Troubleshoot Common Issues for IRCM

Mobility tunnels are not coming up

Check if the CA certificates are configured correctly. To verify this try to join an AP to the controller. If it joins then the certificates are fine. otherwise, if the error is in dtls phase, please reconfigure the CA certificates on the controller

Issues with Mobility tunnel

1. Enable the mobility debugs.

   debug mobility handoff enable

   debug mobility error enable

   debug mobility dtls error enable

   debug mobility dtls event enable

   debug mobility pmtu-discovery enable

   debug mobility config enable

   debug mobility directory enable

2. Reproduce the configuration and verify the output.

   The following is an example of a successful mobility tunnel.

```
*capwapPingSocketTask: Feb 07 09:53:38.507: Client initiating connection on
172.16.0.5:16667 <-> 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.507: Sending packet to 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.508: Received DTLS packet from mobility peer
172.16.0.21 bytes: 48
*capwapPingSocketTask: Feb 07 09:53:38.508: mm_dtls2_process_data_rcv_msg:1207 rcvBufLen
 48 clr_pkt_len 2048 peer ac100015
*capwapPingSocketTask: Feb 07 09:53:38.508: Record    : type=22, epoch=0, seq=0
*capwapPingSocketTask: Feb 07 09:53:38.508:   Hndshk : type=3, len=23 seq=0, frag_off=0,
 frag_len=23
*capwapPingSocketTask: Feb 07 09:53:38.508: Handshake in progress for link
172.16.0.5:16667 <-> 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.508: Sending packet to 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.508: DTLS consumed packet from mobility peer
172.16.0.21 bytes: 48
!
!<--output-omited-->
!
*capwapPingSocketTask: Feb 07 09:53:38.511: dtls2_cert_verify_callback: Forcing
```

```
Certificate validation as success
*capwapPingSocketTask: Feb 07 09:53:38.511: Peer certificate verified.
*capwapPingSocketTask: Feb 07 09:53:38.511: Handshake in progress for link
172.16.0.5:16667 <-> 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.511: Nothing to send on link 172.16.0.5:16667 <->
 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.511: DTLS consumed packet from mobility peer
172.16.0.21 bytes: 503
*capwapPingSocketTask: Feb 07 09:53:38.511: Received DTLS packet from mobility peer
172.16.0.21 bytes: 56
*capwapPingSocketTask: Feb 07 09:53:38.511: mm_dtls2_process_data_rcv_msg:1207 rcvBufLen
 56 clr_pkt_len 2048 peer ac100015
*capwapPingSocketTask: Feb 07 09:53:38.511: Record    : type=22, epoch=0, seq=6
*capwapPingSocketTask: Feb 07 09:53:38.511:   Hndshk : type=13, len=6 seq=3, frag_off=0,
 frag_len=6
*capwapPingSocketTask: Feb 07 09:53:38.523: Handshake in progress for link
172.16.0.5:16667 <-> 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.523: Sending packet to 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.523: Sending packet to 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.523: Sending packet to 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.523: Sending packet to 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.523: Sending packet to 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.524: Sending packet to 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.524: Sending packet to 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.524: DTLS consumed packet from mobility peer
172.16.0.21 bytes: 56
*capwapPingSocketTask: Feb 07 09:53:38.527: Received DTLS packet from mobility peer
172.16.0.21 bytes: 91
*capwapPingSocketTask: Feb 07 09:53:38.527: mm_dtls2_process_data_rcv_msg:1207 rcvBufLen
 91 clr_pkt_len 2048 peer ac100015
*capwapPingSocketTask: Feb 07 09:53:38.527: Record    : type=20, epoch=0, seq=8
*capwapPingSocketTask: Feb 07 09:53:38.527: Connection established for link
172.16.0.5:16667 <-> 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.527: ciperspec 1
*capwapPingSocketTask: Feb 07 09:53:38.527: Nothing to send on link 172.16.0.5:16667 <->
 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.527: DTLS consumed packet from mobility peer
172.16.0.21 bytes: 91
*mmMobility: Feb 07 09:53:38.527: DTLS Action Result message received
*mmMobility: Feb 07 09:53:38.527:  Key plumb succeeded
*mmMobility: Feb 07 09:53:38.527: mm_dtls2_callback: Connection established with
172.16.0.21:16667
*mmMobility: Feb 07 09:53:38.527: mm_dtls2_db_status_up:895 Connections status up for
entry 172.16.0.21:16667
*mmMobility: Feb 07 09:53:38.527: mm_dtls2_callback: DTLS Connection established with
172.16.0.21:16667, Sending update msg to mobility HB
```

