Wireless LAN clients and properly configured work-group bridges are displayed on the WCS location floor maps using a blue rectangle icon, as shown in Figure 3-12. To display WLAN clients on the WCS location floor map, ensure that the **Clients** checkbox option is enabled from the **Layers** dropdown selector at the top of the floor map display, and click **Load** in the left-hand column. To avoid excessive clutter, WCS will display the first 250 WLAN clients on the floor map. To view the location of WLAN clients beyond the first 250, client filtering must be used.

Figure 3-12 WCS WLAN Client Location Map



Note that the graphical location information shown can be filtered by WCS based on the age of the information. Thus in Figure 3-12, WCS displays device location information that has aged up to 15 minutes. This value can be set to 2 or 5 minutes if you would like to view location information received more recently, or ½, 1, 3, 6, 12, or 24 hours for information that is older.

By clicking on the blue chevron ➤ that is displayed to the right of the **Clients** checkbox option, client filtering options can be specified and additional information retrieved, such as:

- The total number of WLAN clients detected on this floor.
- Small icons (shown in Figure 3-12) or standard size icons can be selected. When using small icons, descriptive text is not displayed on the floor map for the client except when a mouse-over is performed. When using standard size icons, an on-screen tag is displayed that is configurable for IP address, user name, MAC address, asset name, asset group, or asset category.
- Either all WLAN clients can be displayed, or filtering can be performed to select which clients to display on the floor map. This can be based on IP address, user name, MAC address, asset name, asset group, asset category, or controller. Additional filtering can be specified for SSID and RF protocol (802.11a or 802.11b/g). As mentioned previously, only up to 250 WLAN clients will be shown at one time on the floor maps. If there are greater than 250 WLAN clients detected,

the total number found will be indicated in the left hand column status area during each communication cycle between WCS and the location appliance. It is recommended that filtering be used to reduce the total number of WLAN clients selected for display if you receive this warning.

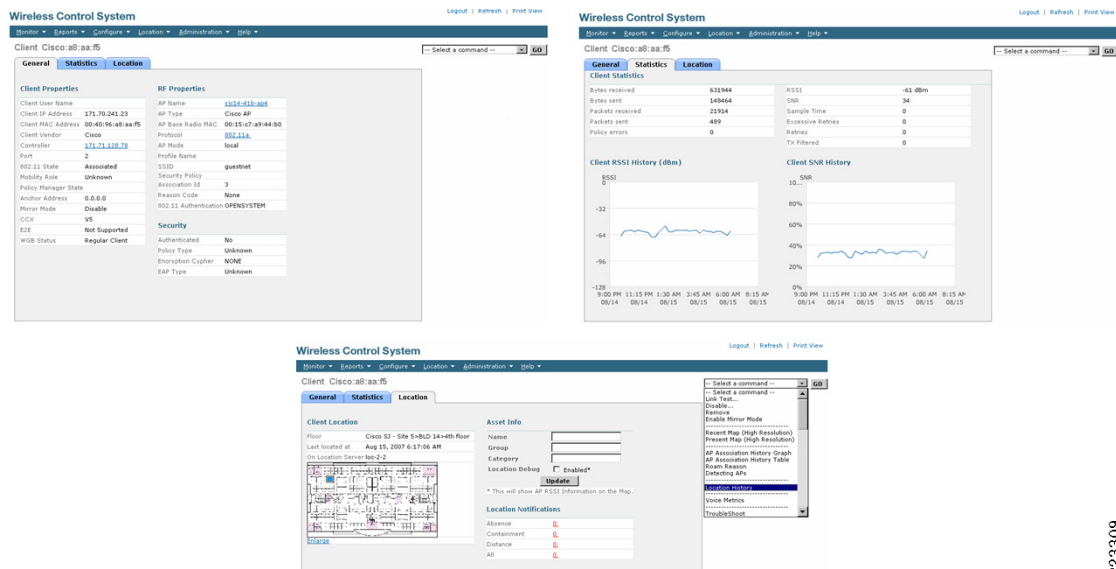
In software Release 4.1 of the Cisco UWN, WLAN controllers provide support for the maximum number of WLAN clients listed in [Table 3-1](#).

Table 3-1 Maximum WLC Client Capacity

Controller Model	WLAN Clients Supported
2006	256
2106	256
4402	2,500
4404	5,000
WiSM	10,000
NM-WLC6	256
NME-WLC8/12	350
3750G	2,500

Complete information on any displayed WLAN client can be obtained simply by left-clicking on the appropriate blue rectangular icon on the floor map, as shown in [Figure 3-13](#). Note that name, group, and category information can be assigned to the client under the “location” submenu, which can then be used to identify the asset on the floor map display.

Figure 3-13 WLAN Client Detailed Information



Note that [Figure 3-13](#) also includes a hyperlinked listing of location notifications as well as a miniature location map showing the client location. By enlarging the map and enabling the Location Debug parameter, WCS displays the last detected RSSI levels of each access point detecting the WLAN client, as shown in [Figure 3-14](#).

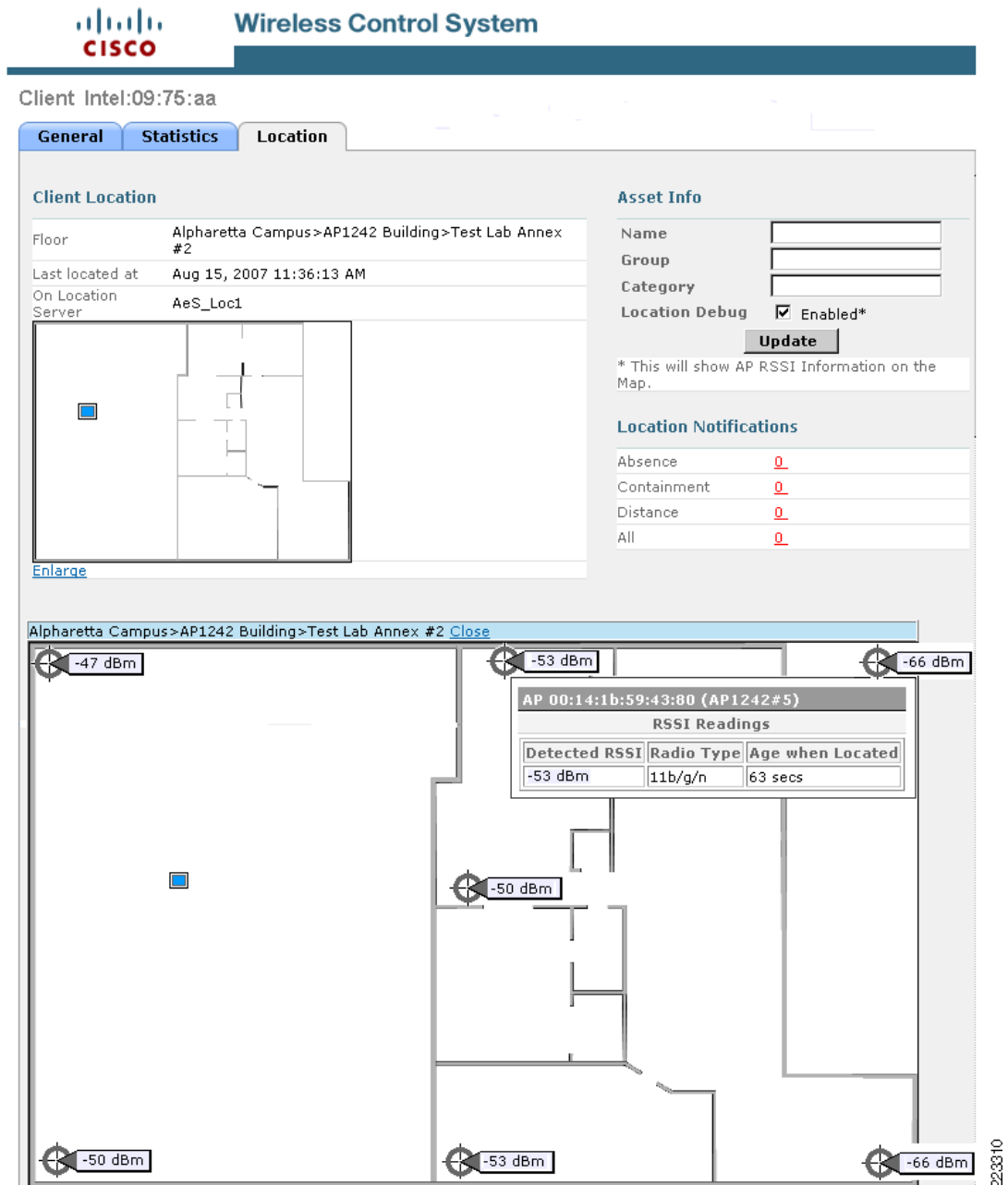
223309

**Note**

The setting of the Location Debug Enable checkbox does not survive a restart of the *locserverd* application or a reboot of the location appliance.

