



8.0 Delta - MSE

James Noxon

Technical Marketing Engineer
Enterprise Networking Market Strategy

August 2014

Agenda

- FastLocate (Packet RSSI Location)
- Presence Analytics
- Visitor Connect Updates
- Facebook for Wi-Fi
- CMX SDK overview

FastLocate

Using Network Data Packet RSSI to perform the location calculation

Location Using Mobile Device Probing

Is delivering diminishing returns

OLD WAY

- Relied Purely on Mobile Devices Probing an Access Point (AP)
 - Sent on most channels - received by neighbor APs on different channels
 - Good for location estimation

WHY IT WILL NOT CONTINUE TO WORK

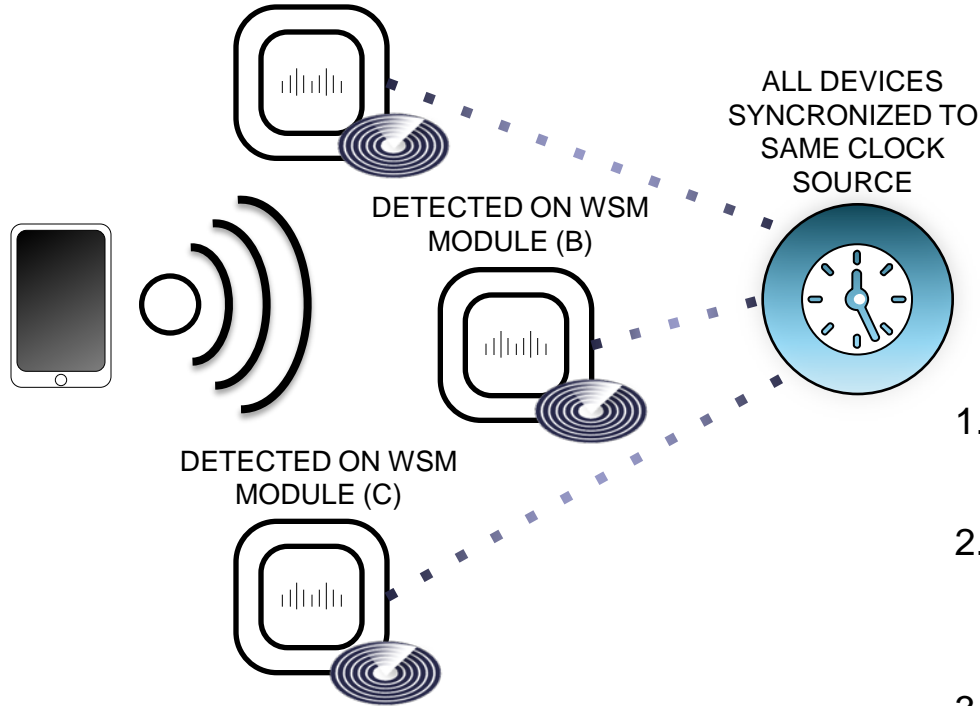
- Client Probing Frequency is Reducing
 - Updates vary from <1 sec to 5 mins depending on:
 - Client
 - OS
 - Driver
 - Battery
 - Current client activity
 - Other
 - Not enough Data Points to accurately represent real-world movement

NEW WAY

- Supplement Mobile Probing with All Network Packets for Higher Location Resolution
 - Initiated by Network – Available More Frequently
 - Provides More Data Points to Accurately Represent End-User Activity
 - Device Agnostic – Consistent Across devices and works even when device is sleeping

So we are Adding More Opportunities

By using RSSI from data packets captured by WSM modules



Synchronization is essential to correlate when a packet is heard across multiple APs.

To achieve this synch, the WLC will push NTP configuration to the APs when FastLocate is enabled.

1. Associated devices send packets for regular data access only to connected access points (A)
2. Other APs (B,C) that “hear” that MAC address talking to associated AP can report on signal strength to WLC/MSE
3. Block Acknowledgement requests are used for quiet devices

The Advantage of Packet RSSI Location

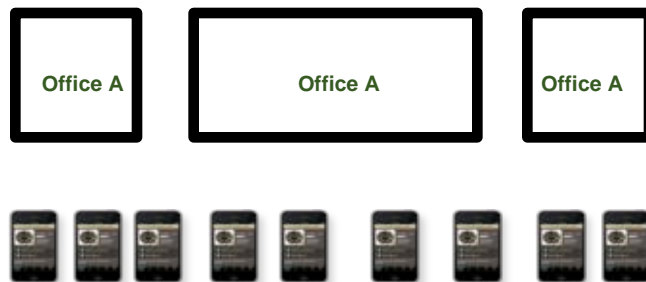
RSSI measurements available with greater frequency

Probe packets based location
calculates on average 2
locations per minute



Probe occurs every 30 Seconds

With FastLocate location can be
calculated on average 9 times
per minute with an active
network packet exchange



FastLocate location updates about every 6 seconds

Note: Current testing is showing that in reality we see location updates on average of approximately every 15 seconds, but engineering is still working on better optimization.

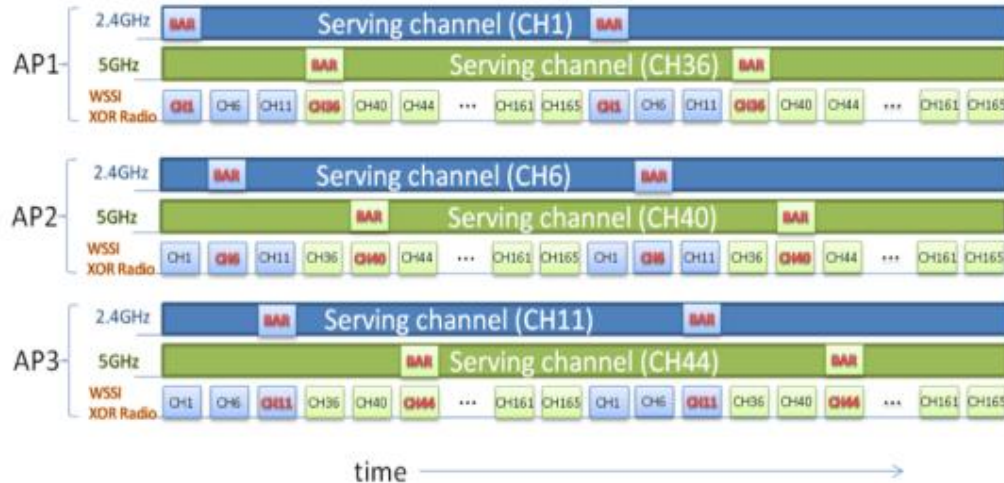
Block Acknowledgement Request (BAR)

Used to help a client generate a network packet

- The client may send periodic packets for ongoing data sessions, which can also be used for RSSI measurements.
 - But in the case where the associated client is quiet for an extended period and the packet RSSI statistics are stale, the APs may help the client generate packets to freshen the RSSI statistics.
- For each associated client keep a counter of complete WSM channel scan cycles since the last RSSI update
 - Reset the counter to 0 each time a packet RSSI update is received from the WSM module
 - If counter is ≥ 10 (**default threshold trigger**) then schedule a BAR during the off channel scan, and reduce the counter to 8 (**default threshold reset value**)
- BAR will be sent after a fixed delay from the start of the scan of the servicing channel

FastLocate Scanning Cycle

Scanning without CleanAir

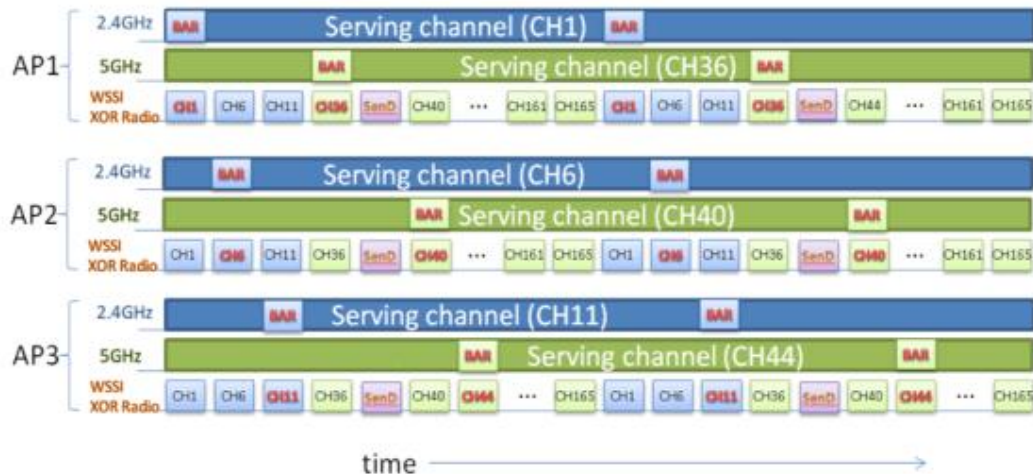


- When a client is constantly sending packets on a channel, network will get a packet **EVERY 4 seconds (250ms x 16 channels)** and be able to gather values once every 4 seconds.
- Location is calculated approximately **1 every 8 seconds. (~8 times per Minute)**

All APs are synchronized via NTP to +/- 10 milliseconds

FastLocate Scanning Cycle (Cont.)

