Cisco Mobility Services Engine

Introduction

This chapter provides configuration and deployment guidelines if you want add the Cisco Mobility Services Engine (MSE) and run Context Aware Services in a Cisco Unified Wireless Network. The purpose of this chapter is to:

- Explain the various elements and framework of the Cisco Mobility Solution
- Provide general deployment guidelines

Note This chapter does not provide configuration details for the MSE and associated components. This information is provided in other documents. See Related Information for a list of documents about the configuration and design of Context Aware Mobility Services. Adaptive wIPS configuration is also not covered in this design guide.

Background Information

The Cisco MSE provides the ability to track the physical location of Network Devices, both wired and wireless, using wireless LAN controllers (WLCs) and Cisco Aironet CAPWAP APs. This solution allows you to track any Wi-Fi device, including clients, active RFID tags, and rogue clients and APs. It was designed with the following requirements:

- Manageability—Cisco Prime Infrastructure is used to administer and monitor the MSE. Moreover, the MSE integrates directly into the wireless LAN architecture, which provides one unified network to manage instead of multiple disparate wireless networks.
- Scalability—The Cisco MSE series can simultaneously track 25,000 elements in CAS and 5,000 APs in wIPS. The CPI can manage multiple Mobility Services Engines for greater scalability. The wireless LAN controller (WLC), CPI, and MSE are implemented through separate devices to deliver greater scalability and performance.
- Security—The WLC, CPI, and MSE provide robust secure interfaces and secure protocols to access data. The MSE records historical location information that can be used for audit trails and regulatory compliance.
- Open and standards based—The MSE has a SOAP/XML API that can be accessed by external systems and applications that can leverage location information from the MSE.

- Easy deployment of business applications—The MSE can be integrated with new business applications such as asset tracking, inventory management, location-based security, or automated workflow management.

Overview

Context Aware Service (CAS) provides the capability for a Wi-Fi 802.11a/b/g/n network to determine the location of a person or object with an active Wi-Fi device, such as a wireless client or active RFID tag and/or associated data that can be passed by the end point through the wireless infrastructure to an upstream client. When a Cisco MSE is added to a Cisco Unified Wireless Network with an appropriately licensed version of CPI, it assumes responsibility for several important tasks:

- Execution of positioning algorithms
- Maintenance of calibration information
- Trigger and dispatch of location notifications
- Process of statistics and historical location
- Depository for geographical information, maps, and all wireless devices

Cisco Prime Infrastructure is the management system that interfaces with the MSE and serves as the user interface (UI) for the services that the MSE provides. Although it is possible to access the MSE directly through SSH or a console session for maintenance and diagnostic purposes, all operator and user interaction with the MSE is typically performed through CPI (for management) or a third-party location client application.

Terminology

With the Cisco *Centralized WLAN Architecture* (functional architecture of Cisco Unified Wireless Networks) and Context Aware Location Services, administrators can determine the location of any 802.11-based device as well as the specific type or status of each device. Clients (associated, probing, and so forth), rogue APs, rogue clients, and active tags can all be identified and located by the system. This information is made available through the API within seconds of an event occurrence and can be retained by the MSE database for historical lookup and security audits.

Mobility Services Engine

MSE supports a suite of mobility services applications. Designed as an open platform, the MSE supports mobility services software in a modular fashion with various configuration options based on network topology and the types of services required. Cisco supports existent and future applications that include:

- Context Aware Services—These applications capture and integrate into business processes detailed contextual information about such things as location, temperature, availability, and applications used. Context Aware applications feature a wide range of location options that include real-time location, presence detection, chokepoint visibility, and telemetry. Support for enhanced received signal strength indication (RSSI) and Time Difference of Arrival (TDOA) technology delivers greater scale accuracy and performance for a broad range of environments.

  Context Aware software consists of two major components:

  - Context Aware Engine for Clients: RSSI, the Cisco location engine, is used to track Wi-Fi clients, rogue clients, rogue APs, and wired clients.

