思科服务支持社区 CSC
最信赖的顶尖专家 最佳IT服务体验
www.csc-china.com.cn

【CSC公开课】第十五期：无线噩梦之AP无法加入WLC故障排查

张国敏

TAC

AP Join WLC troubleshooting

AP Join process
LWAPP/CAPWAPP state machine
Examples
vWLC issue
NGWC issue

AP Join process

LWAPP/CAPWAPP state machine

Examples

vWLC issue

NGWC issue

AP Join Process

WLC Discovery

DTLS/Join

Image Download

Config Check

REG

L3 WLC Address Hunting

AP Discovery Request sent to known and learned WLCs

Broadcast

- Reaches WLCs with MGMT Interface in local subnet of AP
- Use “ip helper-address <ip>” with “ip forward-protocol udp 5246”

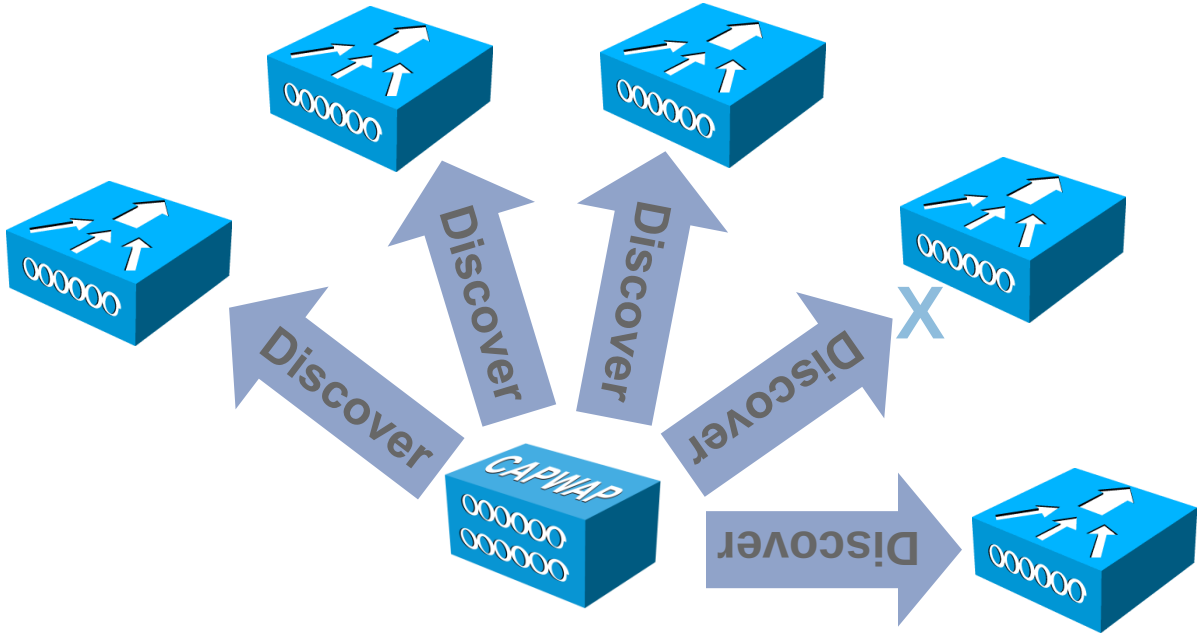
Dynamic

- DNS: *“CISCO-CAPWAP-CONTROLLER.localdomain”*
- DHCP: Option 43 e.g.: `option 43 hex f108.c0a8.0101.c0a8.0202`
- IP address should be management interface IP

Configured (nvram local stored)

- High Availability WLCs – Pri/Sec/Ter/Backup
- Last WLC
- All WLCs in same mobility group as last WLC
- Manual from AP - “capwap ap controller ip address <ip>”

L3 WLC Discovery



AP Tries to Send Discover Messages to All the WLC Addresses that Its Hunting Process Turned Up

L3 WLC Controller - Discovery Algorithm

- Once a list of WLAN controllers is compiled, the AP sends a unicast CAPWAP discovery request message to each of the controllers in the list
- WLAN controllers receiving the CAPWAP discovery messages respond with an CAPWAP discovery response
- CAPWAP discovery response contains important information:

  Controller name, controller type, AP capacity, current AP load, master controller status, AP-manager IP address(es)

- AP waits for its discovery interval to expire, then selects a controller and sends an CAPWAP join request to that controller

WLAN Controller Selection Algorithm

The AP Selects the Controller to Join Using the Following Criteria

1. If the AP has been configured with primary, secondary, and/or tertiary controller, the AP will attempt to join these first (this is resolved in the controller system name field in the CAPWAP discovery response)
2. Primary Backup controller ,secondary Backup controller
3. Attempt to join a WLAN controller configured as a master controller
4. Attempt to join the WLAN controller with the greatest excess AP capacity

Note: This Last Step Provides the Whole System with Automatic AP/WLC Load-Balancing Functionality

