CMX Solution Components

September 4, 2014

This chapter highlights the wireless (Wi-Fi) network infrastructure necessary for providing location services and CMX services within this design guide. A discussion of the Cisco Context Aware Service (CAS), which provides location services, and the technologies behind CAS are also presented. Finally, an introduction to the various CMX services which make use of the location information provided by CAS is discussed.

Wireless Infrastructure

The underlying infrastructure behind all CMX applications and services discussed within this design guide is the Cisco wireless LAN (IEEE 802.11) network infrastructure, which consists of the following hardware:

- Cisco Aironet Access Points (APs)
- Cisco Wireless LAN Controllers (WLCs)
- Cisco Mobility Services Engine (MSEs)
- Cisco Prime Infrastructure

Cisco Aironet Access Points

Cisco Aironet access points provide Wi-Fi connectivity to the network infrastructure. Within this version of the CMX design guide, APs also assist in providing the following services:

- Location services for mobile devices—Cisco Context Aware Service (CAS) provides additional details around how APs participate in providing location services for mobile devices.
- Network connectivity for guest mobile devices.

The Cisco second generation APs in this design guide include the Cisco Aironet 3700, 2700, 3600, and 2600 Series.

Cisco 3700 Series APs are ideal for high-density network environments that use mission-critical, high-performance applications. They feature the industry's first AP with an integrated 802.11ac Wave 1 radio supporting a 4x4 multiple input, multiple output (MIMO) design with three spatial streams for data rates up to 1.3 Gbps. The flexible, modular design of the Cisco 3700 Series provides expansion capability for a future 802.11ac Wave 2 module and advanced services such as the Wireless Security Module (WSM).

Cisco 2700 Series APs are non-modular dual band (5 GHz and 2.4 GHz) 802.11ac access points optimized for adding capacity and coverage to dense Wi-Fi networks. They feature a 3x4 MIMO design with three spatial streams for a maximum data rate up to 1.3 Gbps.

The Cisco 3700 and 2700 Series APs incorporate the Cisco High-Density Experience (HDX), which includes among other features Cisco CleanAir® with enhanced support for 80-MHz channels and updated ClientLink 3.0 with support for 802.11a/b/g/n/ac. Cisco CleanAir® technology is enabled in hardware for both the Cisco 3700 and 2700 Series APs. Cisco ClientLink 3.0 helps improve performance of clients on the wireless LAN (WLAN).

Cisco 3600 Series APs are ideal for customers looking for best-in-class performance in 802.11n environments with high client density. They feature the industry's first 802.11n 4x4 MIMO design with three spatial streams for data rates up to 450 Mbps. The flexible, modular design of the Cisco 3600 Series provides expansion capability for emerging technologies such as the 802.11ac Wave 1 module and advanced services such as the WSM.

Cisco 2600 Series APs are dual band (5 GHz and 2.4 GHz) 802.11n access points ideal for mid-market small, mid-size, or large enterprise customers looking for mission critical performance. They feature a 3x4 MIMO design with three spatial streams for data rates up to 450 Mbps.

The Cisco 3600 and 2600 Series access points support additional technologies, such as Cisco ClientLink 2.0 and Cisco CleanAir®. Cisco CleanAir® technology is also enabled in hardware for both the Cisco 3600 and 2600 Series APs.

The field-upgradeable Wireless Security Module (WSM) has a dedicated dual-band radio with its own antennas enabling 7x24 scanning of all wireless channels in the 2.4 and 5 GHz bands. It offloads concurrent support for monitoring and security services—such as Cisco CleanAir® spectrum analysis, wIPS security scanning, rogue detection, context-aware location, and Radio Resource Management (RRM)—from the internal client/data serving radios within the Cisco 3700 or 3600 Series AP to the WSM. The WSM is required to enable the FastLocate feature (also known as All Packet RSSI or Data RSSI) for improved location currency. Probe Request RSSI versus FastLocate provides further details around the FastLocate feature.

Note The Cisco 3700 Series AP requires 18 Watts and the Cisco 3600 Series AP requires 17 Watts of power with the WSM module. When powering the AP from a Cisco Catalyst switch, the switch port must support either POE+ (IEEE 802.3at standard) which supplies up to 30 Watts or Cisco Universal Power over Ethernet (UPoE) which delivers up to 60 Watts of power per switch port.

Cisco Aironet APs can operate as lightweight or autonomous access points. When functioning as lightweight APs, a wireless LAN controller (WLC) is required. In this design, the 802.11 MAC layer is essentially split between the AP and the WLC. The WLC provides centralized configuration, management, and control for the access points. All designs in this design guide assume lightweight APs.

Further information regarding Cisco Aironet APs can be found in the following at-a-glance document:

http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps10981/at_a_glance_c45-636090.pdf

Note Cisco Meraki wireless LAN infrastructure is not discussed within this version of the CMX design guide.

Cisco Wireless LAN Controllers (WLCs)

Cisco wireless LAN controllers (WLCs) automate wireless configuration and management functions and provide visibility and control of the WLAN. Within this version of the CMX design guide, WLCs also assist in providing the following services:

- Location services for mobile devices—Cisco Context Aware Service (CAS) provides additional details around how WLCs participate in providing location services for mobile devices.
- Network connectivity for guest mobile devices.

Cisco WLC functionality can be within standalone appliances, integrated within Catalyst switch products, or run virtually on the Cisco Unified Computing System (UCS). The Cisco wireless LAN controller platforms included within this version of the CMX design guide include the Cisco 5508 WLC and the Cisco Flex 7510 WLC. The Cisco 5508 and Flex 7510 platforms run Cisco Unified Wireless Network (CUWN) software (also referred as AireOS software). The Cisco 5508 WLC is targeted for mid-sized and large single-site enterprises. Within this design guide it is deployed within the campus supporting APs operating in centralized (local) mode. The Cisco Flex 7510 WLC is targeted for enterprise branch environments. Within this design guide it is deployed as a remote controller supporting APs operating in FlexConnect mode. Campus and Branch Designs in Chapter 4, "CMX Deployment Models" provides details about the deployment of these WLC platforms.

Table 3-1 shows scalability of these platforms in terms of APs, clients, and throughput.

