Welcome

Technical Services Virtual Boot Camp

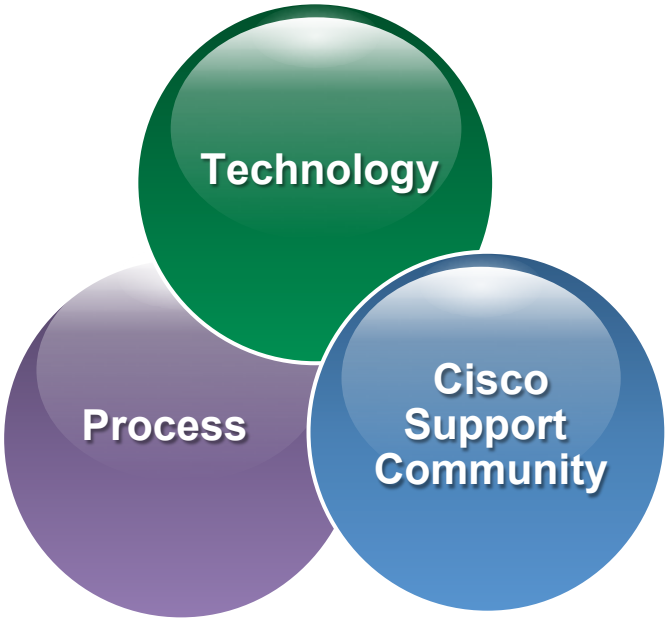
Session 15

Technical Services India Team

Recap – Nexus Session

Technology

- Nexus Overview
- Software Architecture
- Hardware Architecture
- IOS vs NX-OS
- Nexus Release Train Info



Q&A

Today's Agenda (Session 15 - 11th June)

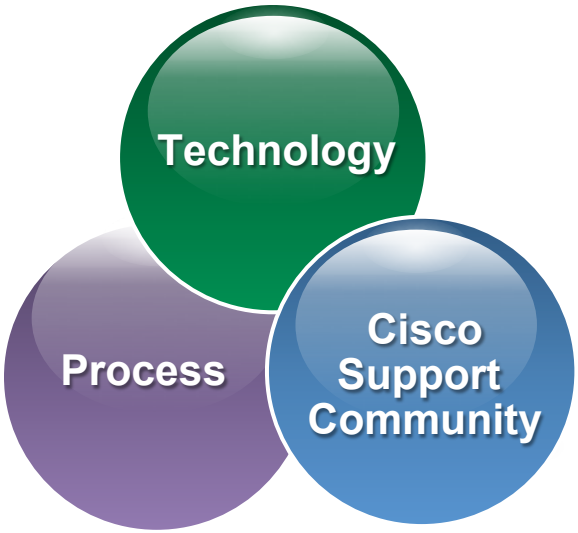
Technology

Mobility with Cisco WLC

- Overview on mobility architecture with Cisco WLC
- Debugging mobility with Cisco WLC's
- State changes when Client is roaming

Client Connectivity Troubleshooting

- Client Join process through WLC
- Debugs to be collected for different scenario



Q&A

Introduction

Nirmal Sodani
Technical Support Manager

Mohit Mmangal
Manager, CSC

Ishaan Sanji
TAC Escalation Engineer

Debashree Barat
Lead, CSC

Ishant Varshney
TAC Escalation Engineer

Shiv Goel
Technical Support Manager

Troubleshooting Client Connectivity

Ishant Varshney

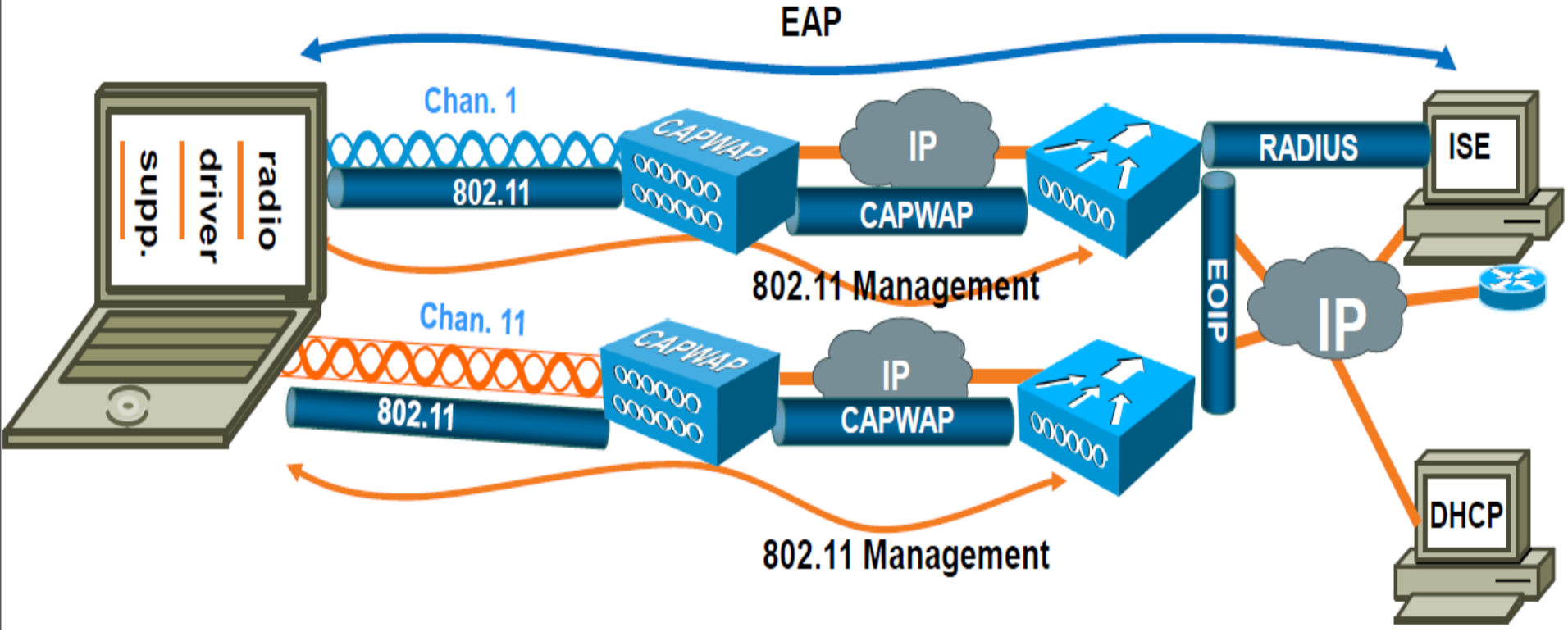
TAC Engineer - Wireless

Agenda

- Client join process
- Required debugs
- Analysis of debugs
- Mobility architecture on WLC
- Types of inter-controller roaming scenarios

A typical wireless setup

Where is client failing to connect? Isolate and remove the parts not in picture



Client join process

Client join process

802.11 Connection states

1. Listen for Beacons
2. Probe Request
3. Probe Response
4. Authentication Request
5. Authentication Response
6. Association Request
7. Association Response
8. (Optional: EAPOL Authentication)
9. (Optional: Encrypt Data)
10. Move User Data

Client join process

Show client detail <mac address>

(Controller) >show client detail x:x:x:x:x:x (mac address of wireless adaptor)

Client MAC Address..... x:x:x:x:x:x

Policy Manager State..... WEBAUTH_REQD

Client join process

802.11 Connection states

Name	Description
8021X_REQD	802.1x (L2) Authentication Pending
DHCP_REQD	IP Learning State
WEBAUTH_REQD	Web (L3) Authentication Pending
RUN	Client Traffic Forwarding

The Client Debug

- A multi-debug macro that goes over all main client states
- (Cisco Controller) >**debug client <MAC Addr of client> (Gives all main states of client)**

```
(Cisco Controller) >debug client 00:16:ea:bb:cc:dd

(Cisco Controller) >show debug

MAC Addr 1..................................... 00:16:EA:BB:CC:DD

Debug Flags Enabled:
  dhcp packet enabled.
  dot11 mobile enabled.
  dot11 state enabled
  dot1x events enabled.
  dot1x states enabled.
  pem events enabled.
  pem state enabled.
  CCKM client debug enabled.
```

- Mobility : debug client + debug mobility handoff enable
- EAP Authentication : Debug client + debug aaa all enable
- Upto 3 address in 7.2 & Upto10 address in 7.3 and higher

Client states

- **Association (Start)**
- L2 Authentication (8021X_REQD)
- Client Address Learning (DHCP_REQD)
- L3 Authentication (WEBAUTH_REQD)
- Client Fully Connected (RUN)
- Deauth/Disassoc

Association

*apfMsConnTask_4: Dec 16 11:30:42.058: 00:1c:58:8e:a5:84 Association received from mobile on BSSID 00:3a:9a:a8:ac:d2..

Applying Local Bridging Interface Policy for station 00:1c:58:8e:a5:84 - vlan 50, interface id 14, interface 'vlan50'
processSsidIE statusCode is 0 and status is 0
processSsidIE ssid_done_flag is 0 finish_flag is 0
STA - rates (8): 130 132 139 12 18 150 24 36 0 0 0 0 0 0 0 0
suppRates statusCode is 0 and gotSuppRatesElement is 1
STA - rates (12): 130 132 139 12 18 150 24 36 48 72 96 108 0 0 0 0
extSuppRates statusCode is 0 and gotExtSuppRatesElement is 0.0.0.0 START (0) Change state to AUTHCHECK (2) last state START (0)

0.0.0.0 AUTHCHECK (2) Change state to 8021X_REQD (3) last state AUTHCHECK (2)

*apfMsConnTask_4: Dec 16 11:30:42.060: 00:1c:58:8e:a5:84 apfPemAddUser2 (apf_policy.c:333) Changing state for mobile 00:1c:58:8e:a5:84 on AP 00:3a:9a:a8:ac:d0 from Idle to Associate

*apfMsConnTask_4: Dec 16 11:30:42.060: 00:1c:58:8e:a5:84 Sending Assoc Response to station on BSSID 00:3a:9a:a8:ac:d2 (status 0) ApVapId 3 Slot 0

Association - Roaming

*apfMsConnTask_1: Dec 16 14:42:18.472: 00:1e:be:25:d6:ec Reassociation received from mobile on BSSID f8:4f:57:a1:d8:a2

..

*apfMsConnTask_1: Dec 16 14:42:18.473: 00:1e:be:25:d6:ec Applying Local Bridging Interface Policy for station 00:1e:be:25:d6:ec - vlan 50, interface id 14, interface 'vlan50'

processSsidIE statusCode is 0 and status is 0

processSsidIE ssid_done_flag is 0 finish_flag is 0

STA - rates (8): 130 132 139 12 18 150 24 36 48 72 96 108 0 0 0 0

suppRates statusCode is 0 and gotSuppRatesElement is 1

STA - rates (12): 130 132 139 12 18 150 24 36 48 72 96 108 0 0 0 0

extSuppRates statusCode is 0 and gotExtSuppRatesElement is 1

*apfMsConnTask_1: Dec 16 14:42:18.473: 00:1e:be:25:d6:ec 192.168.50.100 RUN (20) Deleted mobile LWAPP rule on AP [04:da:d2:28:94:c0]

*apfMsConnTask_1: Dec 16 14:42:18.473: 00:1e:be:25:d6:ec Updated location for station old AP 04:da:d2:28:94:c0-0, new AP f8:4f:57:a1:d8:a0-0

Association – Data rates failed

*apfMsConnTask_6: Sep 12 15:17:48.685: 00:23:a7:00:46:a1 Applying site-specific Local Bridging override for station 00:23:a7:00:46:a1 - vapId 6, site 'default-group', interface 'bp_secure1'
*apfMsConnTask_6: Sep 12 15:17:48.685: 00:23:a7:00:46:a1 Applying Local Bridging Interface Policy for station 00:23:a7:00:46:a1 - vlan 510, interface id 12, interface 'bp_secure1'
*apfMsConnTask_6: Sep 12 15:17:48.685: 00:23:a7:00:46:a1 processSsidIE statusCode is 0 and status is 0
*apfMsConnTask_6: Sep 12 15:17:48.685: 00:23:a7:00:46:a1 processSsidIE ssid_done_flag is 0 finish_flag is 0
*apfMsConnTask_6: Sep 12 15:17:48.685: 00:23:a7:00:46:a1 STA - rates (4): 36 48 72 108 0 0 0 0 0 0 0 0 0 0 0 0
*apfMsConnTask_6: Sep 12 15:17:48.685: 00:23:a7:00:46:a1 suppRates statusCode is 0 and gotSuppRatesElement is 1
*apfMsConnTask_6: Sep 12 15:17:48.685: 00:23:a7:00:46:a1 STA - rates (8): 36 48 72 108 12 18 24 96 0 0 0 0 0 0 0 0
*apfMsConnTask_6: Sep 12 15:17:48.686: 00:23:a7:00:46:a1 extSuppRates statusCode is 18 and gotExtSuppRatesElement is 0
*apfMsConnTask_6: Sep 12 15:17:48.686: 00:23:a7:00:46:a1 Sending Assoc Response to station on BSSID 08:d0:9f:be:0f:b0 (status 18) ApVapId 6 Slot 1