Recommended Solutions

Tunnel flaps periodically

Check if keepalive interval and count configuration is matching on both peers.

Both control and data are down

Check group name configuration: the peer group name must match the local group name on the peer.

Data port is down

Check data port plumbing.

Punting issue is suspected,

Check LSMPI/LFTS debug from kernel.

```
# Enable
echo 5 > /sys/module/lfts/parameters/lfts_log
sysctl lsmpi.transport_log=5

# Disable
echo 0 > /sys/module/lfts/parameters/lfts_log
sysctl lsmpi.transport_log=1
```

Sample output below:

Data for port 16666 (0x411a) and 16667 (0x411b), "Socket lookup for UDP was successful" means LFTS did intercept packet from LSMPI.

```
[LSMPI Trans Rx Verbose] intercept:cause:97
[LSMPI Trans Rx Info] intercept: recvd pkt with ftr len: 28
[LFTS Rx Debug] Intercept: Got udp dest port 16666
[LFTS Rx Verbose] Socket lookup for port: 16666, app_tag: 11, inst_id:0, ether_type: 8
[LFTS Rx Verbose] Socket lookup for UDP was successful.
[LSMPI Trans Rx Verbose] intercept: head ffff8800b3b2d000 data ffff8800b3b2d04e
[LSMPI Trans Rx Debug] intercept:len 101 total_offset 74
[LSMPI Trans Rx Verbose] SKB->Data
ffff8800b3b2d04e: 45000065 c6694000 3f1110cf 1e1e1e08
ffff8800b3b2d05e: 14141416 411a411a 00514c78 00100000
ffff8800b3b2d06e: 00000000 15000a00 00410000 00000144
ffff8800b3b2d07e: 00000000 00000000 23e8187e a1c3da7a
ffff8800b3b2d08e: 7fdd2116 78180cc5 64010016 1e1e1e08
[LSMPI Trans Rx Info] table_id:0x0|client_id:0x0|app_tag:11|inst_id:0
[LSMPI Trans Rx Info] raw_offset:0, opq_info_len:12, transport_punt_hdr_len:16,
opq_data_len:8[LSMPI Trans Rx Verbose] After possible feature header copy
ffff8800b3b2d04e: 45000065 c6694000 3f1110cf 1e1e1e08
ffff8800b3b2d05e: 14141416 411a411a 00514c78 00100000
ffff8800b3b2d06e: 00000000 15000a00 00410000 00000144
ffff8800b3b2d07e: 00000000 00000000 23e8187e a1c3da7a
ffff8800b3b2d08e: 7fdd2116 78180cc5 64010016 1e1e1e08
[LFTS Rx Debug] skb->len 101 proto 8 eth ffff8800b3b2d040 head ffff8800b3b2d000 data
ffff8800b3b2d04e
[LFTS Rx Verbose] netif_rx returned 0
ffff8802296004a0: 0101010c 07001a41 1a410000 00000000
ffff8802296004b0: 45c0006a ba764000 40111afd 14141416
ffff8802296004c0: 1e1e1e08 411a411a 0056fc7c 00100000
[LFTS Tx Debug] SK: length 109, table-id 0x0
[LFTS Tx Debug] SK: mtu 1500, opq-type 0x1
[LFTS Tx Debug] ip dest 30.30.30.8, src 20.20.20.22, protocol id 17
[LFTS Tx Verbose] injected ip packet
ffff8800b4137210: 4500006d cf274000 40110709 14141416
ffff8800b4137220: 1e1e1e08 411b411b 0059a921 00100008