AP Discover/Join – AP Side

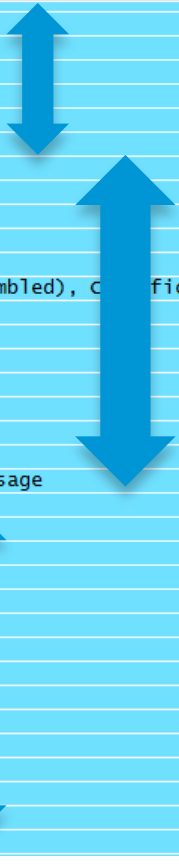
```
*Jan  2 15:41:42.035: %CAPWAP-3-EVENTLOG: Starting Discovery. Initializing discovery latency in discovery responses.
*Jan  2 15:41:42.035: %CAPWAP-3-EVENTLOG: CAPWAP State: Discovery.
*Jan  2 15:41:42.035: CAPWAP Control mesg Sent to 192.168.70.10, Port 5246
*Jan  2 15:41:42.039:           Msg Type   : CAPWAP_DISCOVERY_REQUEST
*Jan  2 15:41:42.039: CAPWAP Control mesg Sent to 192.168.5.55, Port 5246
*Jan  2 15:41:42.039:           Msg Type   : CAPWAP_DISCOVERY_REQUEST
*Jan  2 15:41:42.039: CAPWAP Control mesg Sent to 255.255.255.255, Port 5246
*Jan  2 15:41:42.039:           Msg Type   : CAPWAP_DISCOVERY_REQUEST
*Jan  2 15:41:42.039: CAPWAP Control mesg Recd from 192.168.5.54, Port 5246
*Jan  2 15:41:42.039:           HLEN 2,   Radio ID 0,    WBID 1
*Jan  2 15:41:42.039:           Msg Type   : CAPWAP_DISCOVERY_RESPONSE
*Jan  2 15:41:42.055: CAPWAP Control mesg Recd from 192.168.5.55, Port 5246
*Jan  2 15:41:42.055:           HLEN 2,   Radio ID 0,    WBID 1
*Jan  2 15:41:42.055:           Msg Type   : CAPWAP_DISCOVERY_RESPONSE
*Jan  2 15:41:52.039: %CAPWAP-3-EVENTLOG: Calling wtpGetAcToJoin from timer expiry.
*Jan  2 15:41:52.039: %CAPWAP-3-ERRORLOG: Selected MWAR '5500-5'(index 0).
*Jan  2 15:41:52.039: %CAPWAP-3-EVENTLOG: Selected MWAR '5500-5' (index 2).
*Jan  2 15:41:52.039: %CAPWAP-3-EVENTLOG: Ap mgr count=1
*Jan  2 15:41:52.039: %CAPWAP-3-ERRORLOG: Go join a capwap controller
*Jan  2 15:41:52.039: %CAPWAP-3-EVENTLOG:  Adding Ipv4 AP manager 192.168.5.55 to least load
*Jan  2 15:41:52.039: %CAPWAP-3-EVENTLOG: Choosing AP Mgr with index 0, IP = 192.168.5.55, load = 3..
*Jan  2 15:41:52.039: %CAPWAP-3-EVENTLOG: Synchronizing time with AC time.
*Jan  2 15:41:52.000: %CAPWAP-3-EVENTLOG: Setting time to 15:41:52 UTC Jan 2 2014
*Jan  2 15:41:52.467: %CAPWAP-5-DTLSREQSUCC: DTLS connection created sucessfully peer_ip: 192.168.5.55 peer_port: 5246
```

AP Discover/Join – WLC Side

```
*spamApTask7: Jan 02 15:35:57.295: 04:da:d2:4f:f0:50 Discovery Request from 192.168.5.156:7411
*spamApTask7: Jan 02 15:35:57.296: 04:da:d2:4f:f0:50 ApModel: AIR-CAP2602I-E-K9
*spamApTask7: Jan 02 15:35:57.296: apModel: AIR-CAP2602I-E-K9
*spamApTask7: Jan 02 15:35:57.296: apType = 27 apModel: AIR-CAP2602I-E-K9
*spamApTask7: Jan 02 15:35:57.296: apType: Ox1b bundleApImageVer: 7.6.100.0
*spamApTask7: Jan 02 15:35:57.296: version:7 release:6 maint:100 build:0
*spamApTask7: Jan 02 15:35:57.296: 04:da:d2:4f:f0:50 Discovery Response sent to 192.168.5.156 port 7411
*spamApTask7: Jan 02 15:36:07.762: 44:03:a7:f1:cf:1c DTLS keys for Control Plane are plumbed successfully for AP
192.168.5.156. Index 7
*spamApTask6: Jan 02 15:36:07.762: 44:03:a7:f1:cf:1c DTLS Session established server (192.168.5.55:5246), client
(192.168.5.156:7411)
*spamApTask6: Jan 02 15:36:07.762: 44:03:a7:f1:cf:1c Starting wait join timer for AP: 192.168.5.156:7411
*spamApTask7: Jan 02 15:36:07.764: 04:da:d2:4f:f0:50 Join Request from 192.168.5.156:7411
*spamApTask7: Jan 02 15:36:07.765: 04:da:d2:4f:f0:50 Join resp: CAPWAP Maximum Msg element len = 83
*spamApTask7: Jan 02 15:36:07.765: 04:da:d2:4f:f0:50 Join Response sent to 192.168.5.156:7411
*spamApTask7: Jan 02 15:36:07.765: 04:da:d2:4f:f0:50 CAPWAP State: Join
```

CAPWAP packet capture

Time	Source	Destination	Protocol	Info
51.700480	192.168.2.113	255.255.255.255	CAPWAP	CAPWAP-Control - Discovery Request
51.700857	157.0.9.11	192.168.2.113	CAPWAP	CAPWAP-Control - Discovery Response
51.702155	192.168.2.113	157.0.9.11	CAPWAP	CAPWAP-Control - Discovery Request
51.702178	157.0.9.11	192.168.2.113	CAPWAP	CAPWAP-Control - Discovery Response
51.702530	192.168.2.113	157.0.9.11	CAPWAP	CAPWAP-Control - Discovery Request
51.702548	157.0.9.11	192.168.2.113	CAPWAP	CAPWAP-Control - Discovery Response
71.637735	192.168.2.113	157.0.9.11	DTLSv1.0	Client Hello
71.734112	157.0.9.11	192.168.2.113	DTLSv1.0	Hello Verify Request
71.734731	192.168.2.113	157.0.9.11	DTLSv1.0	Client Hello
71.736486	157.0.9.11	192.168.2.113	DTLSv1.0	Server Hello, Certificate (Fragment)
71.736530	157.0.9.11	192.168.2.113	DTLSv1.0	Certificate (Fragment)
71.736535	157.0.9.11	192.168.2.113	DTLSv1.0	Certificate (Fragment), Certificate (Reassembled), C ficate Request, S
71.890342	192.168.2.113	157.0.9.11	DTLSv1.0	Certificate (Fragment)
71.890365	192.168.2.113	157.0.9.11	DTLSv1.0	Certificate (Fragment)
71.890370	192.168.2.113	157.0.9.11	DTLSv1.0	Certificate (Reassembled)
71.890375	192.168.2.113	157.0.9.11	DTLSv1.0	Client Key Exchange
71.950907	192.168.2.113	157.0.9.11	DTLSv1.0	Certificate Verify
71.950935	192.168.2.113	157.0.9.11	DTLSv1.0	Change Cipher Spec
71.950940	192.168.2.113	157.0.9.11	DTLSv1.0	Encrypted Handshake Message
72.024205	157.0.9.11	192.168.2.113	DTLSv1.0	Change Cipher Spec, Encrypted Handshake Message
72.025950	192.168.2.113	157.0.9.11	DTLSv1.0	Application Data
72.026655	157.0.9.11	192.168.2.113	DTLSv1.0	Application Data
72.027191	157.0.9.11	192.168.2.113	DTLSv1.0	Application Data
73.194644	192.168.2.113	157.0.9.11	DTLSv1.0	Application Data
73.194676	192.168.2.113	157.0.9.11	DTLSv1.0	Application Data
73.240936	157.0.9.11	192.168.2.113	DTLSv1.0	Application Data
73.240964	157.0.9.11	192.168.2.113	DTLSv1.0	Application Data
73.568966	192.168.2.113	157.0.9.11	DTLSv1.0	Application Data
73.570293	157.0.9.11	192.168.2.113	DTLSv1.0	Application Data
73.570307	157.0.9.11	192.168.2.113	DTLSv1.0	Application Data
73.677352	192.168.2.113	157.0.9.11	DTLSv1.0	Application Data
73.677382	192.168.2.113	157.0.9.11	DTLSv1.0	Application Data
73.678685	157.0.9.11	192.168.2.113	DTLSv1.0	Application Data
73.678706	157.0.9.11	192.168.2.113	DTLSv1.0	Application Data
73.685859	192.168.2.113	157.0.9.11	DTLSv1.0	Application Data



