Contents

Introduction

Network Mobility Services Protocol (NMSP) manages communication between the Mobility Services Enginer(MSE) and the Wireless LAN Controller(WLC).

NMSP is a two-way protocol that can be run over a connection-oriented or a connectionless transport.Context-aware switches can use NMSP to communicate with one or more MSEs. NMSP is based upon a bidirectional system of requests and responses between the MSE and access controller. Now let's see how to enable this communication between MSE & WLC.

Here we have used 3850 (IOS based WLC) & MSE for this post.

Problem:

Issues in establishing NMSP tunnel between 3850 & MSE.

Devices Used:

MSE: Virtual MSE 8.0.110 (MR1)

WLC: 3850 3.3.5SE

Prime Infrastructure(PI): 2.2.1

Since NMSP works over SSL(Secure Socket Layer), you have to configure MSE credential at WLC. MSE use its MAC address & Key Hash, so WLC should be aware of these two parameters. You can obtain this detail via MSE CLI as shown below

[root@robin ~]# cmdshell

cmd> show server-auth-info
invoke command: com.aes.server.cli.CmdGetServerAuthInfo
AesLog queue high mark: 50000
AesLog queue low mark: 500

Server Auth Info

MAC Address: 00:50:56:9c:34:89
SHA1 Key Hash: e0afbe2e2abeed5a2f9ffc75f059da6a1bf2bfa0
SHA2 Key Hash: 6ab919e20afc103d025aaf210c2a9dda151af9403ef52e80a35ae1ecb6d3c177
Certificate Type: SSC

Now configuring NMSP settings on a converged access (5760/3850/3650) platform.
Here we have used 3850 for this example. We have to configure MSE MAC address as user-
name and key hash as password. Note: The version running on my 3850 is 3.3.5 SE & SHA2
encryption is used in IOS-XE.

Commands used:

3850c(config)#username 0050569c3489 aaa attribute list NMSP
3850c(config)#
3850c(config)#
3850c(config)#

```
3850c#
3850c#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
3850c(config)#
3850c(config)#username 0050569c3489 aaa attribute list NMSP
3850c(config)#aaa attribute list NMSP
3850c(config-attr-list)#attribute type password 6ab919e20afc103d025aaf210c2a9d$
3850c(config-attr-list)#$zation credential-download wcm_loc_serv_cert local
3850c(config)#
3850c(config)#exit
3850c#
3850c#
3850c#sh run | i aaa
username 0050569c3489 mac aaa attribute list NMSP
aaa new-model
aaa authentication login local_webauth local
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization credential-download default local
aaa authorization credential-download wcm_loc_serv_cert local
aaa accounting update periodic 15
aaa attribute list NMSP
aaa attribute list mse_0050569c3489
aaa session-id common
3850c#
```

In your Prime Infrastructure click: Services > Mobility Services > Synchronize Services
Select the 3850 & click "Change MSE Assignment" button.
Then you need to select the appropriate MSE & Services you want to synchronize between WLC
(3850) & MSE.
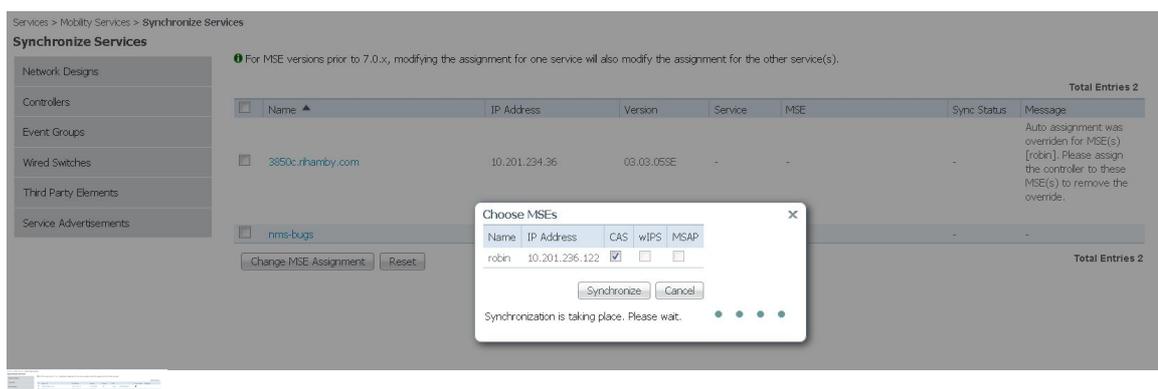
Verify:

After completion of synchronize services you can verify it from WLC, MSE or PI GUI.

Via 3850 CLI:

```
3850c#
3850c#show nmsp status
MSE IP Address    Tx Echo Resp   Rx Echo Req    Tx Data      Rx Data
--------------------------------------------------------------------------
10.201.236.122    9              9              48           14
```

```
3850c#show nmsp subscription de
3850c#show nmsp subscription detail
Mobility Services Subscribed by 10.201.236.122:
Service          Subservice
---------------------------------
RSSI             Mobile Station, Tags
Info             Mobile Station
Statistics       Mobile Station, Tags
Attachment       Wired Station
Location         Subscription



3850c#
```

```
3850c#show nmsp subscription summary
Mobility Services Subscribed
---------------------------------

Server IP        Services
---------------------------------
10.201.236.122   RSSI, Info, Statistics, Attachment, Wired Location

3850c#
```

Via MSE GUI

For MSE v8.0 or higher go to: (https://<MSE_IP>/mseui/)
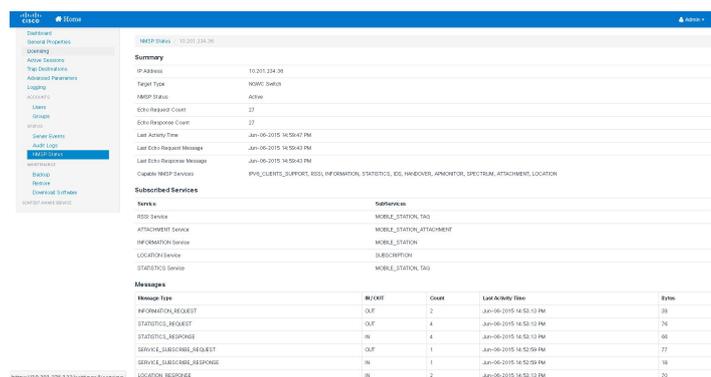
Troubleshoot:

If still NMSP is inactive:

1) Check key hash and if doesnt match enter the hash manually as shown above

2) NTP time sync should be there between MSE & WLC

Debugs:

Failure Scenario:

Failure on hash key validation:

3850c#set trace nmsp connection level debug
3850c#show trace messages nmsp

[06/03/15 22:28:10.762 UTC a27 10241] **Allocated new NMSP connection 0**

[06/03/15 22:28:10.762 UTC a28 10241] sslConnectionInit: SSL_new() conn ssl b3f8a8d0
[06/03/15 22:28:10.762 UTC a29 10241] sslConnectionInit: SSL_do_handshake for conn ssl b3f8a8d0, conn state: INIT, SSL state: HANDSHAKING
[06/03/15 22:28:10.762 UTC a2a 10241] SSL state = 0x6000; where = 0x10; ret = 0x1
[06/03/15 22:28:10.762 UTC a2b 10241] ret_type_string=unknown
[06/03/15 22:28:10.762 UTC a2c 10241] ret_desc_string=unknown
[06/03/15 22:28:10.762 UTC a2d 10241] SSL_state_string=before/accept initialization
[06/03/15 22:28:10.762 UTC a2e 10241] SSL state = 0x6000; where = 0x2001; ret = 0x1
[06/03/15 22:28:10.762 UTC a2f 10241] ret_type_string=unknown
[06/03/15 22:28:10.762 UTC a30 10241] ret_desc_string=unknown
[06/03/15 22:28:10.762 UTC a31 10241] SSL_state_string=before/accept initialization
[06/03/15 22:28:10.762 UTC a32 10241] SSL state = 0x2111; where = 0x2002; ret = 0xffffffff
[06/03/15 22:28:10.762 UTC a33 10241] ret_type_string=unknown
[06/03/15 22:28:10.762 UTC a34 10241] ret_desc_string=unknown
[06/03/15 22:28:10.762 UTC a35 10241] SSL_state_string=SSLv3 read client hello B
 --More-- [06/03/15 22:28:10.762 UTC a36 10241] -- returns WANT_READ for conn ssl b3f8a8d0
[06/03/15 22:28:10.762 UTC a37 10241] sslConnectionInit() success with Connection state: INIT, SSL state: HANDSHAKING
[06/03/15 22:28:10.768 UTC a38 10241] doSSLRecvLoop: **Handshake has not completed for conn 0**
[06/03/15 22:28:10.768 UTC a39 10241] sslConnectionInit: SSL_do_handshake for conn ssl b3f8a8d0, conn state: INIT, SSL state: HANDSHAKING
[06/03/15 22:28:10.768 UTC a3a 10241] SSL state = 0x2111; where = 0x2001; ret = 0x1
[06/03/15 22:28:10.768 UTC a3b 10241] ret_type_string=unknown
[06/03/15 22:28:10.768 UTC a3c 10241] ret_desc_string=unknown
[06/03/15 22:28:10.768 UTC a3d 10241] SSL_state_string=SSLv3 read client hello B
[06/03/15 22:28:10.768 UTC a3e 10241] SSL state = 0x2130; where = 0x2001; ret = 0x1
[06/03/15 22:28:10.768 UTC a3f 10241] ret_type_string=unknown
[06/03/15 22:28:10.768 UTC a40 10241] ret_desc_string=unknown
[06/03/15 22:28:10.768 UTC a41 10241] SSL_state_string=SSLv3 write server hello A
[06/03/15 22:28:10.768 UTC a42 10241] SSL state = 0x2140; where = 0x2001; ret = 0x1
[06/03/15 22:28:10.768 UTC a43 10241] ret_type_string=unknown
[06/03/15 22:28:10.768 UTC a44 10241] ret_desc_string=unknown

[06/03/15 22:28:10.768 UTC a45 10241] SSL_state_string=SSLv3 write certificate A

 --More-- [06/03/15 22:28:10.768 UTC a46 10241] SSL state = 0x2160; where = 0x2001; ret = 0x1

[06/03/15 22:28:10.768 UTC a47 10241] ret_type_string=unknown

[06/03/15 22:28:10.768 UTC a48 10241] ret_desc_string=unknown

[06/03/15 22:28:10.768 UTC a49 10241] SSL_state_string=SSLv3 write certificate request A

[06/03/15 22:28:10.768 UTC a4a 10241] SSL state = 0x2100; where = 0x2001; ret = 0x1

[06/03/15 22:28:10.768 UTC a4b 10241] ret_type_string=unknown

[06/03/15 22:28:10.768 UTC a4c 10241] ret_desc_string=unknown

[06/03/15 22:28:10.768 UTC a4d 10241] SSL_state_string=SSLv3 flush data

[06/03/15 22:28:10.768 UTC a4e 10241] SSL state = 0x2180; where = 0x2002; ret = 0xffffffff

[06/03/15 22:28:10.768 UTC a4f 10241] ret_type_string=unknown

[06/03/15 22:28:10.768 UTC a50 10241] ret_desc_string=unknown

[06/03/15 22:28:10.768 UTC a51 10241] SSL_state_string=SSLv3 read client certificate A

[06/03/15 22:28:10.768 UTC a52 10241] -- returns WANT_READ for conn ssl b3f8a8d0

[06/03/15 22:28:11.068 UTC a53 10241] doSSLRecvLoop: Handshake has not completed for conn 0

[06/03/15 22:28:11.068 UTC a54 10241] **sslConnectionInit: SSL_do_handshake for conn ssl b3f8a8d0, conn state: INIT, SSL state: HANDSHAKING**

[06/03/15 22:28:11.069 UTC a55 10241] Peer certificate Validation Done for conn ssl b3f8a8d0, calling authlist..

