



Network Mobility Services Protocol

- [Information About Network Mobility Services Protocol, on page 1](#)
- [Radioactive Tracing for NMSP, on page 2](#)
- [Enabling NMSP on Premises Services, on page 2](#)
- [Modifying the NMSP Notification Interval for Clients, RFID Tags, and Rogues , on page 3](#)
- [Modifying the NMSP Notification Threshold for Clients, RFID Tags, and Rogues, on page 3](#)
- [Configuring NMSP Strong Cipher, on page 4](#)
- [Verifying NMSP Settings, on page 4](#)
- [Examples: NMSP Settings Configuration, on page 7](#)
- [NMSP by AP Groups with Subscription List from CMX, on page 7](#)
- [Verifying NMSP by AP Groups with Subscription List from CMX, on page 7](#)
- [Probe RSSI Location, on page 9](#)
- [Configuring Probe RSSI , on page 9](#)
- [RFID Tag Support, on page 11](#)
- [Configuring RFID Tag Support, on page 11](#)
- [Verifying RFID Tag Support, on page 12](#)

Information About Network Mobility Services Protocol

Cisco Network Mobility Services Protocol (NMSP) is a secure two-way protocol that can be run over a connection-oriented (TLS) or HTTPS transport. The wireless infrastructure runs the NMSP server and Cisco Connected Mobile Experiences (Cisco CMX) acts as an NMSP client. The controller supports multiple services and multiple Cisco CMXs can connect to the NMSP server to get the data for the services (location of wireless devices, probe RSSI, hyperlocation, wIPS, and so on.) over the NMSP or HTTPS session.

NMSP defines the intercommunication between Cisco CMX and the controller. Cisco CMX communicates to the controller over a routed IP network. Both publish-subscribe and request-reply communication models are supported. Typically, Cisco CMX establishes a subscription to receive services data from the controller in the form of periodic updates. The controller acts as a data publisher, broadcasting services data to multiple CMXs. Besides subscription, Cisco CMX can also send requests to the controller, causing the controller to send a response back.

The following is a list of the Network Mobility Services Protocol features:

- NMSP is disabled by default.
- NMSP communicates with Cisco CMX using TCP, and uses TLS for encryption.

- Wireless intrusion prevention system (wIPS) is supported only over TCP and TLS.
- Bidirectional communication is supported and Cisco CMX can send a message asynchronously over the established channel.



Note HTTPS is not supported for data transport between controller and Cisco CMX.

Radioactive Tracing for NMSP

This feature collects and provides all CMX-related events.

When a controller is added to CMX with an existing logging or serviceability tools, the following occurs:

- CMX reaches out to the controller through SNMP and CLI.
- Configures the CMX hash key on the controller.
- CMX requests the controller to open an NMSP connection.

RA tracing simplifies troubleshooting by allowing:

- RA trace the CMX IP on the controller.
- Collect all logs about it.

Enabling NMSP on Premises Services

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# <code>configure terminal</code>	Enters global configuration mode.
Step 2	nmosp enable Example: Device(config)# <code>nmosp enable</code>	Enables NMSP on premises services. Note By default, the NMSP is enabled on the controller.
Step 3	end Example: Device(config)# <code>end</code>	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Modifying the NMSP Notification Interval for Clients, RFID Tags, and Rogues

NMSP manages communication between the Cisco Connected Mobile Experience (Cisco CMX) and the controller for incoming and outgoing traffic. If your application requires more frequent location updates, you can modify the NMSP notification interval (to a value between 1 and 180 seconds) for clients, active RFID tags, and rogue access points and clients.



Note The TCP port (16113) that the controller and Cisco CMX communicate over must be open (not blocked) on any firewall that exists between the controller and the Cisco CMX for NMSP to function.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# <code>configure terminal</code>	Enters global configuration mode.
Step 2	nmosp notification interval { <i>rssi</i> { <i>clients</i> <i>rfid</i> <i>rogues</i> { <i>ap</i> <i>client</i> } <i>spectrum interferers</i> } <i>interval</i> } Example: Device(config)# <code>nmosp notification interval rssi rfid 50</code>	Sets the NMSP notification interval value for clients, RFID tags, rogue clients, and access points. <i>interval</i> -NMSP notification interval value, in seconds for RSSI measurement. Valid range is from 1 to 180.
Step 3	end Example: Device(config)# <code>end</code>	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Modifying the NMSP Notification Threshold for Clients, RFID Tags, and Rogues

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# <code>configure terminal</code>	Enters global configuration mode.