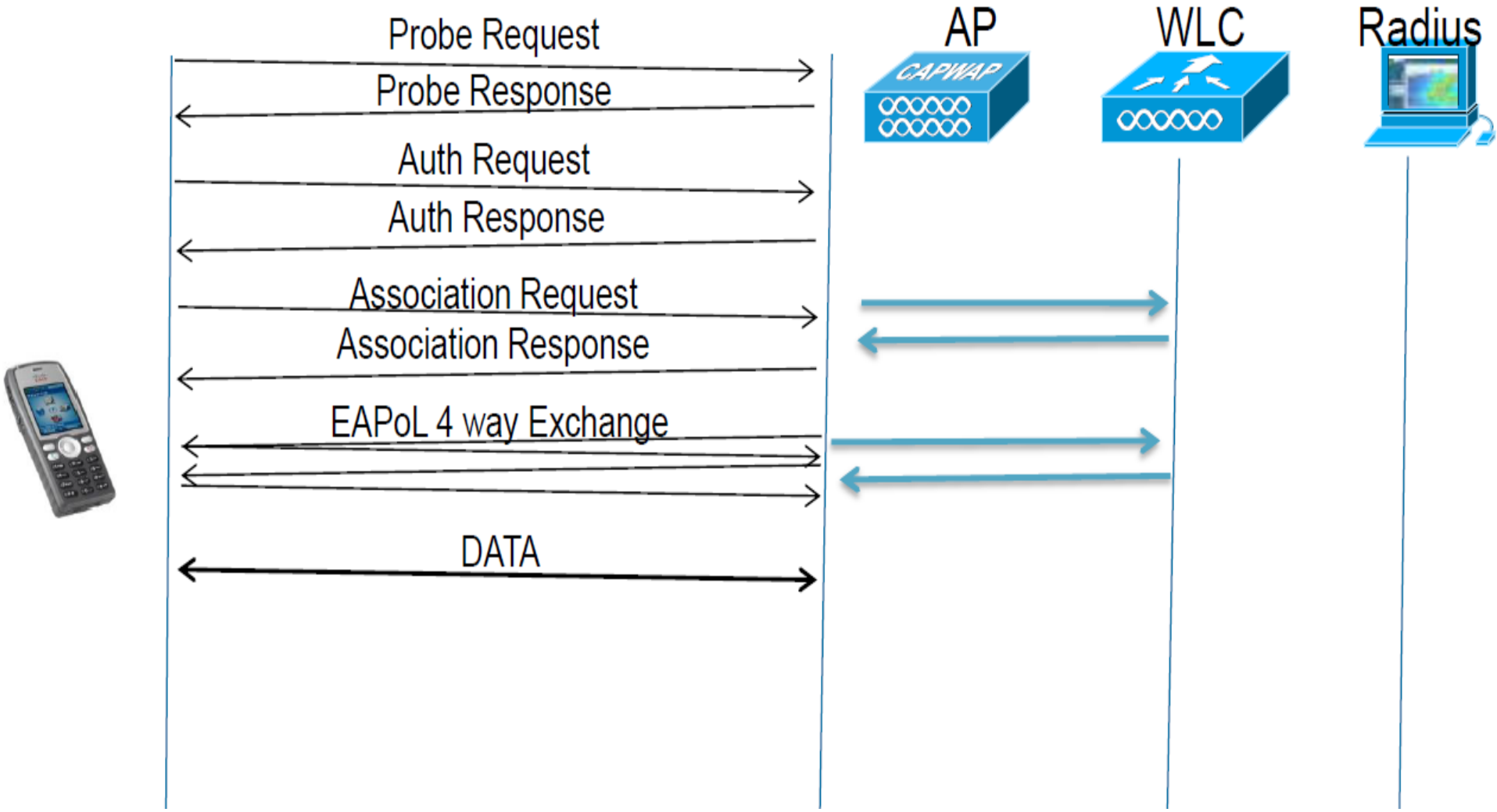
Association – Blacklisted

*apfMsConnTask_0: Dec 16 15:29:40.487: 00:40:96:b5:db:d7 Ignoring assoc request due to mobile in exclusion list or marked for deletion
00:40:96:b5:db:d7 *apfMsConnTask_0: Dec 16 15:29:41.494: 00:40:96:b5:db:d7 Ignoring assoc request due to mobile in exclusion list or marked for deletion
*apfMsConnTask_0: Dec 16 15:29:42.499: 00:40:96:b5:db:d7 Ignoring assoc request due to mobile in exclusion list or marked for deletion
*apfMsConnTask_0: Dec 16 15:29:43.505: 00:40:96:b5:db:d7 Ignoring assoc request due to mobile in exclusion list or marked for deletion

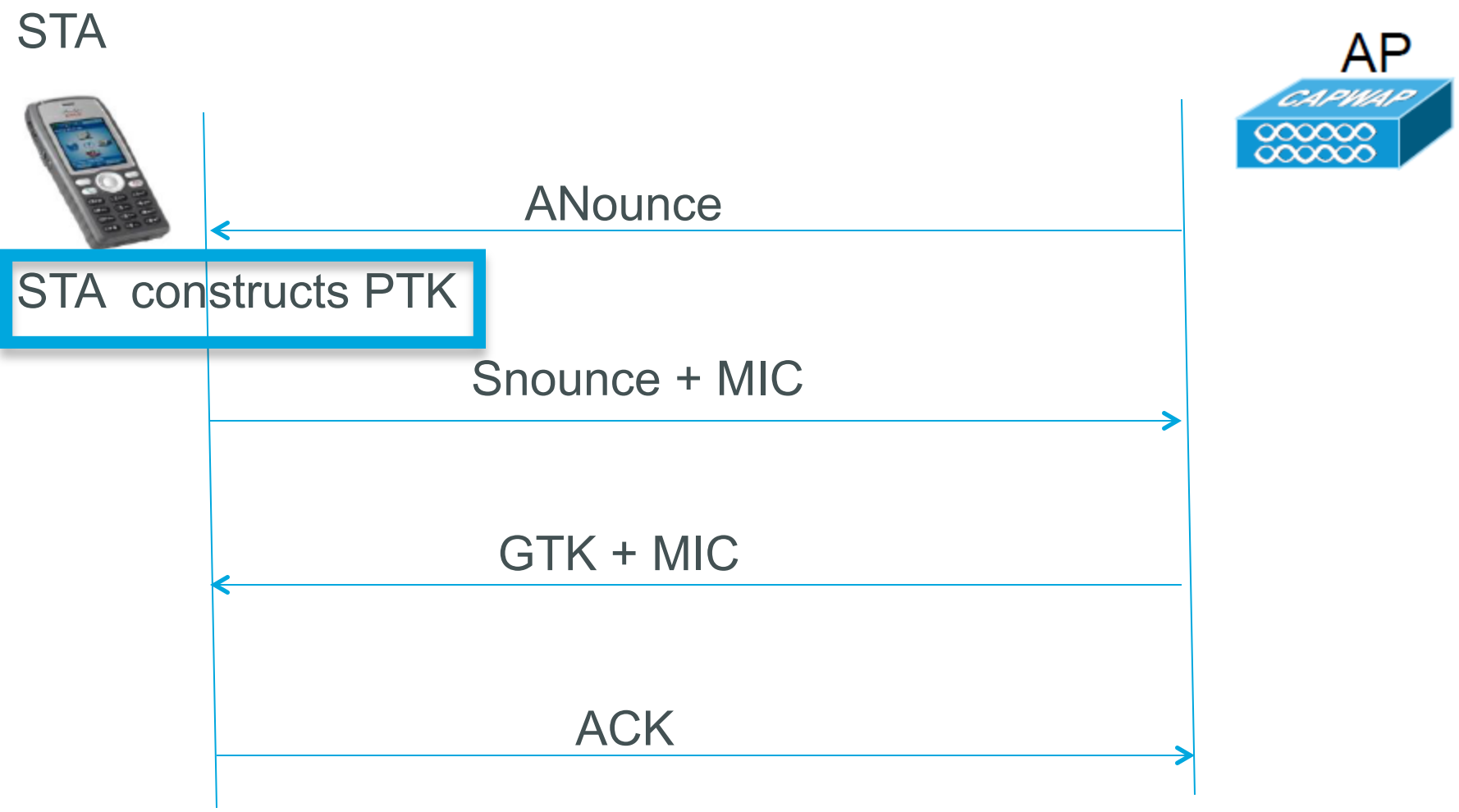
Client states

- Association (Start)
- **L2 Authentication (8021X_REQD)**
- Client Address Learning (DHCP_REQD)
- L3 Authentication (WEBAUTH_REQD)
- Client Fully Connected (RUN)
- Deauth/Disassoc

PSK authentication



EAPOL 4 way exchange



PSK – Successful

*apfMsConnTask_1: Dec 16 15:30:14.920: 00:40:96:b5:db:d7 Association received from mobile on BSSID f8:4f:57:a1:d8:aa
*apfMsConnTask_1: Dec 16 15:30:14.921: 00:40:96:b5:db:d7 Sending Assoc Response to station on BSSID f8:4f:57:a1:d8:aa (status 0)
*spamApTask3: Dec 16 15:30:14.923: 00:40:96:b5:db:d7 Sent 1x initiate message to multi thread task for mobile 00:40:96:b5:db:d7
*Dot1x_NW_MsgTask_7: Dec 16 15:30:14.924: 00:40:96:b5:db:d7 Initiating RSN PSK to mobile 00:40:96:b5:db:d7
*Dot1x_NW_MsgTask_7: Dec 16 15:30:14.924: 00:40:96:b5:db:d7 dot1x - moving mobile 00:40:96:b5:db:d7 into Force Auth state
*Dot1x_NW_MsgTask_7: Dec 16 15:30:14.924: 00:40:96:b5:db:d7 Starting key exchange to mobile 00:40:96:b5:db:d7, data packets will be dropped
*Dot1x_NW_MsgTask_7: Dec 16 15:30:14.924: 00:40:96:b5:db:d7 Sending EAPOL-Key Message to mobile 00:40:96:b5:db:d7
state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00
*Dot1x_NW_MsgTask_7: Dec 16 15:30:14.929: 00:40:96:b5:db:d7 Received EAPOL-Key from mobile 00:40:96:b5:db:d7
*Dot1x_NW_MsgTask_7: Dec 16 15:30:14.929: 00:40:96:b5:db:d7 Ignoring invalid EAPOL version (1) in EAPOL-key message from mobile 00:40:96:b5:db:d7
*Dot1x_NW_MsgTask_7: Dec 16 15:30:14.929: 00:40:96:b5:db:d7 Received EAPOL-key in PTK_START state (message 2) from mobile 00:40:96:b5:db:d7
*Dot1x_NW_MsgTask_7: Dec 16 15:30:14.929: 00:40:96:b5:db:d7 Stopping retransmission timer for mobile 00:40:96:b5:db:d7
*Dot1x_NW_MsgTask_7: Dec 16 15:30:14.929: 00:40:96:b5:db:d7 Sending EAPOL-Key Message to mobile 00:40:96:b5:db:d7
state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00.01
*Dot1x_NW_MsgTask_7: Dec 16 15:30:14.934: 00:40:96:b5:db:d7 Received EAPOL-Key from mobile 00:40:96:b5:db:d7
*Dot1x_NW_MsgTask_7: Dec 16 15:30:14.934: 00:40:96:b5:db:d7 Ignoring invalid EAPOL version (1) in EAPOL-key message from mobile 00:40:96:b5:db:d7
*Dot1x_NW_MsgTask_7: Dec 16 15:30:14.934: 00:40:96:b5:db:d7 Received EAPOL-key in PTKINITNEGOTIATING state (message 4) from mobile 00:40:96:b5:db:d7
*Dot1x_NW_MsgTask_7: Dec 16 15:30:14.934: 00:40:96:b5:db:d7 Stopping retransmission timer for mobile 00:40:96:b5:db:d7
*Dot1x_NW_MsgTask_7: Dec 16 15:30:14.934: 00:40:96:b5:db:d7 0.0.0.0 8021X_REQD (3) Change state to L2AUTHCOMPLETE (4) last state

PSK – Wrong secret

*apfMsConnTask_1: Dec 16 15:25:28.923: 00:40:96:b5:db:d7 Association received from mobile on BSSID f8:4f:57:a1:d8:aa

..

