Converged Access Controller AP Join Issue  
Troubleshoot with Traces

This document describes about trace commands that are used to troubleshoot Access Point (AP) join issues on converged access controllers and some of the common reasons for AP join failure.

- Prerequisites, page 1
- AP Join Sequence and Troubleshoot, page 3
- Common Reasons for AP Join Failure, page 14
- General Technical Tips on Trace Commands, page 17

Prerequisites

You should have basic knowledge on following topics:

Supported Platforms and Releases

The information in this document is based on a Cisco Catalyst 3850 Series Switch that runs software Version 3.3.0 SE.


- Lightweight Access Point (LAP) and Wireless LAN Controller (WLC) configurations for basic operation.

Note

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, make sure that you understand the potential impact of any command.
Associated Products

The following listed products are applicable to all converged access controllers:

- Cisco Catalyst 3560 Series Switches
- Cisco Catalyst 3850 Series Switches
AP Join Sequence and Troubleshoot

AP Join Sequence

The following figure depicts the join sequences between an Access Point and Wireless Control Module (WCM).

Figure 1: Join sequences between an Access Point and Wireless Control Module (WCM).
Troubleshoot

Basic Steps

Perform the following task to troubleshoot the AP join issues on converged access controllers:

1. First, confirm that the AP is able to pull an IP address.
2. From the switch where the AP is plugged in, enter the following command:
   
   ```bash
   # show cdp neighbor <port_id> detail
   ```

   The AP should be connected to the Cisco Catalyst 3850 Series Switch and the switchport must be configured as:
   ```bash
   Interface gig <>
   Switchport mode access
   Switchport access vlan x
   ```
   (Where x is the wireless management interface and vlan x configured on the Cisco Catalyst 3850 Series Switch)

   Note

   3. Make sure that the WLC can ping the IP address and vice versa.

   4. To verify that a wireless mobility controller (MC) is configured on the network, enter the following command:

   ```bash
   #show wireless mobility summary
   ```

   Note

   5. Confirm the AP license is enabled on the MC:

   ```bash
   #show license right-to-use summary
   ```

   6. Authorize the correct country code is enabled:

   ```bash
   #show wireless country configured
   ```

Traces from Controller

If AP fails even after configuration is successful, use the following trace commands on the controller in order to troubleshoot CAPWAP and AP join:

- ```bash
  #Set trace capwap
  ```
- ```bash
  #Set trace capwap ap
  ```
- ```bash
  #Set trace group-ap
  ```

Based on the review of trace outputs, the group-ap traces provides more significant output to troubleshoot the AP join. Hence this trace (unfiltered) is discussed in detail.

Refer to the General Technical Tips on Trace Commands section for more information about filtering options and limitations on this trace.
Sample output (filtered and unfiltered) for `capwap` and `capwap ap` is included for reference.

### Default settings of the `group-ap`

To view the default settings of the `group-ap` trace, enter the following command:

```bash
#show trace settings group-ap
```

<table>
<thead>
<tr>
<th>Buffer Properties</th>
<th>Size</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>capwap/ap/event</td>
<td>0</td>
<td>warning</td>
</tr>
<tr>
<td>dtls/ap/event</td>
<td>0</td>
<td>warning</td>
</tr>
<tr>
<td>iosd-wireless/capwap</td>
<td>0</td>
<td>warning</td>
</tr>
</tbody>
</table>

Feature-Name: `capwap/ap/event`
Filters: None

Feature-Name: `dtls/ap/event`
Filters: None

Feature-Name: `iosd-wireless/capwap`
Filters: None

By default, there are no filters set on any of the traces.

### Clearing the `group-ap`

To clear the trace buffer that corresponds to the `group-ap` trace, enter the following command:

```bash
#set trace control group-ap clear
```

### Setting the trace level `group-ap`

Enter the following command to set the trace level for the `group-ap`:

```bash
#set trace group-ap level ?
```

- debug   Debug-level messages (7)
- default Unset Trace Level Value
- err     Error conditions (3)
- info    Informational (6)
- warning Warning conditions (4)

Use the `#set trace group-ap level debug` to debug while you troubleshoot the issues.