Troubleshooting Lightweight APs

Check the Basics First

Make sure the AP is getting an address from DHCP (check the DHCP server leases for the AP's MAC address)

If the AP's address is statically set, ensure it is correctly configured

Try pinging from AP to controller and vice versa

If pings are successful, ensure the AP has **at least one** method by which to discovery at least a single WLC

Console or telnet/ssh into the controller to run debugs

If you do not have access to APs, use "show cdp neighbors port <x/y> detail" on connected switch to verify if the AP has an IP

Check the Detail

Check ACL (UDP 5246, UDP 12223)

Is option 43 configured for that DHCP scope? Is it the right IP address?

Is the time set correctly on the WLC?

Check license of WLC

Check that default GW in AP is valid

Check time in WLC is valid

Check traplogs on WLC?

Any error messages during debugs?

Run debug and show commands on the AP CLI if possible

Get packet captures and AP and WLC

Check Load Balancing algorithm on the Switch

LAG Can't Reassemble Fragments from Multiple Ports

•Etherchannel load balancing scheme on the switch connecting to the WLC must be src-dst-ip.
•The load balancing scheme can be viewed by issuing the command

show etherchannel load-blance

•This can be configured by using the command shown below in global config mode

port-channel load-balance src-dst-ip

Important Outputs

Debugs to be enabled

On the WLC:

- debug mac addr <AP ethernet mac>

- debug capwap events enable

- debug capwap errors enable

- debug dtls all enable

- debug pm pki enable

On the AP

- debug dhcp detail / - debug capwap client detail / - debug ip udp

Important Outputs

Show Commands

On AP#

show tech

show log

show capwap client rcb

show capwap client config

On WLC>

>show ap join stats summary all / detailed <MAC>

>show ap summary

```
L3500-12# sh capwap client rcb
AdminState                    :  ADMIN_ENABLED
SwVer                         :  7.6.120.0
NumFilledSlots                :  2
Name                          :  L3500-12
Location                      :  default location
MwarName                      :  Cisco_37:c9:84
MwarApMgrIp                   :  157.0.9.11
MwarHwVer                     :  0.0.0.0
ApMode                        :  Bridge
ApSubMode                     :  Not Configured
OperationState                :  UP
CAPWAP Path MTU               :  1485
```