	Command or Action	Purpose
Step 2	location notify-threshold {clients rogues ap tags } <i>threshold</i> Example: Device(config)# location notify-threshold clients 5	Configures the NMSP notification threshold for clients, RFID tags, rogue clients, and access points. <i>threshold</i> - RSSI threshold value in db. Valid range is from 0 to 10, with a default value of 0..
Step 3	end Example: Device(config)# end	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Configuring NMSP Strong Cipher

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	nmosp strong-cipher Example: Device(config)# nmosp strong-cipher	Enable strong ciphers for NMSP server, which contains "ECDHE-RSA-AES128-GCM-SHA256;, ECDHE-ECDSA-AES128-GCM-SHA256;, AES256-SHA256:AES256-SHA;, and AES128-SHA256:AES128-SHA". Normal cipher suite contains, "ECDHE-RSA-AES128-GCM-SHA256;, ECDHE-ECDSA-AES128-GCM-SHA256;, and AES128-SHA".
Step 3	end Example: Device(config)# end	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Verifying NMSP Settings

To view the NMSP capabilities of the controller , use the following command:

```
Device# show nmosp capability
Service          Subservice
-----
RSSI              Rogue, Tags, Mobile Station,
```

```

Spectrum          Aggregate Interferer, Air Quality, Interferer,
Info              Rogue, Mobile Station,
Statistics        Rogue, Tags, Mobile Station,
AP Monitor        Subscription
On Demand Services Device Info
AP Info           Subscription

```

To view the NMSP notification intervals, use the following command:

```

Device# show nmsp notification interval
NMSP Notification Intervals
-----

```

```

RSSI Interval:
Client          : 2 sec
RFID            : 50 sec
Rogue AP        : 2 sec
Rogue Client    : 2 sec
Spectrum        : 2 sec

```

To view the connection-specific statistics counters for all CMX connections, use the following command:

```

Device# show nmsp statistics connection
NMSP Connection Counters
-----

```

```

CMX IP Address: 10.22.244.31, Status: Active
State:

```

```

Connections : 1
Disconnections : 0
Rx Data Frames : 13
Tx Data Frames : 99244
Unsupported messages : 0

```

Rx Message Counters:

ID	Name	Count
1	Echo Request	6076
7	Capability Notification	2
13	Measurement Request	5
16	Information Request	3
20	Statistics Request	2
30	Service Subscribe Request	1

Tx Message Counters:

ID	Name	Count
2	Echo Response	6076
7	Capability Notification	1
14	Measurement Response	13
15	Measurement Notification	91120
17	Information Response	6
18	Information Notification	7492
21	Statistics Response	2
22	Statistics Notification	305
31	Service Subscribe Response	1
67	AP Info Notification	304

To view the common statistic counter of the controller's NMSP service, use the following command:

```

Device# show nmsp statistics summary
NMSP Global Counters
-----

```

```

Number of restarts          :

```

```

SSL Statistics
-----

```

```

Total amount of verifications : 6

```

```

Verification failures           : 6
Verification success           : 0
Amount of connections created  : 8
Amount of connections closed   : 7
Total amount of accept attempts : 8
Failures in accept             : 0
Amount of successful accepts    : 8
Amount of failed registrations : 0

```

AAA Statistics

```

-----
Total amount of AAA requests   : 7
Failed to send requests        : 0
Requests sent to AAA           : 7
Responses from AAA             : 7
Responses from AAA to validate : 7
Responses validate error       : 6
Responses validate success     : 1

```

To view the overall NMSP connections, use the following command:

```
Device# show nmosp status
```

```
NMSP Status
```

```

-----
CMX IP Address  Active    Tx Echo Resp  Rx Echo Req  Tx Data  Rx Data  Transport
-----
127.0.0.1      Active    6              6              1         2         TLS

```

To view all mobility services subscribed by all CMXs, use the following command:

```
Device# show nmosp subscription detail
```

```
CMX IP address 127.0.0.1:
```

```

Service          Subservice
-----
RSSI              Rogue, Tags, Mobile Station,
Spectrum
Info              Rogue, Mobile Station,
Statistics        Tags, Mobile Station,
AP Info           Subscription

