



CHAPTER 1

Overview

This chapter describes the role of the Cisco 3300 Series Mobility Services Engine (MSE), a component of the Cisco Context-Aware Mobility (CAM) Solution, within the overall Cisco Unified Wireless Network (CUWN).

Additionally, Context-Aware Software (CAS), a service supported on the mobility services engine and a component of the Context-Aware Mobility Solution, is addressed.

This chapter contains the following sections:

- [Cisco Context-Aware Mobility Solution Overview, page 1-2](#)
- [Viewing Contextual Information, page 1-3](#)
- [Event Notification, page 1-4](#)
- [Configuration and Administration, page 1-4](#)
- [Mobility Services Engine Synchronization, page 1-6](#)
- [Context-Aware Planning and Verification, page 1-6](#)
- [Monitoring Capability, page 1-6](#)
- [Maintenance Operations, page 1-6](#)
- [System Compatibility, page 1-7](#)

Cisco Context-Aware Mobility Solution Overview

The foundation of the Cisco Context-Aware Mobility Solution is the controller-based architecture of the CUWN. The CUWN includes the following primary components: access points, wireless LAN controllers, the Cisco Wireless Control System (WCS) management application, and the Cisco 3300 Series Mobility Services Engine.

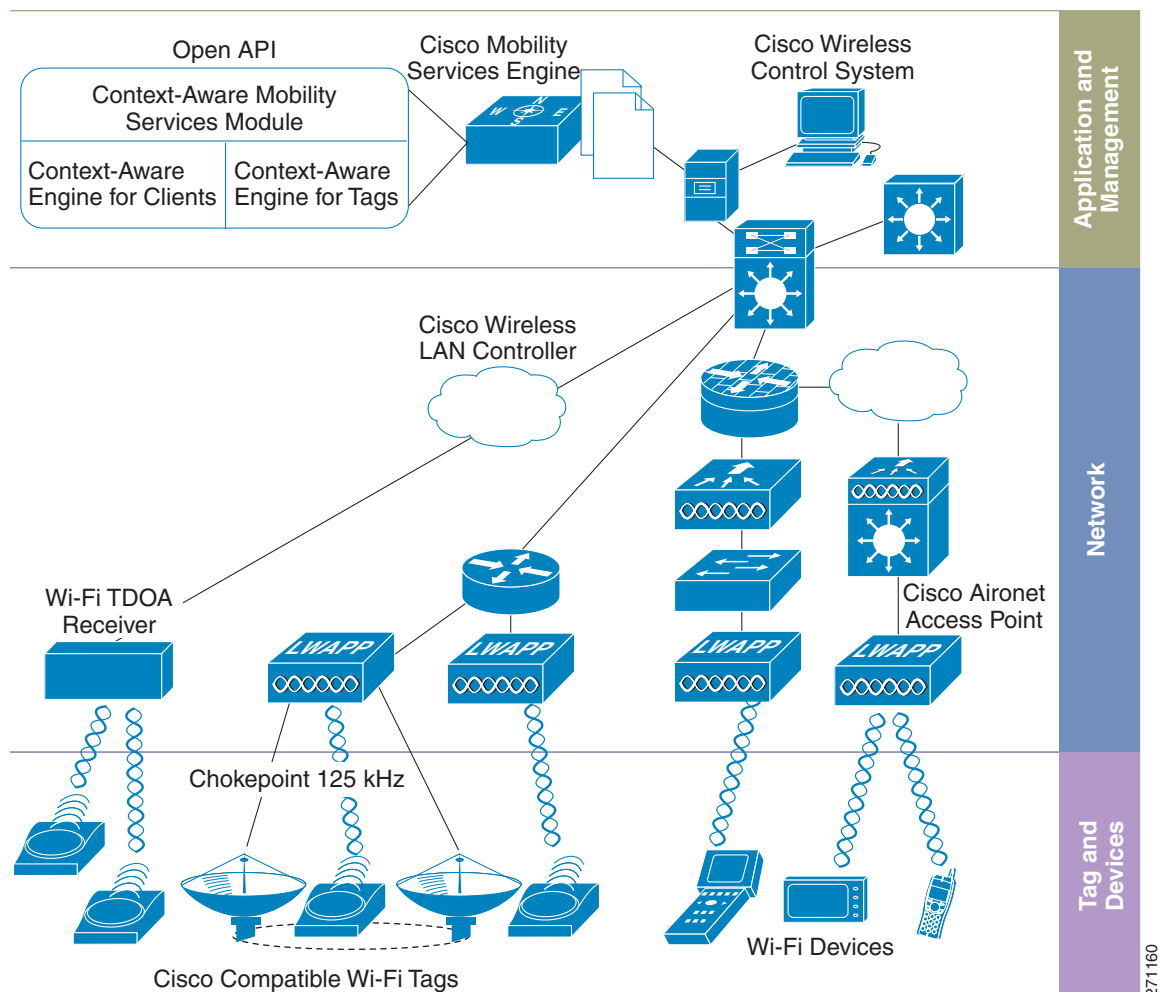
Cisco 3300 Series Mobility Services Engines

The Cisco 3300 Series Mobility Services Engine operates with CAS, which is a component of the Cisco Context-Aware Mobility Solution (see [Figure 1-1](#)).