Scanning with CleanAir



- With CleanAir enabled a time slot is yielded in the module for CleanAir.
- The goal is to provide 14.5% for NOS
 - So when using 250ms dwells we will yield a 175ms slot after each fourth channel scanned ($4 \times 250 + 175$)

All APs are synchronized via NTP to +/- 10 milliseconds

FastLocate Deployment Restrictions

- Requires WLC 8.0 / MSE 8.0 / PI 2.1.x
 - Because new AP image is bundled only in WLC for NTP clock sync functionality on AP
- **No Mixed mode support in first version** - ALL APs must support the NTP IOS module
 - A pure monitor mode deployment will not be supported in this release
 - All APs must be AP3600 / 3700 with Wireless Security modules (WSM) (1:1)
- MSE treats Packet RSSI values the same as Probe Packet RSSI values
 - The overall location calculation algorithm is slightly more complex than previous versions
 - However, you cannot mix Probe and FastLocate data points on the MSE
 - Although Security monitoring can be done simultaneously with FastLocate
- FastLocate has no impact on UNASSOCIATED devices

FastLocate *aka* Packet RSSI Location

Wireless LAN Controller CLI configuration

```
(LaRes1) >config advanced 802.11-abgn pak-rssi-location ?
```

`enable` enable pak-rssi-location on all APs.

`disable` disable pak-rssi-location on all APs.

`threshold` PRL threshold in dbm valid range -50 to -100.Default value is -100

`trigger-threshold` PRL trigger threshold in dbm valid range 1 to 100.

`reset-threshold` PRL reset threshold in dbm valid range 0 to (trigger-threshold-1).

`ntp` PRL NTP Server IP address.Default is the NTP server configured for the WLC

FastLocate, aka Packet RSSI Location

Wireless LAN Controller GUI configuration

- FastLocate is enabled globally under **WIRELESS > Global Configuration**

The screenshot shows the Cisco Wireless LAN Controller GUI. The main navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'WIRELESS' tab is selected, and the 'Global Configuration' page is displayed. The 'Packet RSSI Location' section is highlighted with a red box, and the 'NTP Server' field is highlighted with a black box. The 'NTP Server' field contains the value '172.16.0.1'. A blue arrow points from the text 'Configuration settings are located in the bottom right corner of screen' to the 'Packet RSSI Location' section. Another blue arrow points from the text 'The default is the NTP server for the WLC if no other NTP server address is entered' to the 'NTP Server' field.

Configuration settings are located in the bottom right corner of screen

The default is the NTP server for the WLC if no other NTP server address is entered

Packet RSSI Location Config Parameters³

Enable Packet RSSI Location	<input checked="" type="checkbox"/>
Packet Detection RSSI Minimum (dBm)	-100
Scan Count Threshold for Min. Client Detection (dBm)	10
NTP Server	172.16.0.1

1. Flexconnect Ethernet fallback config parameters are not applicable to APs having multiple ethernet ports.
2. Telnet/SSH can be enabled in APs with non-default credentials only.
3. Packet RSSI Location config parameters are applicable only to 3602/3700 APs with WSSI module.

Once **enabled** the WLC will push NTP configuration to all APs with WSSI modules installed and **stop sending** regular WLC time update messages to these APs

Presence Analytics

Presence Analytics

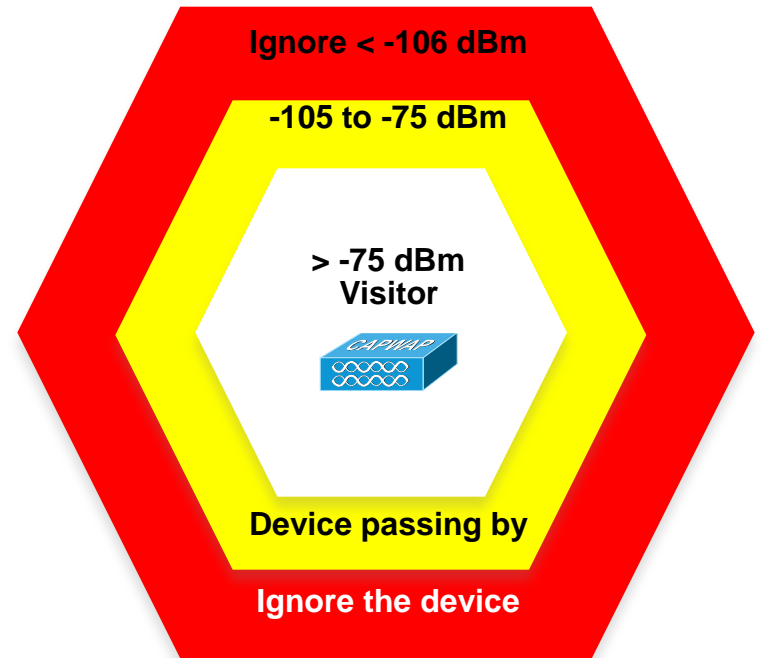
When simply knowing a device is within range is enough

- In many customer deployments there are only a couple of APs in each location, which makes it impossible to use a triangulated location computation.
 - However, users can still leverage Wi-Fi technology to better understand foot traffic pattern and behavior from presence analytics.
- CMX Presence uses RSSI, signal strength of client device, along with duration of high signal strength to determine whether a client device is in the site or just passing by.

Algorithm Used in Presence Analytics

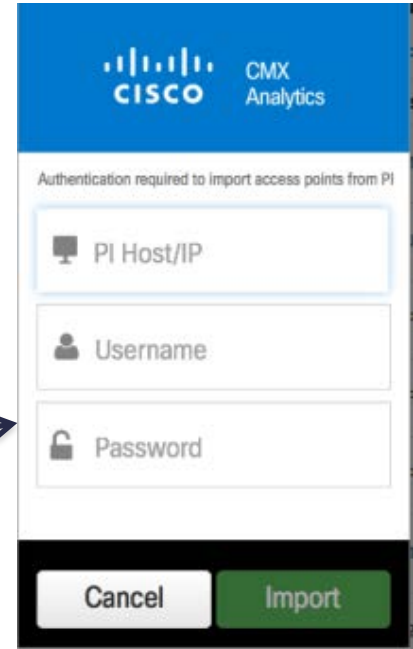
Using RSSI you can determine if a device is inside or outside of a venue

- There are two RSSI threshold values defined for a site, low (-105 dBm default) and high (75 dBm default).
- Clients with RSSI below the low threshold (-105 dBm default) are discarded.
- Clients with RSSI above the low threshold are classified as “passer-by”.
- Clients with RSSI above high threshold over X minutes (default 5) in past Y minutes (default to 15) are classified as visitors.
- Clients with RSSI above high threshold minus 5 in sessions maintain sessions.
- Clients associated with AP in a site are classified as visitors at the site.