  - Context Aware Engine for Tags: The partner (AeroScout) location engine (both RSSI and TDOA) is used to track Wi-Fi active RFID tag.

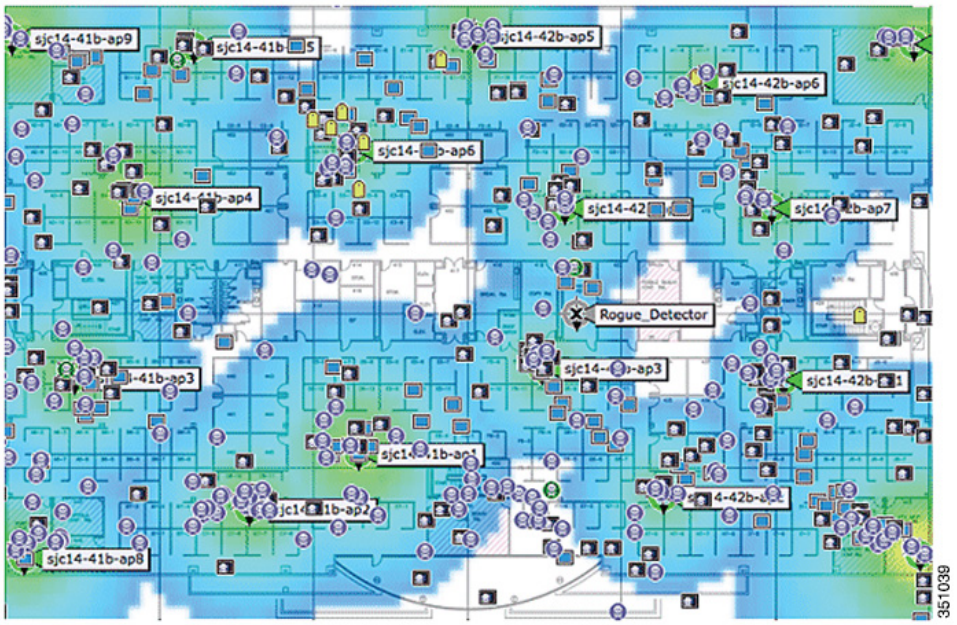
  Third-party software is supported through the MSE API.

- Adaptive Wireless Intrusion Prevention System (wIPS)—wIPS software provides visibility and comprehensive threat prevention for the mobility network through monitoring, alerts, classifying, and remediation of wireless and wired network vulnerabilities.
- Network Mobility Services Protocol—Cisco-defined protocol that is used for secure communication between the WLC and MSE.
- Cisco Prime Infrastructure—Wireless network management system developed and supported by Cisco Systems. Includes these capabilities:
  - WLAN configuration
  - WLAN performance monitoring
  - Reporting (real-time and historical)
  - Graphical view of network (wireless LAN controllers, APs, clients and tags)
- Wireless LAN Controller (WLC)—The centralized Cisco Unified Wireless Network architecture configuration and control device. This controller allows the entire WLAN to operate as an intelligent network that uses wireless as the access medium to support advanced services, unlike legacy 802.11 WLAN infrastructures that are built from autonomous, discrete APs. The Cisco Unified Wireless Network simplifies operational management by collapsing large numbers of managed endpoints—autonomous APs—into a single managed system comprised of one or more WLCs and their corresponding, joined APs.