There are two models of the mobility services engine:

- Cisco 3350 Mobility Services Engine
- Cisco 3310 Mobility Services Engine

Figure 1-1 Context-Aware Mobility Solution



271160

CAS

CAS allows a mobility services engine to simultaneously track thousands of mobile assets and clients by retrieving contextual information such as location, temperature, and availability from Cisco access points.

CAS relies on two engines for processing the contextual information it receives. The *Context-Aware Engine for Clients* processes data received from Wi-Fi clients and the *Context-Aware Engine for Tags* processes data received from Wi-Fi tags; these engines can be deployed together or separately depending on the business need.

Licensing for Clients and Tags

You must purchase licenses from Cisco to retrieve contextual information on tags and clients from access points.

- Licenses for tags and clients are offered separately. (The clients license also includes tracking of rogue clients, rogue access points and wired clients).
- For more information on tags, clients, rogue clients, and rogue access points, refer to Chapter 7, “Context-Aware Planning and Verification.”
- Licenses for tags and clients are offered in various quantities, ranging from 1,000 to 12,000 units. Up to 18,000 Wi-Fi clients and Wi-Fi tags (combined count) are supported depending on the mobility services engine hardware.
 - Cisco 3350 mobility services engine supports up to 18,000 clients and tags (combined count).
 - Cisco 3310 mobility services engine supports up to 2,000 clients and tags (combined count).
- For details on tag and client licenses, refer to the *Cisco 3300 Series Mobility Services Engine Release Note, Release 6.0* at:
http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html
- For details on adding client and tag licenses to the mobility services engine, refer to Chapter 2.

Viewing Contextual Information

The collected contextual information can be viewed in GUI format in the Cisco WCS, the centralized WLAN management platform.

**Note**

However, before you can use Cisco WCS, initial configuration for the mobility services engine is required using a command-line (CLI) console session. Refer to *Cisco 3350 Mobility Services Engine Getting Started Guide* and the *Cisco 3100 Mobility Services Engine Getting Started Guide* at the following link: http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html.

After its installation and initial configuration are complete, the mobility services engine can communicate with multiple Cisco wireless LAN controllers to collect operator-defined contextual information. You can then use the associated Cisco WCS to communicate with each mobility services engine to transfer and display selected data.

You can configure the mobility services engine to collect data for clients, rogue access points, rogue clients, mobile stations, and active RFID asset tags.

Event Notification

A mobility services engine sends event notifications to registered listeners over the following transport mechanisms:

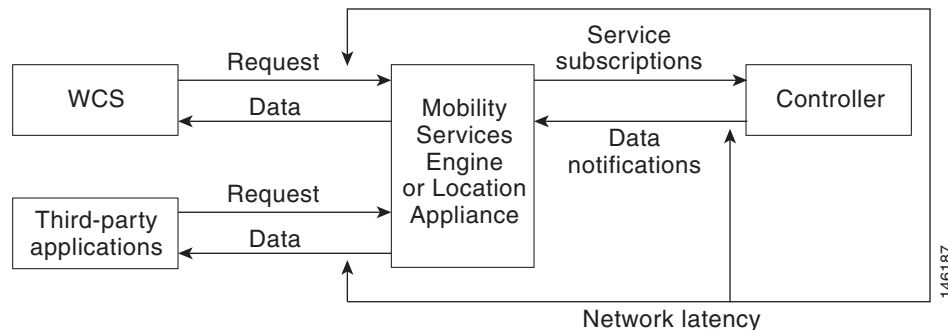
- Simple Object Access Protocol (SOAP)
- Simple Mail Transfer Protocol (SMTP) mail
- Simple Network Management Protocol (SNMP)
- SysLog



Note

Cisco WCS can act as a listener receiving event notifications over SNMP. Without event notification, Cisco WCS and third-party applications need to periodically request location information from location-based services see (see [Figure 1-2](#)).

Figure 1-2 Pull Communication Model



The pull communication model, however, is not suitable for applications that require more real-time updates to location information. For these applications, you can configure the mobility services engine push event notifications when certain conditions are met by the registered listeners.

Configuration and Administration

You can use Cisco WCS to perform different configuration and administrative tasks, including adding and removing a mobility services engine, configuring mobility services engine properties and managing users and groups as summarized below.

Adding and Deleting a Mobility Services Engine

You can use Cisco WCS to add and delete a mobility services engine within the network. You can also define the service supported on the mobility services engine. Refer to [Chapter 2, “Adding and Deleting Systems,”](#) for configuration details.

Editing Mobility Services Engine Properties

You can use Cisco WCS to configure the following parameters on the mobility services engine. Refer to the [Chapter 4, “Configuring and Viewing System Properties,”](#) for configuration details.