How is Presence Analytics Different

- PI is synced with WLC and gathers list of Access Points
 - **These APs do not need to be placed on a map**
- Other maps can co-exist on MSE
- AP information for CMX Analytics can be configured in two ways:
 - Manually import list of APs from a CSV file (from PI or manually generated list)
 - Give credentials of PI and poll AP list
- 3000 sites can be supported (at least 1 AP per site)

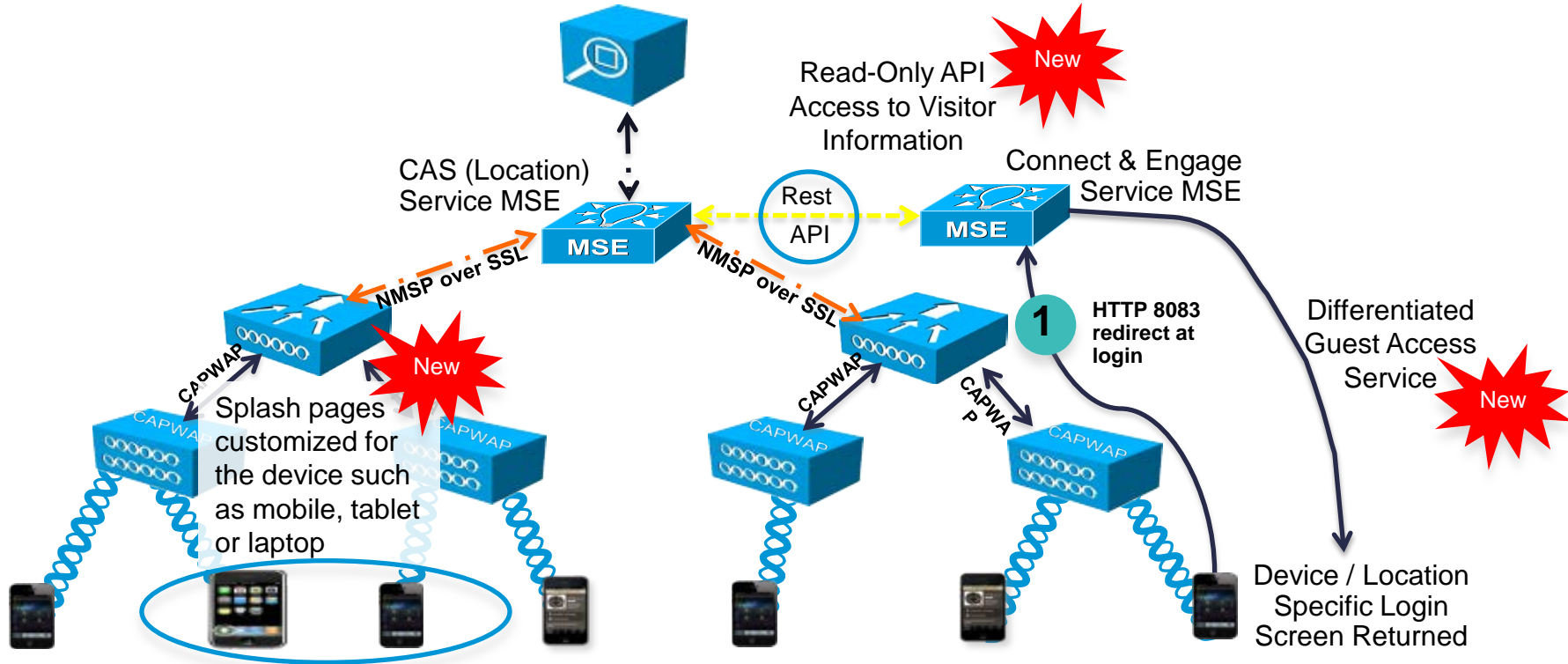


The screenshot shows the CMX Analytics interface. At the top, there is a blue header with the Cisco logo and 'CMX Analytics'. Below the header, a message reads 'Authentication required to import access points from PI'. The form contains three input fields: 'PI Host/IP' with a server icon, 'Username' with a person icon, and 'Password' with a lock icon. At the bottom of the form, there are two buttons: a white 'Cancel' button and a green 'Import' button. An arrow from the text 'Give credentials of PI and poll AP list' in the list points to the form.

Visitor Connect Updates in 8.0

Visitor Connect

8.0 brings a scalable and customizable guest portal





Location-Specific Guest Access

Shopping Mall

Your Name*

Your Phone Number*

Terms and Conditions: [-]

Welcome to the wireless high-speed Internet access system ("Wi-Fi System") at Bao Networks ("BAO"). These "Terms and Conditions of Use", govern your rights and responsibilities and our rights and responsibilities relating to the use of the Wi-Fi System at BAO.

Acceptance of Terms and Conditions of Use
BY CLICKING ON "Logon" ON THE WI-FI SYSTEM SIGN-UP PAGE, YOU REPRESENT THAT:

By clicking Submit, I accept the Terms & Conditions

Submit

**TERMS AND CONDITIONS;
REGISTRATION**

Skip Ad in 8 seconds

5/12/14 - 6/30/14 - SOCIAL COUPON PAGE

2 DAYS ONLY!
\$10 OFF
your purchases of \$25 or more
Friday, May 3, through Saturday, May 4

OFFER CODE: 8W22Z

MC44985200G200000056210

©2014 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

**CUSTOM LANDING
PAGE/VIDEO**

Sign in with Social Networks

Login with Facebook

Login with LinkedIn

Login with Google

No thanks. Continue browsing >>

Powered by Cisco CMX

**SIMPLIFIED SOCIAL
LOGIN**

Customizable Captive Portal

- Often really small visual elements are to read and/or click on when using devices with smaller screens
 - Most customers' use cases are focused on mobile phones and tablets
- In 8.0 the HTML and CSS code was rewritten from the ground up
- Tailored to mobile devices first and foremost
 - Then use CSS Media queries to apply further components to the view or change sizing of elements on screen as screen size gets bigger (for tablets and PC browsers)

8.0 Brings Quota Limiting

- Visitor Connect has two new system-created User Groups, “SOCIAL” and “BASIC” with usage limit as “0” MB (which means usage not tracked) by default
 - Admins can change the usage limits, but not the names
- When usage limits are changed
 - New logins will have the limits applied
 - Existing sessions will not have new limits applied until they re-login
- When redirected to Visitor Connect splash pages, the user is given an option to log in with social network credentials
 - Placed into the “SOCIAL” group if social network credentials are used
 - Placed into the “BASIC” group if no social credentials are used

Quota Limit Implementation

- Upon successful login, the usage limit and mac address will be sent from Visitor Connect to MSE LOC via calling REST API
- MSE LOC categorizes clients into types:
 - Usage limit = 0, MSE LOC does not check usage against the limit
 - Usage limit > 0, MSE LOC checks usage against the limit for visitors with usage limit
- MSE LOC module calculates the last 24 hours (midnight to midnight) usage based on traffic statistic history
 - MSE LOC module is enhanced with a background thread whose job is to check network usage for each type of client against the set limit

Quota Limit Implementation (Cont.)

- When client usage is over the limit, MSE LOC sends NMSP message to WLC to de-authenticate the client
 - MSE LOC receives the NMSP response message and stores the result for each client
 - When user tries to connect again, user will be redirected to Visitor Connect portal
- Visitor Connect first checks whether it is a new user in last 24 hours
 - If new user not checked for usage limit
 - If existing user Visitor Connect will use REST API to query MSE LOC to check for usage in the last 24 hours
 - If quota exceeded user is notified via message on the splash screen

Configuring Visitor Connect

The screenshot displays the 'CMX Connect & Engage' interface. The main content area is titled 'Splash Template Configuration' and shows a four-step process for creating a splash template:

- STEP 1: Create Template Name** - If you would like to collect information from your visitors.
- STEP 2: Create Social Connections** - If you would like to offer Social Network. Address visitors such as Facebook, LinkedIn, and LinkedIn.
- STEP 3: Create Splash Template** - In the table below and attach Template Fields and/or Social Connections to them.
- STEP 4: Assign the Splash Template** - In one or more locations inside your...

Below the steps, it states: 'The first Splash Template you create will be your Default Template. When determining which Splash Template to use, MSE will select the template belonging to the location of the visitor's gateway that the guest user is in. If your location does not have a Splash Template, MSE will look for that location's parent for a Splash Template instead, meaning it would work properly reaching the Default Template. The hierarchy is Zone > Floor > Venue > Campus. You can change the Default Template designation in the table below.'