AP Join process

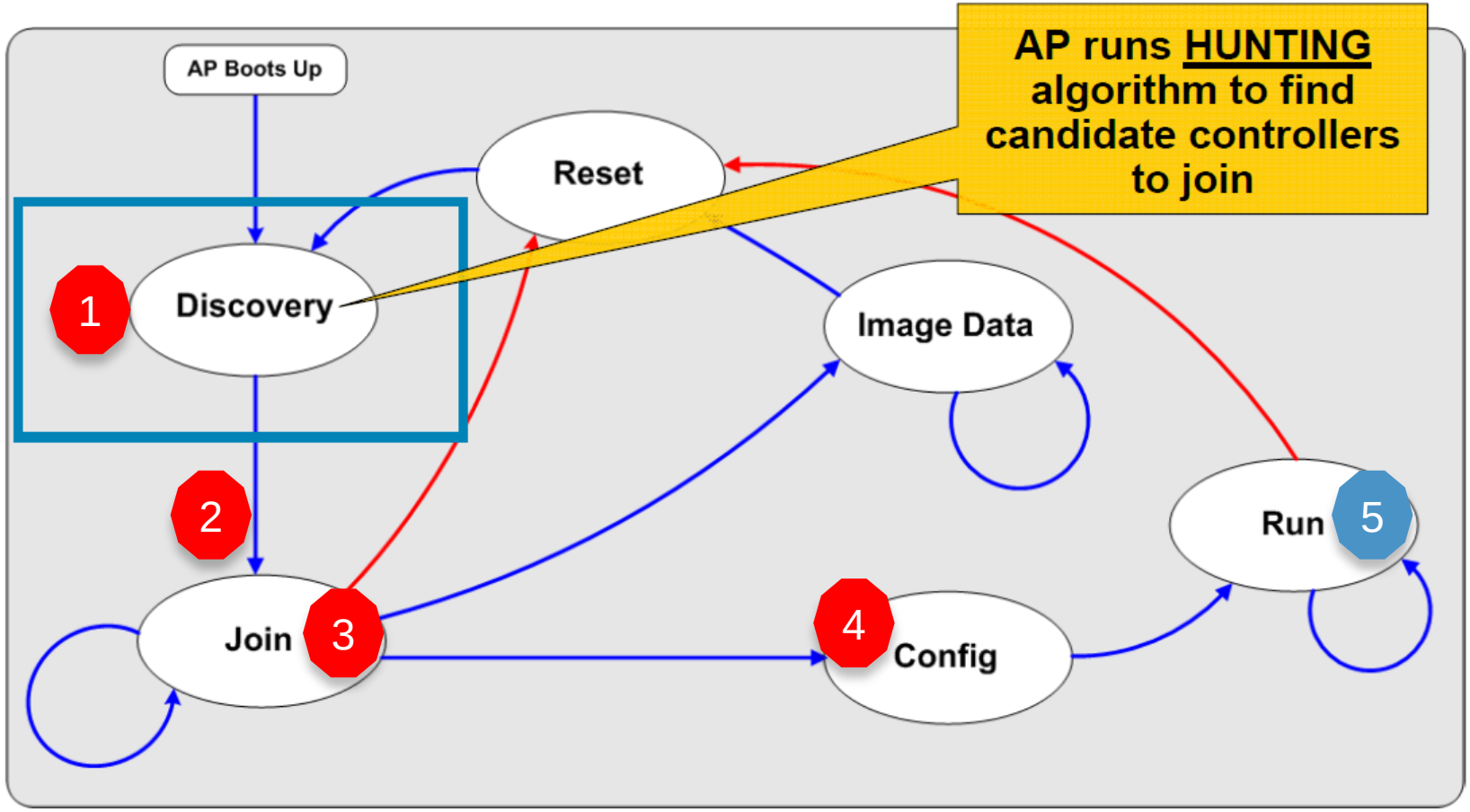
LWAPP/CAPWAPP state machine

Examples

vWLC issue

NGWC issue

LWAPP/CAPWAP AP State Machine



AP Capwap client rcb

```
L3500-12#show capwap client rcb
AdminState              : ADMIN_ENABLED
SwVer                   : 7.6.120.0
NumFilledSlots          : 2
Name                    : L3500-12
Location                : default location
MwarName                : 5508-1
MwarMacAddr             : ffff.ffff.0000
MwarHwVer               : 0.0.0.0
ApMode                  : Local
ApSubMode               : Not Configured
OperationState          : DISCOVERY
```

1

```
L3500-12#show capwap client rcb
AdminState              :
ADMIN_ENABLED
SwVer                   : 7.6.120.0
NumFilledSlots          : 2
Name                    : L3500-12
Location                : default location
MwarName                : Cisco_37:c9:84
MwarApMgrIp             : 157.0.9.11
MwarHwVer               : 0.0.0.0
ApMode                  : Local
ApSubMode               : Not Configured
OperationState          : DTLS SETUP
```

2

```
L3500-12#show capwap client rcb
AdminState              : ADMIN_ENABLED
SwVer                   : 7.6.120.0
NumFilledSlots          : 2
Name                    : L3500-12
Location                : default location
MwarName                : Cisco_37:c9:84
MwarApMgrIp             : 157.0.9.11
MwarHwVer               : 0.0.0.0
ApMode                  : Bridge
ApSubMode               : Not Configured
OperationState          : JOIN
```

3

```
L3500-12#show capwap client rcb
AdminState              : ADMIN_ENABLED
SwVer                   : 7.6.120.0
NumFilledSlots          : 2
Name                    : L3500-12
Location                : default location
MwarName                : Cisco_37:c9:84
MwarApMgrIp             : 157.0.9.11
MwarHwVer               : 0.0.0.0
ApMode                  : Local
ApSubMode               : Not Configure
OperationState          : CFG
```

4

Last AP State Machine


```
L3500-12#show capwap client rcb
AdminState                :
ADMIN_ENABLED
SwVer                  :  7.6.120.0
NumFilledSlots             :  2
Name                   :  L3500-12
Location               :  default location
MwarName                   :  Cisco_37:c9:84
MwarApMgrIp                :  157.0.9.11
MwarHwVer                  :  0.0.0.0
ApMode                 :  Local
ApSubMode                  :  Not Configured
OperationState             :  UP
```

5

AP software mismatch

```
L3500-12#show capwap client  rcb
AdminState                 : ADMIN_ENABLED
SwVer                      : 7.3.1.73
NumFilledSlots             : 0
Name                       : L3500-12
Location                   : default location
MwarName                   : Cisco_37:c9:84
MwarApMgrIp                : 157.0.9.11
MwarHwVer                  : 0.0.0.0
ApMode                     : Local
ApSubMode                  : Not Configured
OperationState             : IMAGE
```

```
APf8c2.885e.cb60#show capwap  client rcb
AdminState                 : ADMIN_ENABLED
SwVer                      : 10.2.110.0
NumFilledSlots             : 2
Name                       : APf8c2.885e.cb60
Location                   : default location
MwarName                   : Cisco_37:c9:84
MwarApMgrIp                : 157.0.9.11
MwarHwVer                  : 0.0.0.0
ApMode                     : Local
ApSubMode                  : Not Configured
OperationState             : DOWN
```

```
*Sep 19 19:37:12.935: %SYS-5-RELOAD: Reload requested by capwap image download proc. Reload Reason: NEW IMAGE DOWNLOAD.
*Sep 19 19:37:12.943: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to administratively down
*Sep 19 19:37:12.943: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to administratively down
*Sep 19 19:37:12.943: %CAPWAP-3-EVENTLOG: LRAD state down. Skip sending PHY_TX_POWER_LEVEL_PAYLOAD

IOS Bootloader - Starting system.
```

sh capwap client config

```
L3500-12# show capwap client config
configMagicMark        0xF1E2D3C4
chkSumV2               11415
chkSumV1               24640
swVer                  7.6.120.0
adminState             ADMIN_ENABLED(1)
name                   L3500-12
location               default location
group name
mwarName               Cisco_37:c9:84
mwarIPAddress          157.0.9.11
mwarName
mwarIPAddress          0.0.0.0
mwarName
mwarIPAddress          0.0.0.0
ssh status             Disabled
ssh config mode        GLOBAL
Telnet status          Disabled
telnet config mode     GLOBAL
numOfSlots             2
spamRebootOnAssert     1
spamStatTimer          180
randSeed               0x0
transport              SPAM_TRANSPORT_L3(2)
transportCfg           SPAM_TRANSPORT_DEFAULT(0)
initialisation         SPAM_PRODUCTION_DISCOVERY(1)
ApMode                 Bridge
ApSubMode              Not Configured
```

AP failure counters: LinkFailure = 56, SpamReboots = 26, ApCrashes = 0

AP Join process
LWAPP/CAPWAPP state machine
Examples
vWLC issue
NGWC issue

AP IP address issue.

*Mar 1 00:04:40.535: %CAPWAP-3-DHCP_RENEW: Could not discover WLC. Either IP address is not assigned or assigned IP is wrong. Renewing DHCP IP.