This RSSI information is collected in a similar fashion to that shown by the **show client detail** *<mac address>* command, and provides an alternative to the CLI command for determining the detected RSSI of WLAN clients (see Figure 3-14).

Figure 3-14 WLAN Client Detected RSSI with Location Debug Enabled



Wireless client device location history may be displayed by selecting **Location History** from the dropdown menu at the top right-hand corner of the screen (illustrated in the location screen view of Figure 3-14) and clicking **Go**. Past location history stored within the location appliance is displayed for the wireless client via the screen shown in Figure 3-15.

Figure 3-15 WLAN Client Location History

Wireless Control System

Monitor ▾ Reports ▾ Configure ▾ Location ▾ Administration ▾ Help ▾

Client Cisco:a8:aa:f5 -- Select a command -- **GO**

Client User Name
Client IP Address 0.0.0.0 Client MAC Address 00:40:96:a8:aa:f5
Client Vendor Cisco

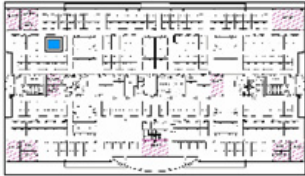
From : Mon Jul 16 03:03:28 EDT 2007
To : Wed Aug 15 10:35:05 EDT 2007

	Time Stamp	Floor
1	Wed Aug 15 10:35:05 EDT 2007	Cisco SJ - Site 5>BLD 14>4th floor
2	Wed Aug 15 08:35:05 EDT 2007	Cisco SJ - Site 5>BLD 14>4th floor
3	Wed Aug 15 06:35:05 EDT 2007	Cisco SJ - Site 5>BLD 14>4th floor
4	Wed Aug 15 04:35:05 EDT 2007	Cisco SJ - Site 5>BLD 14>4th floor
5	Wed Aug 15 02:35:05 EDT 2007	Cisco SJ - Site 5>BLD 14>4th floor

Change selection every 2 secs **Play** **Stop**

Client Location

Location Calculated Wed Aug 15 10:26:33 EDT 2007
Floor Cisco SJ - Site 5>BLD 14>4th floor



[Enlarge](#)

Client Statistics

Data Collected Wed Aug 15 10:21:44 EDT 2007

Bytes received	698622
Bytes sent	170998
Packets received	24165
Packets sent	548
Policy errors	0
RSSI	-60dBm
SNR	32

Client Properties

Data Collected	Wed Aug 15 10:26:33 EDT 2007
Controller	171.71.128.78
Port	2
802.11 State	Associated
Mobility Role	Unknown
Policy Manager State	
Anchor Address	0.0.0.0
CCX	V5
E2E	Not Supported

RF Properties

AP Name	sjc14-41b-ap5
AP Type	Cisco AP
AP Base Radio MAC	00:15:c7:a9:43:10
Protocol	802.11a
AP Mode	local
SSID	
Association Id	10
Reason Code	0
802.11 Authentication	0
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Not Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Timeout	0
WEP State	ENABLE

Security

Authenticated	No
Policy Type	Unknown
Encryption Cypher	S
EAP Type	Unknown

In many cases, it is desirable to sequentially display the location history of a client device in order to better visualize and trace the movement of the client throughout the environment over time. This can be very useful, for example, in security and monitoring applications. Cisco WCS and the location appliance

223811

make it possible to view each location history record in this fashion, played back with a configurable time delay. The granularity of the “movement” shown depends on the interval with which client history records are recorded in the database.

To see location history played back in this fashion, simply click on the **Play** button shown in Figure 3-15.

802.11 Active RFID Tags


The location-aware Cisco UWN readily detects 802.11 Wi-Fi active RFID tags that are compliant with the Cisco Compatible Extensions for Wi-Fi Tags specification (such as those from AeroScout, WhereNet, G2 Microsystems and InnerWireless (PanGo), amongst others) and displays them on WCS floor maps using a yellow tag icon, as shown in Figure 3-16. These asset tags typically do not associate to the WLAN infrastructure and are not typically located on the basis of probe requests). Instead, these asset tags transmit messages to the location-aware UWN on a periodic basis using layer two multicasts. If an asset tag has an optional mode that allows for full WLAN association, those tags will be represented on WCS location floor maps as blue rectangles (WLAN clients) during the time they are operating in this mode.

To display the location of asset tags on the WCS location floor map, ensure that the **Clients** checkbox option is enabled from the **Layers** drop down selector at the top of the floor map display, and click **Load** in the left-hand column. To avoid excessive clutter, WCS will display the first 250 asset tags on the floor map. To view the location of asset tags beyond the first 250, asset tag filtering must be used. It is assumed that all other components of the location-aware Cisco UWN have been properly configured to collect asset tag information.

Figure 3-16 RFID Tag Location Map



The graphical location information shown can be filtered by WCS based on the age of the information. In [Figure 3-16](#) WCS displays location appliance information that has aged up to 15 minutes. This value can be set to 2 or 5 minutes if it is desired to view only very recent location information, or ½, 1, 3, 6, 12, or 24 hours to include information that is older.

By clicking on the blue chevron  that is displayed to the right of the **802.11 Tags** checkbox option, tag filtering options and additional information can be displayed, such as:

- The total number of asset tags detected on this floor can be displayed.
- Small icons (shown in [Figure 3-16](#)) or standard size icons can be selected. When using small icons, text is not displayed on the floor map for the asset tag except when a mouse-over is performed. When using standard size icons, an on-screen tag is displayed, which is configurable for MAC address, asset name, asset group, or asset category.
- Either all asset tags can be displayed or filtering can be performed to select which asset tags to display on the floor map. This can be based on MAC address, asset name, asset group, asset category, or controller. As mentioned previously, only up to 250 asset tags will be shown on the floor maps at any one time. If there are greater than 250 asset tags detected, the total number found will be indicated in the left hand column status area during each communication cycle between WCS and the location appliance. It is recommended that filtering be used to reduce the total number of asset tags selected for display if you receive this warning.


In software Release 4.1 of the Cisco UWN, WLAN controllers provide support for the maximum number of asset tags listed in [Table 3-2](#).

Table 3-2 *Maximum WLC Asset Tag Capacity*

Controller Model	Asset Tags Supported
2006	500
2106	500
4402	1250
4404	2500
WiSM	5000
NM-WLC6	500
NME-WLC8/12	500
3750G	1250

Complete information on any displayed asset tag can be obtained by clicking on the yellow tag icon associated with the tag. WCS responds with the information shown in [Figure 3-17](#). Beginning with software Release 4.1 of the location-aware Cisco UWN, tag telemetry, chokepoint and tag status information are also displayed on the Tag Details screen shown in [Figure 3-17](#), along with enhanced battery reporting information.

Figure 3-17 RFID Tag Detailed Information



Wireless Control System

Tags > Aeroscout Tag 00:0c:cc:5c:05:17

Tag Properties

Vendor	Aeroscout
Controller	10.1.96.18
Battery Life	Batt remaining = 80 %, Days remaining = 0, Tolerance = +/- 20 %, Battery Age = 0

Asset Info

Name	<input type="text"/>
Group	<input type="text"/>
Category	<input type="text"/>
Location Debug	<input checked="" type="checkbox"/> Enabled*

Update

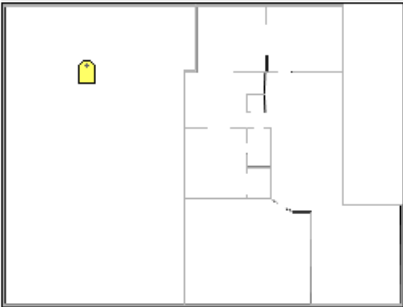
* This will show AP RSSI Information on the Map.