The table below shows the configured splash templates:

Name	Default Template	Template	Location	Design
Any location		N/A	N/A	N/A
Splash Template (Template #1)	Yes	N/A	N/A	N/A
The Site		N/A	N/A	N/A

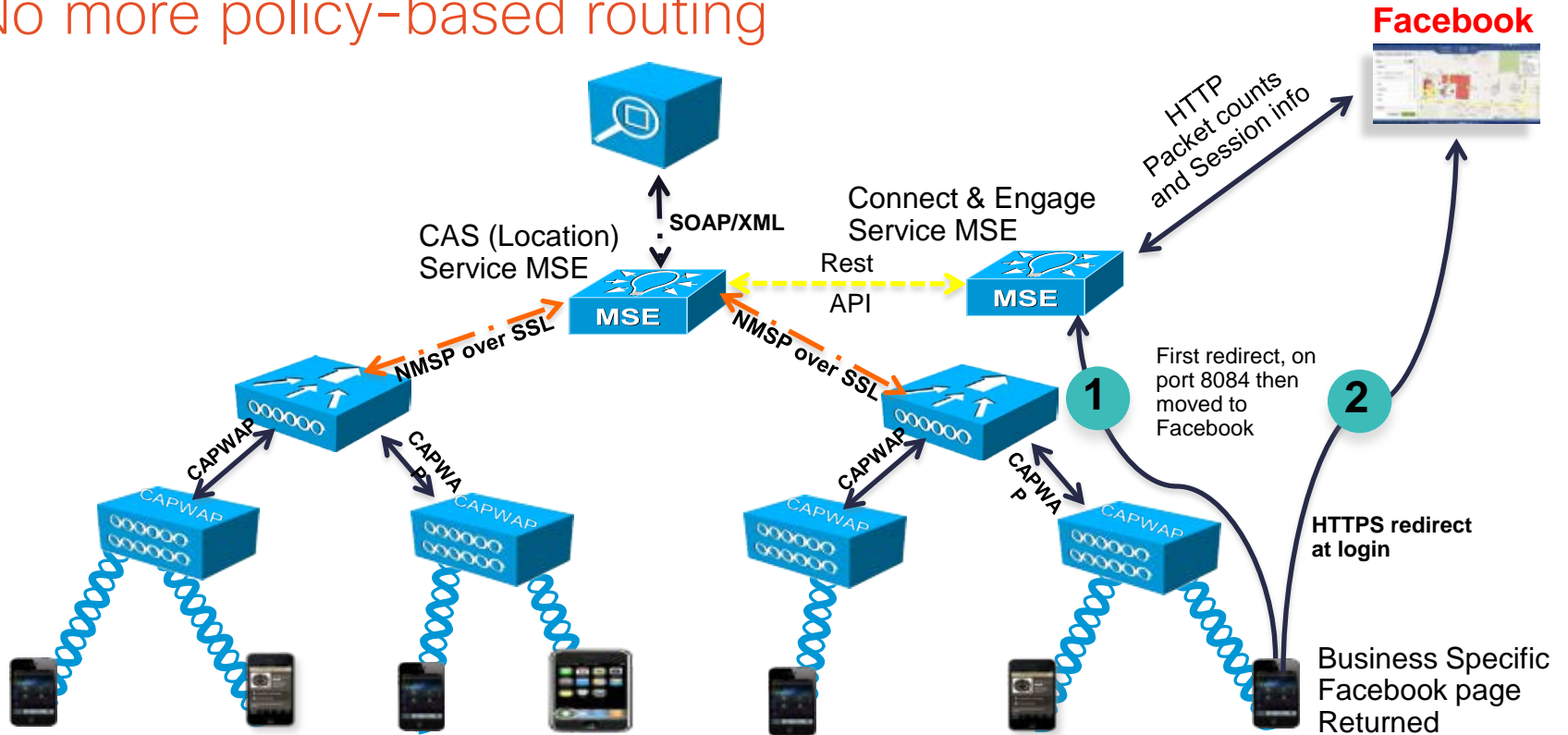
In MSE 8.0 we have dramatically simplified how Visitor Connect is configured. The user only needs to configure items to be collected (i.e., email and name) and zones that this template will be used at. First template will be default for all locations.

