

Verify CMX Location Limitations and Hardware Requirements

Contents

[Introduction](#)

[Components Used](#)

[Hardware Requirements For Low, Standard and High-end Node](#)

[Hardware Specifications of MSE 3365 and MSE 3375](#)

[CMX Limitations](#)

[Consequences of Insufficient Resources and when you exceed the limitations](#)

[Exceeding 400,000 Unique MAC Addresses Per Month](#)

[Exceeding Maximum Amount of Daily Unique MAC Addresses](#)

[Exceeding Number of Map Elements](#)

[Exceeding Number of NMSP Messages Per Second](#)

[Exceeding Number of Northbound Notifications Per Second](#)

[MAC Randomization And Tracking Of Probing Clients](#)

[MAC Randomization](#)

[CMX And Tracking Of Probing Clients](#)

[Relevant Bugs](#)

Introduction

This document describes hardware requirements of Connected Mobile Experience (CMX) Location, its software limitations and potential consequences when you exceed them.

Components Used

- 3504 Wireless LAN Controller (WLC) with image version 8.8.120
- CMX 10.6.1-47 installed on MSE 3375 physical appliance

All the commands, requirements and limitations described in this article are applicable to CMX 10.5 and later that runs either on VMware ESXi (vSphere) or on a physical appliance Mobility Service Engine (MSE) 3365/3375.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Hardware Requirements For Low, Standard and High-end Node

Determined by the amount of resources available, deployed CMX node can either be Low-end, Standard or High-end. CMX that runs on MSE 3365 and 3375 appliance is a High-end by default.

Table 1 shows the hardware requirements (processor (CPU) / memory (RAM) / Disk) for all 3 node types.

Hardware requirements	Low-end	Standard	High-end
CPU cores	8 vCPUs / 4 Physical cores	16 vCPUs / 8 Physical cores	20 vCPUs / 10 Physical cores
Min CPU base frequency	2.3 GHz	2.3 GHz	2.3 GHz
RAM	24 GB	48 GB	64 GB
Storage	550 GB	550 GB	1 TB
Storage type	SSD or SAS HDD	SSD or SAS HDD	SSD or SAS HDD

Table 1. CMX Hardware requirements

Hardware Specifications of MSE 3365 and MSE 3375

Both MSE 3365 and 3375 appliances have enough resources for the deployment of the high end CMX node. Their hardware specifications can be found in the Table 2:

Hardware specifications	MSE 3365	MSE 3375
CPU	10-core Intel E5-2650 v3 @2.4 GHz	12-core Intel Xeon Gold 5118 GHz
Storage	4x 600GB SAS HDD	2x 960GB SATA SSD
Form factor	1U	1U

Table 2. MSE appliance hardware specifications

CMX Limitations

The amount of data the CMX Location can handle heavily depends on the node size. Software limitations of Low, Standard and High end node can be found in the Table 3:

Limitations	Low-end	Standard	High-end
Maximum APs	2,000	5,000	10,000
Maximum unique MAC addresses tracked per day (with or without Hyperlocation)	25,000	50,000	90,000
Hyperlocation support	No	No	Yes
Maximum unique active clients (with Hyperlocation enabled)	X	X	9,000
Maximum unique MAC addresses per month (see note*)	400,000	400,000	400,000
Maximum zones	150	600	900
Maximum map elements	200	750	1000
Maximum MAC location API V3 requests per second	1	10	60
Maximum NMSP messages per second	750	1300	2500
Max northbound	10	50	300

notifications per second			
Max number of northbound notification receivers	5	5	5
Maximum CMX Connect connections per second	10	10	10

Table 3. CMX Location limitations

Note: After the number of unique mac addresses exceeds 400,000 in one month duration, CMX stops is unable to differentiate between new and visitors that return. Other services continue to function unless other limitations are exceeded.

Consequences of Insufficient Resources and when you exceed the limitations

If you exceed the limitations mentioned in the table 3, you can have fatal consequences on your CMX node. Before the installation of a CMX node, ensure to estimate how big the deployment is and decide which deployment size fits your needs.

If the deployment size is simply too big even for several CMX nodes, consider a move to [DNA Spaces](#), Cisco's new cloud based analytics platform that is available to replace CMX. With DNA Spaces, all calculations are offloaded to cloud infrastructure where resources are dynamically allocated based on the load.

All the symptoms and proposed workarounds bellow are based on Technical Assistance Center (TAC) previous experience with deployments that range from single Low-end node to multiple High-end nodes that cover hundreds of locations.