AP not support on current versoin of WLC

```
APf8c2.885e.cb60#show capwap client rcb
AdminState                : ADMIN_ENABLED
SwVer                     : 10.2.110.0
NumFilledSlots            : 2
Name                      : APf8c2.885e.cb60
Location                  : default location
MwarName                  : Cisco_37:c9:84
MwarMacAddr               : ff01.0000.0000
MwarHwVer                 : 0.0.0.0
ApMode                    : Local
ApSubMode                 : Not Configured
OperationState            : DISCOVERY
```

```
APf8c2.885e.cb60#sh capw client rcb
AdminState                : ADMIN_ENABLED
SwVer                     : 8.0.100.0
NumFilledSlots            : 2
Name                      : APf8c2.885e.cb60
Location                  : default location
MwarName                  : test
MwarMacAddr               : 9d00.090e.0000
MwarHwVer                 : 0.0.0.0
ApMode                    : Local
ApSubMode                 : Not Configured
OperationState            : DISCOVERY
```

AP not support on current versoin of WLC

Debug – AP Side

*Mar 1 00:07:22.171: %CAPWAP-3-ERRORLOG: Could Not resolve CISCO-CAPWAP-CONTROLLER
*Mar 1 00:07:22.171: %CAPWAP-3-
ERRORLOG: Discovery response from MWAR 'WLC1'running version 7.0.220.0 is rejected.
*Mar 1 00:07:22.171: %CAPWAP-3-ERRORLOG: Failed to decode discovery response.
*Mar 1 00:07:22.171: %CAPWAP-3-
ERRORLOG: CAPWAP SM handler: Failed to process message type 2 state 2.
*Mar 1 00:07:22.171: %CAPWAP-3-ERRORLOG: Failed to handle capwap control message from controller
*Mar 1 00:07:22.171: %CAPWAP-3-ERRORLOG: Failed to process unencrypted capwap packet from 10.1.1.254
*Mar 1 00:07:22.175: %CAPWAP-3-
ERRORLOG: Discovery response from MWAR 'WLC1'**running version 7.0.220.0 is rejected.**
*Mar 1 00:07:22.175: %CAPWAP-3-ERRORLOG: Failed to decode discovery response.
*Mar 1 00:07:22.175: %CAPWAP-3-
ERRORLOG: CAPWAP SM handler: Failed to process message type 2 state 2.
Translating "CISCO-CAPWAP-CONTROLLER"...domain server (255.255.255.255)

AP not support

Debug – AP Side

*Jan 1 00:30:11.999: %CAPWAP-3-EVENTLOG: Wait DTLS timer has expired
*Jan 1 00:30:11.999: %CAPWAP-3-EVENTLOG: Dtls session establishment failed
*Jan 1 00:30:11.999: %CAPWAP-3-EVENTLOG: CAPWAP State: DTLS Teardown.
APf8c2.885e.cb60#
*Jan 1 00:30:16.999: %CAPWAP-3-EVENTLOG: DTLS session cleanup completed. Restarting capwap state machine.
*Jan 1 00:30:16.999: %CAPWAP-3-EVENTLOG: Previous CAPWAP state was DTLS Setup,numOfCapwapDiscoveryResp = 1.
*Jan 1 00:30:16.999: %CAPWAP-3-EVENTLOG: Attempting to join next controller
*Jan 1 00:30:16.999: %CAPWAP-3-EVENTLOG: Go Join the next controller

*Jan 1 00:30:16.999: %CAPWAP-3-EVENTLOG: Calling wtpGetAcToJoin from timer expiry.
*Jan 1 00:30:16.999: %CAPWAP-3-EVENTLOG: !mwarname
*Jan 1 00:30:16.999: %CAPWAP-3-EVENTLOG: !mwarname
*Jan 1 00:30:16.999: %CAPWAP-3-EVENTLOG: Selected MWAR 'Cisco_37:c9:84' (index 0).
*Jan 1 00:30:16.999: %CAPWAP-3-EVENTLOG: Ap mgr count=0

DTLS setup Fail

```
L3500-12#show capwap client rcb
AdminState              :  ADMIN_ENABLED
SwVer                   :  7.6.120.0
NumFilledSlots          :  2
Name                    :  L3500-12
Location                :  default location
MwarName                :  Cisco_37:c9:84
MwarMacAddr             :  ffff.ffff.0000
MwarHwVer               :  0.0.0.0
ApMode                  :  Local
ApSubMode               :  Not Configured
OperationState          :  DISCOVERY
```

```
L3500-12#show capwap client rcb
AdminState              :  ADMIN_ENABLED
SwVer                   :  7.6.120.0
NumFilledSlots          :  2
Name                    :  L3500-12
Location                :  default location
MwarName                :  Cisco_37:c9:84
MwarApMgrIp             :  157.0.9.11
MwarHwVer               :  0.0.0.0
ApMode                  :  Local
ApSubMode               :  Not Configured
OperationState          :  DTLS SETUP
```

WLC Time

```
(Cisco Controller) >show time

Time..................................... Sat Nov 29 21:50:22 2014

Timezone delta..................................... 0:0
Timezone location.................................. (GMT +8:00) HongKong, Bejing, Chongquing

NTP Servers
   NTP Polling Interval.....................     86400

   Index     NTP Key Index              NTP Server       NTP Msg Auth Status
   -------  ---------------------------------------------------------------------------------
     1            0                          157.0.9.1          AUTH DISABLED

(Cisco Controller) >config time timezone location 25                25. (GMT +8:00) HongKong, Bejing, Chongquing
(Cisco Controller) >config time manual 29/11/14 17:49:10
```

Debug output – WLC Side

*spamApTask4: Jan 01 00:35:15.596: sshpmGetIssuerHandles: ValidityString (current): 2000/01/01/00:35:15

*spamApTask4: Jan 01 00:35:15.596: sshpmGetIssuerHandles: ValidityString (NotBefore): 2014/05/29/06:47:55

*spamApTask4: Jan 01 00:35:15.596: sshpmGetIssuerHandles: ValidityString (NotAfter): 2024/05/29/06:57:55

*spamApTask4: Jan 01 00:35:15.596: sshpmGetIssuerHandles: Current time outside AP cert validity interval: make sure the controller time is set.