Visitor Connect is not supported in IOS-XE 3.6 release

CMX Facebook for Wi-Fi in 8.0

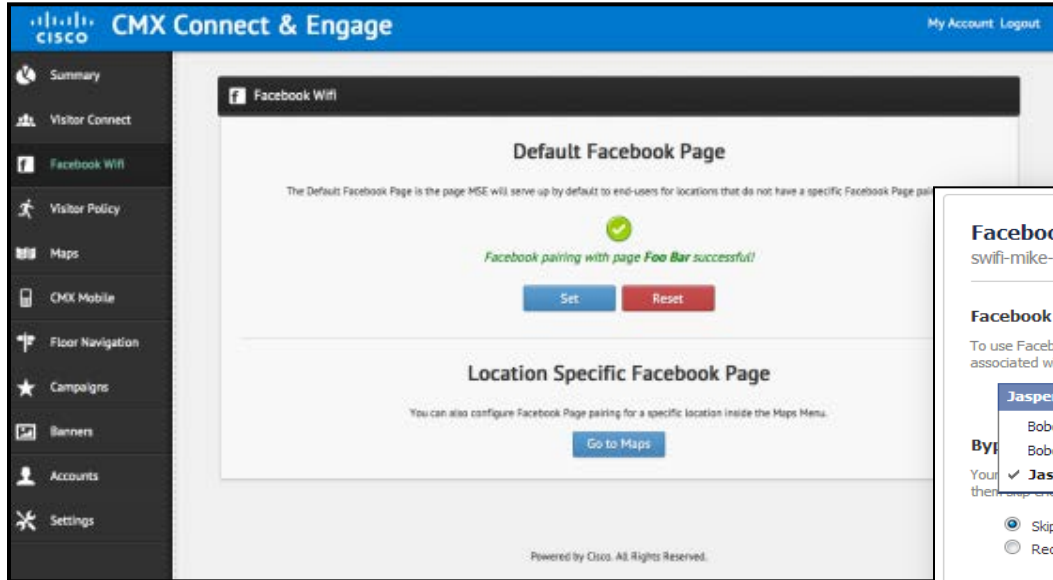
CMX Facebook Wi-Fi

No more policy-based routing



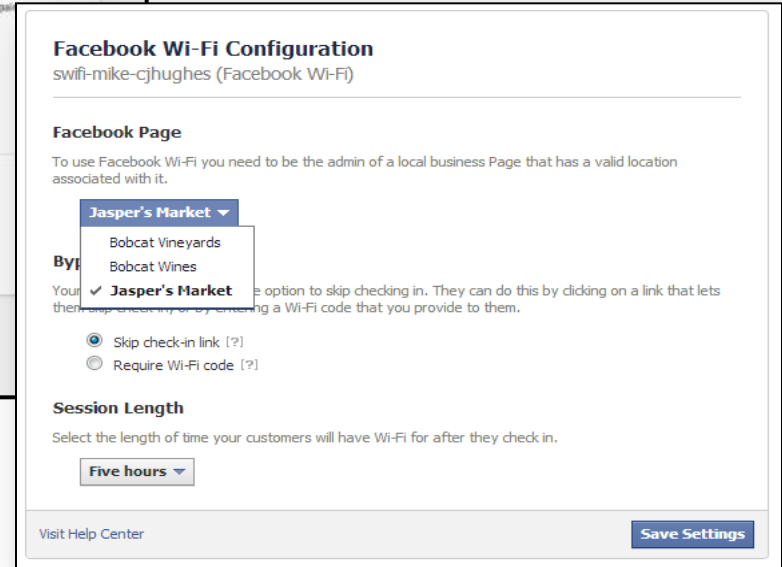
CMX Facebook Wi-Fi

Facebook Wi-Fi configuration: pairing a Facebook page



3. Configure Facebook Wi-Fi parameters.

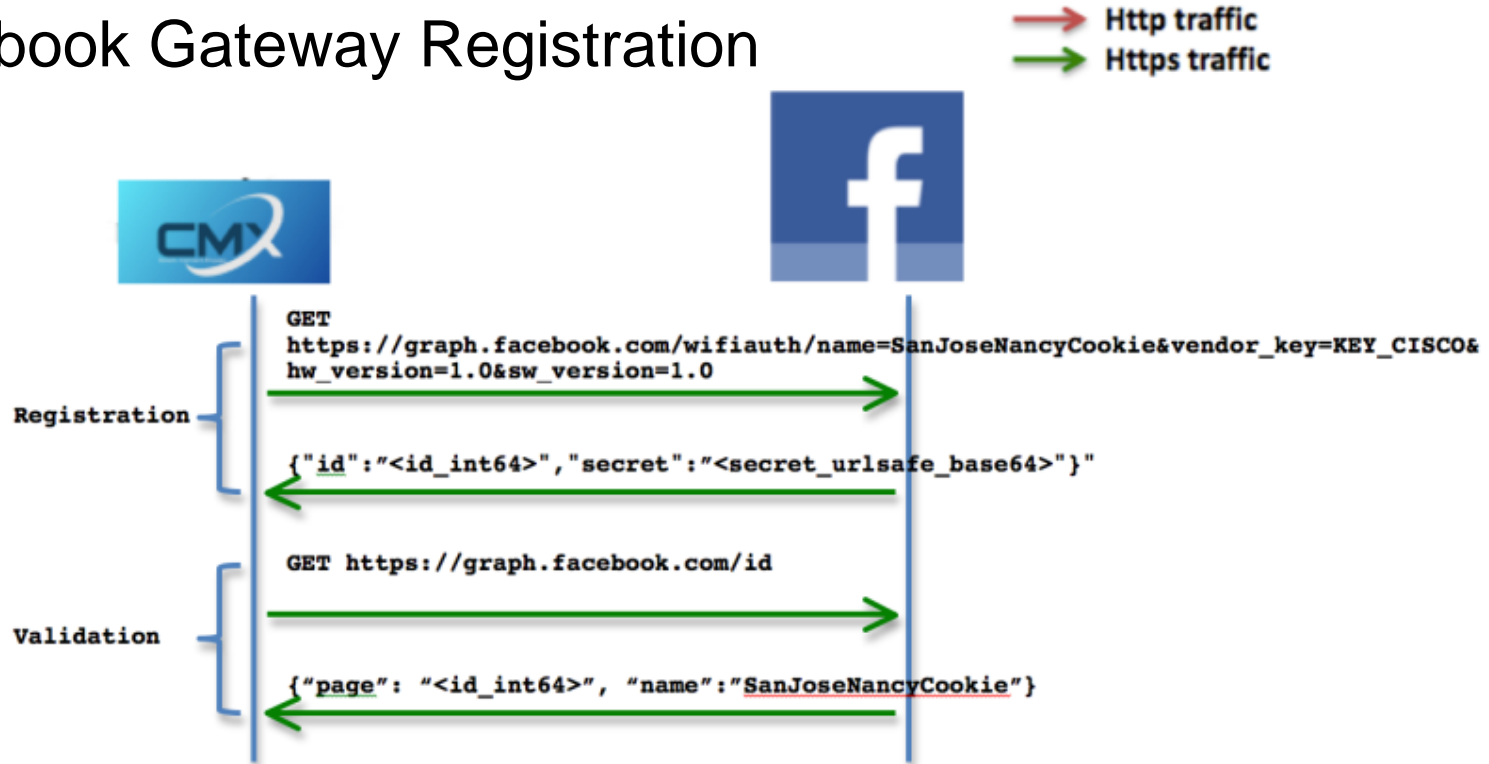
1. Open the Connect & Engage Dashboard.
2. Select Facebook Wi-Fi.



CMX Facebook Wi-Fi

Allows use of the Facebook page as the Wi-Fi captive page

Facebook Gateway Registration



CMX Facebook Wi-Fi

Facebook Wi-Fi configuration: location-specific Facebook page

The image displays two screenshots from the CMX Connect & Engage interface, illustrating the steps to configure a location-specific Facebook page.

Step 1: Navigate to Location. (Indicated by a red box around the 'Pair with Facebook' button in the right screenshot).

Step 2: Select Location. (Indicated by a red box around the 'Floor' selection in the left screenshot).

Step 3: Pair location with Facebook page. (Indicated by a red box around the 'Pair with Facebook' button in the left screenshot).

Step 4: Submit. (Indicated by a red box around the 'Submit' button in the left screenshot).

CMX Guest Onboarding

Capacity guidelines

- Logins per second:
 - **Visitor Connect (benchmark):** Concurrent Login Rate of **45 logins / sec**
 - 401 page to user if limit is exceeded and they need to retry
 - **Facebook (benchmark):** Concurrent Login Rate of **500 logins / sec**
 - 401 page to user if limit is exceeded and they need to retry
- MSE user DB stores last 50,000 MAC addresses that have logged on for authentications (every user creates entry), purged after 160 days (configurable)
 - Cisco recommends separating guest authentication and CAS services on separate MSEs when the number of users exceeds 10,000

CMX Mobile App Server

New CMX Components Delivered in 8.0

TAC Supported

CMX Mobile App Server

Use

- Registers mobile clients with CMX Mobile SDK
- Delivers current location, maps with points of interest, zone. Push Notification to Mobile Apps
- Brokers MAC address resolution for iOS7 devices

Supported by DEV Net Only

CMX Mobile SDK

Use

- Accelerates location-aware Mobile App development on iOS and Android platforms
- Rich libraries support getting current position - (x,y), (lat, long) on a map
- Help mobile app users to connect to the correct Wi-Fi

CMX Sim

Use

- No MSE, no WLC, no APs – no problem
- Enables CMX Mobile App development **without** requiring the infrastructure
- Simulates movement along a pre-defined route or manual movement

CMX Mobile App Server

Installation and upgrade

- Software is distributed as RPM image for Linux, which can be installed on the latest Redhat or Fedora Linux servers. Requirement is Dual Core with 8G RAM for 5000 active app users.
- To install, run the command:
 - `rpm -iv cmx-mobile-app-server-0.version.x86_64.rpm`
- RPM supports upgrade by running the command:
 - `rpm -Uv cmx-mobile-app-server-0.version.x86_64.rpm`
- Version number of rpm can be determined by running the command:
 - `rpm -qi cmx-mobile-app-server`
- Configure Mobile App Server port (8082 default), communication credentials (username and password) using setup menu: `/opt/cmx-mobile-app-server/setup/setup.sh` (to set the username and password)

CMX Mobile App Server

MSE service requirements

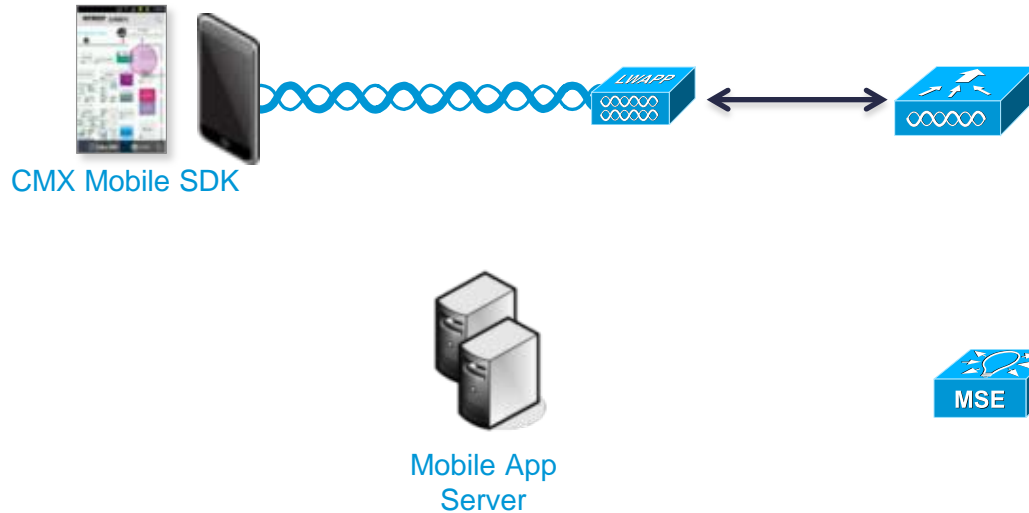
- On MSE do the following:
 - Enable 2 services: 1) Connect & Engage, and 2) CAS services
 - Settings->Connect & Engage -> Setup in the MSE UI and configure the Mobile App server as a destination for location updates
 - Connect and Engage -> Click on Points of Interest -> update floor maps and setup banners and campaigns for push notifications on MSE