*apfMsConnTask_1: Dec 16 15:25:28.925: 00:40:96:b5:db:d7 Sending Assoc Response to station on BSSID f8:4f:57:a1:d8:aa (status 0) ApVapId 6 Slot 1

*spamApTask3: Dec 16 15:25:28.927: 00:40:96:b5:db:d7 Sent 1x initiate message to multi thread task for mobile 00:40:96:b5:db:d7

..

*Dot1x_NW_MsgTask_7: Dec 16 15:25:28.927: 00:40:96:b5:db:d7 Starting key exchange to mobile 00:40:96:b5:db:d7, data packets will be dropped

*Dot1x_NW_MsgTask_7: Dec 16 15:25:28.933: 00:40:96:b5:db:d7 Received EAPOL-Key from mobile 00:40:96:b5:db:d7

config cl;d*Dot1x_NW_MsgTask_7: Dec 16 15:25:28.933: 00:40:96:b5:db:d7 Ignoring invalid EAPOL version (1) in EAPOL-key message from mobile 00:40:96:b5:db:d7

*Dot1x_NW_MsgTask_7: Dec 16 15:25:28.933: 00:40:96:b5:db:d7 Received EAPOL-key in PTK_START state (message 2) from mobile 00:40:96:b5:db:d7

*Dot1x_NW_MsgTask_7: Dec 16 15:25:28.933: 00:40:96:b5:db:d7 Received EAPOL-key M2 with invalid MIC from mobile 00:40:96:b5:db:d7 version 2

*osapiBsnTimer: Dec 16 15:25:30.019: 00:40:96:b5:db:d7 802.1x 'timeoutEvt' Timer expired for station 00:40:96:b5:db:d7 and for message = M2

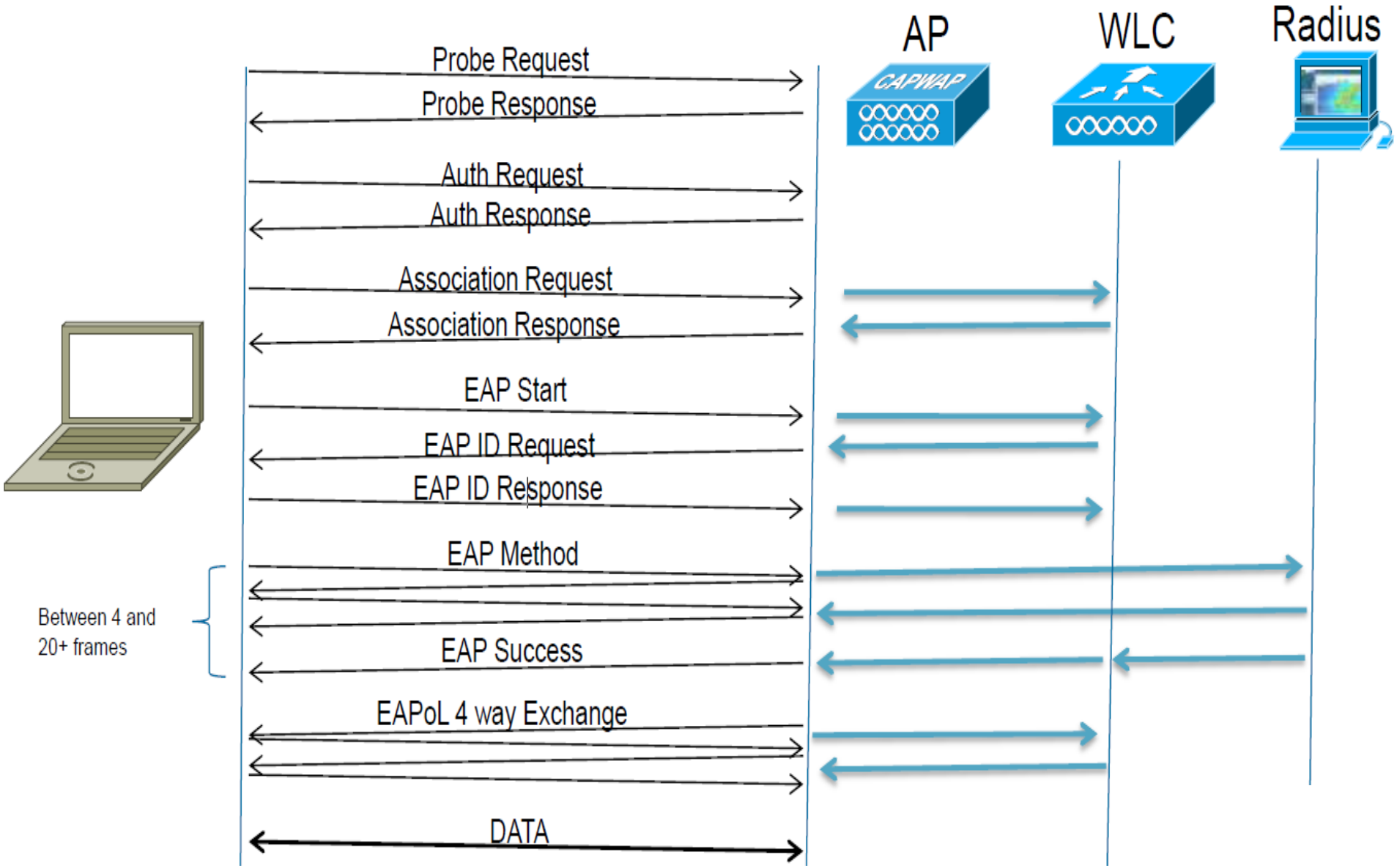
*dot1xMsgTask: Dec 16 15:25:32.019: 00:40:96:b5:db:d7 Retransmit failure for EAPOL-Key M1 to mobile 00:40:96:b5:db:d7, retransmit count 3, mscb deauth count 2

..

*dot1xMsgTask: Dec 16 15:25:32.020: 00:40:96:b5:db:d7 Sent Deauthenticate to mobile on BSSID f8:4f:57:a1:d8:a0 slot 1(caller 1x_ptsm.c:570)

*dot1xMsgTask: Dec 16 15:25:32.020: 00:40:96:b5:db:d7 Scheduling deletion of Mobile Station: (callerId: 57) in 10 seconds

802.1X Authentication



802.1x - Successful

*apfMsConnTask_0: Dec 16 15:36:07.557: 00:40:96:b5:db:d7 Sending Assoc Response to station on BSSID 04:da:d2:28:94:ce (status 0) ApVapId 2 Slot 1
Dot1x_NW_MsgTask_7: Dec 16 15:36:07.559: 00:40:96:b5:db:d7 dot1x - moving mobile 00:40:96:b5:db:d7 into Connecting state
*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.560: 00:40:96:b5:db:d7 Sending EAP-Request/Identity to mobile 00:40:96:b5:db:d7 (EAP Id 1)
*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.566: 00:40:96:b5:db:d7 Received EAPOL START from mobile 00:40:96:b5:db:d7
*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.566: 00:40:96:b5:db:d7 dot1x - moving mobile 00:40:96:b5:db:d7 into Connecting state
*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.566: 00:40:96:b5:db:d7 Sending EAP-Request/Identity to mobile 00:40:96:b5:db:d7 (EAP Id 2)
*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.567: 00:40:96:b5:db:d7 Received EAPOL EAPPKT from mobile 00:40:96:b5:db:d7
*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.567: 00:40:96:b5:db:d7 Received EAP Response packet with mismatching id (currentid=2, eapid=1) from mobile 00:40:96:b5:db:d7
*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.569: 00:40:96:b5:db:d7 Received EAPOL EAPPKT from mobile 00:40:96:b5:db:d7
*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.569: 00:40:96:b5:db:d7 Received Identity Response (count=2) from mobile 00:40:96:b5:db:d7
*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.569: 00:40:96:b5:db:d7 EAP State update from Connecting to Authenticating for mobile 00:40:96:b5:db:d7
*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.569: 00:40:96:b5:db:d7 dot1x - moving mobile 00:40:96:b5:db:d7 into Authenticating state
*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.569: 00:40:96:b5:db:d7 Entering Backend Auth Response state for mobile 00:40:96:b5:db:d7
*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.571: 00:40:96:b5:db:d7 Processing Access-Challenge for mobile 00:40:96:b5:db:d7
*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.571: 00:40:96:b5:db:d7 Entering Backend Auth Req state (id=220) for mobile 00:40:96:b5:db:d7
*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.571: 00:40:96:b5:db:d7 WARNING: updated EAP-Identifier 2 ===> 220 for STA 00:40:96:b5:db:d7
*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.571: 00:40:96:b5:db:d7 Sending EAP Request from AAA to mobile 00:40:96:b5:db:d7 (EAP Id 220)

802.1x - Successful

*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.575: 00:40:96:b5:db:d7 Received EAPOL EAPPKT from mobile 00:40:96:b5:db:d7
*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.575: 00:40:96:b5:db:d7 Received EAP Response from mobile 00:40:96:b5:db:d7 (EAP Id 220, EAP Type 3)
..
*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.718: 00:40:96:b5:db:d7 Entering Backend Auth Response state for mobile 00:40:96:b5:db:d7
*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.719: 00:40:96:b5:db:d7 Processing Access-Accept for mobile 00:40:96:b5:db:d7
*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.719: 00:40:96:b5:db:d7 Resetting web IPv4 acl from 255 to 255

*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.719: 00:40:96:b5:db:d7 Resetting web IPv4 Flex acl from 65535 to 65535

*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.720: 00:40:96:b5:db:d7 Username entry (cisco) already exists in name table, length = 253
*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.720: 00:40:96:b5:db:d7 Username entry (cisco) created in mscb for mobile, length = 253
*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.720: 00:40:96:b5:db:d7 Setting re-auth timeout to 1800 seconds, got from WLAN config.
*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.720: 00:40:96:b5:db:d7 Station 00:40:96:b5:db:d7 setting dot1x reauth timeout = 1800
*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.720: 00:40:96:b5:db:d7 Creating a PKC PMKID Cache entry for station 00:40:96:b5:db:d7 (RSN 2)
*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.721: 00:40:96:b5:db:d7 Sending EAP-Success to mobile 00:40:96:b5:db:d7 (EAP Id 228)
*Dot1x_NW_MsgTask_7: Dec 16 15:36:07.721: 00:40:96:b5:db:d7 Freeing AAACB from Dot1xCB as AAA auth is done for mobile 00:40:96:b5:db:d7

Client states

- Association (Start)
- L2 Authentication (8021X_REQD)
- **Client Address Learning (DHCP_REQD)**
- L3 Authentication (WEBAUTH_REQD)
- Client Fully Connected (RUN)
- Deauth/Disassoc

Client DHCP

- Client is in DHCP_REQD state
- Proxy Enabled:

DHCP Relay/Proxy

Between WLC and Server

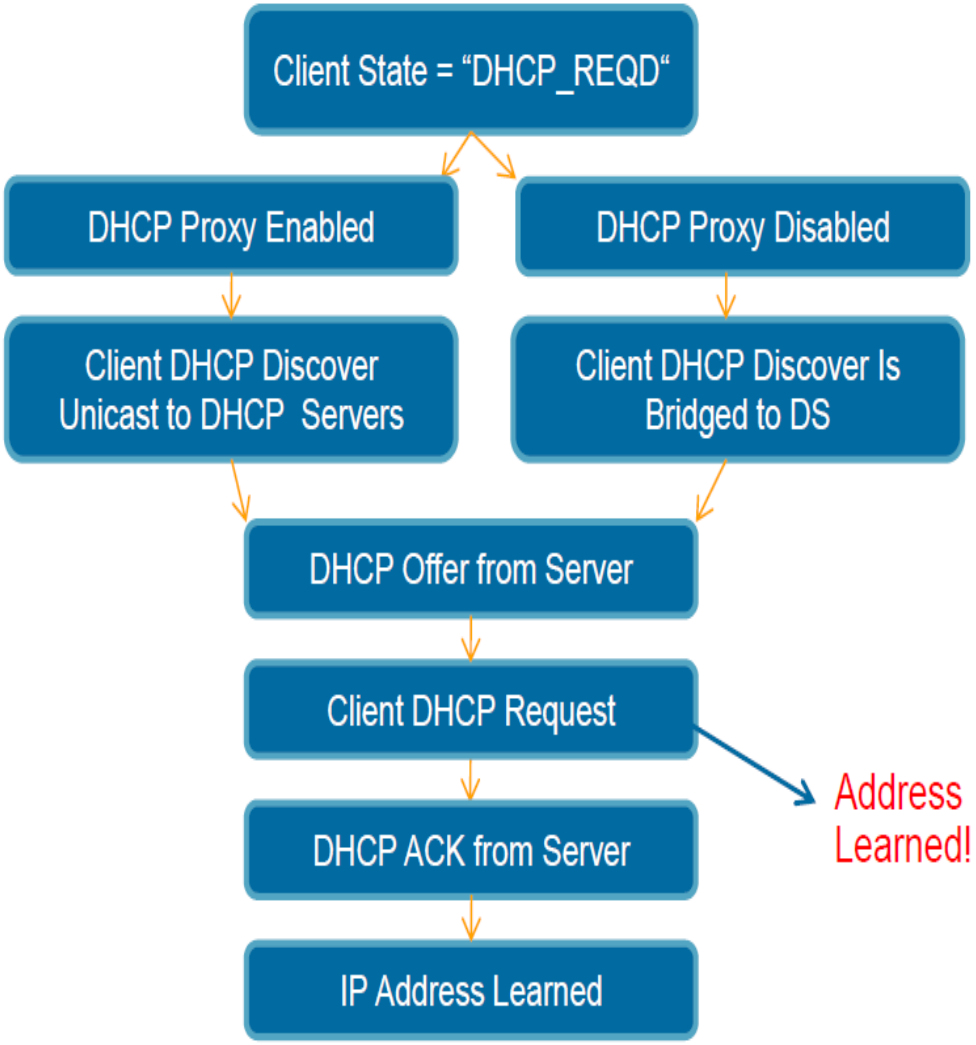
Required for Internal DHCP

- Proxy Disabled:

Between Client and Server

DHCP is broadcast out VLAN

IP helper or other means required



DHCP – Discover

```
DHCP received op BOOTREQUEST (1) (len 308,vlan 5, port 1, encap 0xec03)
DHCP (encap type 0xec03) mstype 0ff:ff:ff:ff:ff:ff

DHCP selected relay 1 - 192.168.50.1 (local address 192.168.50.15, gateway 192.168.50.1, VLAN 50, port 1)
DHCP transmitting DHCP DISCOVER (1)
DHCP   op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1
DHCP   xid: 0xa504e3 (10814691), secs: 0, flags: 0
DHCP   chaddr: 68:7f:74:75:f1:cd
DHCP   ciaddr: 0.0.0.0,  yiaddr: 0.0.0.0
DHCP   siaddr: 0.0.0.0,  giaddr: 192.168.50.15
DHCP sending REQUEST to 192.168.50.1 (len 350, port 1, vlan 50)
```

DHCP – Offer

```
DHCP received op BOOTREPLY (2) (len 308,vlan 50, port 1, encap 0xec00)
DHCP setting server from OFFER (server 192.168.0.21, yiaddr 192.168.50.101)
DHCP sending REPLY to STA (len 418, port 1, vlan 5)
DHCP transmitting DHCP OFFER (2)
DHCP   op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0
DHCP   xid: 0xa504e3 (10814691), secs: 0, flags: 0
DHCP   chaddr: 68:7f:74:75:f1:cd
DHCP   ciaddr: 0.0.0.0,  yiaddr: 192.168.50.101
DHCP   siaddr: 0.0.0.0,  giaddr: 0.0.0.0
DHCP   server id: 1.1.1.1  rcvd server id: 192.168.0.21
DHCP received op BOOTREQUEST (1) (len 335,vlan 5, port 1, encap 0xec03)
DHCP (encap type 0xec03) mstype 0ff:ff:ff:ff:ff:ff
```

DHCP – Request - ACK

```
DHCP selected relay 1 - 192.168.0.21 (local address 192.168.50.15, gateway 192.168.50.1, VLAN 50, port 1)
DHCP transmitting DHCP REQUEST (3)
DHCP   op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1
DHCP   xid: 0xa504e3 (10814691), secs: 0, flags: 0
DHCP   chaddr: 68:7f:74:75:f1:cd
DHCP   ciaddr: 0.0.0.0,  yiaddr: 0.0.0.0
DHCP   siaddr: 0.0.0.0,  giaddr: 192.168.50.15
DHCP   requested ip: 192.168.50.101
DHCP   server id: 192.168.0.21  rcvd server id: 1.1.1.1
DHCP sending REQUEST to 192.168.50.1 (len 374, port 1, vlan 50)

DHCP received op BOOTREPLY (2) (len 312,vlan 50, port 1, encap 0xec00)
192.168.50.101 DHCP_REQD (7) Change state to WEBAUTH_REQD (8) last state DHCP_REQD (7)

192.168.50.101 WEBAUTH_REQD (8) pemAdvanceState2 6662, Adding TMP rule
192.168.50.101 WEBAUTH_REQD (8) Replacing Fast Path rule
  type = Airespace AP Client - ACL passthru
  on AP 04:da:d2:4f:f0:50, slot 0, interface = 1, QOS = 0
  IPv4 A
Plumbing web-auth redirect rule due to user logout
Assigning Address 192.168.50.101 to mobile
```

DHCP – Rejected

```
DHCP transmitting DHCP REQUEST (3)
DHCP   op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1
DHCP   xid: 0xf3a2fca6 (4087544998), secs: 3, flags: 0
DHCP   chaddr: d0:b3:3f:33:1c:88
DHCP   ciaddr: 0.0.0.0,  yiaddr: 0.0.0.0
DHCP   siaddr: 0.0.0.0,  giaddr: 10.87.193.2
DHCP   requested ip: 10.65.8.177
DHCP sending REQUEST to 10.87.193.1 (len 374, port 1, vlan 703)
DHCP selecting relay 2 - control block settings:
dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
dhcpGateway: 0.0.0.0, dhcpRelay: 10.87.193.2  VLAN: 703
DHCP selected relay 2 - NONE

DHCP received op BOOTREPLY (2) (len 308,vlan 703, port 1, encap 0xec00)
DHCP sending REPLY to STA (len 402, port 1, vlan 701)
DHCP transmitting DHCP NAK (6)
DHCP   op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0
DHCP   xid: 0xf3a2fca6 (4087544998), secs: 0, flags: 8000
DHCP   chaddr: d0:b3:3f:33:1c:88
DHCP   ciaddr: 0.0.0.0,  yiaddr: 0.0.0.0
DHCP   siaddr: 0.0.0.0,  giaddr: 0.0.0.0
DHCP   server id: 1.1.1.1  rcvd server id: 10.65.8.1
```

Client states

- Association (Start)
- L2 Authentication (8021X_REQD)
- Client Address Learning (DHCP_REQD)
- L3 Authentication (WEBAUTH_REQD)
- **Client Fully Connected (RUN)**
- Deauth/Disassoc

RUN status

- RUN means: client has completed all required policy states
- “Type 1” is the goal

```
*dot1xMsgTask: Nov 05 14:35:11.838: 2c:54:2d:ea:e7:aa 10.253.42.45 RUN (20) Reached PLUMBFASTPATH: from line
6076Nov  5 *dot1xMsgTask: Nov 05 14:35:11.838: 2c:54:2d:ea:e7:aa 10.253.42.45 RUN (20) Adding Fast Path rule
*dot1xMsgTask: Nov 05 14:35:11.838: 2c:54:2d:ea:e7:aa 10.253.42.45 RUN (20) Fast Path rule (contd...) 802.1P = 5,
DSCP = 0, TokenID = 15206  Local Bridging Vlan = 101, Local Bridging intf id = 18
*dot1xMsgTask: Nov 05 14:35:11.841: 2c:54:2d:ea:e7:aa 10.253.42.45 RUN (20) Successfully plumbed mobile rule
(IPv4 ACL ID 255, IPv6 ACL ID 255)Nov  5 14:35:13 btwlc01 BTWLC01 *pemReceiveTask:
Nov 05 14:35:11.842: 2c:54:2d:ea:e7:aa 10.253.42.45 Added NPU entry of type 1, dtlFlags 0x0
```

Client states

- Association (Start)
- L2 Authentication (8021X_REQD)
- Client Address Learning (DHCP_REQD)
- L3 Authentication (WEBAUTH_REQD)
- Client Fully Connected (RUN)
- **Deauth/Disassoc**

Deauthenticated Client

Idle Timeout

Occurs after no traffic received from Client at AP

Default Duration is 300 seconds

Received Idle-Timeout from AP 00:26:cb:94:44:c0, slot 0 for STA 00:1e:8c:0f:a4:57
apfMsDeleteByMscb Scheduling mobile for deletion with deleteReason 4, **reasonCode 4**
Scheduling deletion of Mobile Station: (callerId: 30) in 1 seconds
apfMsExpireCallback (apf_ms.c:608) Expiring Mobile!
Sent Deauthenticate to mobile on BSSID 00:26:cb:94:44:c0 slot 0(caller apf_ms.c:5094)

Session Timeout

Occurs at scheduled duration (default 1800 seconds)

apfMsExpireCallback (apf_ms.c:608) **Expiring Mobile!**
apfMsExpireMobileStation (apf_ms.c:5009) Changing state for mobile 00:1e:8c:0f:a4:57 on AP 00:26:cb:94:44:c0 **from Associated to Disassociated**
Scheduling deletion of Mobile Station: (callerId: 45) in 10 seconds
apfMsExpireCallback (apf_ms.c:608) Expiring Mobile!
Sent Deauthenticate to mobile on BSSID 00:26:cb:94:44:c0 slot 0(caller apf_ms.c:5094)

Deauthenticated Client

WLAN Change

Modifying a WLAN in anyway Disables and Re-enables WLAN

apfSendDisAssocMsgDebug (apf_80211.c:1855) Changing state for mobile 00:1e:8c:0f:a4:57 on AP 00:26:cb:94:44:c0 from **Associated to Disassociated**
Sent Disassociate to mobile on AP 00:26:cb:94:44:c0-0 (reason 1, caller apf_ms.c:4983)
Sent Deauthenticate to mobile on BSSID 00:26:cb:94:44:c0 slot 0(caller apf_ms.c:5094)

- Manual Deauth

  From GUI: Remove Client

  From CLI: config client deauthenticate <mac address>

apfMsDeleteByMscb Scheduling mobile for deletion with **deleteReason 6, reasonCode 1**
Scheduling deletion of Mobile Station: (callerId: 30) in 1 seconds
apfMsExpireCallback (apf_ms.c:608) Expiring Mobile!
apfMsExpireMobileStation (apf_ms.c:5009) Changing state for mobile 00:1e:8c:0f:a4:57 on AP 00:26:cb:94:44:c0 from Associated to Disassociated
Sent Deauthenticate to mobile on BSSID 00:26:cb:94:44:c0 slot 0(caller apf_ms.c:5094)

Deauthenticated Client

Authentication Timeout

Auth or Key Exchange max-retransmissions reached

Retransmit failure for EAPOL-Key M3 to mobile 00:1e:8c:0f:a4:57, retransmit count 3, mscb deauth count 0
Sent Deauthenticate to mobile on BSSID 00:26:cb:94:44:c0 slot 0(caller 1x_ptsm.c:534)

AP Radio Reset (Power/Channel)

AP disasassociates clients but WLC does not delete entry

Cleaning up state for STA 00:1e:8c:0f:a4:57 **due to event for AP** 00:26:cb:94:44:c0(0)
apfSendDisAssocMsgDebug (apf_80211.c:1855) Changing state for mobile
00:1e:8c:0f:a4:57 on AP 00:26:cb:94:44:c0 from Associated to Disassociated
Sent Disassociate to mobile on AP 00:26:cb:94:44:c0-0 (**reason 1,** caller apf_ms.c:4983)

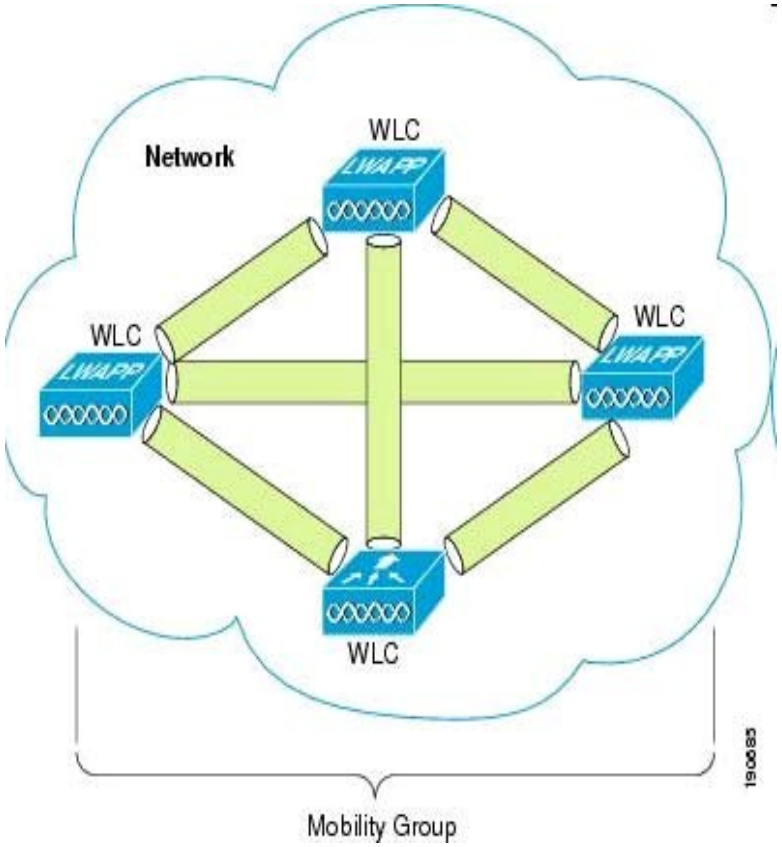
Mobility on the Cisco Wireless Lan Controllers

Ishaan Sanji

TAC Engineer - Wireless

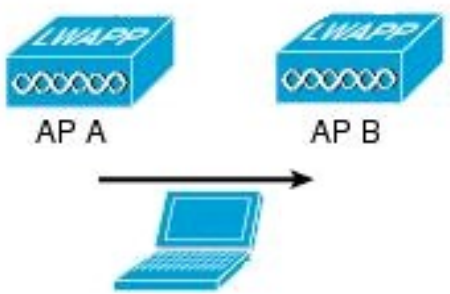
Mobility Group

- Mobility Group:
  - Group of WLC that share client information.