Table 3-1 Wireless LAN Controller Scalability

Platform	Access Points Supported	Clients Supported	Throughput
Cisco 5508	Up to 500	Up to 7,000	Up to 8 Gbps
Cisco 7510	Up to 6,000 APs with up to 2,000 FlexConnect groups	Up to 64,000	Up to 1 Gbps centrally switched traffic

Further information regarding Cisco WLC platforms can be found in the following at-a-glance document:

http://www.cisco.com/en/US/prod/collateral/modules/ps2706/at_a_glance_c45-652653.pdf

Cisco Mobility Services Engine (MSEs)

The Cisco Mobility Services Engine (MSE) is a platform that helps organizations deliver innovative mobile services and improve business processes through increased visibility into the network, customized location-based mobile services, and strengthened wireless security. The following mobility services are supported on the MSE:

- Context Aware Service
- Wireless Intrusion Prevention System (wIPS)
- CMX Analytics (Location and Presence)
- CMX Connect & Engage (includes the Web service for guest access and the Cisco SDK for app development)
- Mobile Concierge Service

Mobility services are supported based upon the licensing of the MSE as shown below:

- Base Location Services (also called the Context Aware Service)—Requires Location Services licensing.
- Wireless Intrusion Prevention System (WIPS)—Requires WIPS licensing.
- CMX Analytics, CMX Connect & Engage, and the Mobile Concierge Service—Requires Advanced Location Services licensing.

This version of the Cisco CMX design guide discusses the following services:

- Location services for mobile devices—Cisco Context Aware Service (CAS) provides additional details around how the MSE participates in providing location services for mobile devices.
- CMX Analytics (both Location Analytics and Presence Analytics)
- CMX Visitor Connect (part of CMX Connect & Engage)

The Cisco MSE is available as a physical appliance or as a virtual appliance. Additional information regarding the Cisco MSE platform can be found in MSE Scalability in Chapter 4, "CMX Deployment Models."

Note Use of the Cisco SDK for mobile app development will be discussed in future versions of the Cisco CMX design guide.

Cisco Prime Infrastructure

Cisco Prime Infrastructure (PI) is the continued evolution of Cisco Prime Network Control System (NCS). It interacts with Cisco wired and wireless infrastructure components to be a central management and monitoring portal. Cisco PI configures and monitors Catalyst switches and routers and it also controls, configures, and monitors all wireless LAN controllers (WLCs) and, by extension, all access points (APs) on the network.

Within the Cisco CMX design guide, Cisco Prime Infrastructure also provides the following services:

- Provides the administrative interface for importing and tuning floor maps for location services.
- Integrates with the Cisco MSE to synchronize floor maps.
- Synchronizes MSE services with WLCs.
- Integrates with CMX Presence Analytics to import APs not associated with any floor map.
- Provides the administrative interface for enabling MSE services such as the Context Aware Service (CAS), CMX Analytics, and CMX Visitor Connect.

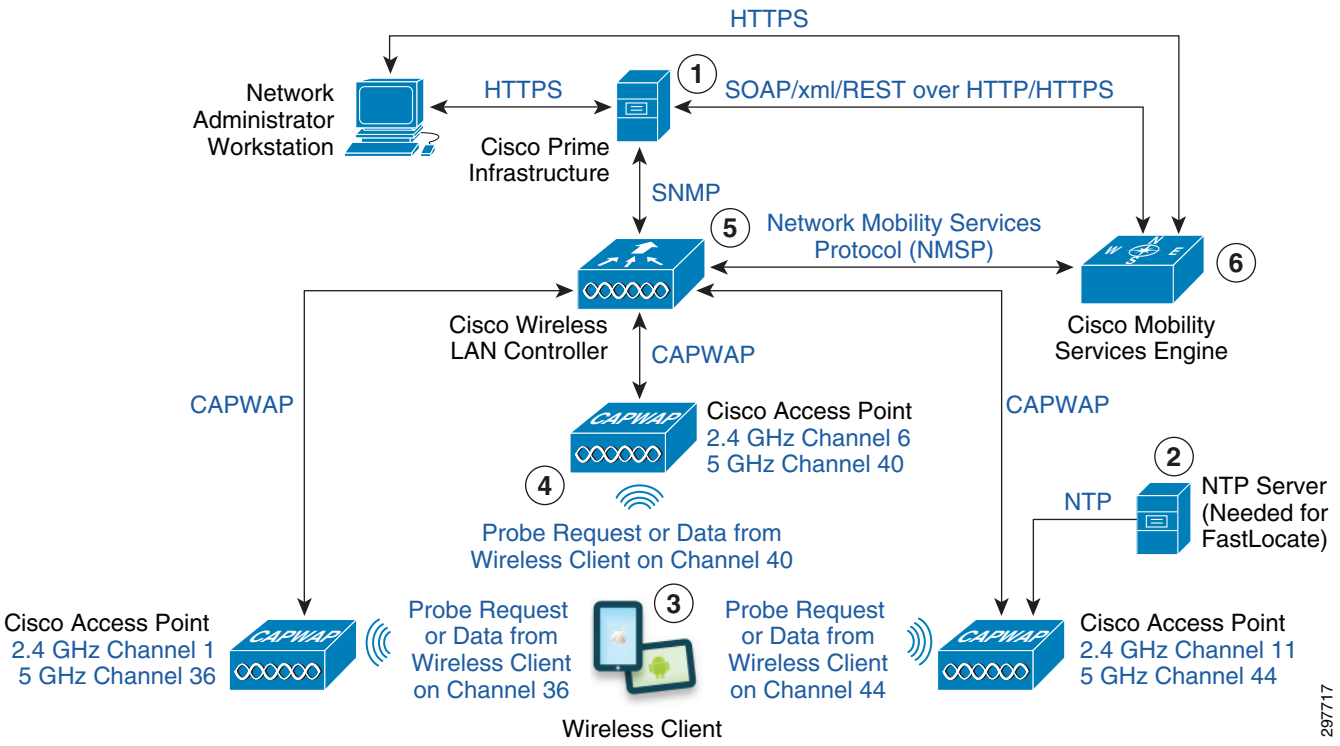
Multiple WLCs and MSEs may be managed and monitored by Cisco Prime Infrastructure. Detailed information regarding floor maps and enabling MSE services via Cisco PI is provided in Chapter 24, "Configuring Cisco Prime Infrastructure."