### Verifying the tracing level

To verify the tracing level, enter the following command:

```bash
#show trace settings group-ap
```

<table>
<thead>
<tr>
<th>Buffer Properties</th>
<th>Size</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>capwap/ap/event</td>
<td>0</td>
<td>debug</td>
</tr>
<tr>
<td>dtls/ap/event</td>
<td>0</td>
<td>debug</td>
</tr>
<tr>
<td>iosd-wireless/capwap</td>
<td>0</td>
<td>debug</td>
</tr>
</tbody>
</table>

Feature-Name: `capwap/ap/event`
Viewing trace output of group-ap

To view the trace output of group-ap, enter the following command:

```
# show trace messages group-ap
```

**Discovery-Request / Response**

```
[11/14/13 14:50:17.484 UTC 702f4a 8528] f84f.57ca.3860 Discovery Request from 10.201.234.24
[11/14/13 14:50:17.484 UTC 702f4b 8528] f84f.57ca.3860 Discovery apType = 0, apModel = AIR-CAP2602I-A-K9, Discovery supportedRadios = 0, incomingRadJoinPriority = 1, Discovery versionNum = 167863296
[11/14/13 14:50:17.484 UTC 702f4c 8528] f84f.57ca.3860 Join Priority Processing status = 0, Incoming Ap's Priority 1, MaxLrads = 50, joined Aps = 0
[11/14/13 14:50:17.484 UTC 702f4e 8528] f84f.57ca.3860 Encode static AP manager 10.201.234.4, AP count 0
[11/14/13 14:50:17.484 UTC 702f4f 8528] acEncodeMwarTypePayload encode mwarType = 0 in capwapMwarTypePayload.
'''

**DTLS-Handshake**