 --More-- [06/03/15 22:28:11.070 UTC a56 10241] Authlist authentication failed for conn ssl b3f8a8d0

[06/03/15 22:28:12.070 UTC a57 10241] Peer Not Validated against the AuthList

[06/03/15 22:28:12.070 UTC a58 10241] SSL state = 0x2182; where = 0x4008; ret = 0x22e

[06/03/15 22:28:12.070 UTC a59 10241] ret_type_string=fatal

[06/03/15 22:28:12.070 UTC a5a 10241] **ret_desc_string=certificate unknown**

[06/03/15 22:28:12.070 UTC a5b 10241] SSL_state_string=SSLv3 read client certificate C

[06/03/15 22:28:12.070 UTC a5c 10241] SSL state = 0x2182; where = 0x2002; ret = 0xffffffff

[06/03/15 22:28:12.070 UTC a5d 10241] ret_type_string=unknown

[06/03/15 22:28:12.070 UTC a5e 10241] ret_desc_string=unknown

[06/03/15 22:28:12.070 UTC a5f 10241] SSL_state_string=SSLv3 read client certificate C

[06/03/15 22:28:12.070 UTC a60 10241] -- **handshake failed for conn ssl b3f8a8d0, ssl_err 1 error = error:140890B2:SSL routines:SSL3_GET_CLIENT_CERTIFICATE:no certificate returned**

[06/03/15 22:28:12.070 UTC a61 10241] **freeing Nmsp conn ssl b3f8a8d0, conn id 0**

Success Scenario:

[06/06/15 17:47:53.600 UTC 4f2 10205] Sending NMSP_APP_MEAS_NOTIFY_MSG to LocServer 0

[06/06/15 17:56:34.305 UTC 4f3 10205] **Allocated new NMSP connection 0**

--More-- [06/06/15 17:56:34.306 UTC 4f4 10205] sslConnectionInit: SSL_new() conn ssl 590a6048

[06/06/15 17:56:34.306 UTC 4f5 10205] sslConnectionInit: SSL_do_handshake for conn ssl 590a6048, conn state: INIT, SSL state: HANDSHAKING

[06/06/15 17:56:34.306 UTC 4f6 10205] SSL state = 0x6000; where = 0x10; ret = 0x1

[06/06/15 17:56:34.306 UTC 4f7 10205] ret_type_string=unknown

[06/06/15 17:56:34.306 UTC 4f8 10205] ret_desc_string=unknown

[06/06/15 17:56:34.307 UTC 4f9 10205] SSL_state_string=before/accept initialization

[06/06/15 17:56:34.307 UTC 4fa 10205] SSL state = 0x6000; where = 0x2001; ret = 0x1

[06/06/15 17:56:34.307 UTC 4fb 10205] ret_type_string=unknown

[06/06/15 17:56:34.307 UTC 4fc 10205] ret_desc_string=unknown

[06/06/15 17:56:34.307 UTC 4fd 10205] SSL_state_string=before/accept initialization