Cisco Context Aware Service (CAS)

The underlying technology behind CMX applications and services is wireless (Wi-Fi) location. Location services are provided to Cisco wireless network infrastructures through the Context Aware Service (CAS) running on the Cisco MSE. CAS provides the location database which is leveraged by CMX applications and services.

Figure 3-1 provides a high-level overview of the information flows between the various hardware components for CAS. It assumes the WLAN within the site has been designed for location services. Detailed information regarding designing the WLAN within the site to support location services is provided in the"CMX Radio Frequency and Location Based Design" part of this design guide.

Figure 3-1 Context Aware Service (CAS) Hardware and Data Flows



Each of the steps in Figure 3-1 is explained below:

Step 1 To be able to collect Wi-Fi location information for a site, the network administrator must first set up the wireless infrastructure to support location services, which includes:

- Importing the floor map for the site into Cisco Prime Infrastructure.
- Correctly sizing and tuning the floor map.
- Placing APs in the correct location on the floor map.
- Enabling the Context Aware Service (CAS) on the MSE.
- Syncing the WLC and MSE through Cisco Prime Infrastructure.

The network administrator accomplishes this by establishing an HTTPS session to the Cisco PI server and using the graphical user interface (GUI).

The network administrator must also synchronize the floor map information with the MSE, which pushes the floor map information to the MSE. The interface between Cisco PI and the MSE uses SOAP/XML & REST messages over HTTPS.

The network administrator must also synchronize MSE services like CAS with the WLC so that the WLC forwards collected data (location, intrusion detection, etc.) from the APs to the MSE.

Additional configuration of the Context Aware Service (CAS), CMX Presence Analytics, CMX Location Analytics, and CMX Visitor Connect must also be done by directly establishing an HTTPS session to the MSE running the associated service.

Detailed information regarding setting up the wireless infrastructure to support location services is provided in the"CMX Configuring the Infrastructure" part of this design guide.

Step 2 FastLocate Only—If the deployment is using the FastLocate feature, the APs need to be time synchronized via NTP so that Wireless Security Modules (WSMs) all simultaneously scan the same channel as they proceed through the scan list. Detailed information regarding the differences between the Context Aware Service using Probe Request Received Signal Strength Indication (RSSI) and the FastLocate feature is provided in Probe Request RSSI versus FastLocate.

Step 3 For the Context Aware Service (CAS) to function, wireless clients must either send Probe Requests on each active channel or associate with an AP and send packets if using the FastLocate feature.

Step 4 Each AP within range of the wireless client either hears Probe Requests sent by the wireless client on the 2.4 GHz channel and/or 5 GHz channel on which the AP is operating or hears packets when the monitoring radio within the WSM module dwells on the channel on which the wireless client is operating on—when the wireless client is associated to an AP and the FastLocate feature is enabled. RSSI information is calculated for the particular client from either the Probe Requests or from packets sent by the wireless client.

A minimum of three APs are needed to determine the X,Y coordinates of the wireless client relative to the floor map. However accuracy is highest when a wireless client is seen by at least four APs. For wireless (Wi-Fi) locations, the APs must be configured onto a floor map within Cisco PI, which is then synchronized with the MSE. If the AP has not been placed on the floor map which is synchronized with the MSE, RSSI information is still calculated by the AP and forwarded to the MSE. However the MSE does not use the RSSI information from the particular AP in determining the X,Y coordinates of the wireless client. If the RSSI values calculated by all of the APs and sent to the MSE are below the RSSI cutoff threshold setting within the MSE, the MSE ignores the calculation and the data point is not stored in the MSE location database. By default this is set for -65 dBm. Information about setting this parameter is provided in Chapter 25, "Configuring the Mobility Services Engine for CMX."

For wireless (Wi-Fi) presence, APs which do not appear on floor maps must be imported to the MSE and associated with a Presence site. Information showing how to do this is provided in Chapter 26, "Configuring CMX Analytics."

If only one AP sees the wireless client and the RSSI value is above the RSSI cutoff threshold, the location of the wireless client is reported to be the X,Y coordinate of the AP itself, relative to the floor map.

Each AP aggregates messages which contain RSSI information and sends them to the WLC which controls the AP approximately every 500 milliseconds via the CAPWAP protocol.

Step 5 The WLC aggregates RSSI information for each client from each AP which it controls and forwards all messages to all MSEs—every two seconds by default—using the Network Mobility Services Protocol (NMSP).

Step 6 Since RSSI information regarding a given wireless client could come from APs on the same floor map, but controlled by different WLCs, the location services (CAS) engine within the MSE aggregates data for five seconds before calculating locations of wireless clients. Once the location calculation is completed, the MSE can update the location (CAS) database for the particular wireless client. Services such as the CMX Analytics engine within the MSE can then make use of the updated information within the location database of the MSE.

Note CMX Analytics has its own database, which is built off of the MSE location database. CMX Analytics periodically pulls information (in batch mode) from the MSE location database. Therefore CMX Location Analytics should not be used for real-time analysis.

Probe Request RSSI versus FastLocate

Prior to WLC and MSE release 8.0, the location services engine within the Context Aware Service (CAS) relied solely on IEEE 802.11 Probe Requests to calculate the location of wireless clients via RSSI information. Probe Requests are sent when the wireless client actively scans for a Basic Service Set (BSS)—in other words an Access Point (AP) with which to join. Probe Requests are good candidates for collecting RSSI information because the wireless client typically probes multiple channels to develop a scan report which is then used by the client to select which BSS/AP to join. Wireless clients typically cycle through 5 GHz and 2.4 GHz channels as they send Probe Requests, waiting for Probe Responses.

Note Probe Requests are not sent simultaneously to all active channels. The wireless client typically sends a probe request on a particular channel and briefly listens for a Probe Response before switching channels and sending another probe request.

In Figure 3-1, three APs operating in both the 2.4 GHz and 5 GHz frequency bands are shown. As the wireless client generates Probe Requests on channels 36, 40, and 44 in the 5 GHz frequency band, each of the APs hears, respectively, the Probe Request.