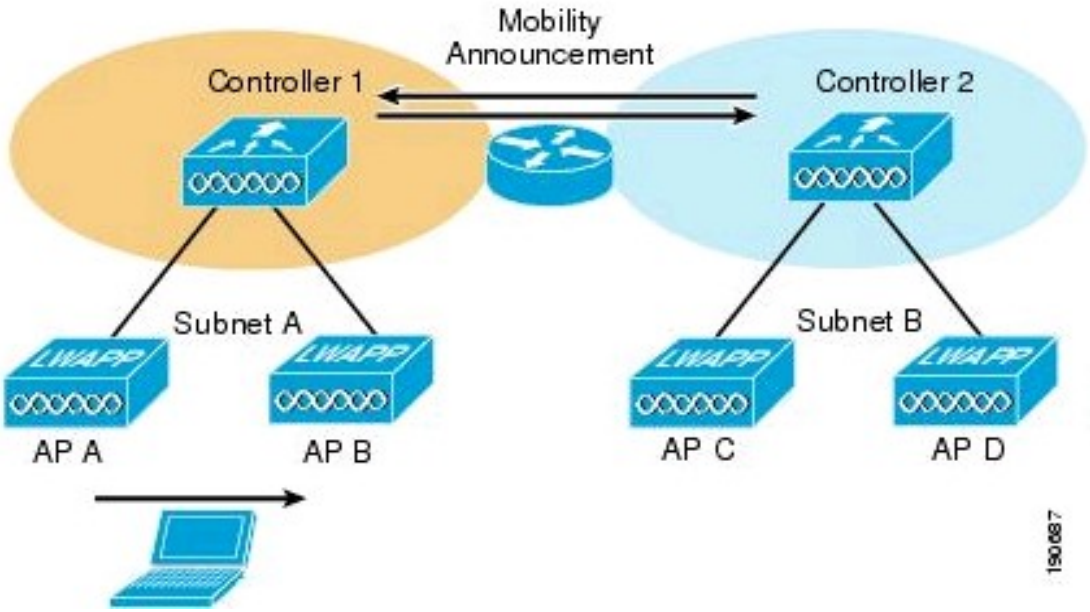
Roaming

- Definition: A station is changing its association from 1 AP within a ESS to another AP
- WLC keeps track of client entry:
  - MAC, ip, security context, QoS, WLAN, AP
- Seamless roaming: roaming is transparent to client applications



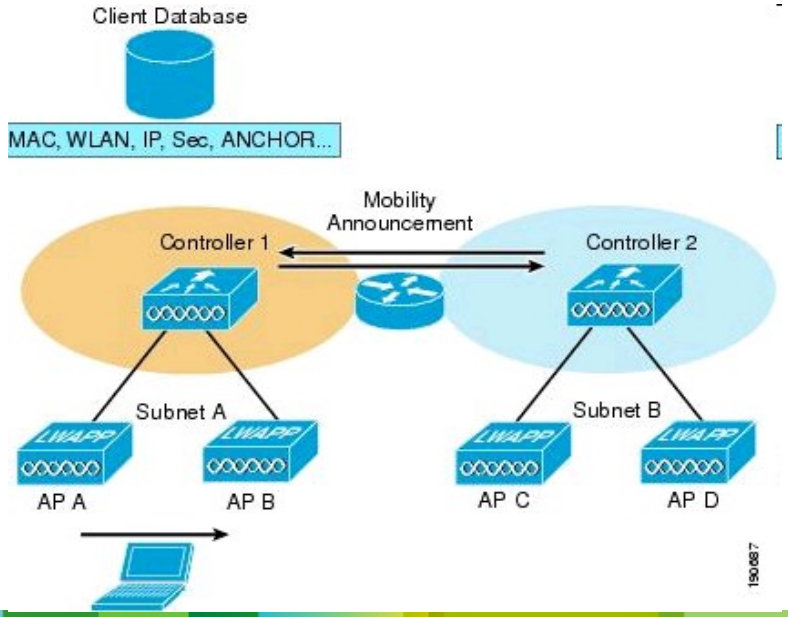
Inter controller roaming

- Layer 2 roaming: dynamic interface in same ip-subnet
- Layer 3 roaming: dynamic interface in different ip-subnet



Layer 2 inter-WLC roaming

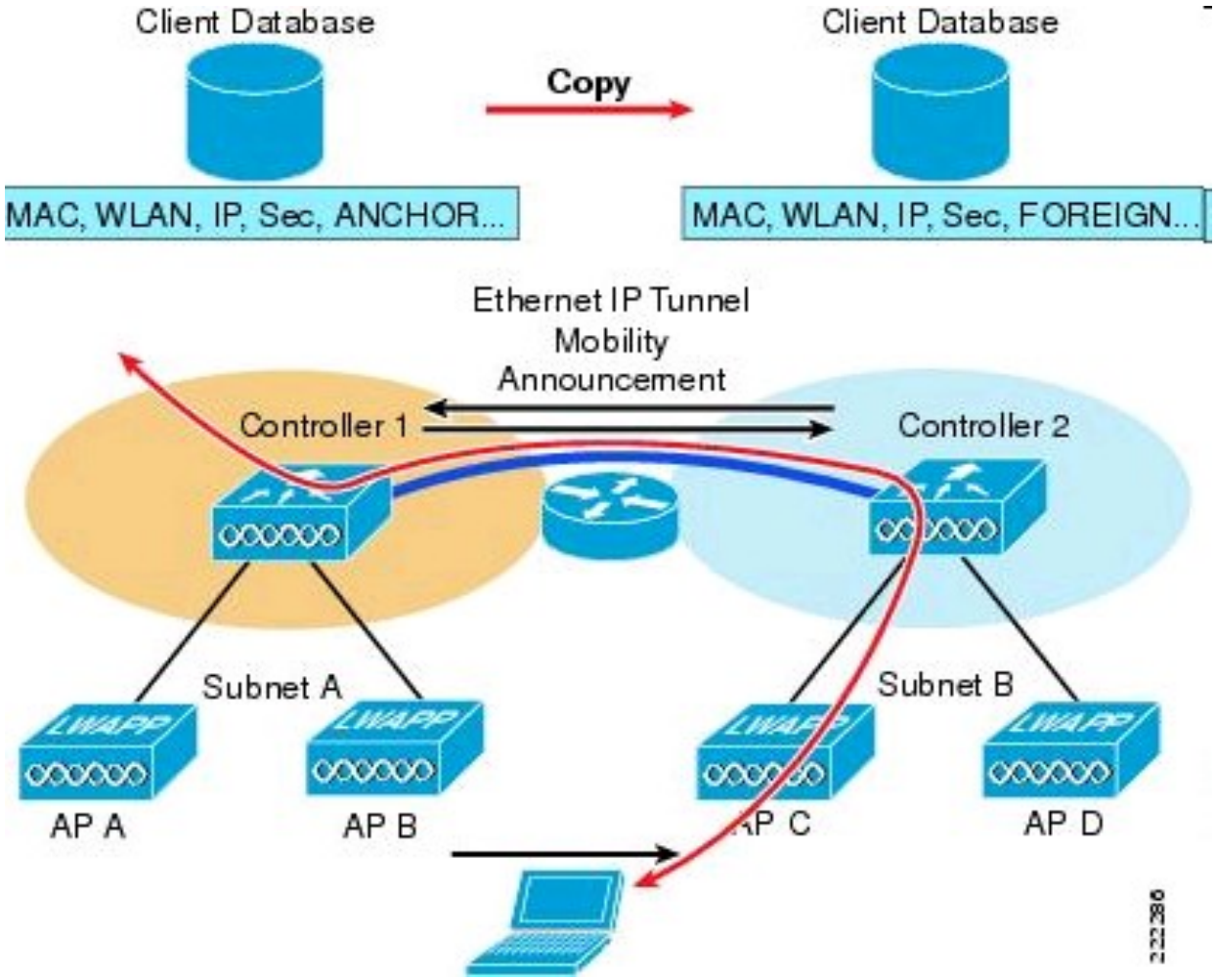
- Mobility Announcement exchanged between WLC
- Database entry copied to other WLC



Layer 3 roaming

- WLAN have dynamic interfaces in different ip-subnet
- Original WLC will keep client entry as anchor
- New WLC will copy client entry and mark as foreign
- Client data will be transferred through mobility tunnel (EoIP)

Symmetric tunneling



Client session

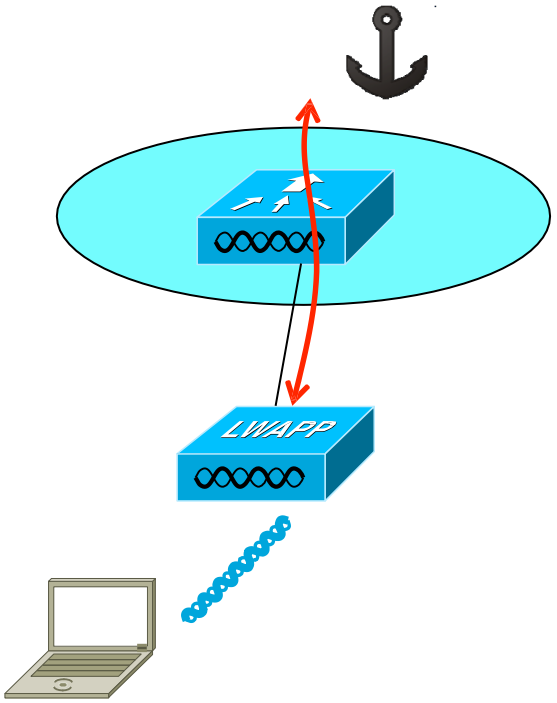
IP point of presence (IP-PoP)

- Ideally the place where IP routing will expect to find the client
- For a WLC is the dynamic interface associated to WLAN

AP association:

- AP is joined to WLC

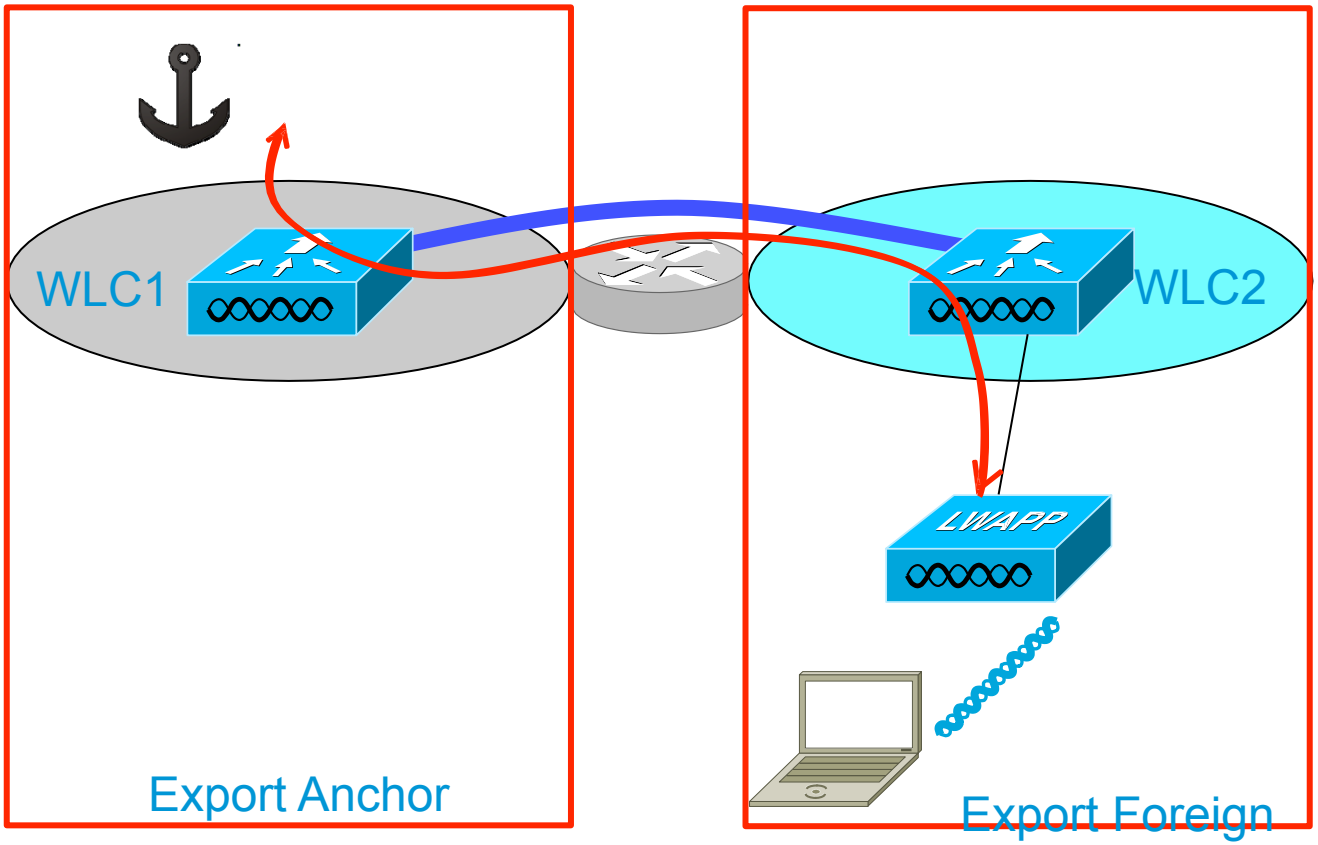
- **Local**:
  - Both IP-PoP and AP provided by same WLC



Client session

- **Export Anchor**:
  - Paired with a **Export Foreign**
  - Only IP PoP is provided, AP will be on other WLC.Packet To client sent in EoIP tunnel Proxy
  - ARP, DHCP relay: packet directly sent to client through the EOIP tunnel (Export Foreign not doing relay)
- **Export Foreign:**
  - Paired with an **Export Anchor**
  - Only AP association provided
  - All client packets are forwarded to anchor through EoIP tunnel. L2 authentication is handled by foreign.

Client session

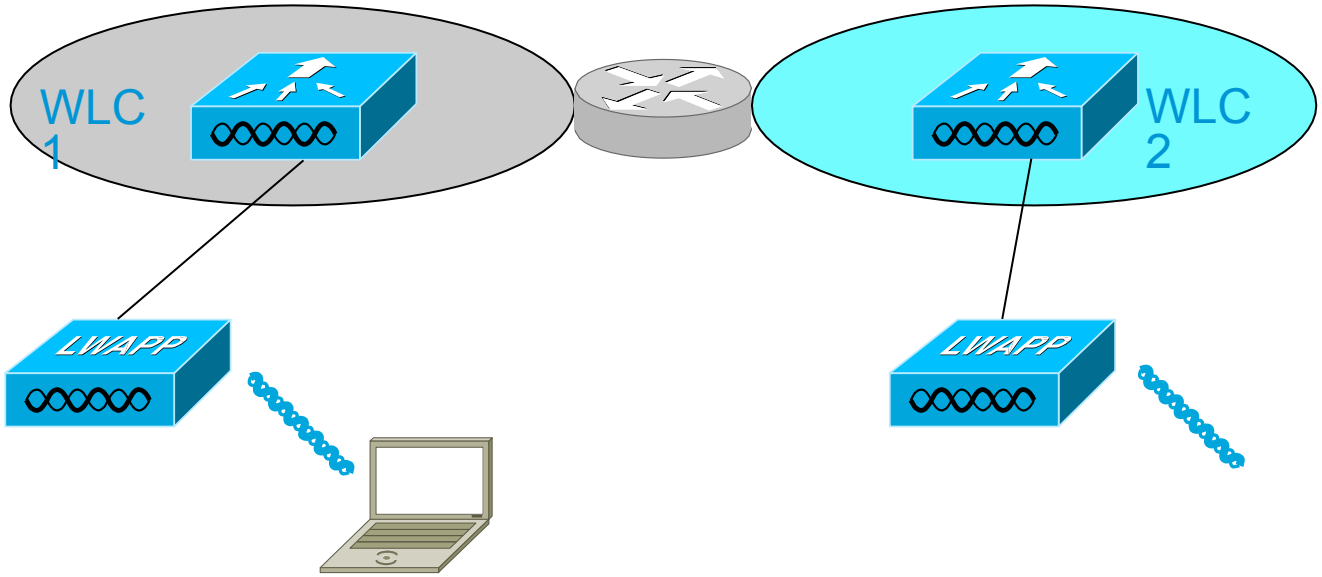


Handoff

- A new client will associate to an AP on the WLC
- WLC send *Mobile Announce* to all peers (multicast from 5.0)

  If no answer is recieved, a local session is created
- If another WLC has client in **local** or **foreign**
  - *Mobile Handoff* is sent
- Whether layer2 or layer3 roaming will occur based on Mobile Announce information

