CHAPTER 6

CMX Additional Considerations

September 4, 2014

This chapter highlights additional considerations when deploying a CMX solution. This includes how fast location information is updated and made available, considerations around specific mobile device platforms such as Apple IOS 8 devices and some Android devices, considerations around the use of 2.4 and 5 GHZ frequency bands when deploying location services and CMX services, and finally considerations around the deployment of the FastLocate feature.

Currency of Location Information

This section discusses how fast location information is processed by the Cisco Context Aware Service (CAS) and made available to devices.

The default WLC aggregation window of two seconds, discussed in Cisco Context Aware Service (CAS) in Chapter 3, "CMX Solution Components," results in an MSE aggregation window of five seconds. Adding in the time required to calculate the location of the wireless client, send a push notification, and update the location database results in the updated location of the client being available in as much as approximately eight seconds after the client was heard via either Probe Requests or via data packets when using the FastLocate feature.

Adjusting the WLC aggregation window down to one second results in an MSE aggregation window of four seconds. Adding in the time required to calculate the location of the wireless client, send a push notification, and update the location database results in the updated location of the client being available in as much as approximately six seconds after the client was heard via either Probe Requests or via data packets when using the FastLocate feature.

Changing the default WLC aggregation window from two seconds to one second does have implications on the overall scalability of the MSE since it will need to process location information more rapidly. MSE Scalability in Chapter 4, "CMX Deployment Models" discusses the scalability of the MSE.

As discussed in Probe Request RSSI versus FastLocate in Chapter 3, "CMX Solution Components," the frequency of Probe Requests from mobile devices is often non-deterministic and may vary from under a second to five minutes, depending upon various factors. Some mobile device platforms may allow an app developer the ability to generate Probe Requests, via the app, while others may not. The deployment of the FastLocate feature can result in RSSI information being seen from the mobile device in as little as every four to six seconds. However this is only if the mobile device generates packets for every scan cycle of the WSM. This may again require an app running on the mobile device to constantly generate traffic. For unresponsive clients, the Block Acknowledgement Request (BAR) feature of FastLocate may still result in the mobile device being seen, but only every 40 to 60 seconds.

It must be recognized by any app developer that the 6-8 second delay in the availability of location information discussed above must be added to the frequency by which the mobile device generates Probe Requests or generates packets when using the FastLocate feature to understand the total delay in the availability of location information regarding that particular mobile device. In addition, this does not include time required to process any push notifications via an application running on a server or an app running on the mobile device itself. Nor does it include transmission delays in sending the push notification to an application running on a server—which is potentially a cloud service—and updating the mobile device's location as shown on floor map running in an app on the mobile device itself.

A thorough understanding of the total delay in updating the client location is essential for the development of effective apps for purposes such as wayfinding. Turn-by-turn navigation, such as that found in outdoor GPS systems, may not be feasible today given the total delay in updating the client location. Wayfinding apps, which show the location of the wireless device on a floor with an arrow providing directions to the indoor destination and periodically update with the new location of the wireless device, may be feasible today. However integration of wireless location technology with additional location technologies such as Bluetooth Low Energy (BLE) may be possible to provide effective turn-by-turn navigation today.

Apple iOS Version 8 Mobile Devices

As of iOS version 8, Apple changed the way mobile devices send Probe Requests. The basic behavior of Apple iOS 8 devices is that if a device is simply sending Wi-Fi Probe Requests while the mobile device is not being used (for instance the device is in the end user's pocket or purse), it uses a random fake MAC address. However if the device connects (associates) to the Wi-Fi network, it uses its real MAC address for Probe Requests and for sending packets.

This use of multiple MAC addresses for iOS 8 devices may add to the complexity of tracking such devices when using Probe Requests. However the focus of location-based services in general continues to shift toward engaging the visitor directly within the venue via their mobile device. In general engaging the visitor within the venue has shown to provide the greatest business value. This can be accomplished through the installation of an app on the mobile device and getting the device to connect to the Wi-Fi network within the venue. Enhancements such as the Fastlocate feature which allow all packets to be utilized to determine client location are largely unaffected by the changes to iOS8. The use of an app on the mobile device may also provide the end user the opportunity to"opt-in" to the use of location services within a given venue, helping to further alleviate any potential privacy concerns.