-- Select a command -- **GO**

-- Select a command --
[Location History](#)

Location

Floor	Alpharetta Campus>AP1242 Building>Test Lab Annex #2
Last located at	Aug 15, 2007 4:16:35 PM
On Location Server	AeS_Loc1
Last Chokepoint	00:0c:cc:60:1e:8a
Chokepoint Encountered	Wed Aug 15 16:00:41 EDT 2007



[Enlarge](#)

Statistics

Bytes received	104877
Packets received	2012

Location Notifications

Absence	0
Containment	0
Distance	0
All	0

Telemetry Data

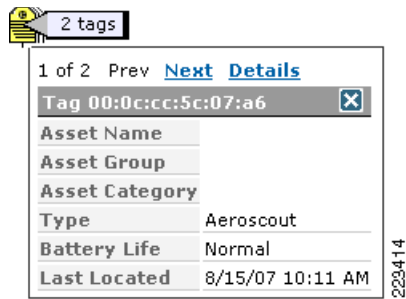
TEMPERATURE : 100.0 degrees Celsius
QUANTITY : 29
MOTION : 29.0576 meters/sec
HUMIDITY : 80 %
MOTIONPROB : Acceleration
FUEL : 29.0576 liters

Emergency Data

Reason:	Panic Button Pressed
---------	----------------------

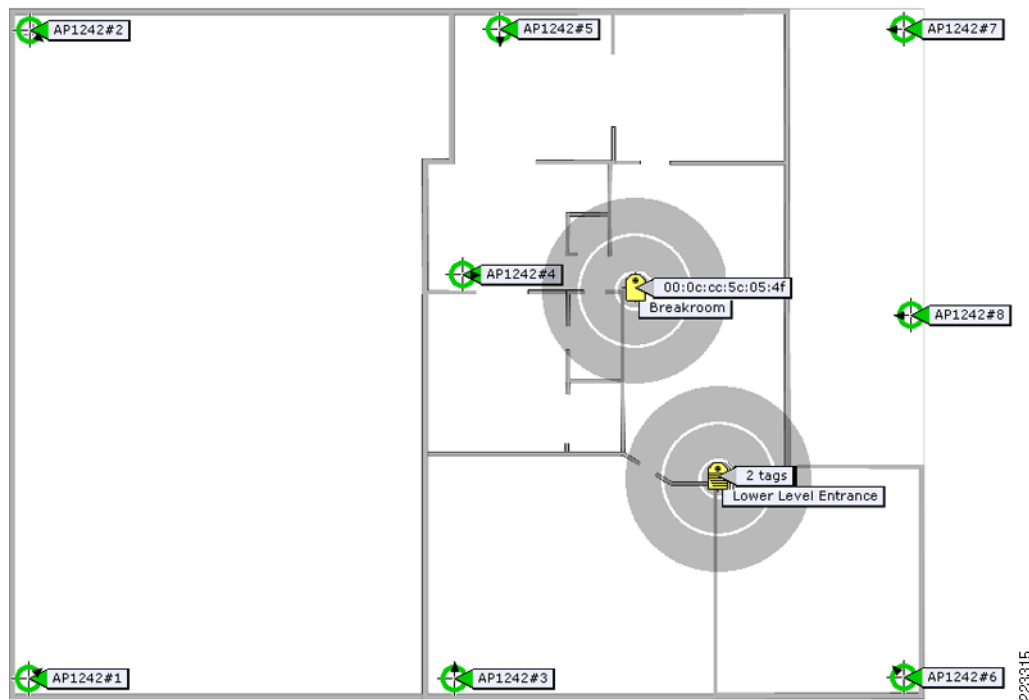
223313

In some cases the location appliance may place two or more asset tags at the same predicted location, such that any attempt to graphically represent them as individual icons would result in almost complete overlap. A tag summary icon (a yellow tag with black horizontal lines) is used to resolve such situations, as shown in [Figure 3-18](#).

Figure 3-18 Tag Summary Icon and Summary Descriptor

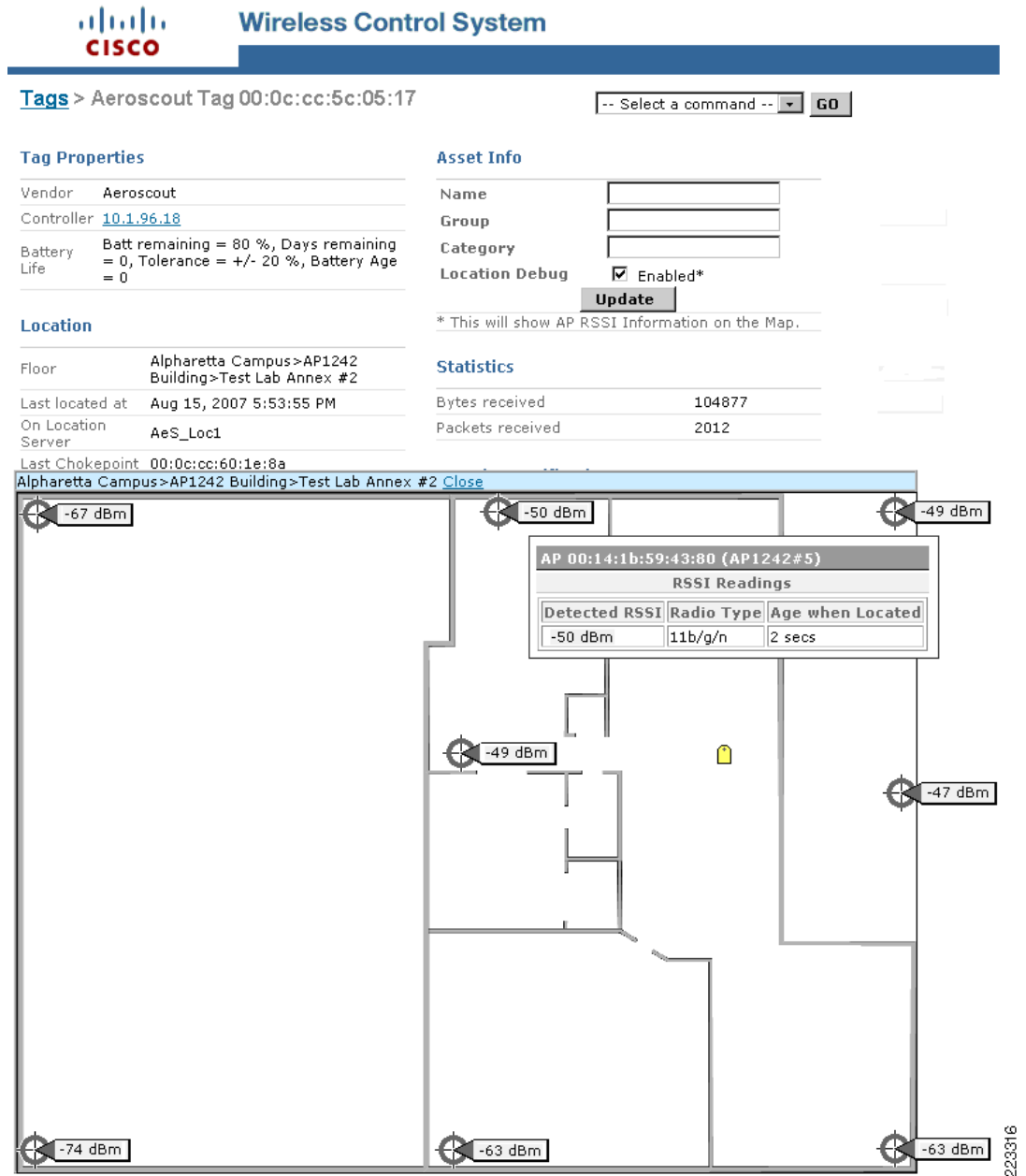
Performing a mouse-over of the tag summary icon brings up a tag summary descriptor shown, which summarizes pertinent tag characteristics. Clicking on “Next” scrolls through the descriptor information for each tag MAC address at this location, and clicking on “Details” at any time brings up the Tag Details panel shown in Figure 3-17.

The tag summary icon becomes especially useful when *chokepoint location* (introduced with software Release 4.1 of the Cisco UWN) is used. When chokepoints have been defined to the system and properly defined on floor maps, the icon of any asset tag that known to be within range of the chokepoint trigger will be placed at the center of the chokepoint icon (shown in Figure 3-19 at the “Breakroom” chokepoint). However, if more than one asset tag is in proximity of the same chokepoint, the tag icons will overlap and usability will suffer. In this situation, the tag summary icon shown in Figure 3-18 once again is used to restore clarity. An example of the tag summary icon being used in this can be seen in Figure 3-19, at the chokepoint labeled “Lower Level Entrance”.

Figure 3-19 Tag Summary Icon and Chokepoint Location

Note that [Figure 3-20](#) also includes a hyperlinked listing of location notifications as well as a miniature location map of the asset tag's location. By enabling the Location Debug parameter and enlarging the map, WCS displays the last detected RSSI levels of each access point detecting the asset tag. This RSSI information is collected in a similar fashion to that shown by the **show rfid detail <mac address>** command, and provides an alternative to the CLI command for determining the detected RSSI of asset tags. As can be seen in [Figure 3-20](#), additional information regarding the radio type and age of the last detected signal strength reading is available by performing a mouse-over of any access point.