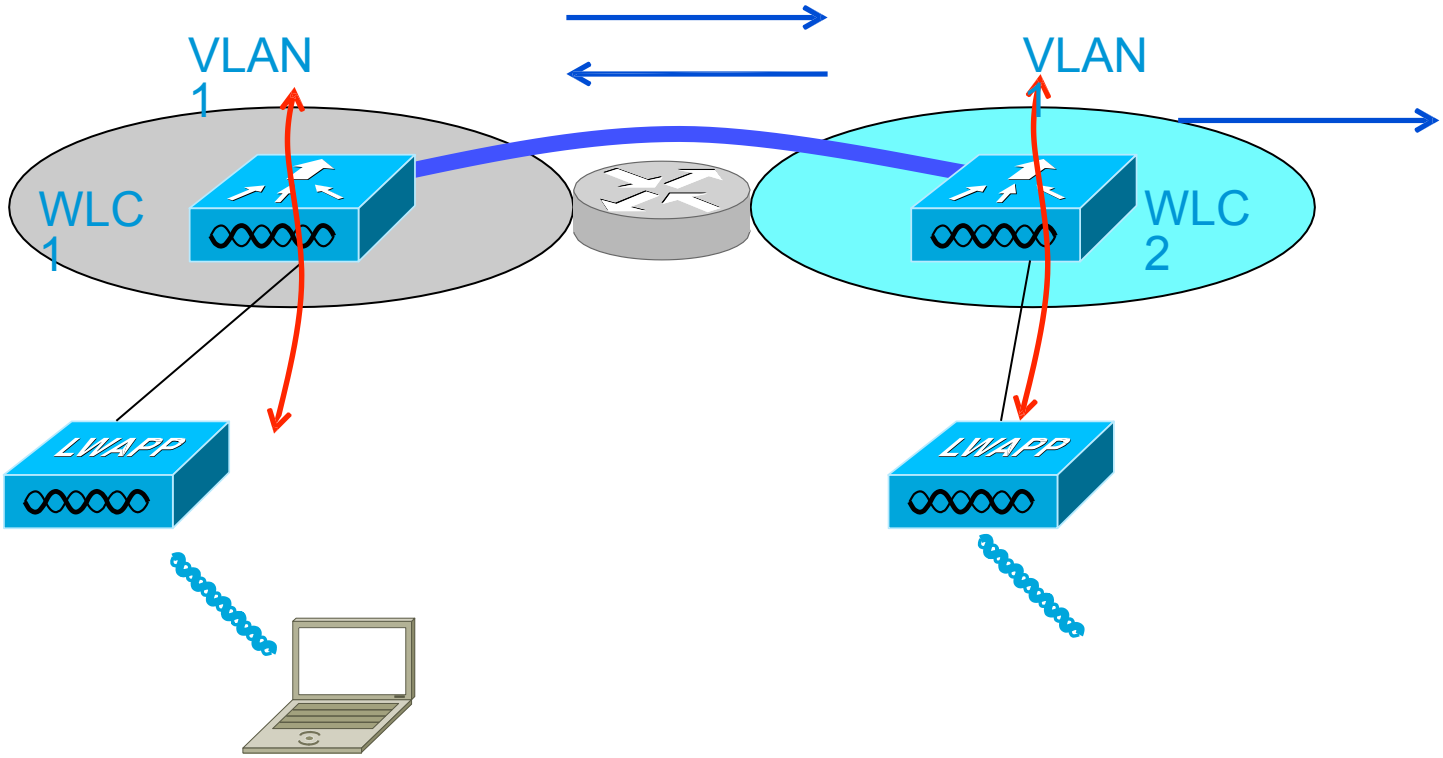
Client session transfer



- STA initially associated on WLC1
- STA roams to WLC2

Local -> Local

Client	L

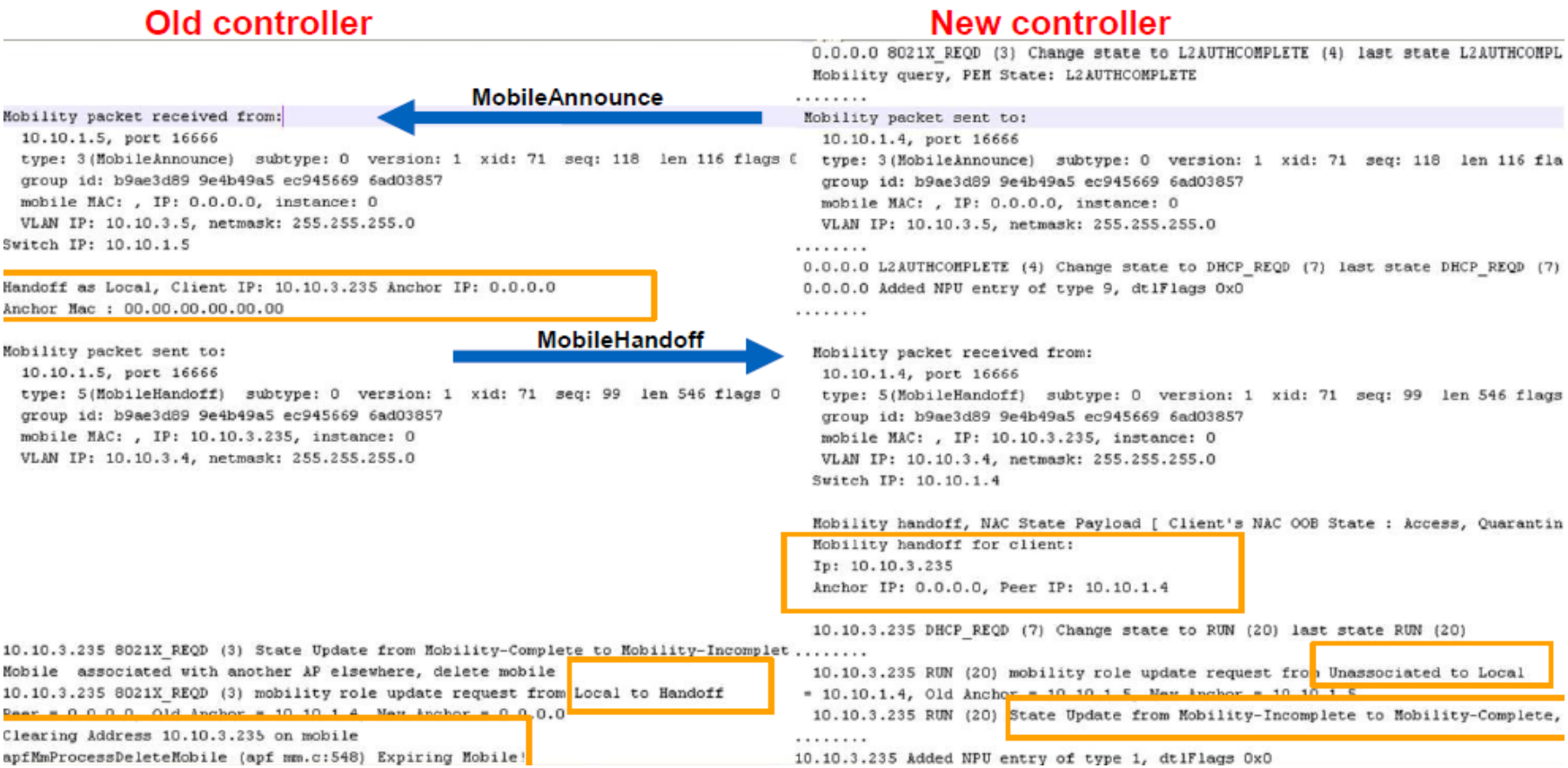


Local -> Local

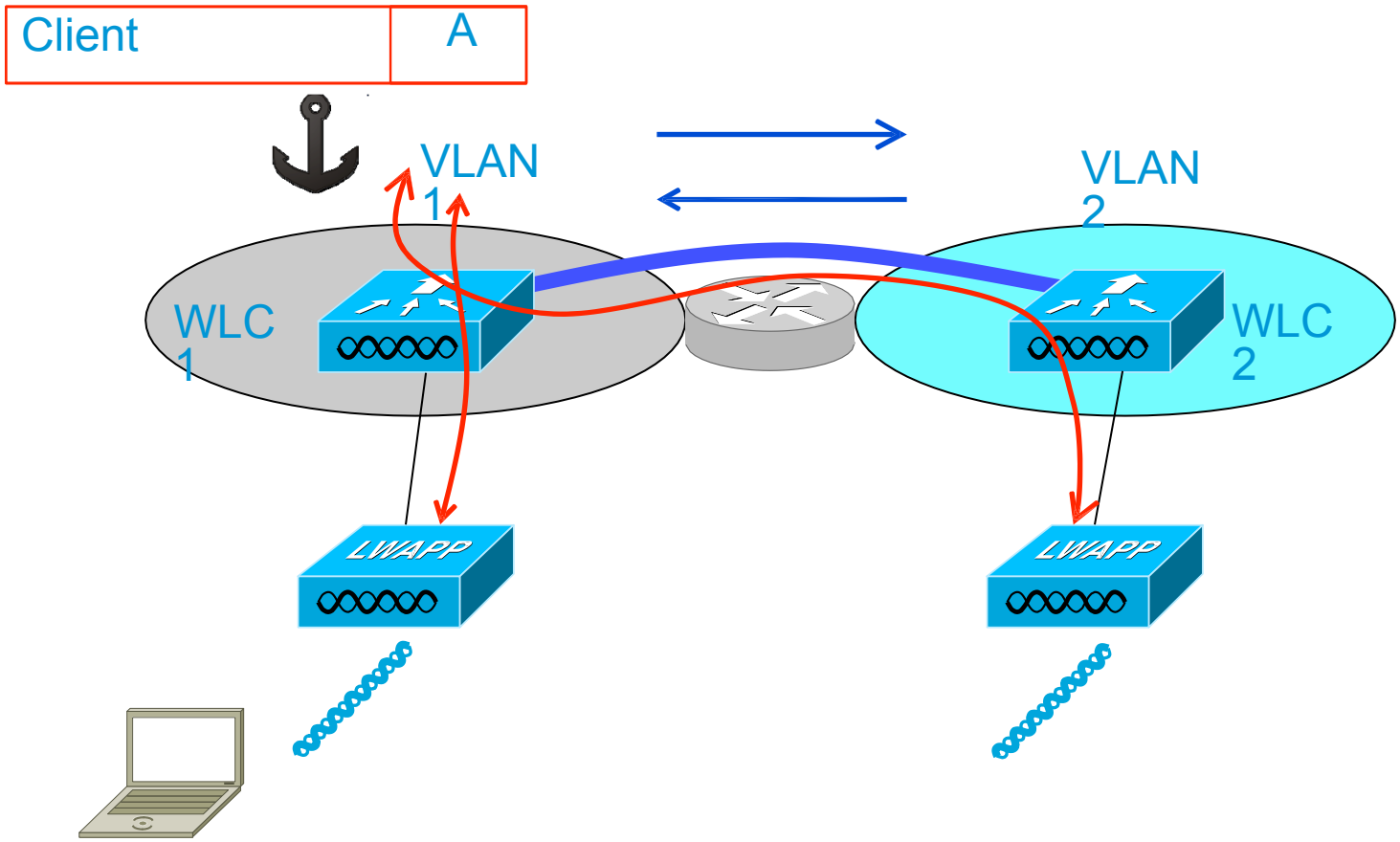
- When both controllers share same subnet for dynamic interface associated to WLAN

- new-WLC -> old-WLC: Mobile announce
- new-WLC <- old-WLC: Mobile Handoff
- Client session is transferred from old to new WLC

Debugs:



Local -> Foreign



Local -> Foreign

- When dynamic interfaces are in different IP subnets

- new-WLC -> old-WLC: Mobile announce
- new-WLC <- old-WLC: Mobile Handoff
- *L3 client info extracted from local*

Debugs:

Old controller

```
Mobility packet received from:
  10.10.1.4, port 16666
  type: 3(MobileAnnounce)  subtype: 0  version: 1  xid: 177  seq: 180
  group id: b9ae3d89 9e4b49a5 ec945669 6ad03857
  mobile MAC:, IP: 0.0.0.0, instance: 0
  VLAN IP: 10.10.3.4, netmask: 255.255.255.0
Switch IP: 10.10.1.4
Handoff as Local, Client IP: 10.10.1.103 Anchor IP: 10.10.1.5
Anchor Nac : f8 66 f2 f8 e8 40
Mobility packet sent to:
  10.10.1.4, port 16666
  type: 5(MobileHandoff)  subtype: 0  version: 1  xid: 177  seq: 204  l
  group id: b9ae3d89 9e4b49a5 ec945669 6ad03857
  mobile MAC:, IP: 10.10.1.103, instance: 0
  VLAN IP: 10.10.1.5, netmask: 255.255.255.0
```

MobileAnnounce

MobileHandoff

```
10.10.1.103 RUN (20) State Update from Mobility-Complete to Mobility-In
Updated location for station old AP 00:16:9c:4b:c4:c0-0, new AP 00:00:0
10.10.1.103 RUN (20) mobility role update request from Local to Anchor
Peer = 10.10.1.4, Old Anchor = 10.10.1.5, New Anchor = 10.10.1.5
```

New controller

```
0.0.0.0 8021X_REQD (3) Change state to L2AUTHCOMPLETE (4) last state L2AUTHCOM
Mobility packet sent to:
  10.10.1.5, port 16666
  type: 3(MobileAnnounce)  subtype: 0  version: 1  xid: 177  seq: 180  len 116
  group id: b9ae3d89 9e4b49a5 ec945669 6ad03857
  mobile MAC:, IP: 0.0.0.0, instance: 0
VLAN IP: 10.10.3.4, netmask: 255.255.255.0
```

```
Mobility packet received from:
  10.10.1.5, port 16666
  type: 5(MobileHandoff)  subtype: 0  version: 1  xid: 177  seq: 204  len 546
  group id: b9ae3d89 9e4b49a5 ec945669 6ad03857
  mobile MAC:, IP: 10.10.1.103, instance: 0
  VLAN IP: 10.10.1.5, netmask: 255.255.255.0
Switch IP: 10.10.1.5
Mobility handoff, NAC State Payload [ Client's NAC OOB State : Access, Quarant
Mobility handoff for client:
  Ip: 10.10.1.103
  Anchor IP: 10.10.1.5, Peer IP: 10.10.1.5
0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) last state DHCP_REQD
10.10.1.103 DHCP_REQD (7) Change state to RUN (20) last state RUN (20)
10.10.1.103 RUN (20) Reached PLUMBFASTPATH: from line 5273
10.10.1.103 RUN (20) Change state to RUN (20) last state RUN (20)
Assigning Address 10.10.1.103 to mobile
Handoff confirm: Pre Handoff PEM State: RUN
10.10.1.103 RUN (20) mobility role update request from Unassociated to Foreign
  Peer = 10.10.1.5, Old Anchor = 10.10.1.5, New Anchor = 10.10.1.5
```

Debugs (continued):

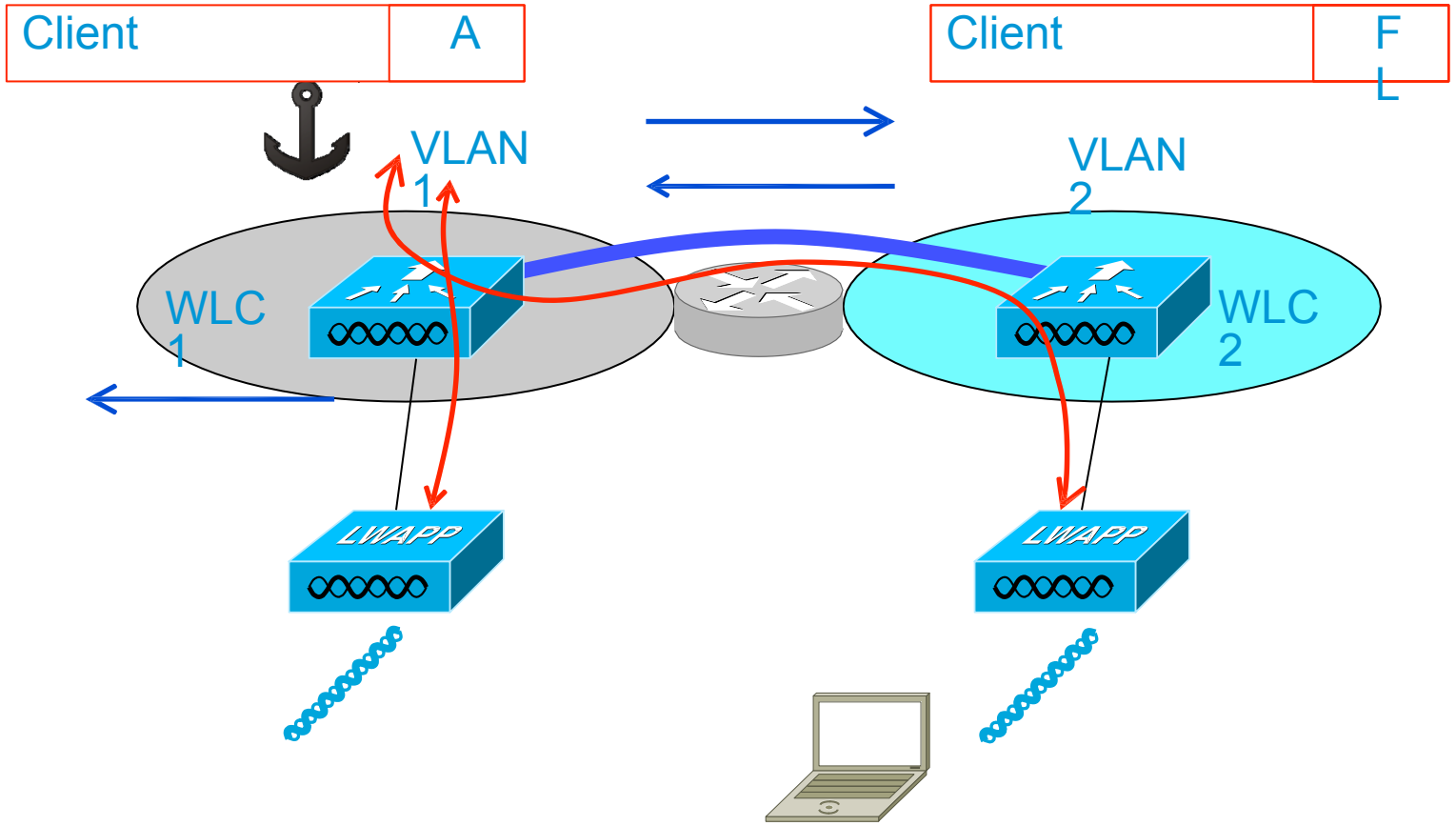
Anchor (Old controller)

```
10.10.1.103 RUN (20) State Update from Mobility-Incomplete to Mobility-Complete,
  mobility role=Anchor, client state=APF_MS_STATE_ASSOCIATED

Mobility Response: IP 10.10.1.103 code Handoff Indication (2),
   reason Client handoff successful - anchor released (1), PEM State RUN, Role Anchor
Set symmetric mobility tunnel for as in Anchor role
10.10.1.103 Added NPU entry of type 1, dtlFlags 0x1
Sending a gratuitous ARP for 10.10.1.103, VLAN Id 0

(Cisco Controller) >show client detail
Client MAC Address.............................
AP MAC Address.................................. 00:00:00:00:00:00
Mobility State.................................. Anchor
Mobility Foreign IP Address..................... 10.10.1.4
```