CMX Analytics may simply view an iOS 8 device which uses a random "fake" MAC address to generate Probe Requests as another device for dwell time, crowding, and device count analysis. So there are no issues with the random "fake" MAC address by itself. However when an iOS 8 device uses a random "fake" MAC address to generate Probe Requests and subsequently uses its real MAC address when it associates to the WLAN, it may be viewed as two devices with CMX Analytics. Likewise, the iOS 8 device may use a different random "fake" MAC address when visiting the same venue on multiple days, weeks, etc. In both situations analytics data such as dwell times, crowding, and device counts may be slightly skewed due to double counting. Also CMX Analytics may not be able to view a single person returning with the same iOS 8 device, but using a different random "fake" MAC address as a repeat visitor. Hence repeat visitors data may be slightly skewed. However if the device connects to the Wi-Fi network during both visits, it uses its real MAC address again and CMX Analytics is able to view this as a repeat visitor.

Overall, the following considerations must already be kept in mind regarding CMX Analytics deployments even without iOS 8 devices.

- Not everybody carries a mobile device. If you do not carry a mobile device with Wi-Fi connectivity, you are not counted by CMX Analytics. A given venue will likely have no idea how many people visited the venue without a mobile device. As a result, analytics data may already be skewed slightly based on visitors who do not carry a mobile device with Wi-Fi connectivity.
- Not everybody leaves their Wi-Fi on all the time. The behavior of those who carry mobile devices is often influenced by their cellular data plan. Those with limited voice, but unlimited data plans, may not enable Wi-Fi connectivity since the data transfer through the cellular network has already been paid for. Those with unlimited voice, but limited data plans, may enable Wi-Fi connectivity since the Wi-Fi network may offer a means of accessing the Internet for "free" without having to use their data plan. If you carry a mobile device, but your Wi-Fi is off, you are not counted by CMX Analytics. A given venue will likely have no idea how many people who visited the venue left their Wi-Fi off. As a result, the analytics data may again be skewed slightly.
- Some visitors to a venue may carry multiple mobile devices, each with Wi-Fi connectivity. These visitors are double counted because there is no concept of a single person carrying two or more devices within CMX Analytics. A given venue will likely have no idea how many people who visited were carrying multiple mobile devices. As a result, the analytics data may be skewed slightly.
- If you change out your mobile device—which for the general population is constantly happening since new models are coming out weekly—you end up with a different MAC address which will appear as a different device. So any analytics data regarding repeat visitors may already be skewed slightly due to repeat visitors changing mobile devices over time and the analytics data may be more and more skewed as the timeframe over which you are viewing repeat visitors increases.
- If your battery drops below a certain threshold, your mobile device may not send active Probes at all and you are not counted. A venue will likely have no idea how many visitors had low battery levels and therefore did not send Probe Requests. As a result, the analytics data may be slightly skewed.

The point of this discussion is that analytics data may already be slightly skewed based upon various factors. iOS 8 may be just one additional factor which may skew analytics data slightly more. Just how much further depends upon how many visitors to the venue are carrying iOS 8 mobile devices, whether their Wi-Fi is on, and whether they are connected to Wi-Fi network within the venue. What CMX Analytics provides is the ability to collect information regarding the behavior of a sample of the larger population who visit a venue with the assumption that the behavior of the overall population of visitors is consistent with the sample. Further, CMX Analytics may provide only one of perhaps many data points about customers' behavior within a venue. Other data points can include direct feedback from staff, sales data, etc. All the data points may be slightly skewed in one way or another. However CMX Analytics may help the venue operator spot trends which can then be acted upon to provide better service to the visitors to the venue.

Android Mobile Devices

Some mobile devices which run the Android operating system do not generate Probe Requests on 5 GHz Wi-Fi channels which are subject to Dynamic Frequency Selection (DFS). DFS is required by the United States FCC in the U-NII-2 band (channels 52-64, 100-116, and 132-140). Access Points operating on any of these channels may not see Probe Requests from Android devices. Hence location accuracy may be degraded if there are insufficient APs running on non-UNII-2 channels operating to accurately calculate the location of Android devices using only Probe RSSI. Analytics data, which is based upon the location database, may also be slightly skewed because of this.