```

To view all mobility services subscribed by a specific CMX, use the following command:

```
Device# show nmosp subscription detail <ip_addr>
```

```
CMX IP address 127.0.0.1:
```

```

Service          Subservice
-----
RSSI              Rogue, Tags, Mobile Station,
Spectrum
Info              Rogue, Mobile Station,
Statistics        Tags, Mobile Station,
AP Info           Subscription

```

To view the overall mobility services subscribed by all CMXs, use the following command:

```
Device# show nmosp subscription summary
```

```

Service          Subservice
-----
RSSI              Rogue, Tags, Mobile Station,
Spectrum
Info              Rogue, Mobile Station,
Statistics        Tags, Mobile Station,
AP Info           Subscription

```

Examples: NMSP Settings Configuration

This example shows how to configure the NMSP notification interval for RFID tags:

```
Device# configure terminal
Device(config)# nmsp notification interval rssi rfid 50
Device(config)# end
Device# show nmsp notification interval
```

This example shows how to configure the NMSP notification interval for clients:

```
Device# configure terminal
Device(config)# nmsp notification interval rssi clients 180
Device(config)# end
Device# show nmsp notification interval
```

NMSP by AP Groups with Subscription List from CMX

The Cisco CMX group support allows you to send only the required Network Mobility Services Protocol (NMSP) data to Cisco CMX (applicable to both on-premises and cloud-based CMX). The Cisco CMX can subscribe to NMSP data of specific APs or AP groups based on the active services in the wireless controller.

This feature helps in load balancing and optimizing the data flow load, when the APs are distributed across different CMX servers. The Cisco CMX server creates a CMX AP group giving it a unique name and groups the APs under it.



Note The Cisco CMX AP Group is the list of Cisco APs managed by the Cisco CMX for location services. This AP group is not the same as the wireless controller AP group.

This feature supports the following services:

- Client
- Probe client filtering
- Hyperlocation
- BLE Services



Note NMSP subscription is available only for those services that are in enabled state in the wireless controller.

Verifying NMSP by AP Groups with Subscription List from CMX

To verify mobility services group subscription summary of all CMX connections, use the following command:

Device# **show nmosp subscription group summary**

```
CMX IP address: 127.0.0.1
Groups subscribed by this CMX server:
Group name: Group1
```

To view the services that are subscribed for an AP group by a CMX connection, use the following command:

Device# **show nmosp subscription group details services** *group-name cmx-IP-address*

```
CMX IP address: 127.0.0.1
CMX Group name: Group1
CMX Group filtered services:
Service          Subservice
-----
RSSI             Mobile Station,
Spectrum
Info
Statistics
```

To view the AP MAC list that is subscribed for an AP group by a CMX connection, use the following command:

Device **show nmosp subscription group detail ap-list** *group-name cmx-IP-address*

```
CMX IP address: 127.0.0.1
CMX Group name: Group1
CMX Group AP MACs:
: 0000.0000.7002 0000.0000.6602 0099.0000.0002 0000.00bb.0002
  0000.0000.5502 0000.0000.5002 0033.0000.0002 00d0.0000.0002
  0010.0010.0002 0000.0006.0002 0000.0002.0002 0000.0000.4002
  0000.0099.0002 0000.0000.a002 0000.7700.0002 0022.0000.0002
  0000.0000.0092 0000.0000.0082 0000.0000.0302 aa00.0000.0002
  0000.0050.0042 0000.0d00.0002 0000.0000.0032 0000.00cc.0002
  0000.0088.0002 2000.0000.0002 1000.0000.0002 0100.0000.0002
  0000.0000.0002 0000.0000.0001 0000.0000.0000
```