ffff8800b4137230: 00000000 00000000 00000000 00000000
ffff8800b4137240: 00000000 00000100 3700006f 01002a01
ffff8800b4137250: 01000000 0003cb58 b0085716 f40bb05a
[LSMPI Trans Tx Debug] get_l3_info_l2_offset: skb->proto: 0x800
[LSMPI Trans Tx Debug] Getting L3 info from skb
[LSMPI Trans Tx Info] Transport Inj, ftr hdr len 16
[LSMPI Trans Rx Debug] L3 info:
table_id:0x0|prio:0x0|pal_if_handle:0x0|fea_hdr_len:16|client_id:0x0
[LSMPI Trans Tx Debug] Using Hdr type: 2|cause: 43
[LSMPI Trans Tx Debug] LSMPI Inject Buf
ffff880229600080: 01020000 0000006d 009d1000 20010000
[LSMPI Trans Rx Verbose] intercept:cause:97
[LSMPI Trans Rx Info] intercept: recvd pkt with ftr len: 28
[LFTS Rx Debug] Intercept: Got udp dest port 16667
[LFTS Rx Verbose] Socket lookup for port: 16667, app_tag: 8, inst_id:0, ether_type: 8
```

```
ffff880229600090: 00000000 00000000 01000001 40002b00
ffff8802296000a0: 0101010c 07001b41 1b410000 00000000
ffff8802296000b0: 4500006d cf274000 40110709 14141416
ffff8802296000c0: 1e1e1e08 411b411b 0059a921 00100008
[LFTS Tx Debug] SK: length 109, table-id 0x0
[LFTS Tx Debug] SK: mtu 1500, opq-type 0x1
[LFTS Tx Debug] ip dest 30.30.30.8, src 20.20.20.22, protocol id 17
[LFTS Tx Verbose] injected ip packet
ffff8800b4137210: 4500006d f5e64000 4011e049 14141416
ffff8800b4137220: 1e1e1e08 411b411b 00599e21 00100008
ffff8800b4137230: 00000000 00000000 00000000 00000000
ffff8800b4137240: 00000000 00000100 3700006f 01002a01
ffff8800b4137250: 01000000 0003cc58 b0086116 f40bb05a
[LSMPI Trans Tx Debug] get_l3_info_l2_offset: skb->proto: 0x800
[LSMPI Trans Tx Debug] Getting L3 info from skb
[LSMPI Trans Tx Info] Transport Inj, ftr hdr len 16
[LSMPI Trans Rx Debug] L3 info:
table_id:0x0|prio:0x0|pal_if_handle:0x0|fea_hdr_len:16|client_id:0x0
[LSMPI Trans Tx Debug] Using Hdr type: 2|cause: 43
[LSMPI Trans Tx Debug] LSMPI Inject Buf
ffff880229600480: 01020000 0000006d 009d1000 20010000
ffff880229600490: 00000000 00000000 01000001 40002b00
[LSMPI Trans Rx Verbose] intercept:cause:97
[LSMPI Trans Rx Info] intercept: recvd pkt with ftr len: 28
[LFTS Rx Debug] Intercept: Got udp dest port 16667
[LFTS Rx Verbose] Socket lookup for port: 16667, app_tag: 8, inst_id:0, ether_type: 8
ffff8802296004a0: 0101010c 07001b41 1b410000 00000000
ffff8802296004b0: 4500006d f5e64000 4011e049 14141416
ffff8802296004c0: 1e1e1e08 411b411b 00599e21 00100008
[LFTS Tx Debug] SK: length 109, table-id 0x0
[LFTS Tx Debug] SK: mtu 1500, opq-type 0x1
[LFTS Tx Debug] ip dest 30.30.30.8, src 20.20.20.22, protocol id 17
```