Unfortunately client probing frequency in most smartphone and tablet devices has been decreasing over time and is also non-deterministic. Probe Request frequency can vary from under a second to five minutes depending on the smartphone or tablet device operating system, wireless driver, current activity on the device, battery usage, etc. Active scanning consumes battery power of mobile devices. Some smartphones disable active scanning altogether below a certain percentage of remaining battery power. Hence, such devices are virtually non-trackable when remaining batter power drops below a certain threshold. Additional information is discussed in Chapter 6, “CMX Additional Considerations.”

Because of the non-deterministic nature of Probe Requests, total location error—which is a function of location accuracy and location currency—is increased. A detailed discussion of the expected location accuracy and location currency of the Cisco Context Aware Service (CAS) is provided in Chapter 13, “Location Fundamentals.”

To alleviate the issue of decreased location currency, Cisco introduced a new feature called FastLocate. FastLocate is implemented in WLC and MSE version 8.0 and requires Prime Infrastructure release 2.1 to enable it. Information regarding how to enable the FastLocate feature is provided in Chapter 23, “Configuring Cisco Wireless LAN Controllers.”

With the FastLocate feature enabled, RSSI information is collected on all data packets transmitted by the wireless client, not just Probe Requests. The FastLocate feature is intended to make the collection of RSSI data more deterministic and more current to reduce movement error, therefore resulting in a reduction in the total location error. The FastLocate feature requires Cisco 3600 or 3700 Series APs with the Wireless Security Module (WSM). The WSM provides a separate, dedicated dual-band radio which allows the AP to monitor other channels for CleanAir or wIPS purposes and simultaneously service data from wireless clients. With the FastLocate feature, WSM channel scanning is synchronized across APs using Network Time Protocol (NTP). The result is that all WSMs within the site listen to the same 5 GHz or 2.4 GHz channel at the same time.

The frequency by which each channel is monitored (also referred to as the return time to channel) influences the currency of location information (also referred to as the location refresh rate) obtained by FastLocate. The frequency by which each channel is monitored is based upon the number of channels within the FastLocate scan list and the dwell time (Tdwell) on each channel. The scan list (also referred to as the off-channel scan list) is the list of channels to be monitored for activity. The dwell time is the amount of time the WSM radio monitors that particular channel along with the time required to change channels. Whether CleanAir is enabled or disabled influences the return time to channel because instead of the channel list being just the channel slots for FastLocate, it has the channels slots for CleanAir as well. Hence the return time to channel is longer when CleanAir is enabled.

The following provides an example based on a U.S. deployment with both 2.4 and 5 GHz (U-NII-1, U-NII-2 non-extended, and U-NII-3 channels) operation with CleanAir enabled.

Channels: 2.4GHz non-overlapping U.S. country channels: 1 6 11

5 GHz U.S. country channels (16 channels, excluding U-NII-2 extended): 36 40 44 48 52 56 60 64 149 153 157 161 165

Dwell time per FastLocate Slot = 250 milliseconds

Dwell time per CleanAir Slot = 175 milliseconds

Based on the above parameters, the WCM scan list would be as follows:

1, 6, 11, 36, X, 40, 44, 48, 52, X, 56, 60, 64, 149, X, 153, 157, 161, 165, X

Each of the numbers (1, 6, 11, …) indicate 250 milliseconds of time that FastLocate dwells on that particular channel collecting RSSI information from wireless devices operating on that channel. Every fifth slot shows an X. Each X indicates 175 milliseconds of time that CleanAir dwells on additional channels not included in the FastLocate scan list.

Given this example, the return time to channel for FastLocate would be estimated as follows:

16 FastLocate channels * 250 milliseconds of FastLocate dwell time per channel = 4,000 milliseconds

Plus

4 CleanAir channels * 175 milliseconds of CleanAir dwell time per channel = 700 milliseconds

4,000 milliseconds + 700 milliseconds = 4,700 milliseconds or approximately 5 seconds.

This allows for both the FastLocate feature and CleanAir to operate simultaneously on the Wireless Security Module (WSM). Increasing the number of channels in the scan list increases the return time to channel. Decreasing the number of channels in the scan list decreases the return time to channel.

The FastLocate feature requires the wireless device to be associated to and communicating with an AP to take advantage of increased currency of location information. To be seen during every scan cycle, which is the optimal currency of location information using the FastLocate feature, the wireless client must be transmitting packets during the time the WCM modules dwell upon the channel which the wireless client is operating.

Note CMX Location Analytics does not necessarily require association of the wireless device to any network. Hence total location accuracy of a CMX Location Analytics deployment which does not involve association of the wireless device to the network may not improve with FastLocate. However for CMX services which involve connecting the wireless device to a network, total location accuracy may improve due to increased currency of location information and additional data points upon which to base location calculations.

One way of accomplishing this is via an app running on the mobile device which transmits packets during every scan cycle, however this may not always be feasible to develop and deploy. Hence FastLocate incorporates an additional feature which keeps track of unresponsive (idle) clients.

Unresponsive clients are devices associated to the wireless infrastructure, but which RSSI information has not been refreshed for a given number of scan cycles. By default this is 10 scan cycles or roughly from 40 to 60 seconds depending on the channel scan list and whether CleanAir is enabled. This is a configurable parameter. Information on configuring this parameter is provided in Chapter 23, "Configuring Cisco Wireless LAN Controllers."

When a wireless client has been determined to be unresponsive, an 802.11 Block Acknowledgement Request (BAR) is sent to the wireless client by the AP to which the client is associated, shortly before scanning the channel to which the particular wireless client is associated, during the next scan cycle. The wireless client should respond to the BAR with a Block Acknowledgement (BA). This ensures that the particular wireless client is heard during that scan cycle and that the RSSI information for that particular wireless client is refreshed.

Connected Mobile Experiences Services

The overall Cisco CMX solution can be broadly separated into three levels of functionality as discussed in Chapter 1, "Connected Mobile Experiences Solution Overview":

- CMX Detect—Detects the presence and/or location of a mobile device within a venue. This mobile device could belong to a customer within a retail establishment, a patient within a healthcare facility, a patron to a museum, a traveler within an airport, an employee within a corporate location, etc. Insight into movement, dwell times, and crowding within the venue can then be acquired to provide improved service.
- CMX Connect—Provides an easy-to-use and scalable method of connecting a mobile device to the guest wireless LAN network within a venue. This can be used to provide some level of context-based services to visitors while at the venue or to potentially gaining insight into the demographics of visitors to the venue via social media sites.
- CMX Engage—Provides context-based services to the visitor through their mobile device as they enter and move through various points-of-interest (POIs) in the venue.