To view CMX-AP grouping details for all CMXs, use the following command:

```
Device# show nmosp subscription group detail all
CMX IP address: 127.0.0.1
Groups subscribed by this CMX server:
Group name: Group1
  CMX Group filtered services:
  Service          Subservice
  -----
  RSSI             Mobile Station,
  Spectrum
  Info
  Statistics

  CMX Group AP MACs:
  : 0000.0000.0003 0000.0000.0002 0000.0000.0001

Group name: Group2
  CMX Group filtered services:
  Service          Subservice
  -----
  RSSI             Tags,
  Spectrum
  Info
  Statistics
```



```

CMX Group AP MACs:
: 0000.0000.0300 0000.0000.0200 0000.0000.0100

Group name: Group3
CMX Group filtered services:
Service          Subservice
-----
RSSI              Rogue,
Spectrum
Info
Statistics

CMX Group AP MACs:
: 0000.0003.0000 0000.0002.0000 0000.0001.0000

```

To view all the AP lists subscribed by all CMXs, use the following command:

```
Device# show nmsp subscription group detail ap-list <group> <cmx-ip>
```

To view all the services subscribed by all CMXs, use the following command:

```
Device# show nmsp subscription group detail services <group> <cmx-ip>
```

Probe RSSI Location

The Probe RSSI Location feature allows the wireless controller and Cisco CMX to support the following:

- Load balancing
- Coverage Hole detection
- Location updates to CMX

When a wireless client is enabled, it sends probe requests to identify the wireless networks in the vicinity and also to find the received signal strength indication (RSSI) associated with the identified Service Set Identifiers (SSIDs).

The wireless client periodically performs active scanning in background even after being connected to an access point. This helps them to have an updated list of access points with best signal strength to connect. When the wireless client can no longer connect to an access point, it uses the access point list stored to connect to another access point that gives it the best signal strength. The access points in the WLAN gather these probe requests, RSSI and MAC address of the wireless clients and forwards them to the wireless controllers. The Cisco CMX gathers this data from the wireless controller and uses it to compute the updated location of the wireless client when it roams across the network.

Configuring Probe RSSI

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 2	wireless probe filter Example: <pre>Device(config)# wireless probe filter</pre>	<p>Enables filtering of unacknowledged probe requests from AP to improve the location accuracy. Filtering is enabled by default.</p> <p>Use the no form of the command to disable the feature. This will forward both acknowledged and unacknowledged probe requests to the controller.</p>
Step 3	wireless probe limit <i>limit-value interval</i> Example: <pre>Device(config)# wireless probe limit 10 100</pre>	<p>Configures the number of probe request reported to the wireless controller from the AP for the same client on a given interval.</p> <p>Use the no form of the command to revert to the default limit, which is 2 probes at an interval of 500 ms.</p>
Step 4	wireless probe locally-administered-mac Example: <pre>Device(config)# wireless probe locally-administered-mac</pre>	<p>Enables the reporting of probes from clients having locally administered MAC address.</p>
Step 5	location algorithm rssi-average Example: <pre>Device(config)# location algorithm rssi-average</pre>	<p>Sets the probe RSSI measurement updates to a more accurate algorithm but with more CPU overhead.</p>
Step 6	location algorithm simple Example: <pre>Device(config)# location algorithm simple</pre>	<p>(Optional) Sets the probe RSSI measurement updates to a faster algorithm with smaller CPU overhead, but less accuracy.</p> <p>Use the no form of the command to revert the algorithm type to the default one, which is <i>rssi-average</i>.</p>
Step 7	location expiry client <i>interval</i> Example: <pre>Device(config)# location expiry client 300</pre>	<p>Configures the timeout for RSSI values.</p> <p>The no form of the command sets it to a default value of 15.</p>
Step 8	location notify-threshold client <i>threshold-db</i> Example: <pre>Device(config)# location notify-threshold client 5</pre>	<p>Configures the notification threshold for clients.</p> <p>The no form of the command sets it to a default value of 0.</p>
Step 9	location rssi-half-life client <i>time-in-seconds</i> Example: <pre>Device(config)# location rssi-half-life client 20</pre>	<p>Configures half life when averaging two RSSI readings.</p> <p>To disable this option, set the value to 0.</p>

What to do next

Use the **show wireless client probing** command to view each probing client (associated and probing only) by batch of 10 MAC addresses.

RFID Tag Support

The controller enables you to configure radio frequency identification (RFID) tag tracking. RFID tags are small wireless battery-powered tags that continuously broadcast their own signal and are affixed to assets for real-time location tracking. They operate by advertising their location using special 802.11 packets, which are processed by access points, the controller, and the Cisco CMX. Only active RFIDs are supported. A combination of active RFID tags and wireless controller allows you to track the current location of equipment. *Active* tags are typically used in real-time tracking of high-value assets in *closed-loop* systems (that is,) systems in which the tags are not intended to physically leave the control premises of the tag owner or originator.