For additional information on how to deal with overloaded CMX, please refer to the document: <https://www.cisco.com/c/en/us/support/docs/wireless/connected-mobile-experiences/214894-optimize-cmx-performance.html>

Exceeding 400,000 Unique MAC Addresses Per Month

Symptoms:

- CMX stops to be able to differentiate between new and visitors that return. Other location services continue to work unless other limitations are exceeded

Workarounds:

- Disable tracking of probing clients
- If network consists of multiple controllers and one High-end node is not enough, consider the split of the load from multiple controllers to multiple CMX nodes
- If one High-end is not enough for a single controller, consider the upgrade of WLC to 8.8 or later version and the usage of a special [CMX Grouping](#) feature that allows single WLC to offload parts of the data to multiple CMX nodes
- Consider the migration to DNA Spaces, a cloud based analytics service that is replaces CMX. All workload is offloaded to the dynamically scalable cloud infrastructure

Exceeding Maximum Amount of Daily Unique MAC Addresses

Symptoms:

- Very slow or broken web interface
- High CPU and memory usage
- Loss of analytics data
- CMX services that crash or are not able to start
- Potentially unrecoverable corruption of data which requires reinstallation
- Error messages inside **locationserver.log** in of techsupport log bundle that says:
`Cleaning up element counts, unique devices 347684, locally administered macs 0 as part of daily midnight job`

Workarounds:

- Stop the track of probing clients at least until CMX is stable again
- Increase the size of the CMX node (Low-end -> Standard -> High-end) or deploy additional CMX nodes to redistribute the load
- Consider the migration to DNA Spaces, a cloud based analytics service that is replaces CMX. All workload is offloaded to the dynamically scalable cloud infrastructure
- If multiple controllers are added to a single CMX, remove all of them and attempt to add them back again one by one each day while you monitor the total daily device count

Exceeding Number of Map Elements

Symptoms:

- Slow web interface, especially Detect & Locate tab
- CMX services that crash
- Loss of analytics data

Workarounds:

- Increase the size of the CMX node (Low-end -> Standard -> High-end) or deploy additional CMX nodes
- Remove some of the map elements

Exceeding Number of NMSP Messages Per Second

This issue is usually observed when large amount of heavily loaded controllers is added to a single CMX node.

Symptoms:

- Slow web interface
- Loss of analytics data
- High CPU and memory usage
- CMX services that crash or are not able to start
- Error messages inside **analyticsserver.log** in of techsupport log bundle that says:
`Notification queue is full - incoming notifications are being rejected. Please increase more processing capacity`

Workarounds:

- Deployment of additional CMX nodes to split the load
- Consider the migration to DNA Spaces, a cloud based analytics service that replaces CMX. All workload is offloaded to the dynamically scalable cloud infrastructure

Exceeding Number of Northbound Notifications Per Second

This issue is usually observed when CMX is configured to send notifications to large number of servers. CMX 10.6.3 has introduced a limitation of 5 northbound notification receivers

Symptoms:

- Notification drops that result in inaccurate/incomplete data on the server that receives notifications

Workarounds:

- Remove some of the configured notification receivers
- Increase the size of the CMX node (Low-end -> Standard -> High-end) or deployment of additional nodes

MAC Randomization And Tracking Of Probing Clients

MAC Randomization

Before the association to the wireless network, wireless devices first need to send a probe request. Device can either probe for a specific SSID that it previously associated to in the past or it can send a “general” probe request, also known as Wildcard.

Any wireless device that listens for probe requests can “hear” a probe, note the device's presence and, if capable, record devices location with accuracy of up to several meters.

Due to growth of privacy concerns, with the release of Cisco IOS 8 in 2014, smartphone manufacturers have started to implement a feature called MAC randomization where devices would use new randomly generated MAC address every time they send a probe request.

When they generate a random mac address that is used to send probe requests, manufacturers can either use universally or locally administered mac addresses.

Locally administered mac addresses have second-least-significant bit of the first octet of the address set to 1. This bit acts as a flag that announces that the mac address is actually a randomly generated one.

There are four possible formats of locally administered MAC addresses (x can be any hex value)

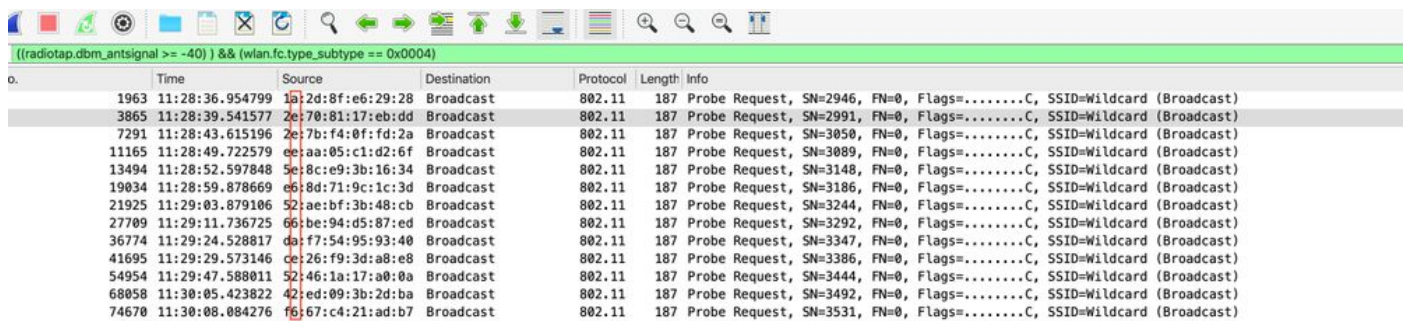
- x2-xx-xx-xx-xx-xx
- x6-xx-xx-xx-xx-xx
- xA-xx-xx-xx-xx-xx
- xE-xx-xx-xx-xx-xx

All other MAC addresses are considered to be universally administered. First 3 octets of universally administered MAC address are called Organizationally Unique Identifier (OUI) and they are specific to manufacturer.