These three levels of functionality are delivered via the following CMX services:

- CMX Analytics (includes Location Analytics and Presence Analytics)
- CMX Connect & Engage (includes CMX Visitor Connect, CMX Facebook Wi-Fi, the CMX Mobile Application Server, and the CMX SDK for mobile app development)

This version of the Cisco CMX design guide discusses CMX Location Analytics, CMX Presence Analytics, and CMX Visitor Connect. The following sections provide a high-level overview of each of the CMX services discussed within this version of the CMX design guide.

CMX Location Analytics

Cisco CMX Location Analytics makes use of the location information collected by the Context Aware Service (CAS) running on the MSE to determine mobile device parameters such as:

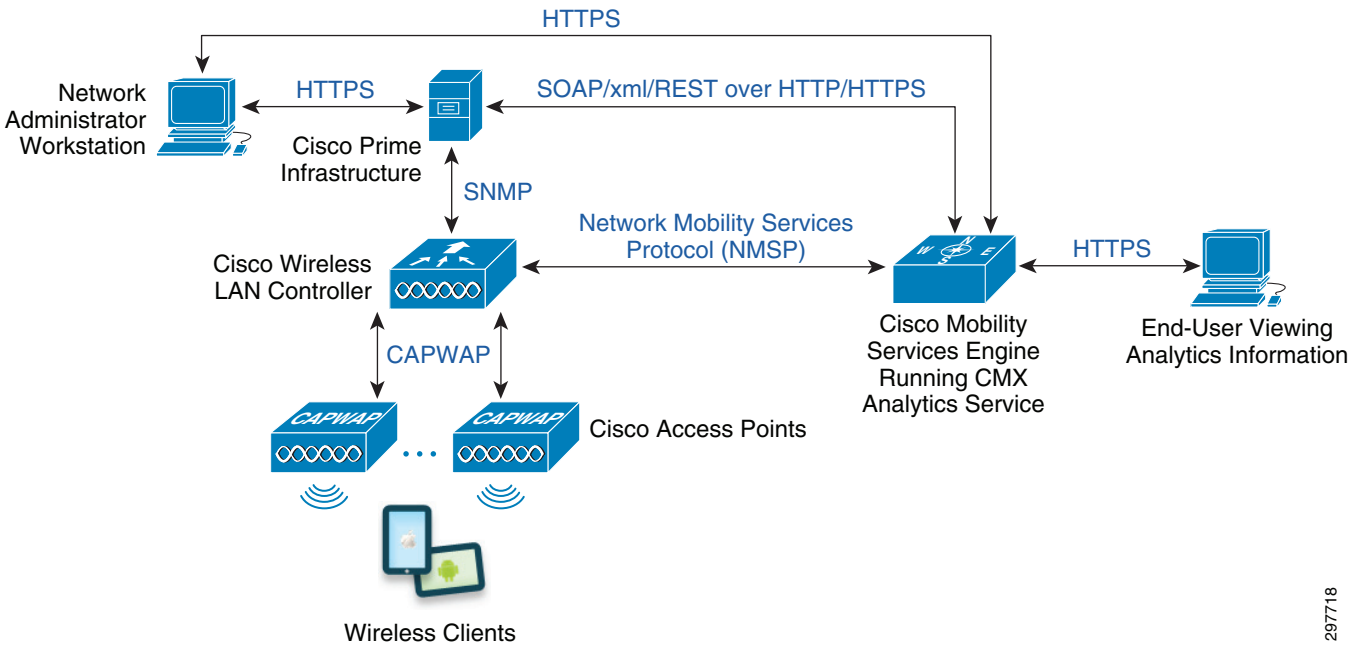
- Dwell time—How long people stay in a specific point.
- Crowding—Popular points at which people stay a long time.
- Path choice—For example, do people usually turn left or right when coming out of an elevator.

CMX Location Analytics aggregates this information for common understanding, so businesses can use this information to better understand how their customers interact with different parts of their venues or environments. Businesses can utilize CMX Location Analytics to help achieve better facility planning, measure changes in their buildings, and improve their interaction with customers.

The basic data used by CMX Location Analytics is in the form of MAC addresses, time, X and Y coordinates, etc. CMX Location Analytics helps aggregate and visualize this data, consisting of anonymous MAC addresses, to help generate insights about the movement and behavior patterns of the people using mobile devices who are visiting a venue. This can be used to help provide better service to visitors of the venue. A venue can be a shop, mall, airport, or city center, provided that it has a network of wireless access points so that devices moving within that space can be located. All wireless (Wi-Fi) devices have unique MAC addresses which are used for communicating with the network infrastructure (access point). Without the use of MAC addresses, the wireless (Wi-Fi) network itself would not operate. All forms of networking utilize some form of unique addressing to deliver information to the correct device. Although there may be privacy concerns around the use of MAC addresses for analytics, it should be noted that MAC addresses are associated with a physical device and are not associated with any specific end-user information.

Figure 3-2 shows a high-level overview of the hardware and information flows for CMX Location Analytics.

Figure 3-2 High-level Overview of Hardware and Information Flows for CMX Location Analytics



As can be seen, the hardware and information flows are basically the same as those shown in Figure 3-1 for the Context Aware Service (CAS). CMX Location Analytics is a separate process which can run on the same MSE that runs the Context Aware Service (location services) or on a separate MSE. MSE Scalability in Chapter 4, "CMX Deployment Models" discusses this further.

Note CMX Location Analytics periodically (approximately every 15 minutes) extracts information from the Context Aware Service (location services) database running on the MSE to aggregate location information from various mobile devices for analysis and/or reporting. Hence the information presented within CMX Location Analytics is not real-time, but historical information. Therefore slight variations

can happen for the same analysis or report taken at different dates due to the historical data. On startup of the CMX Location Analytics service, it can be up to 45 minutes before analytics information is displayed.

CMX Location Analytics data is accessed by establishing an HTTPS session directly to the MSE which runs the Location Analytics service. The functionality of CMX Location Analytics is separated into three tabs located at the top of the CMX Analytics home page:

- Dashboard Tab
- Analytics Tab
- Reports Tab

Each is discussed below.