```
[11/14/13 14:50:27.484 UTC 702f52 8528] acDtlsCallback: entering...
[11/14/13 14:50:27.484 UTC 59 8528] Incremented concurrent handshaking count 1
[11/14/13 14:50:27.484 UTC 5a 8528] f84f.57ca.3860 record=Handshake epoch=0 seq=0
[11/14/13 14:50:27.484 UTC 5b 8528] f84f.57ca.3860 msg=ClientHello len=44 seq=0 frag_off=0 frag_len=44
[11/14/13 14:50:27.485 UTC 5c 8528] f84f.57ca.3860 Handshake in progress...
[11/14/13 14:50:27.489 UTC 5d 8528] f84f.57ca.3860 record=Handshake epoch=0 seq=1
[11/14/13 14:50:27.489 UTC 5e 8528] f84f.57ca.3860 msg=ClientHello len=76 seq=1 frag_off=0 frag_len=76 (with cookie)
[11/14/13 14:50:27.490 UTC 5f 8528] f84f.57ca.3860 Handshake in progress...
[11/14/13 14:50:27.670 UTC 60 8528] f84f.57ca.3860 record=Handshake epoch=0 seq=2
```
[11/14/13 14:50:27.670 UTC 61 8528] f84f.57ca.3860 msg=Certificate len=1146
seq=2 frag_off=0 frag_len=519
[11/14/13 14:50:27.670 UTC 62 8528] f84f.57ca.3860 Handshake in progress...
[11/14/13 14:50:27.670 UTC 63 8528] f84f.57ca.3860 record=Handshake epoch=0 seq=3
[11/14/13 14:50:27.670 UTC 64 8528] f84f.57ca.3860 msg=Certificate len=1146
seq=2 frag_off=519 frag_len=519
[11/14/13 14:50:27.670 UTC 65 8528] f84f.57ca.3860 Handshake in progress...
[11/14/13 14:50:27.670 UTC 66 8528] f84f.57ca.3860 record=Handshake epoch=0 seq=4
[11/14/13 14:50:27.670 UTC 67 8528] f84f.57ca.3860 msg=Certificate len=1146
seq=2 frag_off=1038 frag_len=108
[11/14/13 14:50:27.671 UTC 702f54 8528] acDtlsCallback: entering...
[11/14/13 14:50:27.672 UTC 68 8528] Verify X.509 certificate from wtp 7c69.f604.9460
[11/14/13 14:50:27.673 UTC 702f56 8528] acDtlsCallback Cert validation PENDING
[11/14/13 14:50:27.673 UTC 69 8528] f84f.57ca.3860 Certificate verification - pending...
[11/14/13 14:50:27.673 UTC 6a 8528] f84f.57ca.3860 Handshake in process.. awaiting certificate verification result..
[11/14/13 14:50:27.673 UTC 6b 8528] f84f.57ca.3860 record=Handshake epoch=0 seq=5
[11/14/13 14:50:27.673 UTC 6c 8528] f84f.57ca.3860 msg=ClientKeyExchange len=130 seq=3 frag_off=0 frag_len=130
[11/14/13 14:50:27.673 UTC 702f57 8528] acDtlsCallback: entering...
[11/14/13 14:50:27.674 UTC 6e 8528] Verify X.509 certificate from wtp 7c69.f604.9460
[11/14/13 14:50:27.675 UTC 702f58 8528] acDtlsCallback Cert validation PENDING
[11/14/13 14:50:27.675 UTC 6f 8528] f84f.57ca.3860 Certificate verification - pending...
[11/14/13 14:50:27.675 UTC 70 8528] f84f.57ca.3860 Handshake in process.. awaiting certificate verification result..
[11/14/13 14:50:27.675 UTC 71 8528] f84f.57ca.3860 record=Handshake epoch=0 seq=6
[11/14/13 14:50:27.675 UTC 72 8528] f84f.57ca.3860 msg=CertificateVerify len=258 seq=4 frag_off=0 frag_len=258
[11/14/13 14:50:27.675 UTC 72f5a 8528] acDtlsCallback: entering...
[11/14/13 14:50:27.675 UTC 72f5b 8528] acDtlsCallback: cb->code 3
[11/14/13 14:50:27.676 UTC 73 8528] Verify X.509 certificate from wtp 7c69.f604.9460
[11/14/13 14:50:27.676 UTC 72f5c 8528] acDtlsCallback Cert validation PENDING
[11/14/13 14:50:27.676 UTC 73 8528] f84f.57ca.3860 Certificate verification - pending...
[11/14/13 14:50:27.676 UTC 74 8528] f84f.57ca.3860 Handshake in process.. awaiting certificate verification result..
[11/14/13 14:50:27.677 UTC 75 8528] f84f.57ca.3860 record=ChangeCipherSpec
epoch=0 seq=7  
[11/14/13 14:50:27.677 UTC 702f5d 8528] acDtlsCallback: entering...  
[11/14/13 14:50:27.677 UTC 702f5e 8528] acDtlsCallback: cb->code 3  
[11/14/13 14:50:27.677 UTC 76 8528] Verify X.509 certificate from wtp 7c69.f604.9460  
[11/14/13 14:50:27.678 UTC 702f5f 8528] acDtlsCallback Cert validation PENDING  
[11/14/13 14:50:27.678 UTC 77 8528] f84f.57ca.3860 Certificate verification - pending...  
[11/14/13 14:50:27.678 UTC 78 8528] f84f.57ca.3860 Handshake in process.. awaiting certificate verification result..  
[11/14/13 14:50:27.678 UTC 79 8528] f84f.57ca.3860 record=Handshake epoch=1 seq=0  
[11/14/13 14:50:27.679 UTC 702f60 8528] acDtlsCallback: entering...  
[11/14/13 14:50:27.679 UTC 7b 8528] Verify X.509 certificate from wtp 7c69.f604.9460  
[11/14/13 14:50:27.680 UTC 702f62 8528] acDtlsCallback Cert validation PENDING  
[11/14/13 14:50:27.680 UTC 7c 8528] f84f.57ca.3860 Certificate verification - pending...  
[11/14/13 14:50:27.680 UTC 7d 8528] f84f.57ca.3860 Handshake in process.. awaiting certificate verification result..  
[11/14/13 14:50:27.681 UTC 702f63 8528] acDtlsCallback: entering...  
[11/14/13 14:50:27.681 UTC 702f64 8528] acDtlsCallback: cb->code 3  
[11/14/13 14:50:27.682 UTC 7f 8528] Verify X.509 certificate from wtp 7c69.f604.9460 >> AP Ethernet mac  
[11/14/13 14:50:27.683 UTC 702f65 8528] acDtlsCallback Cert validation SUCCESS.  