OK

*spamApTask6: Nov 29 17:00:28.269: sshpmGetIssuerHandles: ValidityString (current): 2014/11/29/17:00:28

*spamApTask6: Nov 29 17:00:28.269: sshpmGetIssuerHandles: ValidityString (NotBefore): 2010/11/11/06:37:12

*spamApTask6: Nov 29 17:00:28.269: sshpmGetIssuerHandles: ValidityString (NotAfter): 2020/11/11/06:47:12

Debug output – AP Side(1)

*Jan 1 00:37:30.170: %CAPWAP-3-EVENTLOG: Selected MWAR 'Cisco_37:c9:84' (index 0).
*Jan 1 00:37:30.170: %CAPWAP-3-EVENTLOG: Ap mgr count=1
*Jan 1 00:37:30.170: %CAPWAP-3-ERRORLOG: Go join a capwap controller
*Jan 1 00:37:30.170: %CAPWAP-3-EVENTLOG: Choosing AP Mgr with index 0, IP = 0x9D00090B, load = 0..
*Jan 1 00:37:30.170: %CAPWAP-3-EVENTLOG: Synchronizing time with AC time.
*Jan 1 00:38:34.000: %CAPWAP-3-EVENTLOG: Setting time to 00:38:34 UTC Jan 1 2000

*Jan 1 00:38:34.000: %CAPWAP-5-DTLSREQSEND: DTLS connection request sent peer_ip: 157.0.9.11 peer_port: 5246
*Jan 1 00:38:34.000: %CAPWAP-3-EVENTLOG: CAPWAP State: DTLS Setup.
*Jan 1 00:38:34.113: %PKI-3-CERTIFICATE_INVALID_NOT_YET_VALID: Certificate chain validation has failed. The certificate (SN: 68CC62BE0000002452F5) is not yet valid Validity period starts on 13:06:18 UTC Mar 7 2013Peer certificate verification failed 001A
*Jan 1 00:38:34.113: DTLS_CLIENT_ERROR: ../capwap/base_capwap/capwap/base_capwap_wtp_dtls.c:447 Certificate verified failed!
*Jan 1 00:38:34.113: %DTLS-5-SEND_ALERT: Send FATAL : Bad certificate Alert to 157.0.9.11:5246
*Jan 1 00:38:34.113: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to 157.0.9.11:5246
*Jan 1 00:38:34.113: %CAPWAP-3-ERRORLOG: Invalid event 38 & state 3 combination.

*Jan 1 02:10:32.000: %CAPWAP-5-DTLSREQSEND: DTLS connection request sent peer_ip: 157.0.9.11 peer_port: 5246
*Jan 1 02:10:32.295: %DTLS-5-ALERT: Received FATAL : Certificate unknown alert from 157.0.9.11
*Jan 1 02:10:32.295: %CAPWAP-3-ERRORLOG: Bad certificate alert received from peer.
*Jan 1 02:10:32.295: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to 157.0.9.11:5246
*Jan 1 02:10:32.295: %CAPWAP-3-ERRORLOG: Invalid event 40 & state 3 combination.

Debug output – AP Side(2)

00:32:57.027: %DHCP-6-
ADDRESS_ASSIGN: Interface BVI1 assigned DHCP address 192.168.100.12, mask 255.255.255.0, hostname AP881d
.XXXX.9e14

*Jan 1 00:33:13.499: AP has SHA2 MIC certificate - Using SHA2 MIC certificate for DTLS.

*Jan 1 00:33:14.000: %CAPWAP-5-
DTLSREQSEND: DTLS connection request sent peer_ip: 192.168.100.100 peer_port: 5246
*Jan 1 00:33:15.347: %DTLS-5-ALERT: Received FATAL : Certificate unknown alert from 192.168.100.100
*Jan 1 00:33:15.347: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to 192.168.100.100:5246

Country Code

(Cisco Controller) >show country

Configured Country..... AU - Australia
Configured Country Codes
AU - Australia..... 802.11a Indoor,Outdoor / 802.11b / 802.11g

WLC Debug

*spamApTask5: Nov 29 17:19:53.723: 00:1e:bd:e5:06:40 DTLS Session established server (157.0.9.11:5246), client (192.168.2.110:16069)

*spamApTask3: Nov 29 17:19:53.730: 08:17:35:31:a4:80 CAPWAP State: Join
*spamApTask3: Nov 29 17:19:53.890: 08:17:35:31:a4:80 CAPWAP State: Configure

*spamApTask3: Nov 29 17:19:53.890: 08:17:35:31:a4:80 Invalid length (9) countedlen 6 sizeUserPayload 277 for vendor-specific element 0x00409600-unknown (185) from AP 08:17:35:31:A4:80

*spamApTask3: Nov 29 17:19:53.890: 08:17:35:31:a4:80 LWAPP message validation failed for SPAM_VENDOR_SPECIFIC_PAYLOAD(104) in message of len=9 from AP 08:17:35:31:a4:80

*spamApTask3: Nov 29 17:19:53.891: 08:17:35:31:a4:80 AP 08:17:35:31:a4:80: Country code is not configured(US).
*spamApTask3: Nov 29 17:19:53.891: 08:17:35:31:a4:80 **Regulatory Domain Mismatch:** AP 08:17:35:31:a4:80 not allowed to join. Allowed domains: 802.11bg:-CE 802.
*spamApTask3: Nov 29 17:19:53.891: 08:17:35:31:a4:80 Finding DTLS connection to delete for AP (192:168:2:110/16069)
*spamApTask3: Nov 29 17:19:53.891: 08:17:35:31:a4:80 Disconnecting DTLS Capwap-Ctrl session 0x17a9e238 for AP (192:168:2:110/16069)

*spamApTask3: Nov 29 17:19:53.891: 08:17:35:31:a4:80 CAPWAP State: Dtls tear down

AP Debug

*Nov 29 17:17:47.679: %CAPWAP-3-EVENTLOG: Selected MWAR 'Cisco_37:c9:84' (index 0).
*Nov 29 17:17:47.679: %CAPWAP-3-EVENTLOG: Ap mgr count=1
*Nov 29 17:17:47.679: %CAPWAP-3-ERRORLOG: Go join a capwap controller
*Nov 29 17:17:47.679: %CAPWAP-3-EVENTLOG: Adding Ipv4 AP manager 157.0.9.11 to least load
*Nov 29 17:17:47.679: %CAPWAP-3-EVENTLOG: Choosing AP Mgr with index 0, IP = 157.0.9.11, load = 0..
*Nov 29 17:17:47.679: %CAPWAP-3-EVENTLOG: Synchronizing time with AC time.
*Nov 29 17:17:48.000: %CAPWAP-3-EVENTLOG: Setting time to 17:17:48 UTC Nov 29 2014

*Nov 29 17:17:48.390: %CAPWAP-5-DTLSREQSUCC: DTLS connection created sucessfully peer_ip: 157.0.9.11 peer_port: 5246
*Nov 29 17:17:48.390: %CAPWAP-3-EVENTLOG: Dtls Session Established with the AC 157.0.9.11,port= 5246
*Nov 29 17:17:48.390: %CAPWAP-3-EVENTLOG: CAPWAP State: Join.
*Nov 29 17:17:48.390: %CAPWAP-3-EVENTLOG: Join request: version=117864448
*Nov 29 17:17:48.390: %CAPWAP-3-EVENTLOG: Join request: hasMaximum Message Payload
*Nov 29 17:17:48.390: %CAPWAP-3-EVENTLOG: Sending Join Request Path MTU payload, Length 1376