[06/06/15 17:56:34.307 UTC 4fe 10205] SSL state = 0x2111; where = 0x2002; ret = 0xffffffff
[06/06/15 17:56:34.307 UTC 4ff 10205] ret_type_string=unknown
[06/06/15 17:56:34.307 UTC 500 10205] ret_desc_string=unknown
[06/06/15 17:56:34.307 UTC 501 10205] SSL_state_string=SSLv3 read client hello B
[06/06/15 17:56:34.307 UTC 502 10205] -- returns WANT_READ for conn ssl 590a6048
[06/06/15 17:56:34.307 UTC 503 10205] sslConnectionInit() success with Connection state: INIT, SSL state: HANDSHAKING
--More-- [06/06/15 17:56:34.309 UTC 504 10205] doSSLRecvLoop: Handshake has not completed for conn 0
[06/06/15 17:56:34.309 UTC 505 10205] **sslConnectionInit: SSL_do_handshake for conn ssl 590a6048, conn state: INIT, SSL state: HANDSHAKING**
[06/06/15 17:56:34.309 UTC 506 10205] SSL state = 0x2111; where = 0x2001; ret = 0x1
[06/06/15 17:56:34.309 UTC 507 10205] ret_type_string=unknown
[06/06/15 17:56:34.309 UTC 508 10205] ret_desc_string=unknown
[06/06/15 17:56:34.309 UTC 509 10205] SSL_state_string=SSLv3 read client hello B
[06/06/15 17:56:34.309 UTC 50a 10205] SSL state = 0x2130; where = 0x2001; ret = 0x1
[06/06/15 17:56:34.309 UTC 50b 10205] ret_type_string=unknown
[06/06/15 17:56:34.309 UTC 50c 10205] ret_desc_string=unknown
[06/06/15 17:56:34.309 UTC 50d 10205] SSL_state_string=SSLv3 write server hello A
[06/06/15 17:56:34.310 UTC 50e 10205] SSL state = 0x2140; where = 0x2001; ret = 0x1
[06/06/15 17:56:34.310 UTC 50f 10205] ret_type_string=unknown
[06/06/15 17:56:34.310 UTC 510 10205] ret_desc_string=unknown
[06/06/15 17:56:34.310 UTC 511 10205] SSL_state_string=SSLv3 write certificate A
[06/06/15 17:56:34.310 UTC 512 10205] SSL state = 0x2160; where = 0x2001; ret = 0x1
[06/06/15 17:56:34.310 UTC 513 10205] ret_type_string=unknown
--More-- [06/06/15 17:56:34.310 UTC 514 10205] ret_desc_string=unknown
[06/06/15 17:56:34.310 UTC 515 10205] SSL_state_string=SSLv3 write certificate request A
[06/06/15 17:56:34.310 UTC 516 10205] SSL state = 0x2100; where = 0x2001; ret = 0x1
[06/06/15 17:56:34.310 UTC 517 10205] ret_type_string=unknown
[06/06/15 17:56:34.310 UTC 518 10205] ret_desc_string=unknown
[06/06/15 17:56:34.310 UTC 519 10205] SSL_state_string=SSLv3 flush data
[06/06/15 17:56:34.310 UTC 51a 10205] SSL state = 0x2180; where = 0x2002; ret = 0xffffffff
[06/06/15 17:56:34.310 UTC 51b 10205] ret_type_string=unknown
[06/06/15 17:56:34.310 UTC 51c 10205] ret_desc_string=unknown
[06/06/15 17:56:34.310 UTC 51d 10205] SSL_state_string=SSLv3 read client certificate A
[06/06/15 17:56:34.310 UTC 51e 10205] -- returns WANT_READ for conn ssl 590a6048
[06/06/15 17:56:34.610 UTC 51f 10205] doSSLRecvLoop: Handshake has not completed for conn 0
[06/06/15 17:56:34.610 UTC 520 10205] sslConnectionInit: SSL_do_handshake for conn ssl 590a6048, conn state: INIT, SSL state: HANDSHAKING
[06/06/15 17:56:34.616 UTC 521 10205] Peer certificate Validation Done for conn ssl 590a6048, calling authlist..
[06/06/15 17:56:34.622 UTC 522 10205] Authlist authentication successful for conn ssl 590a6048
 [06/06/15 17:56:35.616 UTC 523 10205] Peer Validated against the AuthList
[06/06/15 17:56:35.616 UTC 524 10205] SSL state = 0x2180; where = 0x2001; ret = 0x1
[06/06/15 17:56:35.616 UTC 525 10205] ret_type_string=unknown
[06/06/15 17:56:35.616 UTC 526 10205] ret_desc_string=unknown
[06/06/15 17:56:35.616 UTC 527 10205] SSL_state_string=SSLv3 read client certificate A
[06/06/15 17:56:35.633 UTC 528 10205] SSL state = 0x2190; where = 0x2001; ret = 0x1
[06/06/15 17:56:35.633 UTC 529 10205] ret_type_string=unknown
[06/06/15 17:56:35.633 UTC 52a 10205] ret_desc_string=unknown
[06/06/15 17:56:35.633 UTC 52b 10205] SSL_state_string=SSLv3 read client key exchange A