Figure 3-20 Asset Tag Detected RSSI with Location Debug Enabled



Asset tag location history may be displayed by selecting **Location History** from the dropdown menu at the top right-hand corner of the screen shown in Figure 3-20 and then clicking on **Go**. Past location history stored within the location appliance will be displayed for the asset tag, along with last values recorded for location statistics, tag telemetry, battery and “emergency” status, as shown in Figure 3-21.

Figure 3-21 Asset Tag Location History

Wireless Control System

Monitor ▾ Reports ▾ Configure ▾ Location ▾ Administration ▾ Help ▾

Aer scout Tag 00:0c:cc:5c:05:17 -- Select a command -- **GO**

Asset Name _____ Asset Group _____
 Asset Category _____ MAC Address 00:0c:cc:5c:05:17

From : Wed Aug 15 17:10:37 EDT 2007
 To : Wed Aug 15 19:07:40 EDT 2007

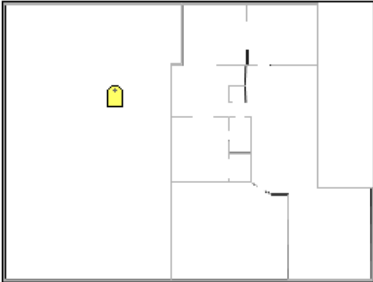
	Time Stamp	Floor	Battery Status
1	Wed Aug 15 19:07:40 EDT 2007	Alpharetta Campus>AP1242 Building>Test Lab Annex #2	80 %
2	Wed Aug 15 19:06:40 EDT 2007	Alpharetta Campus>AP1242 Building>Test Lab Annex #2	80 %
3	Wed Aug 15 19:05:40 EDT 2007	Alpharetta Campus>AP1242 Building>Test Lab Annex #2	80 %

Change selection every 2 secs **Play** **Stop**

Location

Location Calculated Wed Aug 15 19:08:39 EDT 2007

Floor Alpharetta Campus>AP1242 Building>Test Lab Annex #2



[Enlarge](#)

Tag Statistics

Data Collected Wed Aug 15 19:08:36 EDT 2007

Bytes received 162597

Packets received 3122

Telemetry Data

TEMPERATURE : 100.0 degrees Celsius

QUANTITY : 29

MOTION : 29.0576 meters/sec

MOTIONPROB : No Movement

FUEL : 29.0576 liters

Emergency Data

Reason: Panic Button Pressed

Tamper State: Inactive

Tag Properties

Data Collected Wed Aug 15 19:07:39 EDT 2007

Controller 10.1.96.18

Battery Status 80 %

223317

In many cases, it is desirable to sequentially display the location history of an asset tag so as to better visualize and trace the movement of the asset tag (and the attached asset) throughout the environment over time. This can be very useful, for example, in establishing a trail of motion in security and monitoring applications. Cisco WCS and the location appliance make it possible to do this by playing back each location history record with a configurable time delay. The granularity of the “movement” shown depends on the interval with which client history records are recorded in the database.

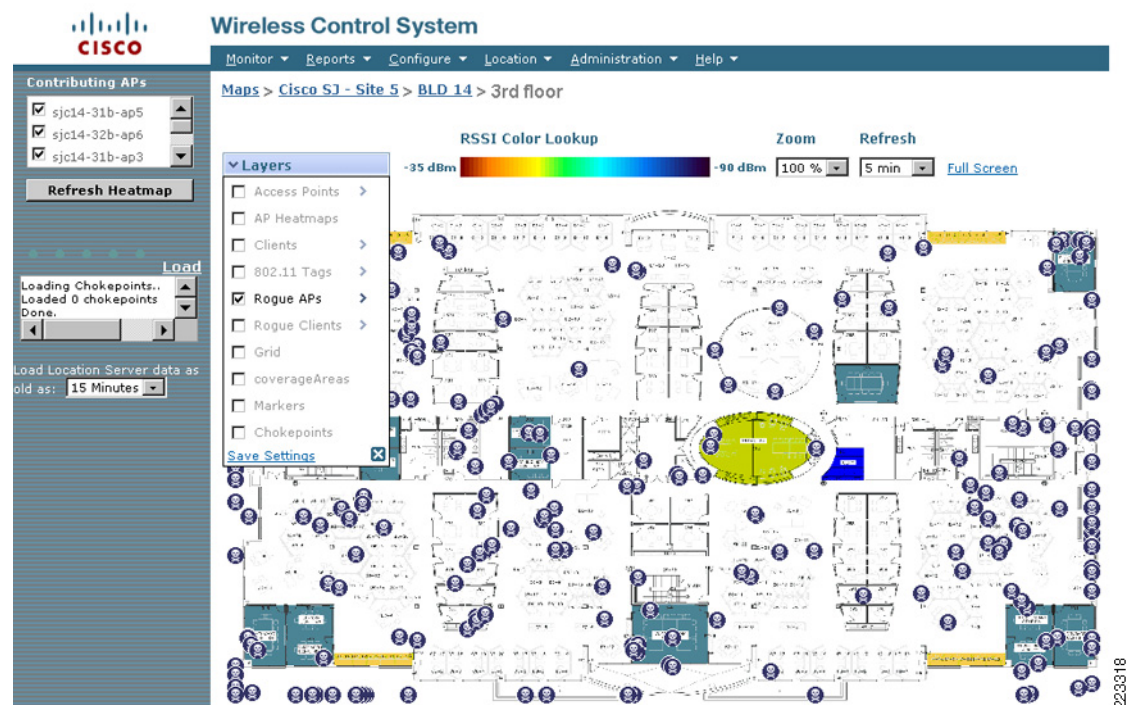
To see location history played back in this fashion, simply click the **Play** button shown in Figure 3-21 and past location history should start being displayed both in tabular form and graphically. Large amounts of location history data may be more readily viewed by reducing the “Change Selection Every” interval shown in Figure 3-21 from 2 seconds to 1 second.

Rogue Access Points

Rogue access points are access points that are detected by the wireless LAN infrastructure and determined not to be members of the same RF group or WLAN system. In addition, any devices that are participating as members of ad-hoc networks are also detected as rogue access points (but with a rogue type of AD_HOC, unless location appliance rogue access point polling has been configured to exclude ad-hoc rogues).

Rogue access points are indicated on WCS location floor maps using an icon representing a skull-and-crossbones within a black circle, as shown in Figure 3-22. They may be totally wireless, connected to the same wired infrastructure as the detecting WLAN, or connected to an entirely different wired infrastructure. To display rogue access points on the WCS location floor map, ensure that the **Rogue APs** checkbox option is enabled from the **Layers** dropdown selector at the top of the floor map display, and click **Load** in the left-hand column. To avoid excessive clutter, WCS will display the first 250 rogue access points on the floor map. To view the location of rogue access points beyond the first 250, rogue access point filtering must be used.

Figure 3-22 Rogue Access Point Location Map



It is possible to filter the location information displayed by the WCS based on the age of the information. In Figure 3-22 WCS displays location appliance information that has aged up to 15 minutes. Alternatively, this value could be set to 2 or 5 minutes for more recent location information or ½, 1, 3, 6, 12, or 24 hours for older information.

By clicking on the blue chevron ➤ that is displayed to the right of the **Rogue APs** checkbox, rogue access point filtering options can be specified and additional information can be displayed, such as:

- The total number of rogue access points detected on this floor.
- Small icons (shown above) or standard size icons can be selected. When using small icons, text is not displayed on the floor map for the rogue access point except when a mouse-over is performed. When using standard size icons, an on-screen tag displaying the MAC address of the rogue access point appears.
- Either all rogue access points can be displayed, or filtering can be performed to select which rogue access points to display on the floor map. This is based primarily on MAC address but can be augmented by filtering on the state of the rogue detection (Alert, Known, Acknowledged, Contained, Threat, or Known Contained) as well as whether or not the rogue access point was seen to be connected to the same wired network as the detecting wireless system. As mentioned previously, only up to 250 rogue access points will be shown at any one time on floor maps. If there are greater than 250 rogue access points detected, the total number found will be indicated in the left hand column status area during each communication cycle between WCS and the location appliance. It is recommended that filtering be used to reduce the total number of rogue access points selected for display if you receive this warning.

In software Release 4.1 of the Cisco UWN, WLAN controllers provide support for the maximum number of rogue access points shown in [Table 3-3](#).