The network administrator may simply choose to disable U-NII-2 channels on APs via the WLC configuration. However this may reduce the number of available channels in the 5 GHz spectrum from 21 channels to 9 channels when implementing a 20 MHz channel within the U.S. regulatory domain. Similar results may be seen in other regulatory domains. The number of individual channels is further reduced when implementing 40 MHz channels.

In large venues with multiple access points, this may result in the network administrator having to re-use 5 GHz channels. This could result in higher co-channel interference (CCI), reducing the effective throughput of the WLAN. Hence the network administrator must balance location considerations with channel selection and channel width for the optimal solution for the particular venue.

2.4 GHz vs. 5 GHz Mobile Devices

Not all mobile devices support both the 2.4 GHz and 5 GHz frequencies. In particular, some older mobile devices support only 2.4 GHz frequencies. Hence when deploying a WLAN for location services within a given venue, it is recommended to deploy the WLAN using both 2.4 GHz and 5 GHz frequency bands. This ensures that devices which operate only in the 2.4 GHz frequency band are seen and location can be calculated for these devices. Since CMX Analytics pulls information from the MSE location database, this helps to optimize analytics data as well.

FastLocate Deployment Restrictions

The initial version of FastLocate supported has several deployment restrictions.

The FastLocate feature is a global parameter configured on CUWN (AireOS) wireless LAN controllers running software version 8.0. MSE software version 8.0 is also required. The only access points which support FastLocate are the modular Cisco 3600 and 3700 Series APs with Wireless Security Modules (WSMs) installed. The Cisco 3600 and 3700 Series APs also support direct time synchronization via NTP, required for FastLocate to operate. Wireless clients must be connected to the WLAN in order to generate data packets for FastLocate. The APs with WSMs must also handle wireless client traffic.

The MSE is capable of processing RSSI from probe requests as well as data packets. When other (older or non-modular) APs are mixed with Cisco 3600 or 3700 Series APs with WSM modules, the MSE will receive RSSI information from both data packets and probe requests. The MSE supports this deployment, but care needs to be exercised in implementing this type of deployment.

- Best results are achieved when all APs are Cisco 3600 or 3700 Series APs with WSM modules.
- If APs have to be mixed, it helps to achieve some separation between APs capable of processing RSSI from probe requests only and APs capable of processing RSSI from FastLocate (Data RSSI). One way of doing this is using different floors.
- If APs have to be mixed on the same floor try to have zones defined where location refresh requirements are more stringent and other zones that have lower location refresh requirements.
- Do not mix APs in a manner such that every other AP or every 5th AP in the zone is a Cisco 3600 or 3700 Series with a WSM module capable of FastLocate. This could result in unpredictable location results.

FastLocate is currently not supported for FlexConnect deployments with CUWN (AireOS) wireless LAN controllers running software version 8.0.100 and MSE software version 8.0.100.

Given the restrictions discussed above, the following are suggestions as to the possible deployment of FastLocate for location (CAS) services.

- FastLocate is currently not an option for small branches using FlexConnect as shown in Topology #3 in Figure 4-1.
- FastLocate may be a good choice for new standalone sites such as small campuses and large branches which have their own dedicated MSE, WLC, and APs onsite, as shown in Topology #1 in Figure 4-1. In such deployments, it is recommended to deploy Cisco 3700 series APs, since these access points support 802.11ac as well as the WSM module.
- FastLocate may also be a good choice for existing standalone sites such as small campuses and large branches which have their own dedicated MSE, WLC, and APs onsite. In this type of deployment, it may be possible to upgrade all of the access points to Cisco 3600 or 3700 Series APs with WSM modules before implementing location (CAS) services. Again, it is recommended to upgrade to Cisco 3700 series APs, since these access points support 802.11ac as well as the WSM module.
- For standalone sites such as larger campuses with multiple buildings which also have their own dedicated MSE, WLC, and APs onsite, upgrading all of the access points to Cisco 3600 or 3700 Series APs with WSM modules before implementing location (CAS) services may not be feasible due to the amount of time it would take to upgrade all access points in every campus building. Such deployments may also be implementing location (CAS) services through Probe Request RSSI already. As individual floors within the buildings are upgraded to Cisco 3600 or 3700 Series APs with WSM modules, FastLocate may be utilized on a floor-by-floor basis. Again, it is recommended to upgrade to Cisco 3700 series APs since they support 802.11ac as well as the WSM module.