  In the Cisco Unified Wireless Network architecture, APs are *lightweight*, which means that they cannot act independently of a WLC. APs are typically *zero-touch* deployed, and no individual configuration of APs is required. The APs learn the IP address of one or more WLCs through a controller discovery algorithm and then establish a trust relationship with a controller through a join process. Once the trust relationship is established, the WLC pushes firmware to the AP, if necessary, and a run-time configuration. APs do not store a configuration locally.
- Clients—All devices associated with controller-based, lightweight APs on a wireless network.
- Rogue Access Point—Any AP that is determined not to be part of the wireless LAN mobility group that detected it. This consists of all non-system APs within RF range of a lightweight APs, which includes those on the wired network or those on another wired network (such as an AP of a neighbor). Because all lightweight APs use a hash as part of the beacon frame with a special key, even spoofed infrastructure APs are identified as rogue APs rather than mistaken to be legitimate APs flagged in CPI as spoof APAPs.
- Rogue Clients—All devices that are associated to rogue APs.
- Active RFID Tags—Wi-Fi device that can be detected and located on a Wi-Fi network. There is wide variety of Wi-Fi compatible tags available in the market. Tags offer a range of features that include telemetry, such as motion and environmental data such as temperature and humidity, call buttons, indoor and outdoor operation, intrinsically safe versions, and flexible mounting options.

  The MSE provides the ability to track up to 25,000 devices (tags, clients, and rogue clients/APs). Figure 11-1 is an example of a floor map as shown in the CPI, and displays tags, clients, rogue clients and rogue APs. The floor map illustrates the scale and variety of classes of devices that can be tracked by the MSE. CPI provides the capability to define search parameters to display only in a subset of devices. For example, a biomedical user might want to see only infusion pumps and EKG machines named with friendly identifiers rather than rogue devices or devices with cryptic MAC or IP addresses.

Figure 11-1 CPI Floor Map with Tracked Devices



Map Legend:

- Client—Blue square monitor
- Tag—Yellow vertical rectangle
- Rogue AP—Circle with skull-and-crossbones (red = malicious, green = friendly, gray = unclassified)
- Rogue Client—Blue square monitor with skull-and-crossbones

Technology Background Information

There are two technologies that are used to track Wi-Fi devices with the Cisco Mobility Solution:

- RSSI—Received signal strength indication
- TDOA—Time difference of arrival

For details on these technologies, see *Wi-Fi Location-Based Services Design Guide*, at:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/WiFiLBS-DG.html

Note This reference is to an older release but the information is still valid.

RSSI

RSSI is the measured power of a received radio signal. The packets transmitted by any wireless device are received at multiple APs (provided that those APs listen on the channel on which the frame was transmitted). The APs forward these packets to the wireless LAN controller along with the correspondent RSSI information measured at the AP. The wireless LAN controller aggregates this information on a per device basis from different APs. This data is forwarded to the MSE through NMSP. The Context Aware Services that reside on the MSE use the RSSI data received from one or more WLCs

to determine the location of a wireless device. RSSI is usually preferred for indoor or low ceiling environments, which can result in reflection of the signals. Unlike TDOA, RSSI does not require exact time synchronization amongst APs. With the measured RSSI values from different APs, the probability of the location of a device is calculated at different points on the floor. Based on this probability, the location is returned as the estimated location.

Time Difference on Arrival

The time difference on arrival (TDOA) mechanism is the preferred method to determine device location when you track tags in outdoor and outdoor-like environments, such as indoor, high-ceiling environments. With TDOA, the location of a WLAN device is determined based on the time of arrival of the signal that it transmits as seen by three or more time-synchronized Wi-Fi TDOA receivers. The time of arrival data is collected and reported to the Context Aware Engine for Tags that reside on the MSE, which computes the time differences of arrival between multiple pairs of Wi-Fi TDOA receivers. The time required for a given message to be received by different Wi-Fi TDOA receivers is proportional to the length of the transmission path between the mobile transmitting device and each TDOA receiver. This mechanism of calculation device location requires time synchronization between the Wi-Fi TDOA receivers.

In order to compute a position accurately, this method requires a set of at least three Wi-Fi TDOA receivers. The distance between Wi-Fi TDOA receivers is relatively larger than the distance between APs that are required for indoor RSSI positioning. As with RSSI positioning, this method relies on unidirectional communication (tag transmitting notification frame, no association required).