Mobile App Server Running

- Starting/Stopping server
 - /etc/init.d/cmx-mobile-app-server start
 - /etc/init.d/cmx-mobile-app-server stop
 - Starts up immediately after a reboot
- Status
 - /etc/init.d/cmx-mobile-app-server status

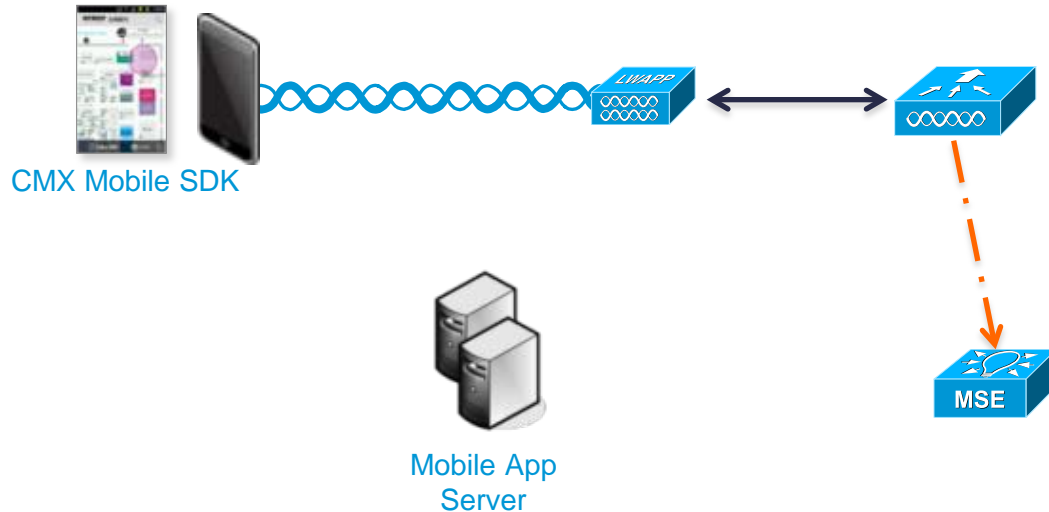
```
{Fri May 9 18:58:32 PST 2014} Getting status of CMX Mobile App Server ...
{Fri May 9 18:58:32 PST 2014} --CMX Mobile App Server Redis service      : RUNNING
{Fri May 9 18:58:32 PST 2014} --CMX Mobile App Server Apache service   : RUNNING
{Fri May 9 18:58:32 PST 2014} --CMX Mobile App Server Apache SDK service : NOT ENABLED
{Fri May 9 18:58:32 PST 2014} Completed getting status of CMX Mobile App Server ...
```

Workaround for iOS7



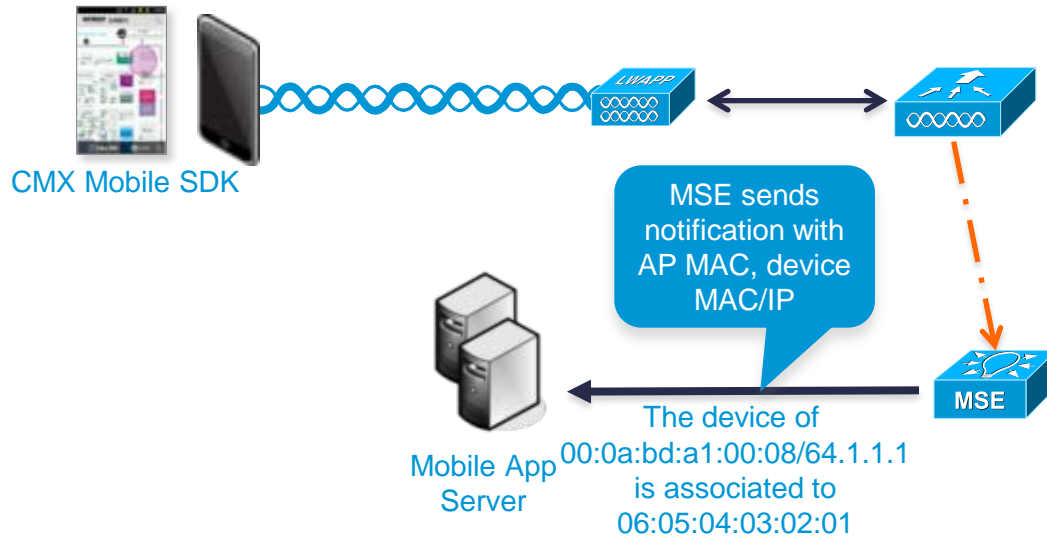
1. Mobile device needs to associate with Cisco Wi-Fi network running with MSE

Workaround for iOS7



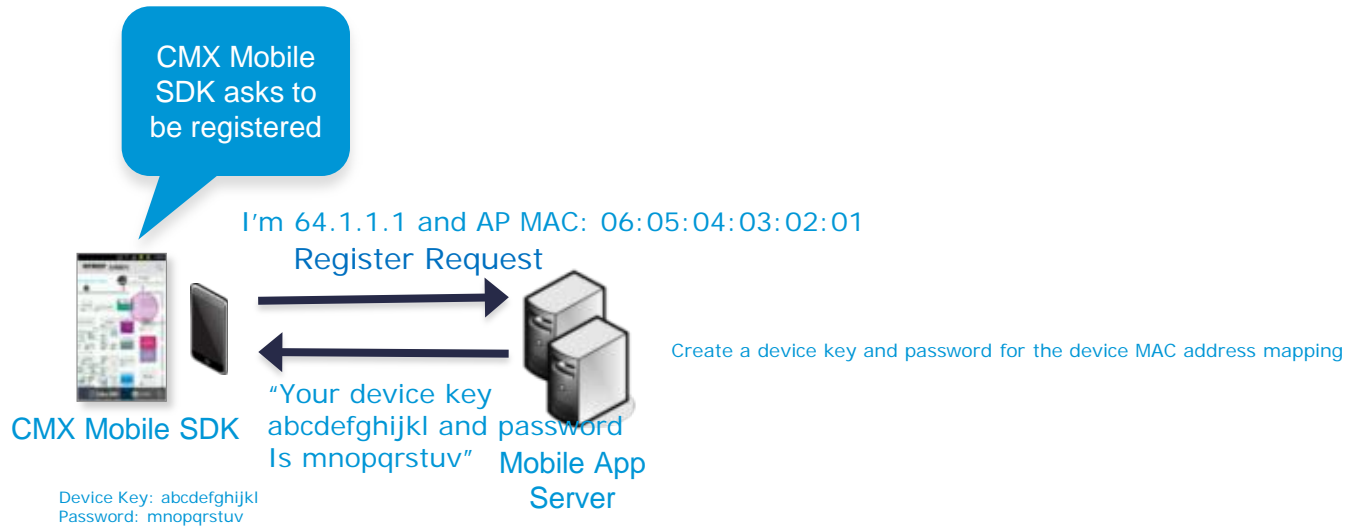
2. Through NMSPEX exchanges, MSE notices the device is associated