Each manufacturer has assigned certain number of unique OUIs assigned.

In the over-the-air captures of an iPhone that runs IOS 12.3, which sends probe requests, we see that probe requests are sent every few seconds if the screen of the device is on, and every couple of minutes if screen of the device is off.

We see that locally administered bit is set to 1. With the release of IOS 14 and Android 10, randomized mac address is also used when the device associates to the network. Devices usually use a single randomized locally administered mac address per SSID.



The image shows a Wireshark capture of 802.11 Probe Request frames. The filter is ((radiotap.dbm_antsignal >= -40)) && (wlan.fc.type_subtype == 0x0004). The table below summarizes the captured frames:

Time	Source	Destination	Protocol	Length	Info
1963	1b:2d:8f:e6:29:28	Broadcast	802.11	187	Probe Request, SN=2946, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
3865	70:81:17:eb:dd	Broadcast	802.11	187	Probe Request, SN=2991, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
7291	7b:f4:0f:fd:2a	Broadcast	802.11	187	Probe Request, SN=3050, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
11165	aa:05:c1:d2:6f	Broadcast	802.11	187	Probe Request, SN=3089, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
13494	5e:8c:e9:3b:16:34	Broadcast	802.11	187	Probe Request, SN=3148, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
19034	e6:8d:71:9c:1c:3d	Broadcast	802.11	187	Probe Request, SN=3186, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
21925	52:ae:bf:3b:48:cb	Broadcast	802.11	187	Probe Request, SN=3244, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
27709	66:be:94:d5:87:ed	Broadcast	802.11	187	Probe Request, SN=3292, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
36774	da:f7:54:95:93:40	Broadcast	802.11	187	Probe Request, SN=3347, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
41695	ce:26:f9:3d:a8:e8	Broadcast	802.11	187	Probe Request, SN=3386, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
54954	52:46:1a:17:a0:0a	Broadcast	802.11	187	Probe Request, SN=3444, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
68058	42:ed:09:3b:2d:ba	Broadcast	802.11	187	Probe Request, SN=3492, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
74670	f6:67:c4:21:ad:b7	Broadcast	802.11	187	Probe Request, SN=3531, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)

CMX And Tracking Of Probing Clients

CMX has the ability to track clients that only probe. This option is enabled by default.

In order to exclude clients that use locally administered MAC addresses, check the "Enable Locally Administered MAC Filtering" option under **System > Settings > Filtering**.

This field is present in CMX 10.5.x, but has been removed from the 10.6.x web interface and has been enabled by default.

Tracking

Filtering

Location Setup

Mail Server

> Controllers and
Maps Setup

Upgrade

High Availability

Filtering Parameters

Duty Cycle Cutoff (Interferer) RSSI Cutoff (Probing Only Client) Exclude Probing Only clients Enable Locally Administered MAC Filtering Enable Location MAC Filtering Enable Location SSID Filtering

Some manufacturers decide not to use locally administered addresses when they probe. CMX has no way to distinguish between random, non-locally administered MAC address from actual real MAC address of the device. This means that one such client device can get recorded as a new client every time it sends a new probe request. While in use, in a 1 minute period an average smartphone probes couple of times. On CMX, such device is recorded as multiple different clients each time. This completely skews the CMX analytics and sometimes lead to almost unusable analytics data.

When they associate to the same SSID, devices always use a single MAC address that never changes (this address can either be real or locally administered random MAC). The amount of associated clients is always be lower or equal than the amount of clients that send only probes.

The track of clients that only probe is not supposed be used as a visitor counter. It can however be used to track daily trends (for example, if Wednesday is busier than Tuesday), but even that data can be inaccurate due to extremely high variations.

Cisco TAC often deals with issues on larger deployments (airports, malls, open public areas), where the track of clients that only probe introduces extremely large number of unique MAC addresses per day, which even high-end CMX nodes cannot handle (90,000+ per day).

If you track only associated clients, you lower the total number of recorded clients, but makes the collected analytics data accurate.

Cisco TAC strongly recommends to enable "Exclude Probing Only clients" option.

Relevant Bugs

- Cisco bug ID [CSCvg25953](#) - Enabling Location SSID Filtering disables the exclusion of locally administered MACs and vice versa
- Cisco bug ID [CSCvo43574](#) - CMX filters out associated locally administered MAC addresses

- Cisco bug ID [CSCvs85182](#) - Cmxos verify command is wrong about HDD min requirements