Refer to the *Context Aware Service Software Configuration Guide*, at:

http://www.cisco.com/en/US/docs/wireless/mse/3350/7.0/CAS/configuration/guide/CAS_70.html

Active RFID Tags

Cisco Compatible Extensions (CCX)-compliant active RFID tags are detected on a Wi-Fi network based on tag notification frames that are sent by the tag and received by an 802.11 AP. The tag notification frame rate can be programmed based on the specific use case scenario. Typically, tags are configured to transmit tag notification frames every 3-5 minutes to optimize frequent location updates and battery life. The call button feature provides the ability to trigger events based on push button on the tag. This enables advanced functionality, such as emergency reporting or parts replenishment. Some tags provide more than one call button. The second call button can be programmed for additional functionality. Tags can store pre-programmed messages that can be received by the wireless network infrastructure. A battery is used to power active tags, which provides up to four years of battery life. Battery life is dependent upon a number of tag configuration parameters that includes the frequency of tag notification frame transmission and repetition rate. Tags can report on their battery level and alert when low. Tags can also have a built-in motion sensor to transmit tag notification frames upon movement. This helps to conserve battery life when the tag is stationary; configure the tags to transmit less frequently when they do not move.

There is another category of tags that add advanced sensor technology to accurately monitor the condition of an asset, such as its ambient temperature, in addition to other location and status information. These sensor tags use standard Wi-Fi networks to transport the asset location and sensor data and do not require dedicated or proprietary sensor networks.

Wi-Fi RFID tags that are compliant with the CCX for Wi-Fi Tags specification can optionally pass tag telemetry information to the location-aware Cisco UWN as part of their tag message payload. Telemetry information is received by APs and collected by the WLCs. At MSE startup, the MSE subscribes for all the service in which it is interested, such as the measurements for tags. The WLC continues to send the MSE notifications at the end of each aggregation cycle.

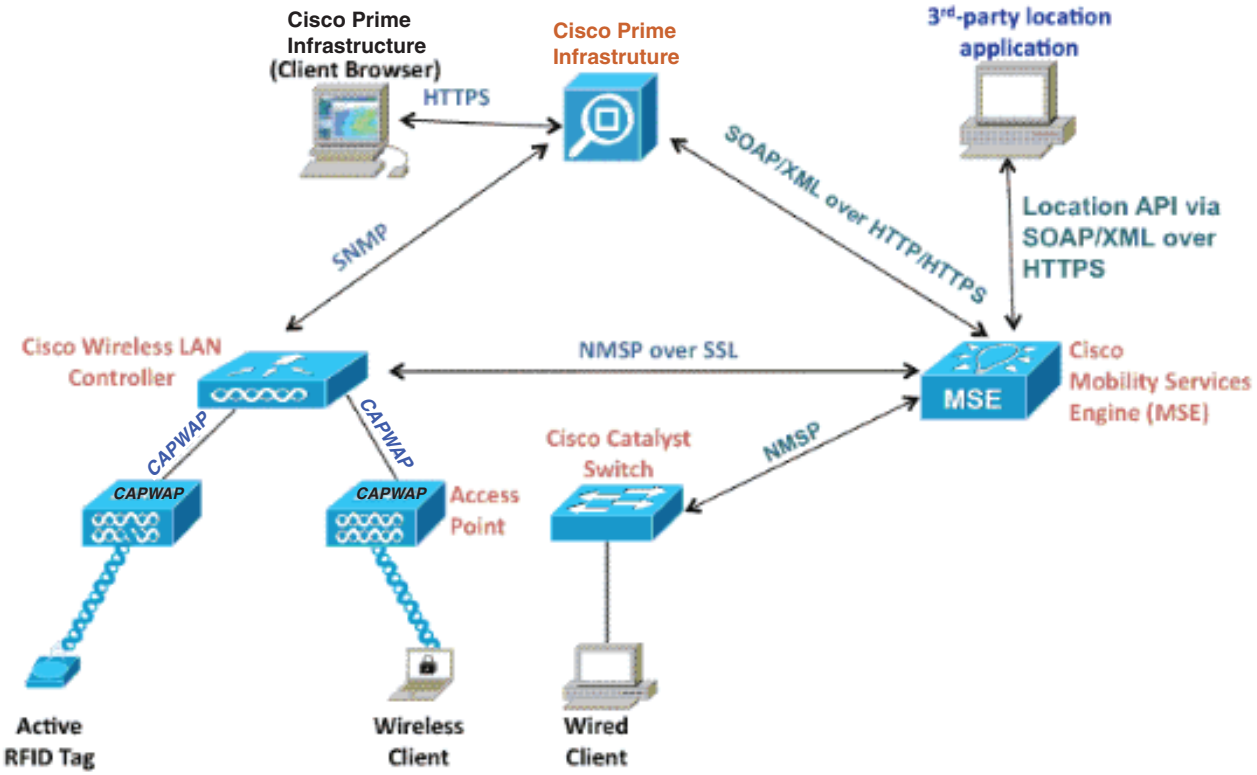
Telemetry information is transmitted from a CCX-compatible tag and is received by one or more APs and/or location receivers, that is, Wi-Fi TDOA receivers, which, in turn, pass the telemetry information to their respective registered WLAN controllers. If the tags are configured to send multiple frame copies (or bursts) per channel, the controller eliminates any duplicate tag telemetry and passes the distilled telemetry values to the MSE. The database in the MSE is updated with the new telemetry information and makes it available to location clients through the MSE SOAP/XML API.