Workaround for iOS7



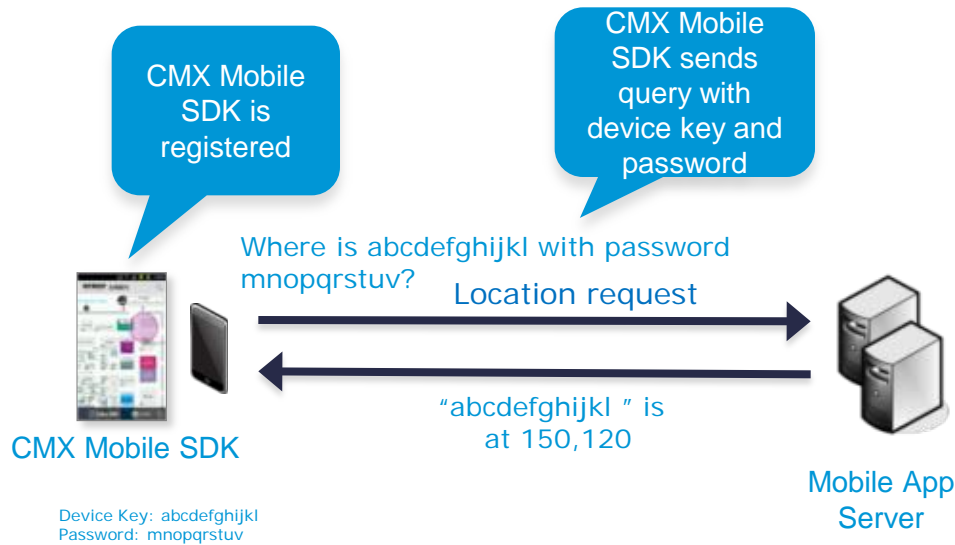
3. MSE sends notification to Mobile App Server with AP MAC, device IP, and device MAC

Workaround for iOS7



4. CMX Mobile SDK asks Mobile App Server to register with its IP address and AP MAC. Responds with device key and password.

Workaround for iOS7



5. Now the CMX Mobile SDK is registered.
The location can be requested using device key and password.

SDK – Reference Only

CMX SDK



CMX Connect SDK consists of:

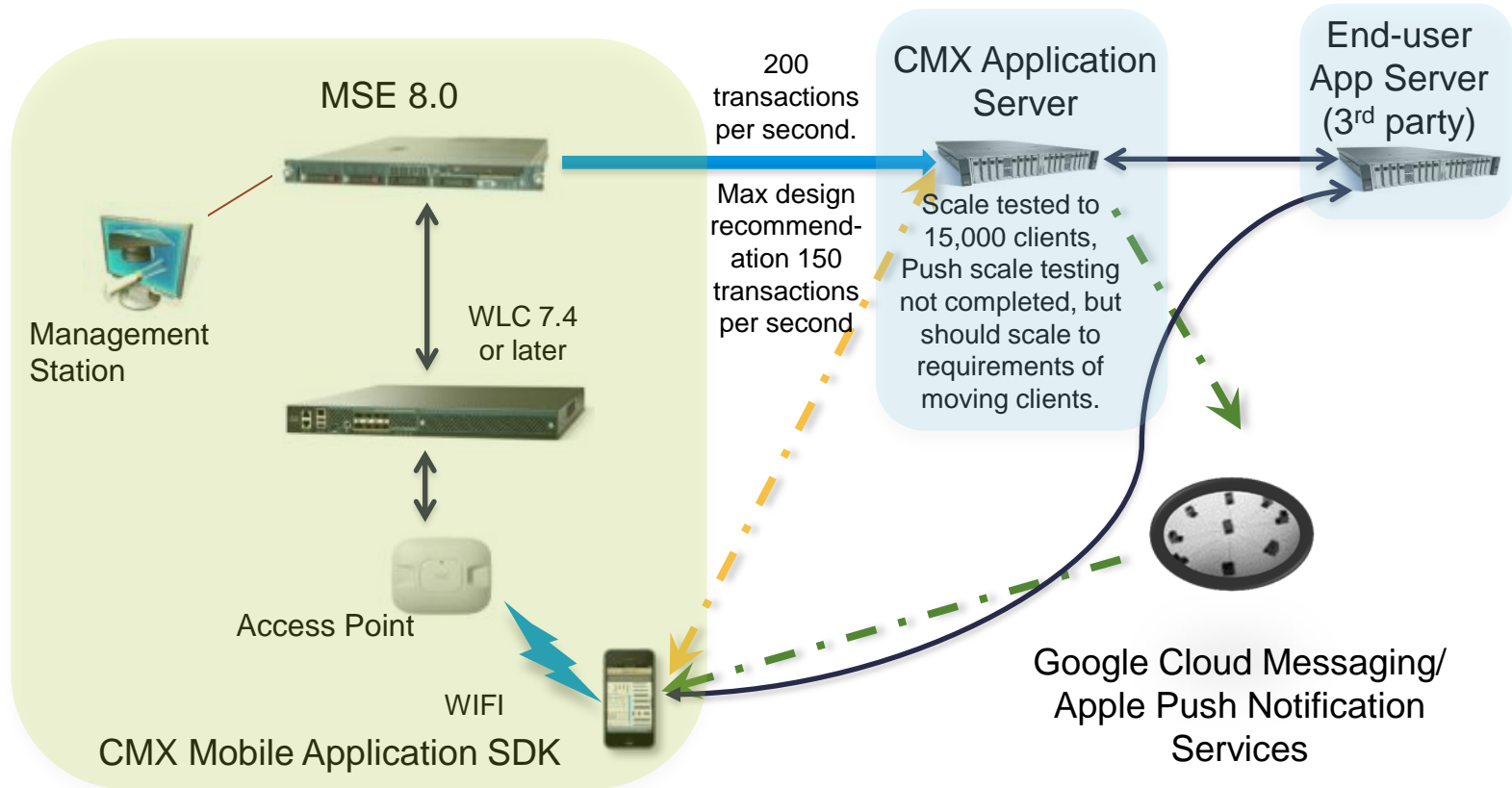
- Android SDK and sample app
- iPhone SDK and sample app
- Cisco CMX Application Server SDK

What Does the CMX App SDK Provide?

- App SDK is part of the overall **CMX Engage** strategy
- App SDK leverages CMX's location capability to provide indoor "find me" capabilities and other app-enabled services
- It is a software development kit (client side and server side) for iOS and Android platforms



CMX SDK Architecture

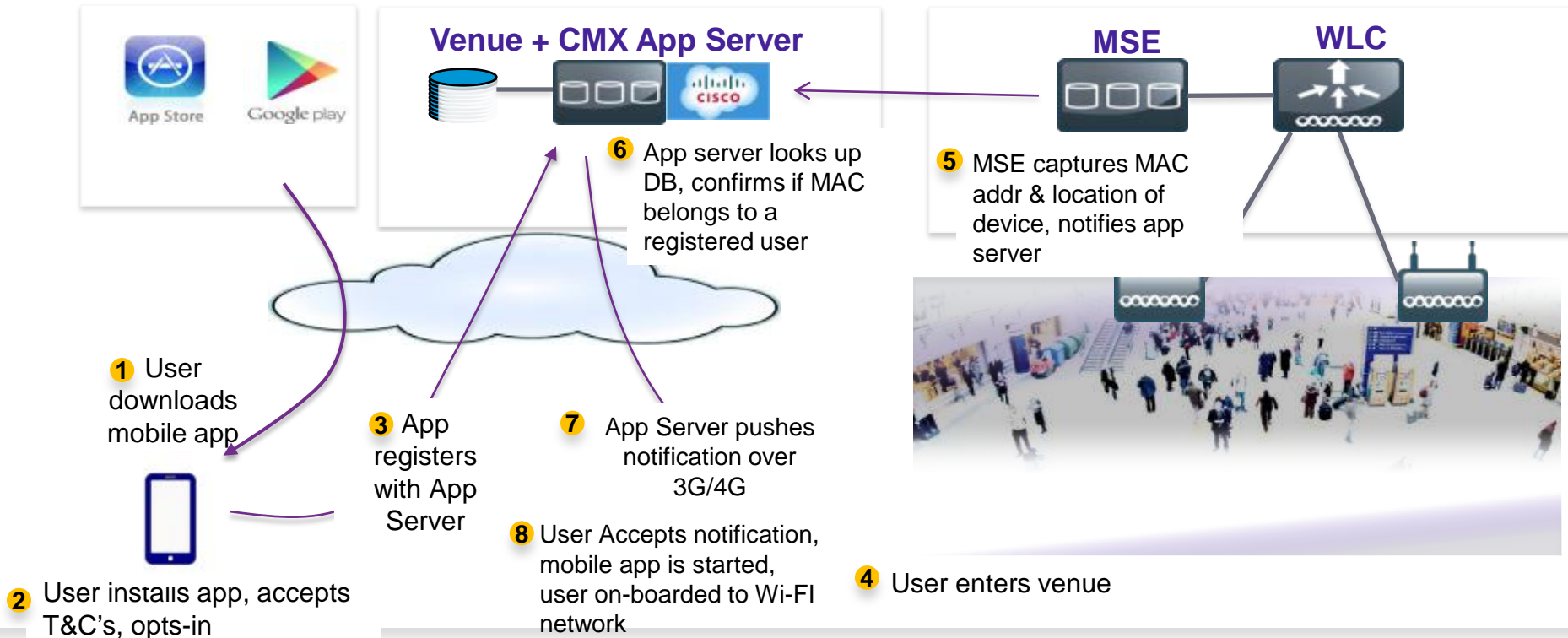


What is Needed to use the CMX SDK?