Table 3-3 Maximum WLC Rogue Access Point Capacity

Controller Model	Rogue APs Supported
2006	125
2106	125
4402	625
4404	625
WiSM	1250
NM-WLC6	125
NME-WLC8/12	125
3750G	625

Complete information on any displayed rogue access point can be obtained simply by left-clicking the cursor on the circular skull-and-crossbones icon representing the desired rogue access point on the floor map. Doing this yields a screen containing detailed information as shown in [Figure 3-23](#). Note however, there is no RSSI information displayed for rogue access points when the location map is enlarged. Using the dropdown menu located in the upper right-hand corner, location history and playback information for the rogue access point in question can be accessed, similar in format and function to that described previously for WLAN clients and 802.11 active RFID tags.

Figure 3-23 Rogue Access Point Detailed Information

Wireless Control System [Logout](#) | [Refresh](#) | [Print View](#)

Monitor ▾ Reports ▾ Configure ▾ Location ▾ Administration ▾ Help ▾

[Alarms](#) > Rogue - 00:1c:b0:eb:e2:30

General

Rogue MAC Address	00:1c:b0:eb:e2:30
Vendor	Unknown
Rogue Type	AP
On Network	No
Owner	
State	Alert
SSID	loc-wlc-04
Channel Number	6
Containment Level	Unassigned
Radio Type	b/g
Strongest AP RSSI	-77
No. of Rogue Clients	0
Created	Aug 15, 2007 3:23:13 PM
Modified	Aug 16, 2007 6:50:35 PM
Generated By	Controller
Severity	Minor
Previous Severity	Minor

Annotations

Annotations go here.

[Add](#)

Message

Rogue AP '00:1c:b0:eb:e2:30' with SSID 'loc-wlc-04' and channel number '6' is detected by AP 'sjc14-32b-ap9' Radio type '802.11b' with RSSI '-77' and SNR '1'.

Help

Rogue AP '00:1c:b0:eb:e2:30' with SSID 'loc-wlc-04' and channel number '6' is detected by AP 'sjc14-32b-ap9' Radio type '802.11b' with RSSI '-77' and SNR '1'.

Location Notifications

Absence	0
Containment	0
Distance	0
All	0

Location

Floor	Cisco SJ - Site 5>BLD 14>3rd floor
Last located at	Aug 16, 2007 6:59:12 PM
On Location Server	loc-2-2

[Enlarge](#)

[Rogue Clients](#)

[Event History](#)

-- Select a command -- [GO](#)

Set State to 'Unknown - Alert'

Set State to 'Known - Internal'

Set State to 'Acknowledged - External'

1 AP Containment

2 AP Containment

3 AP Containment

4 AP Containment

[Location History](#)

223319

Rogue Clients

Rogue clients are clients associated to rogue access points. Rogue clients are displayed on the WCS location floor maps using a black rectangle icon with a skull-and-crossbones, as shown in Figure 3-24. To display rogue clients on the WCS location floor map, ensure that the **Rogue Clients** checkbox option is enabled from the **Layers** dropdown selector at the top of the floor map display, and click **Load** in the left-hand column. To avoid excessive clutter, WCS will display the first 250 rogue clients on the floor map. To view the location of rogue clients beyond the first 250, rogue client filtering must be used.

Figure 3-24 Rogue Client Location Map



It is possible to filter the location information displayed by WCS based on the age of the information. In Figure 3-24 WCS displays location appliance information that has aged up to 15 minutes. Alternatively this value could be set to 2 or 5 minutes for more recent location information or ½, 1, 3, 6, 12 or 24 hours for older information.

By clicking on the blue chevron ▶ that is displayed to the right of the **Rogue Clients** checkbox, rogue client filtering options can be specified and additional information can be displayed, such as:

- The total number of rogue clients detected on this floor.
- Small icons (shown above) or standard sized icons can be selected. When using small icons, no text is displayed on the floor map for the rogue client except when a mouse-over is performed. When using standard size icons, an on-screen tag displays the rogue client's MAC address.
- Either all rogue clients can be displayed or filtering can be performed to select which rogue clients to display on the floor map. Filtering can be based on the MAC address of rogue access point to which it is believed the rogue client is associated or it can be based on the state of the rogue client (alert, contained or threat). As mentioned previously, only up to 250 rogue clients will be shown at any one time on floor maps. If there are greater than 250 rogue clients detected, the total number

found will be indicated in the left hand column status area during each communication cycle between WCS and the location appliance. It is recommended that filtering be used to reduce the total number of rogue clients selected for display if you receive this warning.

In software Release 4.1 of the Cisco UWN, WLAN controllers provide support for the maximum number of rogue clients shown in [Figure 3-24](#).

Table 3-4 Maximum WLC Rogue Client Capacity

Controller Model	Rogue Clients
2006	100
2106	100
4402	500
4404	500
WiSM	1000
NM-WLC6	100
NME-WLC8/12	100
3750G	500

Complete information on any displayed rogue client can be obtained simply by left-clicking the cursor on the rectangular black skull-and-crossbones icon representing the desired rogue client on the floor map. This yields the screen shown in [Figure 3-25](#). However, RSSI information is not displayed for rogue access points when the location map is enlarged.

Using the dropdown menu located in the upper right-hand corner, you can access location history and playback information for the rogue client that is similar in format and function to that described previously for WLAN clients, active RFID tags and rogue access points.

Figure 3-25 Rogue Client Detailed Information

Wireless Control System

Rogue Client "00:16:6f:1b:4b:dc"

Client MAC Address	00:16:6f:1b:4b:dc
Number of detecting APs	2
First Heard	Fri Aug 17 01:44:47 2007
Last Heard	Fri Aug 17 01:53:13 2007
Rogue AP MAC Address	00:14:1b:b6:ed:c0
Status	Alert

-- Select a command -- GO

- Select a command --
- Set State to 'Unknown-Alert'
-
- 1 AP Containment
- 2 AP Containment
- 3 AP Containment
- 4 AP Containment
-
- Map (High Resolution)
-
- Location History

Location

Floor	Cisco SJ - Site 5>BLD 14>3rd floor
Last located at	Aug 16, 2007 6:59:07 PM
On Location Server	loc-2-2

Location Notifications

Absence	0
Containment	0
Distance	0
All	0

Enlarge

It is important to understand how localization of rogue access points and clients differs from that of WLAN clients and asset tags. Recall from prior discussion that WLAN clients transmit probe requests periodically across multiple channels. Because infrastructure access points are spending the vast majority of their time on their assigned channels, these probe requests tend to be detected quickly and relayed to the controllers to which the access points are registered. Asset tags do not transmit probe requests but rather multicast tag messages on the channels for which the tags have been configured. These multicasts are quickly detected by infrastructure access points operating on these channels in the vicinity of the asset tags.

Rogue devices may not be operating on the same channels to which your infrastructure access points have been assigned. Because of this, these rogue devices may be detected during periodic off-channel scans conducted by infrastructure access points. For an LWAPP access point operating in local mode, this off-channel scans typically occur for about 500 milliseconds out of every 180 seconds of operation (or about 50 milliseconds per non-primary channel per 180 second interval).

Workgroup Bridges

Some Cisco autonomous access points can connect to the Cisco UWN in a special mode of operation known as workgroup bridge (WGB) mode. Access points configured as workgroup bridges can provide wireless connectivity to the Cisco UWN for groups of wired clients, making the wired clients essentially appear as wireless clients to the UWN. Cisco AP1121, AP1130, AP1231, AP1240, and AP1310 access points containing Cisco IOS Release 12.4(3g)JA or greater (on 32-MB access points) or Cisco IOS Release 12.3(8)JEB or greater (on 16-MB access points) can be configured for workgroup bridge mode.



Note

For further information about the configuration of workgroup bridges and their role in the Cisco UWN, refer to *The Workgroup Bridge in a Lightweight Environment* located at the following URL: http://cisco.com/en/US/docs/wireless/access_point/12.4_3g_JA/configuration/guide/s43hot.html#wp1059452.

The default roaming behavior for workgroup bridges is to delay active scanning for potential access point roam candidates until the WGB has lost its association. While such behavior may be perfectly acceptable when workgroup bridges are used in stationary applications, it can cause concern in mobile WGB applications (such as a mobile cart-based array of Ethernet-only medical equipment) because of the following:

- Delaying the search for potential access point roam candidates until association is lost can introduce unnecessary application delays, which may negatively the performance of mobile timing-sensitive applications and cause application lockups or time-outs.
- Depending on the environment, mobile workgroup bridges may move about for considerable distances while associated to the same access point. In this case, the default WGB behavior will result in an absence of probe requests, causing the location appliance to rely on stale probe request RSSI information and potentially leading to poor WGB location fidelity until the WGB is faced with a roaming event.