[11/14/13 14:50:27.683 UTC 80 8528] f84f.57ca.3860 Certificate verification - passed!  
[11/14/13 14:50:27.706 UTC 81 8528] f84f.57ca.3860 Connection established!  
[11/14/13 14:50:27.706 UTC 82 8528] f84f.57ca.3860 DTLS Connection 0x5789a5e0 established on local port 5246  
[11/14/13 14:50:27.706 UTC 83 8528] f84f.57ca.3860 Setting DTLS MTU for link to peer 10.201.234.24:18759  
[11/14/13 14:50:27.706 UTC 84 8528] Load Balancer: Platform Not supported, Exiting from ctrl_tunnel_lb  
[11/14/13 14:50:27.706 UTC 85 8528] Capwap Control DTLS key plumbing: Get SA resources from LB for AP IP 10.201.234.24, rc = 4  
[11/14/13 14:50:27.706 UTC 86 8528] Plumbing DTLS keys for local 10.201.234.4:5246 and peer 10.201.234.24:18759, anc_sw_id 0, anc_asic_id 0, res_sw_id 0, res_asic_id 0  
The above output is from the AP point of view, therefore only messages sent by AP are seen.

Join Request-Response

[11/14/13 14:50:27.712 UTC 702f6b 8528] f84f.57ca.3860 Join Request from 10.201.234.24:18759

[11/14/13 14:50:27.712 UTC 702f6c 8528] f84f.57ca.3860 For phy port iif id 0x01088ec00000003b, control session - anc sw id 0, anc asic id 0, res sw id 0, res asic id 0 in RCB for AP 10.201.234.24

[11/14/13 14:50:27.712 UTC 8f 8528] Creating WTP 0x3823a0f0 for AP f84f.57ca.3860 with hardware encryption flag = TRUE


[11/14/13 14:50:27.712 UTC 702f6e 8528] CAPWAP Interface-Name CAPWAP WCM Client f84f57ca3860 used for IIF ID allocation

[11/14/13 14:50:27.712 UTC 702f6f 8528] CAPWAP IIF ID Allocation Successful! ID:0x00d2a98000000796 for AP 10.201.234.24, AP hash 1 [This indicates generation of a capwapx interface seen in show ip interface brief]

[11/14/13 14:50:27.712 UTC 702f70 8528] Adding Node to AVL Tree with IIF id:0xd2a98000000796

[11/14/13 14:50:27.712 UTC 702f71 8528] WTP IIF ID Type: 0

[11/14/13 14:50:27.712 UTC 702f72 8528] Timer created successfully for WTP IIF ID: 0xd2a98000000796

Examples and Technotes, Cisco IOS XE Release Denali 16.1.1
Added IIF ID to AVL Tree Database

Encode static AP manager 10.201.234.4, AP count 0

Join resp: CAPWAP Maximum Msg element len = 87

Join Response sent to 10.201.234.24:18759

CAPWAP State: Join

CAPWAP Interface ID Acked Id-0x00d2a98000000796 by IIF - IIF status = 0x1001, for AP 10.201.234.24, rcb->ap_registered = 1

Not ready to send Config Status Response to AP 10.201.234.24 as SPI ACK is not received

Unable to find entry for PhyIfId: 0x1088ec00000003b from AVL Tree

Unable to find entry for PhyIfId: 0x1088ec00000003b from AVL Tree

Not ready to send Config Status Response to AP 10.201.234.24 as SPI ACK is not received

Register LWAPP event for AP f84f.57ca.3860 slot 1

Register LWAPP event for AP f84f.57ca.3860 slot 0

Added PhyIfId: 0x1088ec00000003b to AVL Tree Database

Get the Interface name from the Phy-Port-IIF-ID:0x1088ec00000003b

--- Phy-IIF-ID = 0x1088ec00000003b------

Not ready to send Config Status Response to AP 10.201.234.24 as SPI ACK is not received

CSP-SPAM:Input monitor name after copying from vapcb to vap data is wireless-avc-basic

CSP-SPAM:Output monitor name after copying from vapcb to vap data is wireless-avc-basic

CSP-SPAM:Input monitor name after copying from vapcb to vap data is wireless-avc-basic

CSP-SPAM:Output monitor name after copying from vapcb to vap data is wireless-avc-basic

RSN Capabilities: (26)
[11/14/13 14:50:27.714 UTC 702f8b 8528] [0000] 30 18 01 00 00 0f ac 02 02 00 00 0f ac 02 00 0f
[11/14/13 14:50:27.714 UTC 702f8c 8528] [0016] ac 04 01 00 00 0f ac 02 28 00
[11/14/13 14:50:27.714 UTC 702f8d 8528] WARP IEs: (12)
[11/14/13 14:50:27.714 UTC 702f8e 8528] [0000] dd 0a 00 c0 b9 01 00 00 00 08 01 01
[11/14/13 14:50:27.715 UTC 702f8f 8528] f84f.57ca.3860 Not ready to send Config Status Response to AP 10.201.234.24 as SPI ACK is not received
[11/14/13 14:50:27.715 UTC 702f90 8528] Physical interface Info: IIF-Id = 0x1088ec00000003b, Message Code = 0x802, Interface Name ->gigabitethernet1/0/24, Interface Type = 0x92, Client Ntruncated
[11/14/13 14:50:27.715 UTC 702f91 8528] Updated AVL entry for phyIifid: 0x1088ec00000003b macAddr:f84f.57ca.3860, phyIfName: gigabitethernet1/0/24 Number of APs on this Phy <truncated>
[11/14/13 14:50:27.725 UTC 702f92 8528] capwap opaque data f84f.57ca.3860 length = 0
[11/14/13 14:50:27.725 UTC 702f93 8528] No update; will insert f84f.57ca.3860
Configuration Status Request-Response/Update Request-Response
[11/14/13 14:50:27.869 UTC 702f94 8528] f84f.57ca.3860 Configuration Status from 10.201.234.24 as SPI ACK is not received
[11/14/13 14:50:27.870 UTC 702f95 8528] f84f.57ca.3860 CAPWAP State: Configure