Dashboard Tab

The Dashboard tab provides a quick and easy way of visualizing device counts and dwell times of devices in various zones and timeframes throughout the venue. The CMX Analytics Dashboard can be customized by the CMX administrator by adding or deleting pages and widgets, which include:

- For Location Analytics sites, whether device count or dwell time is displayed
- For Presence Analytics sites, whether device count, dwell time, or conversion percentage is displayed
- Whether the information is displayed in bar chart or line chart format
- The particular zone from the floor map to be included within the widget
- The start and end dates to be displayed
- The start and end times of the day to be displayed

Further details regarding the CMX Analytics Dashboard are provided in Chapter 26, "Configuring CMX Analytics."

CMX Analytics Tab

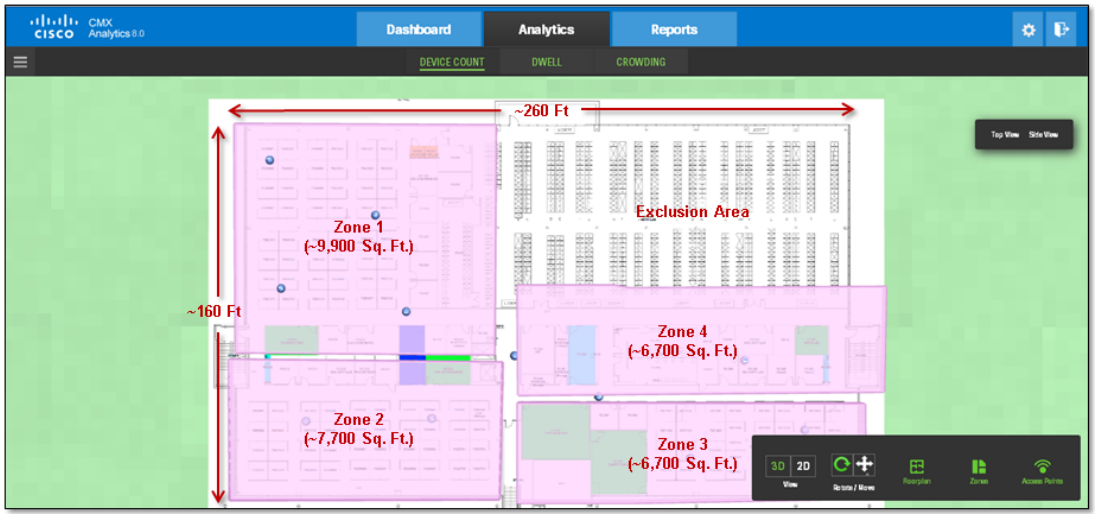
The CMX Analytics tab is used to perform deeper analysis on devices that pass through the venue. The results can be viewed in 3D or 2D within the environment. Various types of analysis can be performed, including:

- Zone Analysis—Provides aggregated parameters such as dwell time, number of devices, and crowding for each zone defined.
- Alternative Path Analysis—Shows a breakdown of the percentage of devices going to each destination from each starting point and vice versa.
- Heat Maps—Provides a graphical representation of point data which can be viewed on the map in such a way that areas of higher concentration appear darker.
- Typical Locations—Provides parameters such as dwell time, number of devices, and crowding for different areas of the building.

Zones within CMX Analytics represent separate areas within a venue where analytics information is aggregated. Zones are configured as coverage areas which are defined on a floor plan within Cisco Prime Infrastructure (PI). It is recommended that zones should be configured to be no smaller than approximately 1,000 square feet. Figure 3-3 provides an example of zones configured on a floor plan (as

viewed through the CMX Analytics tab) within a venue. Note that the building dimensions and zone sizes have been added to the figure.

Figure 3-3 Example of Location Analytics Zones



Note When changing zone names or adding new zones, it should be noted that analytics data will only be available for that zone on and after the date on which the zone name was changed or the new zone was added. Hence the CMX administrator should carefully plan zones such that changing zone names and/or adding and deleting zones is kept to a minimum.

Further details regarding the configuration of zones are provided in Chapter 24, "Configuring Cisco Prime Infrastructure."

CMX Reports

The CMX Location Analytics reporting facility provides a more regular and manager-oriented set of information through the provision of parameterized templates to measure various common trends and patterns that occur over a period of time in a particular zone. The time window for CMX Location Analytics reports is typically longer than for CMX Location Analytics analysis, discussed in CMX Analytics Tab.

The CMX Location Analytics Reports tab has the following reports:

- Conversion Percentage Report—Estimates the percentage of people who were in the vicinity of the actual zone before entering that zone.
- Detected vs. Connected Devices Report—Shows an overview of the number of devices that were connected to the network and the devices that were merely probing during a given time period for a particular zone.
- Daily Visitors and Dwell Times Report—Shows both the number of devices and the average time spent in a zone across several days.
- Hourly Visitors and Dwell Times Report—Shows both the number of devices and the average time spent in a zone across several hours.

- Movement between Zones Report—Provides a breakdown of all zones at specific points as devices passes to and from the focus zone.
- Repeat Visitors Report—Of the visitors who appeared within the venue within a defined time window (particular day, week, month, etc.), shows how frequently those same visitors returned to the venue since a defined start date (which can be before the time window).

Reports can be viewed directly on the MSE—requiring direct web access (HTTPS) to the MSE—or exported as an Adobe Acrobat (.pdf) file and manually emailed or printed.

Differences in CMX Reports, Dashboard, and Analysis

CMX Reports and the CMX Dashboard operate off an aggregated (i.e., summarized) database which is smaller than the full CMX Analytics (analysis) database, which is restricted by default to 8 million points. This is to provide a fast response for the CMX Dashboard and CMX Reports. For this reason less history may be available for Analysis than for Reporting. Information within the aggregated database is updated approximately every hour.

CMX Reports and the CMX Dashboard also use a slightly different interpretation of a visit than CMX Analytics (analysis). For CMX Reports and the CMX Dashboard, a visit refers to a device seen that day at the site. If a device arrives at the zone or site, leaves for a few hours, and arrives at the zone or site again, it is still viewed as the device having visited the zone or site that day one time. For CMX Analytics (analysis), a visit to a zone refers to a device seen in that zone. If the device moves to another zone and is seen, then moves back to the original zone, CMX Analytics counts that as two visits to the original zone and 1 visit to the other zone. Alternatively, if the device is seen in a zone or site, is then not seen for more than hour, and re-appears in the zone or site, CMX Analytics counts that as two visits to the zone or site.