In the case of a tag that passes telemetry value, NMSP is designed to efficiently transport telemetry values from multiple tags in a similar fashion. Telemetry traffic from multiple tags is aggregated by the WLC with each NMSP endpoint capable of performing NMSP frame fragmentation and reassembly if required. All tag data can be included in the northbound notifications, which includes telemetry, call buttons, chokepoint encounters, and so forth.

System Architecture

The MSE integrates with the Cisco centralized wireless LAN architecture as shown in Figure 11-2. The MSE sits out of the data path of the wireless LAN and receives data from the WLC through NMSP. Cisco Prime Infrastructure is used to configure the MSE. Once configured, the MSE is self-contained.

Figure 11-2 System Architecture



When you deploy the Context Aware solution, consideration must be given to the type of devices tracked and the maximum device count. You can track any of the five device types (Wi-Fi clients, active RFID tags, rogue clients, rogue APs, or wired clients) to be configured individually or for simultaneous tracking.

One MSE can be managed by only one CPI, that is, a single MSE cannot be managed by multiple CPI instances, but a single CPI can manage multiple MSEs. When the number of devices to be managed exceeds the capacity of a single MSE, you need to deploy multiple, independent MSEs. The ability to deploy multiple MSEs for scaling applies to all services currently supported on MSE. The maximum number of devices that can be tracked by one Cisco MSE 3355 is 25,000 devices (combination of Wi-Fi clients, active RFID tags, rogue clients, rogue APs, and wired clients) as part of Context Aware Service. The older model Cisco MSE 3310 can track up to 2,000 devices, while the Cisco MSE 3350 can track up to 18,000 devices. When the number of devices to be managed exceeds the capacity of a single MSE box, multiple, independent MSE appliances need to be deployed. This can require MSEs on specific controllers, especially on large campuses where roaming of clients or assets can cross different physical buildings or domains. In this instance, controllers can communicate with a maximum of 10 MSE appliances.

Cisco lightweight APs operate in a unique dual mode that detect devices both on the channels where they service clients and also on all other channels if they periodically background scan while still provide data access to their wireless clients. The gathered raw location data is then forwarded from each AP to its associated WLC through the LWAPP or standards-based CAPWAP protocol. Data is transported between the WLC and the MSE through a secure NMSP connection.

Cisco Prime Infrastructure is used to manage and configure the MSE, and it can also become the visual front-end of the MSE to display Wi-Fi devices that are tracked. All device (wired and wireless) details and specific historical location information can be accessed with the MSE northbound API. CPI uses this interface to visualize location information, as well as view and configure Context Aware parameters.