[11/14/13 14:50:27.870 UTC 702f96 8528] f84f.57ca.3860 New unsupported Payload 254 in message from AP f84f.57ca.3860, Return SUCCESS
[11/14/13 14:50:27.870 UTC 702f97 8528] f84f.57ca.3860 Decoding new unsupported Payload 254 in message from AP f84f.57ca.3860, Return SUCCESS
[11/14/13 14:50:27.870 UTC 702f98 8528] Invalid channel 11 spacificed for the AP AP2602I-1, slotId = 0
[11/14/13 14:50:27.870 UTC 702f99 8528] Invalid channel 56 spacificed for the AP AP2602I-1, slotId = 1
[11/14/13 14:50:27.870 UTC 702f9a 8528] f84f.57ca.3860 Updating IP info for AP f84f.57ca.3860 -- static 0, 10.201.234.24/255.255.255.224, gtw 10.201.234.2
[11/14/13 14:50:27.870 UTC 702f9b 8528] f84f.57ca.3860 Updating IP 10.201.234.24 ===> 10.201.234.24 for AP f84f.57ca.3860
[11/14/13 14:50:27.870 UTC 702f9c 8528] LWAPP message validation failed for SPAM Vendor Specific Payload(104) in message of len=7 from AP f84f.57ca.3860
[11/14/13 14:50:27.870 UTC 702f9d 8528] f84f.57ca.3860 Failed to validate vendor specific message element
[11/14/13 14:50:27.871 UTC 702fab 8528] f84f.57ca.3860 LMAPP message validation failed for SPAM Vendor Specific Payload(104) in message of len=7 from AP f84f.57ca.3860
[11/14/13 14:50:27.870 UTC 702fac 8528] f84f.57ca.3860 Failed to validate vendor specific message element
[11/14/13 14:50:27.871 UTC 702fad 8528] f84f.57ca.3860 Setting MTU to 1485
[11/14/13 14:50:27.871 UTC 702f9e 8528] f84f.57ca.3860 Platform not Supported, exiting Load Balancer function
[11/14/13 14:50:27.871 UTC 702faf 8528] load balancer rc=4 for AP 10.201.234.24, IIF ID:0x000d2a98000000796
[11/14/13 14:50:27.871 UTC 702fb0 8528] opaque data size 0 with capwap interface create f84f.57ca.3860
[11/14/13 14:50:27.871 UTC 702fb1 8528] spiCapwapParams->
Data Tunnel Create timer started for 240 seconds timeout

Data Tunnel created - tunnel type NON_CRYPTO, load balancer support Not supported, tunnel mtu 1449,
anc_sw_id 0, ancasic_id 0, res_sw_id 0, res_asic_id 0
anc_wp_iif_id 0x0000000000000000, res_wp_iif_id 0x0000000000000000

Not ready to send Config Status Response to AP 10.201.234.24 as SPI ACK is not received

Associated. Last AP failure was due to Configuration changes, reason: controller reboot command

CAPWAP data tunnel create message.

CAPWAP data_tunnel_create called

Data tunnel id = 0xda9800000796

Tunnel Entry not found for AP (10.201.234.24, 18759)

CAPWAP IDB init complete

capwap_interface_status_update: tunnel 0xda9800000796 status 0

Received CAPWAP Tunnel SPI update opaque size 0

Received CAPWAP Interface update opaque len 0

Received CAPWAP Tunnel SPI update opaque data len 0 with capwap server update

Received CAPWAP Interface update opaque len 0

SPI IIF ACK: Capwap Data Tunnel create successful for iifid:0xda9800000796 AP:10.201.234.24

Received CAPWAP Interface update opaque len 0

SPI IIF ACK: Capwap Data Tunnel Created Successfully for IIFID: 0xda9800000796 AP: 10.201.234.24

OK to send Config Status Response to AP 10.201.234.24

Notify PM (done).

SNMP Register: Ca1 HWIDB 32f44570

capwap_port_hashitem added: slot 1 slotunit 24 vlan 1104

Sending multicast payload to ap AP2602I-1, mcast_mode 0, mcast group 0.0.0.0
Examples and Technotes, Cisco IOS XE Release Denali 16.1.1

Converged Access Controller AP Join Issue Troubleshoot with Traces

Troubleshoot

[11/14/13 14:50:27.933 UTC 702fbd 8528] f84f.57ca.3860 Config status response sent to 10.201.234.24:18759


[11/14/13 14:50:27.933 UTC 702fbf 8528] f84f.57ca.3860 Configuration update request for Band Select Cfg sent to 10.201.234.24:18759

[11/14/13 14:50:27.933 UTC 702fc0 8528] f84f.57ca.3860 Configuration update request for HaConfig message sent to 10.201.234.24:18759

[11/14/13 14:50:27.934 UTC 702fc1 8528] f84f.57ca.3860 Configuration update request for AP NGWC Qos sent to 10.201.234.24:18759


[11/14/13 14:50:28.122 UTC 702fc3 8528] f84f.57ca.3860 Received LWAPP Up event for AP f84f.57ca.3860 slot 0!

[11/14/13 14:50:28.122 UTC 702fc4 8528] f84f.57ca.3860 Radio state change for slot: 0 state: 2 cause: 0 detail cause: 0


[11/14/13 14:50:28.122 UTC 702fc7 8528] f84f.57ca.3860 Sending the remaining config to AP 10.201.234.24:18759


[11/14/13 14:50:28.123 UTC 702fce 8528] capwap opaque data f84f.57ca.3860 length = 0

[11/14/13 14:50:28.123 UTC 702cdf 8528] capwap opaque data f84f.57ca.3860 length = 0
Common Reasons for AP Join Failure

This section describes about common causes of AP join failures.

Problem 1: The AP on the Cisco Catalyst 3850 Series Switch is not in the wireless management VLAN

#show run interface Gigabitethernet 1/0/22

interface GigabitEthernet 1/0/22
description AP
switchport access vlan 25
switchport mode access