[06/06/15 17:56:35.635 UTC 52c 10205] SSL state = 0x21a0; where = 0x2001; ret = 0x1
[06/06/15 17:56:35.636 UTC 52d 10205] ret_type_string=unknown
[06/06/15 17:56:35.636 UTC 52e 10205] ret_desc_string=unknown
[06/06/15 17:56:35.636 UTC 52f 10205] SSL_state_string=SSLv3 read certificate verify A
[06/06/15 17:56:35.636 UTC 530 10205] SSL state = 0x21c0; where = 0x2001; ret = 0x1
[06/06/15 17:56:35.636 UTC 531 10205] ret_type_string=unknown
[06/06/15 17:56:35.636 UTC 532 10205] ret_desc_string=unknown
--More-- [06/06/15 17:56:35.636 UTC 533 10205] SSL_state_string=SSLv3 read finished A
[06/06/15 17:56:35.636 UTC 534 10205] SSL state = 0x21d0; where = 0x2001; ret = 0x1
[06/06/15 17:56:35.636 UTC 535 10205] ret_type_string=unknown
[06/06/15 17:56:35.636 UTC 536 10205] ret_desc_string=unknown
[06/06/15 17:56:35.636 UTC 537 10205] SSL_state_string=SSLv3 write change cipher spec A
[06/06/15 17:56:35.636 UTC 538 10205] SSL state = 0x21e0; where = 0x2001; ret = 0x1
[06/06/15 17:56:35.636 UTC 539 10205] ret_type_string=unknown
[06/06/15 17:56:35.636 UTC 53a 10205] ret_desc_string=unknown
[06/06/15 17:56:35.636 UTC 53b 10205] SSL_state_string=SSLv3 write finished A
[06/06/15 17:56:35.637 UTC 53c 10205] SSL state = 0x2100; where = 0x2001; ret = 0x1
[06/06/15 17:56:35.637 UTC 53d 10205] ret_type_string=unknown
[06/06/15 17:56:35.637 UTC 53e 10205] ret_desc_string=unknown
[06/06/15 17:56:35.637 UTC 53f 10205] SSL_state_string=SSLv3 flush data
[06/06/15 17:56:35.637 UTC 540 10205] SSL state = 0x3; where = 0x20; ret = 0x1
[06/06/15 17:56:35.637 UTC 541 10205] ret_type_string=unknown
[06/06/15 17:56:35.637 UTC 542 10205] ret_desc_string=unknown
[06/06/15 17:56:35.637 UTC 543 10205] SSL_state_string=SSL negotiation finished successfully
[06/06/15 17:56:35.637 UTC 544 10205] SSL state = 0x3; where = 0x2002; ret = 0x1
--More-- [06/06/15 17:56:35.637 UTC 545 10205] ret_type_string=unknown
[06/06/15 17:56:35.637 UTC 546 10205] ret_desc_string=unknown
[06/06/15 17:56:35.637 UTC 547 10205] SSL_state_string=SSL negotiation finished successfully
[06/06/15 17:56:35.637 UTC 548 10205] SSL_do_handshake() succeeded for conn ssl 590a6048
[06/06/15 17:56:35.637 UTC 549 10205] NMSP connection success! for conn 0