Network Mobility Services Protocol

- Network mobility services protocol, on page 1
- Radioactive tracing for NMSP, on page 2
- Enable NMSP on premises services (CLI), on page 2
- Modify the NMSP notification interval for clients, RFID tags, and rogues (CLI), on page 3
- Modify the NMSP notification threshold for clients, RFID tags, and rogues (CLI), on page 4
- Configure NMSP strong cipher (CLI), on page 4
- Verify NMSP settings, on page 5
- Examples: NMSP settings configuration, on page 7
- NMSP by AP groups with subscription list from CMX, on page 7
- Verify NMSP by AP groups with subscription list from CMX, on page 8
- Probe RSSI location, on page 9
- Configure probe RSSI (CLI), on page 10
- RFID tag support, on page 11
- Configure RFID tag support (CLI), on page 11
- Verify RFID tag support, on page 12

Network mobility services protocol

A Network Mobility Services Protocol (NMSP) is a secure two-way wireless communication protocol that

- enables bi-directional data exchange between Cisco wireless controllers and Cisco Connected Mobile Experiences (CMX)
- supports both publish-subscribe and request-reply communication models over connection-oriented transports such as TLS, and
- allows controllers to provide multiple services including device location, probe RSSI, hyperlocation, and wIPS to multiple CMX clients.

The wireless infrastructure runs the NMSP server, while Cisco Connected Mobile Experiences (Cisco CMX) acts as the NMSP client.

Cisco CMX communicates to the controller over a routed IP network. 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. In addition to subscriptions, Cisco CMX can send requests to the controller. The controller sends a response to Cisco CMX.

This 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.
- TCP and TLS support the wireless intrusion prevention system (wIPS).
- The system supports bidirectional communication, and Cisco CMX sends messages asynchronously over the established channel.

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

Radioactive tracing for NMSP

A radioactive trace event is a CMX service feature that

- enables the collection of all CMX-related events from network controllers
- configures secure connections through SNMP and CLI for real-time event tracing, and
- provides comprehensive troubleshooting by gathering controller logs associated with the CMX IP via RA tracing.

This feature also configures the CMX hash key on the controller, and requests the controller to open an NMSP connection.

Enable NMSP on premises services (CLI)

Enable Network Mobility Services Protocol (NMSP) on your network controller to support communication with on-premises services.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enable NMSP on premises services.

Example:

```
Device(config)# nmsp enable
```

Note
By default, the NMSP is enabled on the controller.

Step 3 Return to privileged EXEC mode.

Example:

```
Device(config)# end
```

Alternatively, press Ctrl-Z to exit global configuration mode.

Modify the NMSP notification interval for clients, RFID tags, and rogues (CLI)

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 set the NMSP notification interval to a value between one and 180 seconds for clients, active RFID tags, rogue access points, and clients.

Note The TCP port (16113) used for communication between the controller and Cisco CMX must be open on any firewall separating the two systems to enable NMSP operation.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Set the NMSP notification interval value for clients, RFID tags, rogue clients, and APs.

Example:

```
Device(config)# nmsp notification interval {rssi {clients | rfid | rogues {ap | client} |
spectrum | interferers} interval 50}
```

interval-NMSP notification interval value, in seconds for RSSI measurement. The valid range is from one to 180.

Step 3 Return to privileged EXEC mode.

Example:

```
Device(config)# end
```

Alternatively, you can also press ***Ctrl-Z*** to exit global configuration mode.

Modify the NMSP notification threshold for clients, RFID tags, and rogues (CLI)

Change the threshold for NMSP notifications based on RSSI for clients, RFID tags, and rogue devices.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the NMSP notification threshold for clients, RFID tags, rogue clients, and APs.

Example:

```
Device(config)# location notify-threshold {clients | rogues ap | tags} threshold 5
```

The *threshold*- RSSI threshold value is in dB. The valid range is from zero to 10, with a default value of zero..

Step 3 Return to privileged EXEC mode.

Example:

```
Device(config)# end
```

Alternatively, press ***Ctrl-Z*** to exit global configuration mode.

Configure NMSP strong cipher (CLI)

Enable strong cipher suites for NMSP server to enhance security for device communication.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enable strong ciphers for NMSP server.

Example:

```
Device(config)# nmsp strong-cipher
```

Strong ciphers for NMSP server 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 Return to privileged EXEC mode.

Example:

```
Device(config)# end
```

Alternatively, press ***Ctrl-Z*** to exit global configuration mode.

Verify NMSP settings

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

```
Device# show nmsp 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 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 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 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 command:

```
Device# show nmsp 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 command:

```
Device# show nmsp 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 command:

```
Device# show nmsp 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

Device# show nmsp 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

An NMSP subscription by AP groups is a network data management feature that

- enables Cisco CMX to subscribe only to specific Network Mobility Services Protocol (NMSP) data from designated AP groups based on the active services in the wireless controller
- helps distribute and balance network data load among multiple CMX servers, and
- restricts NMSP data transmission to those services enabled on the wireless controller.