The Cisco Mobility Solution consists of two location engines with a single unified API. The location engines are:

- Context Aware Engine for Clients (Cisco engine)—Can be used for both Clients and Tags
- Context Aware Engine for Tags (partner engine)—AeroScout-based TAG solution

The **Context Aware Engine for Clients** is an RSSI-based solution that is ideal for tracking Wi-Fi client devices in indoor spaces (for example, offices, hospitals, or other low-ceiling environments). This engine ships by default on all Cisco MSE servers. The tracking licenses of the Context Aware Engine for Clients can be shared between Clients and Tags.

The **Context Aware Engine for Tags** has the ability to use both an RSSI and TDOA-based engine and is intended to be used when you track Wi-Fi devices in indoor, low-ceiling (RSSI), indoor high-ceiling (TDOA), and outdoor (TDOA) environments. This engine is also installed by default on all MSE platforms and is license enabled. The tracking licenses of the Context Aware Engine for Tags can be used only for Tags. For client tracking you need to purchase the following additional components:

- Tag tracking license for the MSE with appropriate Tag count (TDOA or RSSI)
- Wi-Fi TDOA location receivers (if and when required)
- LR license for each Wi-Fi TDOA receiver

When a Cisco MSE is added to a Cisco Unified Wireless Network, the MSE assumes responsibility for the following important tasks:

- Execution of positioning algorithms
- Maintenance of calibration information
- Triggering and dispatch of location notifications
- Processing of statistics and historical location

Cisco Prime Infrastructure is the management platform for the MSE servers and is the user interface (UI) for the services that the MSE provides. The MSE is accessed directly through SSH or a console session for maintenance and diagnostic purposes. All operator and user interaction with the MSE is usually through CPI. The integration of a Cisco MSE into a Cisco Unified Wireless Network architecture immediately enables improvements to base-level location capabilities, which include:

- Scalability—If you add a Cisco MSE, it increases the scalability of the Cisco Unified Wireless Network from on-demand tracking of a single device at a time to a maximum tracking capacity of up to 25,000 simultaneous devices (WLAN clients, RFID tags, rogue APs, and rogue clients) per MSE. For deployments that require support of greater numbers of devices, additional MSE appliances can be deployed and managed under one or more CPI servers.
- Historical and statistics trending—The MSE records and maintains historical location and statistics information for clients and tags. This information is available for viewing through CPI or with third-party location clients. This historical information can be used for location trending, asset loss investigation, RF capacity management, and facilitation of network problem resolution. Historical parameters are configured in Cisco Prime Infrastructure.

Related Information

The following references provide additional information about the Cisco Mobility Services Engine.

- *Cisco 3355 Mobility Services Getting Started Guide*

http://www.cisco.com/en/US/docs/wireless/mse/3355/user/guide/mse_qsgmain.html

- *Cisco 3350 Mobility Services Getting Started Guide*

http://www.cisco.com/en/US/docs/wireless/mse/3350/quick/guide/mse_qsgmain.html

- *Cisco 3310 Mobility Services Engine Getting Started Guide*

http://www.cisco.com/en/US/docs/wireless/mse/3310/quick/guide/MSE3310_GSG.html

- *Cisco Mobility Services Engine - Context Aware Mobility Solution Deployment Guide*

http://www.cisco.com/en/US/products/ps9742/products_tech_note09186a00809d1529.shtml

- *Cisco Context Aware Service Configuration Guide*

http://www.cisco.com/en/US/docs/wireless/mse/3350/6.0/CAS/configuration/guide/msecg_ch7_CAS.html

- *Cisco 3300 Series Mobility Services Engine Licensing and Ordering Guide*

http://www.cisco.com/en/US/docs/wireless/mse/3350/7.3/CAS_Configuration_Guide/Guide/msecg_Overview.html

- *Wi-Fi Location-Based Services 4.1 Design Guide* (old release but information is still useful)

http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/WiFiLBS-DG.html

- Mobility Groups FAQ

http://www.cisco.com/en/US/products/ps6366/products_qanda_item09186a00809a30cc.shtml