- **General Properties:** Enables you to assign a contact name, username, password, and HTTP for the mobility services engine.
- **NMSP Parameters:** Enables you to modify Network Mobility Services Protocol (NMSP) parameters such as echo and neighbor dead intervals as well as response and retransmit periods. NMSP is the protocol that manages communication between the mobility services engine and the controller or a location-capable Catalyst switch. Transport of telemetry, emergency, and chokepoint information between the mobility services engine and the controller is managed by this protocol.
- **Active Sessions:** Enables you to view active user sessions on the mobility services engine.
- **Trap Destinations:** Enables you to specify which Cisco WCS or Cisco Security Monitoring, Analysis and Response System (CS-MARS) network management platform is the recipient of SNMP traps generated by the mobility services engine.
- **Advanced Parameters:** Enables you to set the number of days events are kept, set session time out values, set an absent data interval cleanup interval, and enable or disable Advanced Debug.

Editing CAS Properties

You can use Cisco WCS to configure the following parameters for CAS. Refer to [Chapter 7, “Context-Aware Planning and Verification,”](#) for configuration details.

Location of an element (client, tag, rogue client or rogue access point) is one of the components that is retrieved from access points by the Context-Aware Software (CAS) installed on a mobility services engine. CAS also retrieves contextual information such as temperature and asset availability about a client or tagged asset from access points.



Note

Context-Aware Software incorporates and expands the function of Cisco location-based services software.

- **Tracking Parameters:** Enables you to define the mobile assets (such as client stations, active asset tags; and rogue clients and access points) that you want to actively track, set limits on how many of a specific mobile asset you want to track, and disable tracking and reporting of ad hoc rogue clients and access points.
- **Filtering Parameters:** Enables you to define filters to exclude probing clients as well as tags and non-probing clients based on their MAC addresses.
 - Probing clients are clients that are associated to another controller but whose probing activity causes them to be seen by another controller and counted as a client by the *probed* controller as well as its *primary* controller.
- **History Parameters:** Enables you to specify how often the mobility services engine collects historical data on client station, rogue access point, and asset tags from controllers to manage the amount of data stored on the mobility services engine hard drive.
- **Presence Parameters:** Enables you to enable location presence on a mobility services engine to provide expanded Civic (city, state, postal code, country) and GEO (longitude, latitude) location information beyond the Cisco default setting (campus, building, floor, and X, Y coordinates). This information can then be requested by clients on a demand basis for use by location-based services and applications.
- **Import and Export Asset Information:** Enables you to import a file of formatted asset information from an external server and to export asset information to an external server.
- **Import Civic Information:** Enables you to import a file with civic information for use by the presence parameter for expanded location information.

- **Location Parameters:** Enables you to specify whether the mobility services engine retains its calculation times and how soon the mobility services engine deletes its collected RSSI measurement times. It also enables you to apply varying smoothing rates to manage location movement of an element.
- **Notification Parameters:** Enables you to define how often notifications are generated or resent by the mobility services engine. You can also enable forwarding of northbound notifications for tags to third-party applications.

Managing Users and Groups

You can use Cisco WCS to add, delete, and edit user session and user group parameters as well as add and delete host access records. Refer to [Chapter 5, “Managing Users and Groups,”](#) for configuration details.

Mobility Services Engine Synchronization

Cisco WCS pushes network designs (logical maps of elements), controllers and event definitions to the mobility services engine to maintain accurate location information between the mobility services engine and controller. Cisco WCS provides you with two ways to synchronize: manual and automatic (auto-sync). Refer to [Chapter 3, “Synchronizing Mobility Services Engines,”](#) for specifics.

Context-Aware Planning and Verification

To plan and optimize access point deployment, you can use Cisco WCS to calibrate linear or data points. Additionally, you can analyze the location accuracy of non-rogue and rogue clients and asset tags on an area or floor map using the accuracy tool, and you can use chokepoints to enhance location accuracy for tags. Refer to [Chapter 7, “Context-Aware Planning and Verification,”](#) for specifics.

Monitoring Capability

You can use Cisco WCS to monitor alarms, events, and logs generated by mobility services engine. You can also monitor the status of mobility services engines, clients, and tagged assets. Additionally, you can generate a utilization report for the mobility services engine to determine CPU and memory utilization as well as counts for clients, tags and rogue access points and clients. Refer to Chapter 8, [Chapter 8, “Monitoring the System and Services,”](#) for specifics.

Maintenance Operations

You can back up mobility services engine data to a predefined FTP folder on Cisco WCS at defined intervals, and restore the mobility services engine data from that Cisco WCS. Other mobility services engine maintenance operations that you can perform include: downloading new software images to all associated mobility services engines from any Cisco WCS station, defragmenting the mobility services engine database, restarting a mobility services engine, shutting down a mobility services engine and clearing mobility services engine configurations. Refer to [Chapter 9, “Performing Maintenance Operations,”](#) for specifics.

**Note**

Details on recovering GRUB and root passwords for the mobility services engine using the command-line interface (rather than Cisco WCS) is also addressed in Chapter 9.

System Compatibility

**Note**

Refer to the *Cisco 3300 Mobility Services Engine Release Note* for the latest system (controller, WCS, mobility services engine) compatibility information, feature support, and operational notes for your current release at:

http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html