Cisco CMX group support lets you send the required Network Mobility Services Protocol (NMSP) data to Cisco CMX, whether it is deployed on-premises or in the cloud.

You can create a CMX AP group on the Cisco CMX server, assign a unique name, and group APs under it.

Note The CMX AP group lists Cisco APs managed by Cisco CMX for location services. This group is different from the AP groups on the wireless controller.

This feature supports these services:

- Client
- Probe client filtering
- Hyperlocation
- BLE Services

Note NMSP subscription is available only for services enabled on the wireless controller.

Verify NMSP by AP groups with subscription list from CMX

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

```
Device# show nmsp 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 command:

```
Device# show nmsp subscription group details services cmx-IP-addrress

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 command:

```
Device# show nmsp subscription group detail ap-list group-name cmx-IP-addrress

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 command:

```
Device# show nmsp 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 command:

```
Device# show nmsp subscription group detail ap-list
```

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

```
Device# show nmsp subscription group detail services
```

Probe RSSI location

A probe RSSI location is a wireless networking feature that

- allows wireless controllers and Cisco CMX to collect and use the received signal strength indication (RSSI) from client probe requests associated with the identified Service Set Identifiers (SSIDs)
- enables functions such as load balancing, coverage hole detection, and location updates, and
- supports the precise tracking of wireless clients as they move within the network.

After connecting to an AP, the client scans in the background and keeps a list of strong APs. If it loses connection, the client uses this list to reconnect. The APs in the WLAN gather probe requests, RSSI data, and

MAC addresses of wireless clients, then forward this information to the wireless controller s. Cisco CMX receives this data from the controller and calculates the client's updated location.

Configure probe RSSI (CLI)

Improve client location accuracy by configuring probe RSSI handling and related settings using commands.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enable filtering of unacknowledged probe requests from AP to improve the location accuracy.

Example:

```
Device(config)# wireless probe filter
```

Filtering is enabled by default.

Use the **no** form of the command to disable the feature. This forwards both acknowledged and unacknowledged probe requests to the controller.

Step 3 Configure the number of probe request reported to the wireless controller from the AP for the same client on a given interval.

Example:

```
Device(config)# wireless probe limit limit-value 10 interval 100
```

Use the **no** form of the command to revert to the default limit, which is two probes at an interval of 500 ms.

Step 4 Enable the reporting of probes from clients having locally administered MAC address.

Example:

```
Device(config)# wireless probe locally-administered-mac
```

Step 5 Set the probe RSSI measurement updates to a more accurate algorithm but with more CPU overhead.

Example:

```
Device(config)# location algorithm rssi-average
```

Step 6 (Optional) Set the probe RSSI measurement updates to a faster algorithm with smaller CPU overhead, but less accuracy.

Example:

```
Device(config)# location algorithm simple
```

Use the **no** form of the command to revert the algorithm type to the default one, that is *rssi-average*.

Step 7 Configure the timeout for RSSI values.

Example:

```
Device(config)# location expiry client interval 300
```

The **no** form of the command sets it to a default value of 15.

Step 8 Configure the notification threshold for clients.

Example:

```
Device(config)# location notify-threshold client threshold-db 5
```

The **no** form of the command sets it to a default value of zero.

Step 9 Configure half life when averaging two RSSI readings.

Example:

```
Device(config)# location rssi-half-life client time-in-seconds 20
```

To disable this option, set the value to zero.

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

An RFID tag is a small wireless battery-powered tracking device that

- broadcasts its own signal for real-time location tracking, and
- operates using special 802.11 packets processed by APs, wireless controllers, and Cisco CMX.

The controller enables you to configure radio frequency identification (RFID) tag tracking. Only active RFIDs are supported. A combination of active RFID tags and wireless controller allows you to track the current location of equipment. Use *Active* tags to track high-value assets in *closed-loop* systems. These tags remain within the control premises of the owner.

General guidelines

- You can verify the RFID tags on the controller .
- The controller supports high availability for RFID tags.

Configure RFID tag support (CLI)

Enable and configure RFID tag tracking features for WLANs managed by the device using commands.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enable RFID tag tracking.

Example:

```
Device(config)# wireless rfid
```

The default value is enabled.

Use the **no** form of this command to disable RFID tag tracking.

Step 3 Configure the RFID tag data timeout value to cleanup the table.

Example:

```
Device(config)# wireless rfid timeout timeout-value 90
```

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.

Verify RFID tag support

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

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

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

```
Device# show wireless rfid stats

RFID stats :
==============
RFID error db full : 0
RFID error invalid paylod : 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 expireed count : 0
RFID total query insert : 0
RFID error invalid rssi count : 0
```

To view the NMSP notification interval, use the 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
```