Mobility tunnels are going down

Check if peer IP addresses are correctly configured.

```
Device#show wireless mobility summary
Mobility Summary
Wireless Management VLAN: 10
Wireless Management IP Address: 9.10.10.17
Mobility Control Message DSCP Value: 48
Mobility Keepalive Interval/Count: 10/3
Mobility Group Name: test123-mob
Mobility Multicast Ip: 0.0.0.0
Link Status is Control Link Status : Data Link Status
DTLS Status is Control DTLS Status : Data DTLS Status
Controllers configured in the Mobility Domain:
 IP              Public Ip         Group Name                    Multicast IP       Link
 Status     DTLS Status              PMTU
───────────────────────────────────────────────────────────────────────────────────────
9.10.10.17        N/A              test123-mob                   0.0.0.0            N/A
          N/A
9.10.10.22        9.10.10.22       test123-mob                   0.0.0.0            UP
   : UP      Key Plumbed  : Key Plumbed  1385
9.10.10.24        9.10.10.24       test123-mob                   0.0.0.0            UP
   : UP      Key Plumbed  : Key Plumbed  1385
```

Recommended Solution

Check if the mobility group name is the same on the peer controllers.

```
Device#show wireless mobility summary
Mobility Summary
Wireless Management VLAN: 10
```

```
Wireless Management IP Address: 9.10.10.17
Mobility Control Message DSCP Value: 48
Mobility Keepalive Interval/Count: 10/3
Mobility Group Name: test123-mob
Mobility Multicast Ip: 0.0.0.0
Link Status is Control Link Status : Data Link Status
DTLS Status is Control DTLS Status : Data DTLS Status
Controllers configured in the Mobility Domain:
 IP            Public Ip        Group Name                      Multicast IP      Link
  Status    DTLS Status              PMTU
_____
9.10.10.17       N/A             test123-mob                     0.0.0.0           N/A
             N/A
9.10.10.22       9.10.10.22      test123-mob                     0.0.0.0           UP
   : UP     Key Plumbed : Key Plumbed  1385
9.10.10.24       9.10.10.24      test123-mob                     0.0.0.0           UP
   : UP     Key Plumbed : Key Plumbed  1385
```

Check if the peers are added with data link encryption

```
Device#show running-config | inc mobility
wireless mobility group member ip 9.10.10.22 public-ip 9.10.10.22 group test123-mob
data-link-encryption
wireless mobility group member ip 9.10.10.24 public-ip 9.10.10.24 group test123-mob
data-link-encryption
wireless mobility group name test123-mob
```

Check if mping and cping of the peers working from AireOS controller.

```
Device>mping 9.10.10.24
Send count=3, Receive count=3 from 9.10.10.24
Device>cping 9.10.10.17
Send count=3, Receive count=3 from 9.10.10.17
```

DTLS keys plumb status shows NA

Check if the SSC (trust-point) configurations are fine on the box.

```
Device#show running-config | inc trust
```

Check if the data-link-encryption is used while configuring the mobility peers.

```
Device#show running-config | inc mobility
wireless mobility group member ip 9.10.10.22 public-ip 9.10.10.22 group test123-mob
data-link-encryption
wireless mobility group member ip 9.10.10.24 public-ip 9.10.10.24 group test123-mob
data-link-encryption
```

Tunnels are not coming up immediately

1. Wait for at least five minutes. Generally, it takes a minimum of five minutes for the tunnels to come up after the reboot.

2. Check if the IP addresses are same.

3. Check if the MAC address is same on AireOS controller.There was an issue on the EWLC, if the software load is changed, the MAC address of the wireless management interface is getting changed.

Possible Cause

Recommended Solution 1 - Disable and enable the radio on client

1. From the Anyconnect tool, disable and enable the radio.

2. From the **Control Panel** > **Network and Internet** > **Network Connections** window, try disabling and enabling the wireless interface.