Access points configured in WGB mode do not respond to broadcast Radio Measurement Requests that are sent as a result of the Cisco Compatible Extensions Location Measurement parameter being enabled. Therefore, Cisco Compatible Extensions Location Measurement cannot be used as a mechanism with which to trigger consistent periodic probing in work group bridges.

The Cisco IOS CLI **mobile station** command can be used on the workgroup bridge to provide a significant degree of improvement in workgroup bridge location fidelity. When you enable this setting in the workgroup bridge, it causes it to perform an active scan when it detects low access point RSSI,

excessive radio interference, or a high percentage of frame loss. The workgroup bridge will use the information it learns from the active scan to determine whether any access points offering better service are available to it, and will roam to a new access point before it loses its current association.

The basic format of the command is:

mobile station period <seconds> **threshold** <dBm>

where the value for **period** denotes how often the workgroup bridge checks the RSSI of its currently associated access point, and the value for **threshold** specifies the absolute value of the minimum acceptable access point RSSI in dBm. The default values are 20 seconds and 70 dBm respectively.

**Note**

Complete details regarding the configuration of the Cisco IOS **mobile station** command can be found in *Cisco IOS 12.4(3g)JA for Access Points and Bridges, “mobile station” command reference page* located at the following URL:

http://cisco.com/en/US/docs/wireless/access_point/12.4_3g_JA/command/reference/cr43main.html#wp2593116

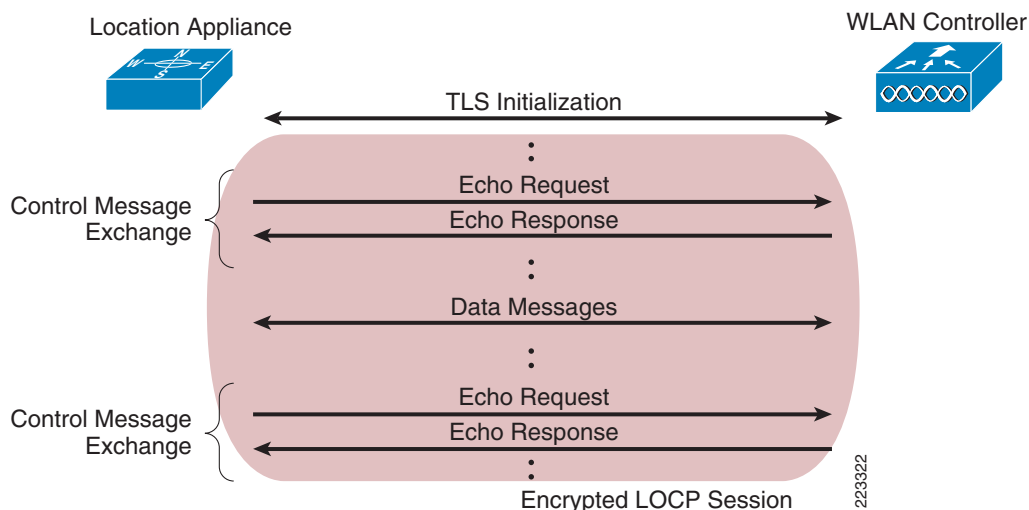
The values for period and threshold should be adjusted for your specific environment in order to balance the need for consistent and regular probe requests against the possibility of excessive roaming.

Decreasing the threshold value to a very low value, causing an active scan to always occur at each period interval, for example, will typically improve the location fidelity of work group bridges that seldom roam significantly. The trade-off with doing this however, is that such settings may also increase the frequency with which the workgroup bridge roams. However, this trade-off is generally viewed as equitable since in properly deployed environments with good coverage and access point placement, the increase in WGB roaming should be negligible whereas the improvement in mobile workgroup bridge location fidelity in cases where there is seldom roaming between access points can be very significant

Cisco Location Control Protocol (LOCP)

Cisco Unified Wireless Network (CUWN) software Release 4.1 introduces the Cisco Location Control Protocol (LOCP), an architectural enhancement that improves communication efficiency and supports new capabilities between the location appliances and one or more WLAN controllers. LOCP is a bi-directional protocol that can be run over a connection-oriented or connectionless transport. LOCP provides for an ongoing exchange of control messages that allows either endpoint to determine if its partner is still active.

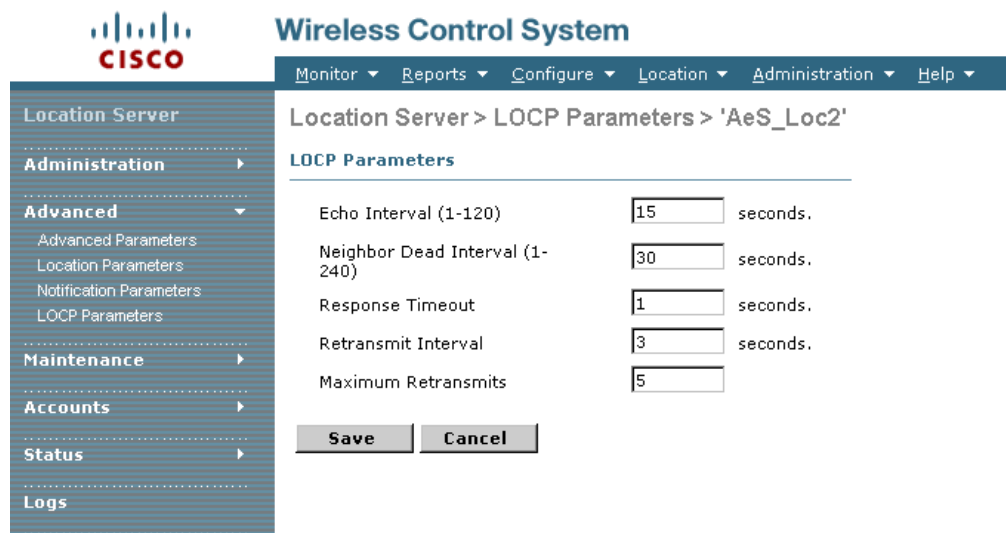
Figure 3-26 illustrates the basic LOCP packet flow between the location appliance and each WLAN controller.

Figure 3-26 Location Appliance WLAN Controller LOCP Session

In Release 4.1 the location appliance is pre-configured by the user with regard to the IP addresses of the controllers it is to communicate with. Once the connection between the controller and the location appliance is initialized, an encrypted TLS session is established between the two endpoints over which all further LOCP traffic will travel. Each endpoint periodically verifies that its partner is active and ready to accept requests by participating in Echo Request/Response control message exchange, as shown in Figure 3-26.

If a location appliance detects that a WLC is no longer responding, it will temporarily disable any other requests to that WLC until the WLC becomes active again. The connection between the location appliance and the WLC can be maintained for multiple exchanges (the typical case) or can be initiated and disconnected for each data request.

The basic parameters controlling the LOCP session between the location appliance and the WLAN controllers defined to it are specified using the Location Servers > LOCP Parameters panel, as shown in Figure 3-27.

Figure 3-27 Setting LOCP Session Parameters

The meaning of the LOCP session parameters shown in [Figure 3-27](#) are as follows:

- *Echo Interval*—The minimum time interval, in seconds, between echo requests sent from the location appliance to the WLAN controller. Valid values are 1 to 120 seconds, with the default value being 15 seconds.
- *Neighbor Dead Interval*—The minimum time interval, in seconds, that the location appliance will wait before marking a WLAN controller not responding to its Echo Requests as “dead”. This value should not be less than twice the Echo Interval. Recommended values are 2 to 240 seconds, with the default value being 30 seconds.
- *Response Timeout*—The maximum time interval, in seconds, within which the WLAN controller must respond to requests sent by the location appliance. Valid values are 1 to 99,999 seconds, with the default value being 1 second.
- *Retransmit Interval*—The minimum time interval, in seconds, the location appliance waits before retransmitting a LOCP request when it does not get a response back from the WLAN controller. Valid values are 1 to 99,999 seconds, with the default value being 3 seconds.
- *Maximum Retransmits*—The maximum number of retransmissions that will be attempted by the location appliance when a response is not received for a LOCP Request. Valid values are 1 to 99,999 attempts, with the default value being 5 attempts.

Note that the first two parameters are applicable only to Echo Request and Echo Reply control messages while the remaining parameters pertain to all data messages (such as Information and Measurement Requests and Responses).