Because of this difference in the interpretation of visits between CMX Reports and CMX Dashboard and CMX Analytics (analysis), the information within each output may appear different even though the same zones or sites and dates were selected.

CMX Presence Analytics

CMX Presence Analytics is targeted for customer locations with a small number (perhaps only one or two) of APs. These are referred to as “sites” from a Presence Analytics perspective. Hence sites are just logical groups of APs with the following attributes:

- A globally unique ID
- A globally unique name
- A description

In deployments with only one or two APs per site, CMX Location Analytics is of limited value since the infrastructure cannot track user movement with any degree of accuracy with only one or two APs. Further, there may be no need to track user movement in a small venue. However customers may still wish to collect analytics information, such as the percentage of passing customers who actually visit the site, the dwell times of customers within the site, and the crowding of the site during various times of the day. This information can be useful for staffing and promotional activities within the small venue.

The behavior of CMX Presence Analytics is as follows:

- If a wireless device is detected at a power level below the Low RSSI Threshold (default of -95 dB), the wireless client is discarded (ignored) from Presence Analytics.

- If a wireless device is detected at a power level above the Low RSSI Threshold, the wireless client is classified as a passer-by.
- If a wireless device is detected at a power level above the High RSSI Threshold (default of -75 dB), for a time period greater than the Dwell Time used to classify the wireless device as a visitor (default of 5 minutes), during the Time Period used to classify the wireless device as a visitor (default of 15 minutes)—then the wireless device is classified as a "visitor".
- If a wireless device is detected at a power level above the High RSSI Threshold, for a time period less than the Dwell Time used to classify the wireless device as a visitor, during the Time Period used to classify the wireless device as a visitor—then the session is maintained. Note that the wireless device has already been classified as a "passer-by".
- If a wireless device associates to the AP at the site, the wireless device is classified as a "visitor".

Internally, Presence Analytics data is persisted to the internal MSE database. As with Location Analytics, Presence Analytics data should only be viewed as "off-line" analytics, meaning that the use cases should be historical only, not real-time. Presence statistics information includes:

- Site
- Number of visitors to the site
- Total devices seen
- Number of new visitors to the site
- Number of visits to the site
- Average dwell time at the site
- Average number of repeat visitors as of the past month

CMX Presence Analytics represents somewhat of a sub-set of the functionality of CMX Location Analytics, in that the analytics information, i.e. dwell times, device counts, and crowding, are based on the entire site versus individual floors or zones within a site.

CMX Visitor Connect

CMX Visitor Connect is part of the CMX Connect & Engage service which runs on the MSE. CMX Visitor Connect is an easy-to-use method of connecting a mobile device to the guest WLAN within a venue utilizing the MSE and optionally social media sites. Along with guest Internet connectivity, CMX Visitor Connect provides the following functionality:

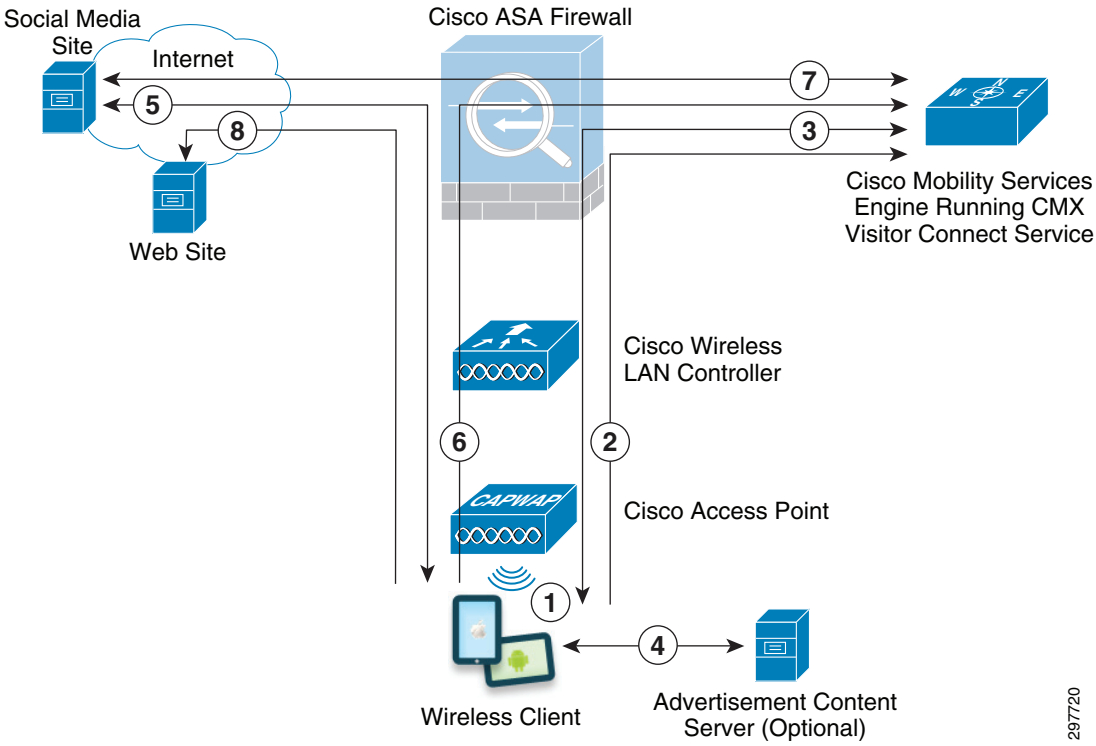
- The ability to push a customizable splash page to the guest mobile device during the login process, requesting basic information such as name and email address.
- The ability to push Terms & Conditions to the guest mobile device for use of the guest Wi-Fi service.
- The ability to authenticate the guest via any of the social media connectors currently supported by CMX Visitor Connect including Facebook, LinkedIn, and Google+.
- The ability to allow the guest to "opt-out" and still access the Internet without logging in to social media.
- The optional ability to push promotional/advertisement content to the guest device during the login process.
- The ability for the guest device to temporarily dis-associate to the guest Wi-Fi, then re-associate, without having to log in again.