Recommended Solution 2 - Check if the AP status is enabled

```
Device##show ap status
AP Name                                 Status                  Mode            Country
-----------------------------------------------------------------------
ap_3802_abc                   Enabled                       FlexConnect          IN
```

Recommended Solution 3 - Check if the AP state is registered

```
AP Name                              Slots    AP Model  Ethernet MAC   Radio MAC
Location            Country      IP Address                             State
----------------------------------------------------------------------------------
ap_3802_abc                             3      3802I    a0e0.af4d.1d88 70db.9899.49e0
   default location    IN        9.10.10.144                           Registered
```

Recommended Solution 4 - Check if the AP admin and operational status of radio is enabled

```
Device#show ap dot11 5ghz summary
AP Name                          Mac Address    Slot   Admin State   Oper State   Width
   Txpwr          Channel
----------------------------------------------------------------------------------
ap_3802_abc              70db.9899.49e0  1       Enabled       Up
20      1/6 (16 dBm)    (60)
```

Recommended Solution 5 - Check if the AP country is valid

```
Device#show ap summary
Number of APs: 1

AP Name                              Slots    AP Model  Ethernet MAC   Radio MAC
Location            Country      IP Address                             State
----------------------------------------------------------------------------------
ap_3802_abc                             3      3802I    a0e0.af4d.1d88 70db.9899.49e0 default
location      IN         9.10.10.144                             Registered
```

Recommended Solution 5 - Check if the AP is broadcasting the BSSIDs

```
Device#show ap name ap_3802_abc wlan dot11 5ghz
WLAN ID    BSSID
------------------------
7          70db.9899.49ef
6          70db.9899.49ee
1          70db.9899.49ed
14         70db.9899.49ec
13         70db.9899.49eb
10         70db.9899.49ea
9          70db.9899.49e9
```

Note   Default behavior is WLANs whose WLAN ID below 16 will be pushed to AP.If you don't want this limitation then you need to create new site tag.

Recommended Solution 6 - Check if the radio interface is enabled on the AP

```
ap_2802_abc#show ip int brief
Interface          IP-Address      Method     Status                   Protocol    Speed
   Duplex
wired0             9.10.10.189     DHCP       up                       up          1000
     full
wired1             unassigned      unset      down                     down        n/a
```

```
      unknown
apphostintf1     unassigned     DHCP          up                            up          n/a
    n/a
wifi0            n/a            n/a           up             up                           n/a
    n/a
wifi1            n/a            n/a           administatively down  down      n/a
 n/a
```

Recommended Solution 7 - Check if the power level of the AP radio is good

```
abc-mob-1#show ap dot11 5ghz summary
AP Name                          Mac Address     Slot    Admin State    Oper State    Width
   Txpwr          Channel
_____

ap_3802_abc              70db.9899.49e0  1       Enabled        Up
20      1/6 (16 dBm)   (60)
```

Recommended Solution 8 - Check if the Channel number is good one (should be 60 or 64 for 5gz radios)

```
abc-mob-1#show ap dot11 5ghz summary
AP Name                          Mac Address     Slot    Admin State    Oper State    Width
   Txpwr          Channel
_____

ap_3802_abc              70db.9899.49e0  1       Enabled        Up
20      1/6 (16 dBm)   (60)
```

Recommended Solution 9 - Check if the client is in exclusion list (you can check using two commands)

```
Device#show wireless client summary
Number of Local Clients: 1

MAC Address    AP Name                                 WLAN   State
Protocol Method    Role
-------------------------------------------------------------------------------------------------
1491.82b8.fdd4 ap_3802_abc                             9      Run              11n(5)
 None      Local

Number of Excluded Clients: 1

MAC Address    AP Name                        WLAN    State           Protocol Method

-------------------------------------------------------------------------------------------------
1232.1233.1234                                0       Excluded        N/A     None


Device#show wireless exclusionlist
Excluded Clients

MAC Address       Description                  Exclusion Reason
Time Remaining
-------------------------------------------------------------------------------------------------
1232.1233.1234    test                         Manually Excluded
        N/A
```

Recommended Solution 10 - Check if the wlan is enabled

```
Device#show wlan summary

Number of WLANs: 14

WLAN Profile Name                    SSID                          Status
--------------------------------------------------------------------------------
1    abc-mob-open                    abc-mob-open                  UP
2    abc-mob-mab                     abc-mob-mab                   UP
```