*Nov 29 17:17:48.390: %CAPWAP-5-SENDJOIN**: sending Join Request** to 157.0.9.11
*Nov 29 17:17:48.393: %CAPWAP-3-ERRORLOG: Invalid event 10 & state 5 combination.
*Nov 29 17:17:48.393: %CAPWAP-3-ERRORLOG: CAPWAP SM handler: Failed to process message type 10 state 5.
L3500-12#
*Nov 29 17:17:51.554: %CAPWAP-3-EVENTLOG: Retransmission Count= 0 Max Re-Transmission Value=5

*Nov 29 17:17:51.554: %CAPWAP-3-EVENTLOG: Sending packet to AC

WLC> show ap join stats detail

(Cisco Controller) >**show ap join stats detailed** 08:17:35:31:a4:80

Sync phase statistics
- Time at sync request received..... Not applicable
- Time at sync completed..... Not applicable

Discovery phase statistics
- Discovery requests received..... 40
- Successful discovery responses sent..... 40
- Unsuccessful discovery request processing..... 0
- Reason for last unsuccessful discovery attempt..... Not applicable
- Time at last successful discovery attempt..... Nov 29 17:20:11.893
- Time at last unsuccessful discovery attempt..... Not applicable

Join phase statistics
- Join requests received..... 14
- Successful join responses sent..... 14
- Unsuccessful join request processing..... 0
- Reason for last unsuccessful join attempt..... Not applicable
- Time at last successful join attempt..... Nov 29 17:20:22.231
- Time at last unsuccessful join attempt..... Not applicable

Configuration phase statistics

- Configuration requests received..... 31
- Successful configuration responses sent..... 3
- Unsuccessful configuration request processing..... 11
- Reason for last unsuccessful configuration attempt..... **Regulatory domain check has failed for the AP**

MESH AP issue

(Cisco Controller) >config country CN,AU

Changing country code could reset channel & RRM grouping configuration.
If running in RRM One-Time mode, reassign channels after this command.
Check customized APs for valid channel values after this command.
Are you sure you want to continue? (y/n) Y

Error - Command failed - Mesh APs not currently supported by Multiple-Country. Use Single-Country or remove Mesh APs from network

(Cisco Controller) >

WLC debug (Multicountry code configured)

*spamApTask5: Nov 30 02:01:51.874: 00:1e:bd:e5:06:40 DTLS Session established server (157.0.9.11:5246), client (192.168.2.117:16069)
*spamApTask5: Nov 30 02:01:51.874: 00:1e:bd:e5:06:40 Starting wait join timer for AP: 192.168.2.117:16069

*spamApTask2: Nov 30 02:01:51.876: 08:17:35:31:a4:80 Join Request from 192.168.2.117:16069

*spamApTask2: Nov 30 02:01:51.876: 00:1e:bd:e5:06:40 Deleting AP entry 192.168.2.117:16069 from temporary database.
*spamApTask2: Nov 30 02:01:51.877: 08:17:35:31:a4:80 **Bridge AP can not join MultiCountry Controller:** Bridge mode AP 192.168.2.117:16069 cannot be supported on Multi Country Control
*spamApTask2: Nov 30 02:01:51.877: 08:17:35:31:a4:80 Finding DTLS connection to delete for AP (192:168:2:117/16069)
*spamApTask2: Nov 30 02:01:51.877: 08:17:35:31:a4:80 Disconnecting DTLS Capwap-Ctrl session 0x17aa76b8 for AP (192:168:2:117/16069)

*spamApTask2: Nov 30 02:01:51.877: 08:17:35:31:a4:80 CAPWAP State: Dtls tear down
*spamApTask2: Nov 30 02:01:51.877: acDtlsPlumbControlPlaneKeys: lrad:192.168.2.117(16069) mwar:157.0.9.11(5246)
*spamApTask2: Nov 30 02:01:51.878: 08:17:35:31:a4:80 DTLS keys for Control Plane deleted successfully for AP 192.168.2.117
*spamApTask2: Nov 30 02:01:51.884: 08:17:35:31:a4:80 Join Request failed!

AP Log

```
AP70ca.9b6b.4e77#
*Sep  1 21:00:43.075: %MESH-3-TIMER_EXPIRED: Mesh Lwapp join timer expired
*Sep  1 21:00:43.075: %MESH-3-TIMER_EXPIRED: Mesh Lwapp join failed expired
*Sep  1 21:00:43.075: %MESH-6-LINK_UPDOWN: Mesh station 70ca.9b6b.4e77 link Down
*Sep  1 21:01:02.175: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to 192.168.1.7:5246
*Sep  1 21:01:02.182: %MESH-6-CAPWAP_RESTART: Mesh Capwap re-started
*Sep  1 21:01:13.000: %CAPWAP-5-DTLSREQSEND: DTLS connection request sent peer_ip: 192.168.1.7 peer_port: 5246
*Sep  1 21:01:13.239: %CAPWAP-5-DTLSREQSUCC: DTLS connection created sucessfully peer_ip: 192.168.1.7 peer_port: 5246
*Sep  1 21:01:13.239: %CAPWAP-5-SENDJOIN: sending Join Request to 192.168.1.7
*Sep  1 21:01:18.240: %CAPWAP-5-SENDJOIN: sending Join Request to 192.168.1.7
*Sep  1 21:02:13.001: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to 192.168.1.7:5246
*Sep  1 21:02:24.000: %CAPWAP-5-DTLSREQSEND: DTLS connection request sent peer_ip: 192.168.1.7 peer_port: 5246
*Sep  1 21:02:24.239: %CAPWAP-5-DTLSREQSUCC: DTLS connection created sucessfully peer_ip: 192.168.1.7 peer_port: 5246
*Sep  1 21:02:24.242: %CAPWAP-5-SENDJOIN: sending Join Request to 192.168.1.7
*Sep  1 21:02:29.240: %CAPWAP-5-SENDJOIN: sending Join Request to 192.168.1.7
*Sep  1 21:03:24.001: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to 192.168.1.7:5246
*Sep  1 21:03:31.740: %MESH-3-TIMER_EXPIRED: Mesh Lwapp join timer expired
*Sep  1 21:03:31.740: %MESH-3-TIMER_EXPIRED: Mesh Lwapp join failed expired
*Sep  1 21:03:31.740: %MESH-6-LINK_UPDOWN: Mesh station 70ca.9b6b.4e77 link Down
*Sep  1 21:03:34.000: %CAPWAP-5-DTLSREQSEND: DTLS connection request sent peer_ip: 192.168.1.7 peer_port: 5246
*Sep  1 21:03:49.709: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to 192.168.1.7:5246
*Sep  1 21:03:49.709: %MESH-6-CAPWAP_RESTART: Mesh Capwap re-started
*Aug 24 09:53:10.000: %CAPWAP-5-DTLSREQSEND: DTLS connection request sent peer_ip: 192.168.1.6 peer_port: 5246
*Aug 24 09:53:10.449: %CAPWAP-5-DTLSREQSUCC: DTLS connection created sucessfully peer_ip: 192.168.1.6 peer_port: 5246
*Aug 24 09:53:10.449: %CAPWAP-5-SENDJOIN: sending Join Request to 192.168.1.6
*Aug 24 09:53:15.451: %CAPWAP-5-SENDJOIN: sending Join Request to 192.168.1.6
AP70ca.9b6b.4e77#
```