```shell
#show run | inc wireless
wireless mobility controller
wireless management interface Vlan1104
```
Configured Country Codes
BE - Belgium : 802.11a Indoor,Outdoor/ 802.11b / 802.11g

#show log
*%LWAPP-3-RD_ERR8: 1 wcm: Country code (US) not configured for AP 0c:68:03:eb:9b:20
*%LWAPP-3-RD_ERR4: 1 wcm: Invalid regulatory domain 802.11bg:-E 802.11a:-E for AP 0c:68:03:eb:9b:20

Problem 5: The wireless mobility controller is not defined

#show wireless mobility summary

<table>
<thead>
<tr>
<th>Mobility Agent Summary:</th>
<th>Mobility Role</th>
<th>Mobility Agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobility Protocol Port</td>
<td>16666</td>
<td></td>
</tr>
<tr>
<td>Mobility Switch Peer Group Name</td>
<td>:</td>
<td></td>
</tr>
<tr>
<td>Multicast IP Address</td>
<td>0.0.0.0</td>
<td></td>
</tr>
<tr>
<td>DTLS Mode</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Mobility Domain ID for 802.11r</td>
<td>0xac34</td>
<td></td>
</tr>
<tr>
<td>Mobility Keepalive Interval</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Mobility Keepalive Count</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Mobility Control Message DSCP Value</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Switch Peer Group Members Configured</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

Link Status is Control Link Status : Data Link Status
The status of Mobility Controller:
<table>
<thead>
<tr>
<th>IP</th>
<th>Public IP</th>
<th>Link Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>- : -</td>
</tr>
</tbody>
</table>

#show log
*%LWAPP-3-AP_LICENSE_REQUEST_ERR: 1 wcm: License request failed for AP 0c:68:03:eb:9b:20 - AP License Request timedout, ensure MC link is up, Resetting AP

Problem 6: The AP has mesh code on it

The following message does not indicate any current issue but it is quite generic. Examine the AP console log for further diagnosis until additional logging is added.
*%CAPWAP-3-SPI_TUNNEL_CREATE_ACK_NOT_REC: 1 wcm: Dropping discovery request from AP 0c68.03eb.9b20 - SPI Tunnel Create Ack not received[...It occurred 3 times/sec!.

Problem 7: The AP3700 is connected to a Cisco Catalyst 3850 Series Switch that runs 3.3.0SE

#show log
*%CAPWAP-3-DISC_UNSUPPORTED_AP: 1 wcm: Rejecting discovery request from unsupported AP 08cc.68b4.4780 [...It occurred 2 times/sec!.

Problem 8: The controller time is outside the AP certificate validity interval

#show clock
*00:14:59.459 GMT0:0 Thu Jan 1 1970

#show log
*Jan 1 00:05:51.338: %PKI-3-CERTIFICATE_INVALID_NOT_YET_VALID: Certificate chain validation has failed. The certificate (SN: 17978AAD00000036823E) is not yet valid. Validity period starts on 04:25:46 GMT0:0 Jun 8 2013
Problem 9: The AP authorization list is enabled on the WLC; the AP is not in the authorization list