Recommended Solution 11 - Check if the policy profile is enabled

```
Device#show wireless profile policy summary

Number of Policy Profiles: 12

Policy Profile Name              Description                                   Status
---------------------------------------------------------------------------------------
pp-open
 ENABLED
pp-dot1x
 ENABLED
asim43-policy
ENABLED
guest-policy-tag
DISABLED
default-flex-profile
DISABLED
```

Recommended Solution 12 - Try creating a new UNIQUE wlan and join the client to it

```
wlan abc-mob-mab 2 abc-mob-mab
mac-filtering default
no security wpa akm dot1x
no security wpa wpa2 ciphers aes
no shutdown
```

Recommended Solution 13 - If localmode scenario, check if the switching is central

```
Device#show running-config | sec named-policy-profile
wireless profile policy named-policy-profile
 aaa-override
 no central switching    → this is wrong, it should be "central switching" for locamode.
 cts sgt 2222
 ipv4 dhcp opt82 format apname
 nac
 no shutdown
```

Recommended Solution 14 - Make sure the client is near the AP physically

In the lab, place the client near the APs.

Recommended Solution 15 - Check if the auto-anchor configuration is enabled on the policy profile. It should not be enabled

```
Device#show running-config | sec pp-dot1x
wireless profile policy pp-dot1x
aaa-override
mobility anchor
cts inline-tagging
vlan 11
no shutdown
```

Recommended Solution 16 - Check if the ISE/AAA server is reachable

```
Device#
srihari-mob-1#test aaa group radius wpr wpr123 new-code
The process for the command is not responding or is otherwise unavailable
User successfully authenticated

USER ATTRIBUTES

username             0    "wpr"
Message-Authenticato 0    <hidden>
security-group-tag   0    "0015-25"
```

```
Device#ping 9.10.8.247
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 9.10.8.247, timeout is 2 seconds:
!!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
srihari-mob-1#
```

Recommended Solution 17 - Client is NOT able to get authenticated

1. Check if the client is in exclusion state.

2. Check if the credentials are same as configured on ISE/Local

3. Check if the secuty types are configured correctly on the client for this ssid.

4. Check if the ISE is able receive the request

5. Check the live-logs on ISE to see why the client is not getting authenticated.

AP Issues - Admin status is up, but oper status is down

Recommended Solution 1 - check if the "show ap tag summary" has no misconfiguration

```
Device#show ap tag summary
Number of APs: 1

AP Name                 AP Mac          Site Tag Name           Policy Tag Name
RF Tag Name             Misconfigured   Tag Source
_____

ap_2802_abcdef          500f.804c.5d42  default-site-tag        pt-all
default-rf-tag                    No              Static
```

Check if the wifi radios are up on AP using "show ip interface brief" If they are down, to do devshell and bring them up.

```
Device#devshell
EXITING CISCO SHELL. PLEASE EXECUTE EXIT IN DEVSHELL TO GET BACK TO CISCO SHELL.
BusyBox v1.23.2 (2018-06-19 13:03:00 PDT) built-in shell (ash)
Device:/# ifconfig wifi1 up
Device:/#ifconfig wifi0 up
```

Check the country code on AP and Controller for that AP

On the controller

```
Device#show ap status
AP Name                              Status    Mode         Country
-------------------------------------------------------------------
ap_2802_abcdefg                      Enabled   Local        IN
```

Check if the global dot11 radio is shutdowned from configuration

```
Device#config term
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#no ap dot11 5ghz shutdown
Device(config)#no ap dot11 24ghz shutdown
```

Check if the country code for the AP and the radios on AP has same

On the controller

```
Device#show ap status
AP Name                              Status    Mode         Country
-------------------------------------------------------------------
```

```
ap_3802_abcdefg                    Disabled   Local          IN
ap_1852_abcdefg_hi                 Enabled    FlexConnect    IN
```