WLC debug (Auth-list missed add AP's MAC)

*spamApTask3: Nov 30 02:05:09.119: 08:17:35:31:a4:80 Join Request from 192.168.2.117:16070

*spamApTask3: Nov 30 02:05:09.119: 00:1e:bd:e5:06:40 Deleting AP entry 192.168.2.117:16070 from temporary database.
*spamApTask3: Nov 30 02:05:09.120: c4:71:fe:d3:ec:4f spamProcessJoinRequest : RAP, **Check MAC filter**

*spamApTask3: Nov 30 02:05:09.120: 08:17:35:31:a4:80 In AAA state 'Idle' for AP 08:17:35:31:a4:80
*spamApTask3: Nov 30 02:05:09.120: c4:71:fe:d3:ec:4f Mesh AP username c471fed3ec4f.
*spamApTask0: Nov 30 02:05:09.121: 08:17:35:31:a4:80 Finding DTLS connection to delete for AP (192:168:2:117/16070)
*spamApTask0: Nov 30 02:05:09.121: 08:17:35:31:a4:80 Disconnecting DTLS Capwap-Ctrl session 0x17aa7a18 for AP (192:168:2:117/16070)
*spamApTask0: Nov 30 02:05:09.121: 08:17:35:31:a4:80 CAPWAP State: Dtls tear down
*spamApTask0: Nov 30 02:05:09.121: acDtlsPlumbControlPlaneKeys: lrad:192.168.2.117(16070) mwar:157.0.9.11(5246)
*spamApTask0: Nov 30 02:05:09.121: 08:17:35:31:a4:80 DTLS keys for Control Plane deleted successfully for AP 192.168.2.117
*spamApTask3: Nov 30 02:05:09.127: 08:17:35:31:a4:80 Join Request failed!

WLC Traplog:

AAA Authentication Failure for UserName:c471fed3ec4f User
Type: WLAN USER

Add AP's MAC to auth-list

(Cisco Controller) >config auth-list add mic c4:71:fe:d3:ec:4f

(Cisco Controller) >show auth-list

Authorize MIC APs against Auth-list or AAA ..... disabled
Authorize LSC APs against Auth-List ..... disabled
APs Allowed to Join
  AP with Manufacturing Installed Certificate.... yes
  AP with Self-Signed Certificate..... no
  AP with Locally Significant Certificate..... no

Mac Addr	Cert Type	Key Hash
c4:71:fe:d3:ec:4f	MIC	

(Cisco Controller) >

Or Ap# test mesh mode local / AP#clear capwap private-config

WLC>show ap join stats

(Cisco Controller) >show ap join stats detailed 08:17:35:31:a4:80

Sync phase statistics
- Time at sync request received..... Not applicable
- Time at sync completed..... Not applicable

Discovery phase statistics
- Discovery requests received..... 36
- Successful discovery responses sent..... 36
- Unsuccessful discovery request processing..... 0
- Reason for last unsuccessful discovery attempt..... Not applicable
- Time at last successful discovery attempt..... Nov 30 02:12:10.102
- Time at last unsuccessful discovery attempt..... Not applicable

Join phase statistics
- Join requests received..... 8
- Successful join responses sent..... 1
- Unsuccessful join request processing..... 8
- Reason for last unsuccessful join attempt..... **RADIUS authorization is pending for the AP**
- Time at last successful join attempt..... Nov 30 02:12:20.433
- Time at last unsuccessful join attempt..... Nov 30 02:12:20.436

AP Join process

LWAPP/CAPWAPP state machine

Examples

vWLC issue

NGWC issue

Known Issue: AP(s) not joining vWLC

An AP must be at software version 7.3.1.35 and above to successfully join a virtual controller.
Virtual controllers use SSC in order to validate an AP before joining.

The AP is a new AP with 7.3 and does NOT have hash can join virtual WLC readily:
ap#show capwap client config

(Cisco Controller) >configure certificate ssc hash validation disable
APf866.f267.67af#test capwap erase
APf866.f267.67af#test capwap restart

As part of the mobility configuration, if there is a virtual controller in the network, the administrator needs to add a hash key of the virtual controller in all the peer controllers. If adding another peer controller, the consideration is to add the hash (shown in the SSC output above) to the mobility group member.

(Cisco Controller) >config mobility group member add 10.10.11.30
(Cisco Controller) >config mobility group member hash 10.10.11.30
bd7bb60436202e830802be1e8931d539b67b2537

AP Join process
LWAPP/CAPWAPP state machine
Examples
vWLC issue
NGWC issue

Converged Access Controller/ NGWC AP Join Issue

Problem 1: The AP on the Catalyst 3850 Series Switch is not in the wireless management VLAN.
Problem 2: The AP model is unsupported.
Problem 3: The AP count license is not enabled on the controller.
Problem 4: The regulatory domain is mismatched.
Problem 5: The wireless mobility controller is not defined.
Problem 6: The AP has mesh code on it.
Problem 7: The AP3700 is connected to a Catalyst 3850 Series Switch that runs 3.3.0SE.
Problem 8: The controller time is outside the AP certificate validity interval.
Problem 9: The AP authorization list is enabled on the WLC; the AP is not in the authorization list.
Problem 10: The MIC AP Policy is disabled.

Useful Link

http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/70333-lap-registration.html

http://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/119286-lap-notjoin-wlc-tshoot.html

http://www.cisco.com/c/en/us/support/docs/wireless/virtual-wireless-controller/113677-virtual-wlan-dg-00.html

http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-vlan/117551-troubleshoot-ap-00.html

Thank you.