- Prime Infrastructure – configuration of maps
- Mobility Services Engine
 1. **CAS Service** to calculate location updates and send notifications to CMX Cloud Server
 2. **Connect and Engage Service** (was " **CMX Browser Engage**") to configure PATHS, Points of Interest, Zone Push Notifications and Banners
- CMX Application Server – receives presence events from MSE, configuration from MSE and sends push notifications to clients (via Google/Apple), interface with mobile clients, can be polled by 3rd party application server
- CMX Mobile Application SDK – Android and iOS SDK

Mobile App Experience

Improving Mobile App experience with CMX SDK



CMX Mobile Application SDK for Endpoints

SDK for Apple iOS

- Supports iOS version 6.x and higher
- Download the CMX SDK and install it
- Configure Xcode Project and dependencies

SDK for Android Platform

- Devices with minimum Android version of 2.3 or higher
- Import libraries into workspace and set dependencies
- Create new application and add dependency on CMX SDK
- Add permissions and required settings into application's manifest file
- Add map into application
- Publish application

All Support for the SDK is Through DevNet Website

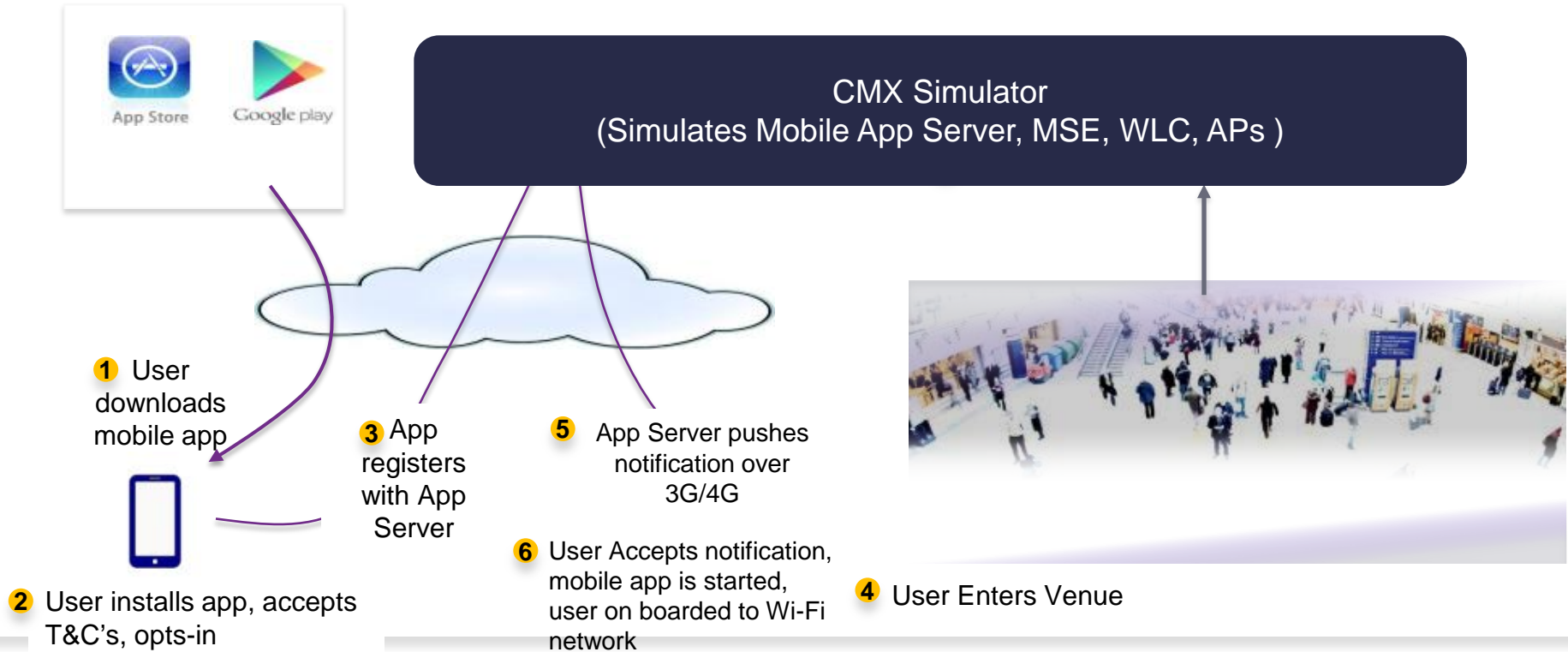
Cisco DevNet

<https://developer.cisco.com/>

The screenshot shows the Cisco DevNet website interface. At the top, there is a blue header with the Cisco logo and 'DevNet' text. On the right side of the header, there are links for 'Welcome!', 'Log In', and 'Register'. Below the header, there is a navigation menu with a 'Menu' dropdown and a search bar. The main content area features a 'Welcome to DevNet!' banner with a blue background, stating 'The complete resource for everything developer @ Cisco. It's free, easy, and simple to join, become a member, and discuss with the rest of the community.' There are 'Join' and 'Discuss' buttons. To the right of the banner is a 'Dive into DevNet at Cisco live!' event announcement for May 19-22, 2014, in San Francisco, CA, with a 'Find out more' button. Below the banner is an 'Explore: DevNet' section with a subtitle 'Use this tool to explore content within DevNet.' This section includes three filter categories: 'Community' (All, Dev Centers, Industry Leadership, Cool Stuff, Featured Product, Forums), 'Technology' (All, Networking, Collaboration, Data Center), and 'Content Type' (All, Code Samples, API's, SDK's, Tools, Test). At the bottom of the explore section, there is a 'Sort by' dropdown menu with options: Recommended, A-Z, Oldest, Newest, and Surprise Me.

CMX Simulator – Reference Only

CMX Mobile Simulator Experience



CMX SDK Server Simulator

- Node.js package can be installed on Windows, Linux, or Mac
- Documentation is included with the package
- Default user route



Supported Through the DevNet Website

Cisco DevNet
<https://developer.cisco.com/>

The screenshot displays the Cisco DevNet website interface. At the top, there is a blue header with the Cisco logo and 'DevNet' text. Navigation links for 'Welcome!', 'Log In', and 'Register' are visible. Below the header, there is a search bar and a 'Menu' dropdown. The main content area features a 'Welcome to DevNet!' banner with a 'Join' button and a 'Discuss' button. To the right, there is a 'Dive into DevNet at Cisco live!' banner for a May 19-22, 2014 event in San Francisco, CA, with a 'Find out more' button. Below the banners, there is an 'Explore: DevNet' section with a search bar and filters for 'Community', 'Technology', and 'Content Type'. The 'Community' filter includes 'All', 'Dev Centers', 'Industry Leadership', 'Cool Stuff', 'Featured Product', and 'Forums'. The 'Technology' filter includes 'All', 'Networking', 'Collaboration', and 'Data Center'. The 'Content Type' filter includes 'All', 'Code Samples', 'API's', 'SDK's', 'Tools', and 'Test'. At the bottom of the 'Explore' section, there is a 'Sort by' dropdown menu with options: 'Recommended', 'A', 'Z', 'Oldest', 'Newest', and 'Surprise Me'.

Thank you.