```bash
#show ap auth-list
Authorize MIC APs against AAA : Enabled
Authorize LSC APs against Auth-List : Disabled

APs Allowed to Join:
AP with Manufacturing Installed Certificate : Enabled
AP with Self-Signed Certificate : Disabled
AP with Locally Significant Certificate : Disabled
```

Problem 10: The MIC AP Policy is disabled

```bash
#show ap auth-list
Authorize MIC APs against AAA : Disabled
Authorize LSC APs against Auth-List : Disabled

APs Allowed to Join:
AP with Manufacturing Installed Certificate : Disabled
AP with Self-Signed Certificate : Disabled
AP with Locally Significant Certificate : Disabled
```

General Technical Tips on Trace Commands

This section provides some helpful tips on filtering options and limitations on trace commands.
Before you begin with troubleshoot procedure, clear all previously collected traces for the specific feature. In this case, capwap, group-ap, and all filtered traces.

- # Set trace control capwap
- # Set trace control group-ap
- # Set trace control sys-filtered-trace (this command clears the filtered traces and cannot be run on a per-feature basis)

AP join on converged access controllers makes use of the radio MAC address of the AP. So, when you set a filter for the trace, make use of the radio or base MAC address of the AP.

Enter the `show ap join stats summary` command to find the radio MAC address of the AP.

Issues with certificates are handled by IOSd and require the use of debugs, not traces. For further diagnosis use the following debugs:

- #debug crypto pki API
- #debug crypto pki callbacks
- #debug crypto pki server
- #debug crypto pki transactions
- #debug crypto pki messages