Cisco Unified Wireless Network software Release 4.1 introduces the initial phase of LOCP. In this release, LOCP is used to augment traditional SNMP polling by transporting Cisco Compatible Tag Extensions for Wi-Fi tags telemetry and notification traffic from WLAN controllers to the location appliance. This traffic includes:

- Cisco Compatible Extensions for Wi-Fi tag telemetry, such as:
 - Motion, temperature, pressure, humidity, distance, quantity and status.
 - Battery state and predicted remaining life.
- High priority Cisco Compatible Extensions tag traffic, such as:
 - Call button, tag detached and tamper alert events.
 - Entry into the range of a chokepoint trigger.
 - Vendor-specific tag information used by third party location clients.

**Note**

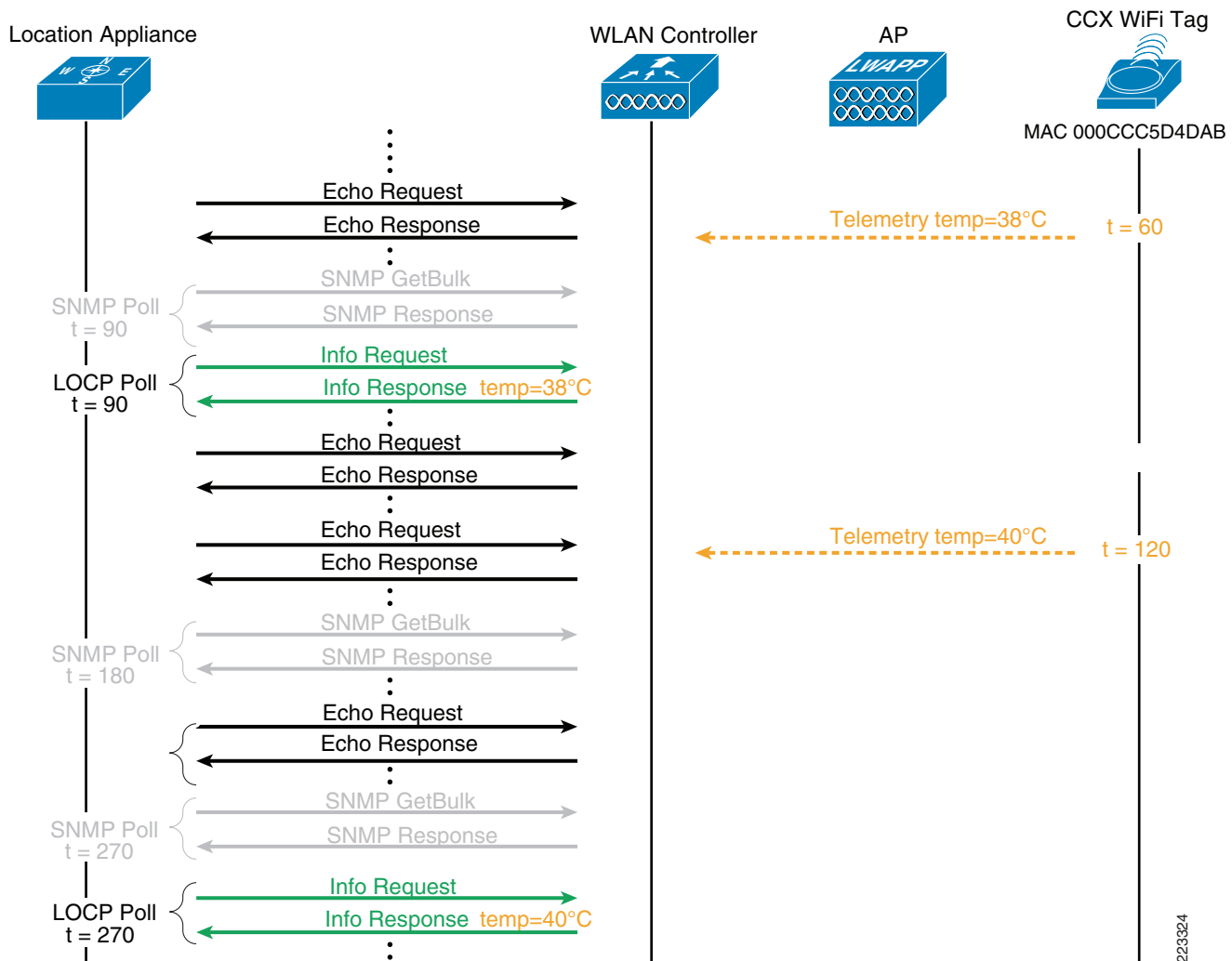
Commencing with software Release 4.2, the Location Control Protocol (LOCP) receives additional enhancements and evolves into the Network Mobility Services Protocol (NMSP).

Asset Tag Telemetry Using LOCP

Beginning with Cisco UWN software Release 4.1, Wi-Fi RFID tags compliant with the Cisco Compatible Extensions for Wi-Fi Tags specification may optionally pass tag telemetry information to the location-aware Cisco UWN as part of their tag message payload. This telemetry information is received by access points and collected by WLAN controllers. The location appliance periodically polls the WLAN controllers for tag telemetry using LOCP Information Requests. The controller will respond with the telemetry information it has received for each tag MAC address since the last LOCP polling

cycle via a LOCP Information Response frame. These frames (as well as the polling exchange process) are illustrated in Figure 3-28. Keep in mind that all frames shown between the location appliance and the WLAN controller travel are encrypted.

Figure 3-28 LOCP Information Request Polling



As you may have noticed in Figure 3-27, the LOCP polling interval is not directly configured in the location appliance configuration. Rather, it is derived from the asset tag SNMP polling interval occurring between the location appliance and WLAN controllers. In order to determine when a LOCP poll should be sent, the location appliance evaluates the following conditions during each controller polling cycle:

- Whether the controller software release supports LOCP. LOCP polls will not be sent to controllers that are not LOCP-capable.
- If the time interval since the last LOCP poll is 180 seconds, then LOCP polling will be performed during this asset tag SNMP polling cycle. LOCP Information Requests will be sent to all LOCP-capable controllers currently defined to the location appliance.
- If the interval since the last LOCP poll < 180 seconds, then LOCP polling will not be performed during this asset tag SNMP polling cycle.

The LOCP polling interval used by a location appliance to collect asset tag telemetry information in software Release 4.1 can be calculated from the asset tag SNMP polling interval using the following formula¹:

$$Poll_{NMSP} = \left\lceil \frac{180}{Poll_{TAG}} \right\rceil * Poll_{TAG}$$

$Poll_{LOCP}$ represents the LOCP polling interval and $Poll_{TAG}$ specifies the poll interval at which the location appliance polls the controller for asset tag location information via SNMP. Both of these values are specified in seconds. The value for $Poll_{TAG}$ is configured in WCS using Location Servers > Polling Parameters. For example, using an asset tag SNMP polling interval ($Poll_{TAG}$) of 120 seconds, the LOCP polling interval ($Poll_{LOCP}$) used by the location appliance is calculated to be 240 seconds.

Figure 3-28 helps to provide clarity to understanding the relationship between LOCP and SNMP polls and their impact on the receipt of tag telemetry. We see that temperature telemetry is transmitted from a Cisco Compatible Extensions for Wi-Fi Tags compatible tag with MAC address 00:0C:CC:5D:4D:AB at time $t=60$ seconds. This transmission is received by one or more access points. These access points pass the telemetry information (temperature of 38°C in our example) to their respective registered WLAN controllers. Since Figure 3-28 shows that the SNMP poll occurring at time $t=90$ seconds is the very first poll (which also implies that no previous LOCP polls have occurred), the controller will receive a LOCP poll at time $t=90$ seconds as well. This is indicated in the figure by the receipt of the Information Request frame. The controller responds to the poll by passing any accumulated tag telemetry information to the location appliance in a LOCP Information Response frame.

If tags are configured to send multiple frame copies (or bursts) per channel, the controller eliminates any duplicate tag telemetry and passes the distilled telemetry values to the location appliance. The location appliance then updates its databases with this telemetry information and makes it available to location clients via the SOAP/XML API.

Subsequent inbound telemetry is handled in an analogous fashion. For example, in Figure 3-28 at time $t=120$ seconds we see an inbound temperature telemetry update indicating that the temperature has increased to 40 °C. The aforementioned cycle of events would reoccur, culminating in the telemetry update being transmitted to the location appliance at time $t=270$ seconds. It is important to understand why the tag telemetry is passed to the location appliance at time $t=270$ seconds and not at time $t=180$ seconds, which is where we observe an SNMP poll occurring. As explained earlier, LOCP polling only occurs if the time delta since the last LOCP poll is 180 seconds or more. At time $t=180$ seconds, the time delta since the previous LOCP poll is only 90 seconds, thus no LOCP poll occurs at that time.