- The optional ability to determine if a guest has logged in via social media or logged in anonymously and enforce different usage quotas based on that. This includes preventing a returning guest device from accessing the guest Wi-Fi network if it exceeds the daily usage quota and also isolating the device from the guest Wi-Fi network if it exceeds the daily usage quota.

Note that the splash page, Terms & Conditions, and promotional content are automatically sized appropriately for the mobile device type.

Figure 3-4 shows a high-level overview of the hardware and information flows for a guest mobile device utilizing CMX Visitor Connect to access the Internet.

Figure 3-4 High-level Overview of Hardware and Information Flows for CMX Visitor Connect



Each of the steps in the figure above is explained below:

Step 1 The mobile device must first associate to an AP which broadcasts the B2C guest SSID / WLAN within the venue.

Note CMX Visitor Connect is often implemented to provide guest Wi-Fi and Internet connectivity for consumers visiting a venue (discussed in CMX Visitor Connect Use Case Story in Chapter 7, "CMX Use Case Stories"). Hence the guest WLAN is also referred to as the Business-to-Consumer (B2C) guest WLAN within this design guide to differentiate it from other types of guest Wi-Fi connectivity which may be implemented by an organization within a venue, such as corporate sponsored guest access. This is because different types of guest Wi-Fi connectivity may have different requirements for authentication, access control, etc.

The B2C guest WLAN is configured with no Layer 2 security (i.e., an open SSID) with Layer 3 Web Passthrough. Detailed information regarding configuration of the B2C Guest WLAN on Cisco WLCs for CMX Visitor Connect is provided in Chapter 23, "Configuring Cisco Wireless LAN Controllers."

Step 2 The end-user of the mobile device opens their web browser to reach a web site on the Internet. The web session is then redirected by the Cisco WLC to the CMX Visitor Connect service running on the MSE. The specific URL to which the guest mobile device is redirected is:

http://<MSE_IP_Address>:8083/visitor/social.do

MSE_IP_Address corresponds to the IP address of the MSE server. The CMX Visitor Connect service runs on a separate TCP port (8083) from other MSE services, such as the administrative web interface. Hence from a security perspective, it is recommended to limit mobile devices which associate to the B2C Guest WLAN to only reach TCP port 8083 of the MSE. The designs shown within this design guide assume that B2C guests are terminated outside of a Cisco ASA firewall, which provides stateful access control for B2C guest mobile devices. B2C Guest Access for CMX Visitor Connect in Chapter 4, "CMX Deployment Models" discusses the network infrastructure design and ASA firewall policy in more detail.

Step 3 On re-direction of the web session, CMX Visitor Connect presents the end-user with a splash page for registration, terms & conditions, and the option for the end-user to login via social media sites.

The splash page is customizable and can be used to collect information such as the Name and Email Address of the visitor. Multiple splash pages can be configured within Visitor Connect, each used for a different venue in which the visitor is logging in or even for different points of interest (POIs) within a single venue. This is because the Context Aware Service, also running on the MSE, is aware of the location of the mobile device based on one or more of the following:

- When the mobile device generates Probe Requests, for instance before associating with the AP.
- When the mobile device associated with the AP.
- When the mobile device generates packets and if the FastLocate feature is enabled for the particular venue.

Step 4 Optional: Optionally, CMX Visitor Connect can be configured to present marketing content, such as promotional ads, coupons, etc. to the mobile device. The actual content may be located on another server which must be accessible to the mobile device.

Step 5 If CMX Visitor Connect is configured to allow the end-user to log in via one of the social media connectors supported (Facebook, LinkedIn, or Google+) and if the end-user chooses to log-in via social media site, the web session is redirected to the social media site. The end-user then enters their credentials for the particular social media site. This requires the CMX administrator to have previously configured the CMX Visitor Connect connector for the particular social media site. CMX Visitor Connect uses a variation of the OAuth 2.0 protocol for authentication to the Wi-Fi network via social media site.

Step 6 On entering user credentials in the social media site, the browser of the mobile device is again re-directed back to the CMX Visitor Connect service running within the MSE, along with an authorization code.

Step 7 The CMX Visitor Connect service running on the MSE authenticates that the end-user logged into the social media site by sending the authorization code, along with a ClientID and a Secret which was previously obtained during the configuration of the social media connector within the CMX Visitor Connect service on the MSE.

The CMX Visitor Connect service running on MSE software release 8.0 supports two user groups—the Social user group and the Basic user group. These groups are used to distinguish whether a mobile device's end-user has logged in via a social media site or has accessed the guest WLAN anonymously. Note that the anonymous access to the guest WLAN requires the CMX administrator to enable that option within the CMX Visitor Connect service on the MSE.

The distinction between user groups can be used to provide different quota limits for the amount of traffic which a mobile device can send or receive per day based upon whether the device is placed into the Social user group or the Basic User group. If a quota is configured for a particular user group and if the mobile device exceeds that quota for the day, the mobile device is disassociated from the AP. If the mobile device reconnects to the guest WLAN, any web sessions are automatically redirected to a web page within the MSE indicating that the end-user has exceeded their quota for the day. Note that the time interval (daily from midnight to midnight) is not currently configurable and is based on the time zone of the MSE itself, not the time zone of the particular venue.

The MSE enforces quota limits by periodically collecting traffic information from the WLCs for wireless devices which have quota limits set (identified by the MAC address of the device) through the NMSP protocol. Removal of a device from the WLAN is initiated by the MSE authorizing disassociation of the wireless client, also through the NMSP protocol.

Step 8 After authenticating that the end-user logged into the social media site, the CMX Visitor Connect service running within the MSE re-directs the web browser of the mobile device to the original site which the end-user was attempting to reach. Alternatively, CMX Visitor Connect can redirect the web browser of the mobile device to a site pre-determined by the CMX administrator.

Detailed information regarding configuration of the MSE for CMX Visitor Connect is provided in Chapter 27, “Configuring CMX Visitor Connect.”

CMX Visitor Connect is dependent upon the wireless infrastructure design for guest Internet access. B2C Guest Access for CMX Visitor Connect in Chapter 4, “CMX Deployment Models” presents a method of providing guest wireless access using an anchored wireless LAN controller design and discusses an example of the configuration of the Internet Edge ASA security appliance interfaces for supporting CMX Visitor Connect.