General Guidelines

- You can verify the RFID tags on the controller.
- High Availability for RFID tags are supported.

Configuring RFID Tag Support

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	wireless rfid Example: Device(config)# wireless rfid	Enables RFID tag tracking. The default value is enabled. Use the no form of this command to disable RFID tag tracking.
Step 3	wireless rfid timeout <i>timeout-value</i> Example: Device(config)# wireless rfid timeout 90	Configures the RFID tag data timeout value to cleanup the table. The timeout value is the amount of time that the controller maintains tags before expiring them. For example, if a tag is configured to beacon every 30 seconds, we recommend that you set the timeout value to 90 seconds (approximately three times the beacon value). The default value is 1200 seconds.

Verifying RFID Tag Support

To view the summary of RFID tags that are clients, use the following command:

```
Device# show wireless rfid client
```

To view the detailed information for an RFID tag, use the following command:

```
Device# show wireless rfid detail <rfid-mac-address>
```

```
RFID address 000c.cc96.0001
Vendor Cisco
Last Heard 6 seconds ago
Packets Received 187
Bytes Received 226

Content Header
=====
  CCX Tag Version 0
  Tx power: 12
  Channel: 11
  Reg Class: 4
CCX Payload
=====
  Last Sequence Control 2735
  Payload length 221
  Payload Data Hex Dump:
00000000 00 02 00 00 01 09 00 00 00 00 0c b8 ff ff ff 02 |.....|
00000010 07 42 03 20 00 00 0b b8 03 4b 00 00 00 00 00 00 |.B. ....K.....|
00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00000030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00000040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
```

To view the summary information for all known RFID tags, use the following command:

```
Device# show wireless rfid summary
```

```
Total RFID entries: : 16
Total Unique RFID entries : 16
RFID ID VENDOR Closet AP RSSI Time Since Last Heard
0012.b80a.c791 Cisco 7069.5a63.0520 -31 3 minutes 30 seconds ago
0012.b80a.c953 Cisco 7069.5a63.0460 -33 4 minutes 5 seconds ago
0012.b80b.806c Cisco 7069.5a63.0520 -46 15 seconds ago
0012.b80d.e9f9 Cisco 7069.5a63.0460 -38 4 minutes 28 seconds ago
0012.b80d.ea03 Cisco 7069.5a63.0520 -43 4 minutes 29 seconds ago
0012.b80d.ea6b Cisco 7069.5a63.0460 -39 4 minutes 26 seconds ago
0012.b80d.ebe8 Cisco 7069.5a63.0520 -43 3 minutes 21 seconds ago
0012.b80d.ebeb Cisco 7069.5a63.0520 -43 4 minutes 28 seconds ago
0012.b80d.ec48 Cisco 7069.5a63.0460 -42 4 minutes 7 seconds ago
0012.b80d.ec55 Cisco 7069.5a63.0520 -41 1 minute 52 seconds ago
```

To view the location-based system RFID statistics, use the following command:

```
Device# show wireless rfid stats
```

```
RFID stats :
=====
RFID error db full : 0
RFID error invalid payload : 0
RFID error invalid tag : 0
RFID error dot11 hdr : 0
```

```
RFID error pkt len : 0
RFID error state drop : 0
RFID total pkt received : 369
RFID populated error value : 0
RFID error insert records : 0
RFID error update records : 0
RFID total insert record : 16
RFID ccx payload error : 0
RFID total delete record : 0
RFID error exceeded ap count : 0
RFID error record remove : 0
RFID old rssi expired count : 0
RFID smallest rssi expired count : 0
RFID total query insert : 0
RFID error invalid rssi count : 0
```

To view the NMSP notification interval, use the following command:

```
Device# show nmosp notification interval
```

```
NMSP Notification Intervals
-----
```

```
RSSI Interval:
```

```
Client           : 2 sec
RFID             : 50 sec
Rogue AP         : 2 sec
Rogue Client     : 2 sec
Spectrum         : 2 sec
```