While Figure 3-28 illustrates the simple case of a single tag passing only a single telemetry value, it should be noted that LOCP is designed to efficiently transport telemetry values from multiple tags just as easily. Each Information Response frame allows multiple tag MAC addresses to be specified by the controller, with each MAC address being associated with one or more telemetry values. For example, instead of passing only temperature telemetry, the tag shown in Figure 3-28 could include temperature, pressure, humidity and so on. All of this information would be included in the Information Response transmitted at the next LOCP poll. Inbound telemetry traffic from multiple tags would be aggregated by the controller in a similar fashion, with each LOCP endpoint capable of performing LOCP frame fragmentation and reassembly if necessary.

With the exception of battery state information which can be “pushed” via asynchronous northbound notifications from the location appliance, tag telemetry is made available to location clients only via the SOAP/XML API.

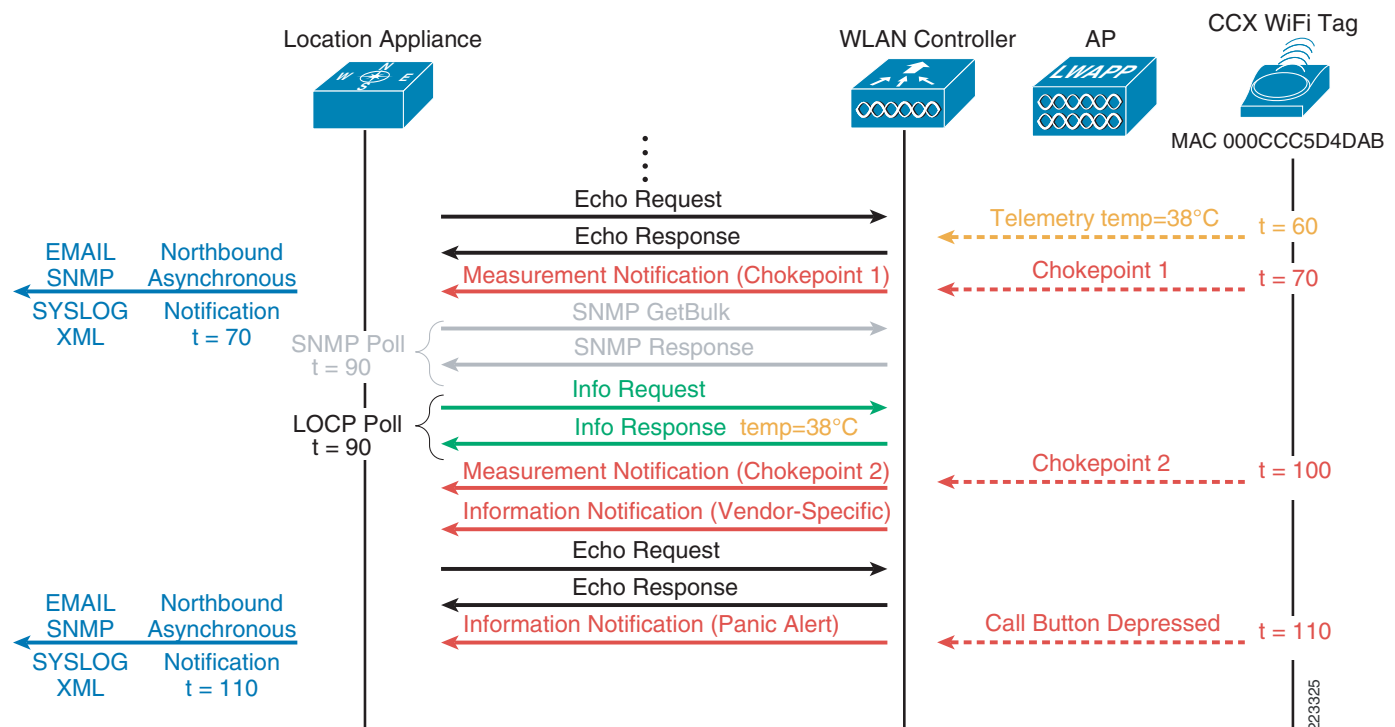
1. $\lceil x \rceil$ represents the application of the ceiling function to the positive integer x . This rounds up x upwards, returning the smallest integer that is greater than or equal to x .

For information regarding tag telemetry deployment considerations, refer to [Tag Telemetry and Notification Considerations](#), page 6-27.

Asset Tag Notifications Using LOCP

Beginning with Cisco UWN software Release 4.1, Wi-Fi active RFID tags compliant with the Cisco Compatible Extensions Wi-Fi tag specification can pass optional high priority, chokepoint and vendor-specific notification events to the location-aware Cisco UWN. Indication of high-priority tag events are received by one or more access points via tag multicast messages frames that contain additional payload information indicating the nature of the event. This information is typically dispatched by asset tags at the time the tag detects that the event has occurred. Once received by the WLAN controller, these time-critical events are handled outside the polled LOCP polling process and passed immediately to the location appliance using a LOCP Notification frame, as shown in [Figure 3-29](#).

Figure 3-29 LOCP Notifications



[Figure 3-29](#) shows the two basic types of LOCP notifications supported in Cisco UWN software Release 4.1, the *Measurement Notification* and the *Information Notification*:

- Measurement Notifications**—In Release 4.1, measurement notifications are used to convey information regarding the identity of any chokepoint proximity devices into whose range a tag may have entered. Tags compliant with the Cisco Compatible Extensions for Wi-Fi Tags specification include chokepoint identification in the tag content field (such as the chokepoint MAC address). This information is passed to the location appliance along with the tag MAC address in real time, and can be used by location clients (such as WCS) to indicate that a tag is now within range (or out of range) of a particular chokepoint.

- *Information Notifications*—In Release 4.1, information notifications are used to convey vendor-specific data and tag high-priority events, such as:
 - When a tag user depresses a tag call button
 - When a tag detects that it has been removed from its carrier or attached asset
 - When a tag detects tampering.
 - When any other high-priority tag events occur.

While each tag vendor is responsible for determining the precise set of capabilities they choose to include in their product offering, the Cisco Compatible Extensions for Wi-Fi Tags specification provides for high-priority information to be uniformly included in the tag content field. This information is passed to the location appliance along with the tag MAC address, and can be used by location clients (such as WCS) to indicate that a high-priority tag event has taken place.

The Cisco Compatible Extensions for Wi-Fi Tags specification allows each tag vendor to pass vendor-specific information (such as proprietary tag messages or additional vendor-specific chokepoint information) from their tags into the Cisco UWN in real time. Vendor-specific information will be made available unaltered to location clients via the SOAP/XML API interface of the Cisco location appliance. Vendor-specific information that is sent within a high-priority event can also be “pushed” to location clients from the location appliance via an asynchronous northbound notification from the location appliance to location clients using SMTP, UDP-Syslog, SNMP traps or SOAP transports. Location clients must be capable of receiving and processing these notifications on the aforementioned ports in order to provide real-time notification of such events to end users.

Figure 3-29 clearly indicates that unlike tag telemetry, there is no dependency on any polling mechanism between the location appliance and the WLAN controller. LOCP notifications will be generated from the WLAN controller to the location appliance as tags communicate those events. High-priority tag events, vendor specific data and chokepoint in-range information are not aggregated by WLAN controllers in Release 4.1 of the Cisco UWN. Each incoming tag multicast message bearing such information, received by a WLAN controller from each registered access point, results in the generation of an information notification or a measurement notification frame from the WLAN controller to the location appliance.

No dependency exists between the transmission of tag telemetry and the transmission of chokepoint, high-priority or vendor specific information. For example, a tag may be relaying telemetry information about an asset as it traverses through the range of chokepoints in an environment. As seen in Figure 3-29, the tag telemetry is retained by the WLAN controller until the next LOCP polling interval, whereas indication of chokepoints that are in-range is sent immediately by the WLAN controller to the location appliance in the form of a measurement notification.

In addition to providing updated information to clients via the SOAP/XMP API (for example, when a location client issues a XML GetTagInfo or GetTagLocation request), the location appliance can also dispatch external asynchronous northbound notifications upon receipt of LOCP measurement or information notifications (refer once again to Figure 3-29). These external northbound notifications are sent for the following conditions using SNMP, SMTP, SOAP or UDP-Syslog transports:

- Call Button, Tag Tampering, or Tag Detached
- Chokepoint in-range
- Other Priority Events (user defined)

For information regarding deployment considerations surrounding tag notifications, refer to [Tag Telemetry and Notification Considerations, page 6-27](#).