Foreign (New controller)

```
10.10.1.103 RUN (20) State Update from Mobility-Incomplete to Mobility-Complete
   mobility role=Foreign, client state=APF_MS_STATE_ASSOCIATED
10.10.1.103 RUN (20) Change state to RUN (20) last state RUN (20)
Configured Anchor for mobile. Sending Igmp query
Mobility Response: IP 10.10.1.103 code Handoff (1),
    reason Handoff success (0), PEM State RUN, Role Foreign(3)
Set symmetric mobility tunnel for as in Foreign role
10.10.1.103 Added NPU entry of type 1, dtlFlags 0x1

(Cisco Controller) >show client detail
Client MAC Address.............................
AP MAC Address.................................. 00:26:cb:94:44:c0
Mobility State.................................. Foreign
Mobility Anchor IP Address...................... 10.10.1.5
```

Foreign -> Local

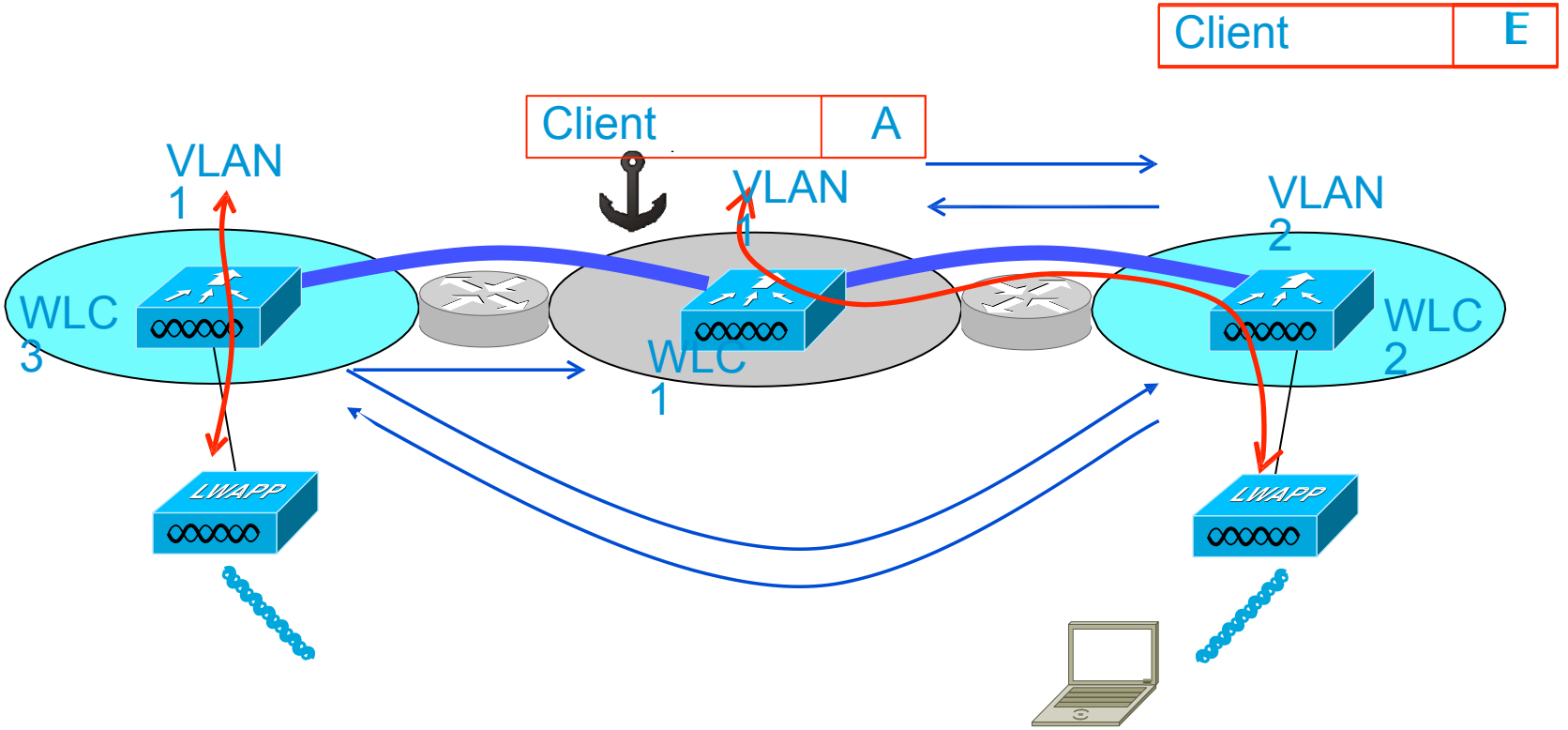


Foreign -> Local (1)

- Client roams back to an AP joined to current anchor

- new-WLC -> old-WLC: Mobile announce
- new-WLC <- old-WLC: Mobile Handoff
- *L3 client info extracted from foreign*

Foreign -> Local (2)

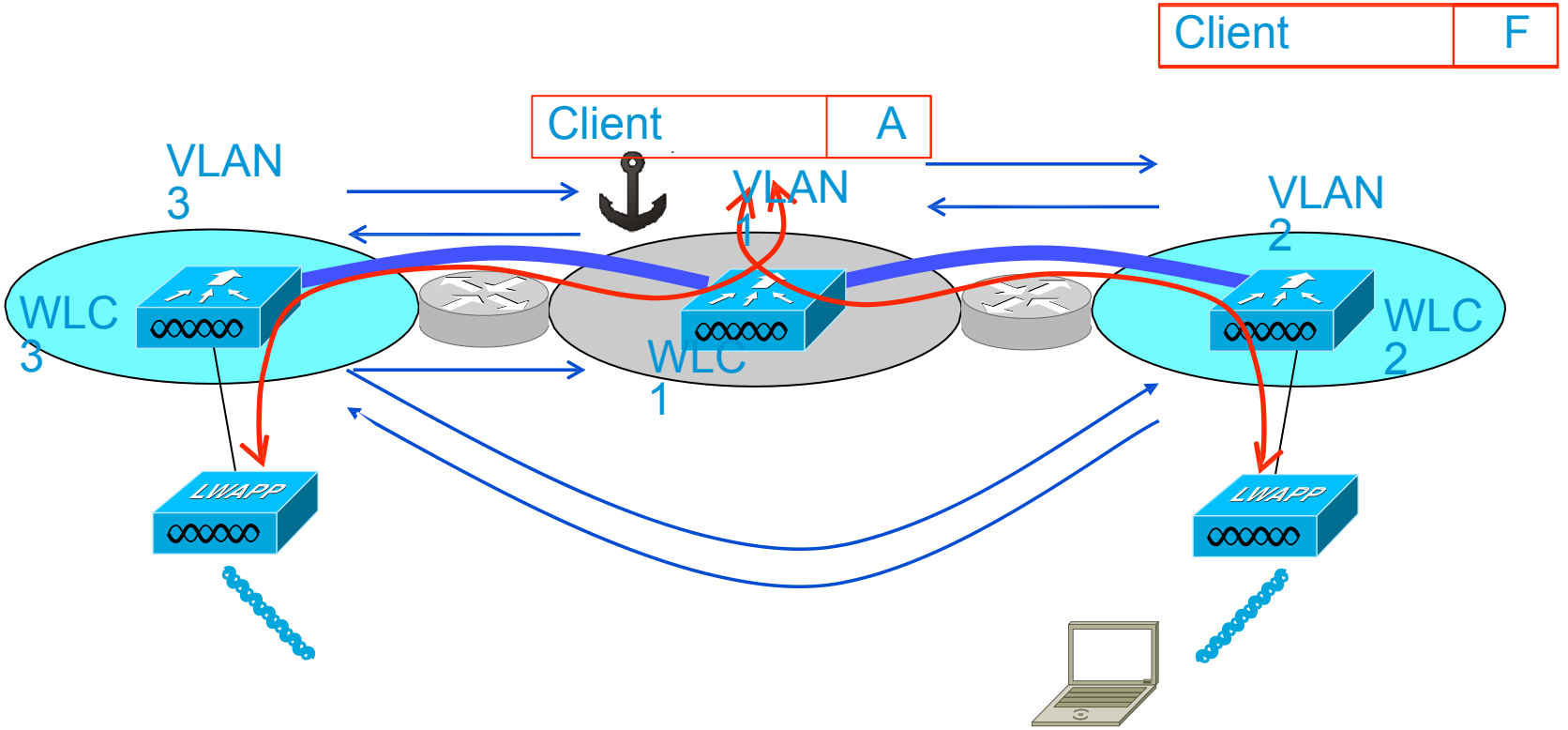


Foreign -> Local (2)

- New WLC share same subnet as current anchor
- New WLC is not current anchor

- new-WLC -> old-WLC: Mobile announce
- new-WLC <- old-WLC: Mobile Handoff
- *L3 client info extracted from foreign*
- old-WLC -> Anchor : Mobile Handoff End
- old-WLC <- Anchor : Mobile Handoff End ACK

Foreign -> Foreign

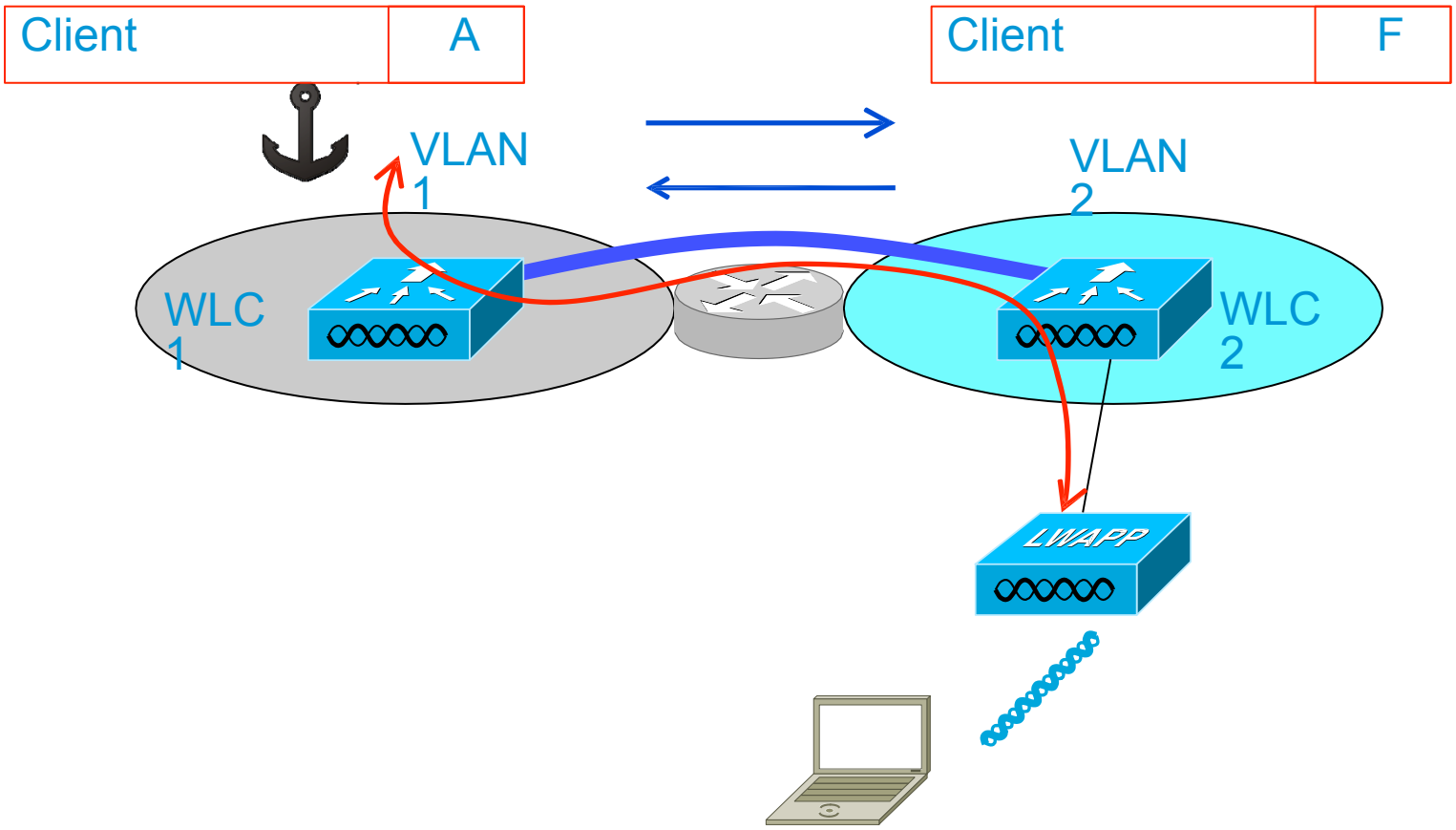


Foreign -> Foreign

- New WLC in different subnet than anchor

- new-WLC -> old-WLC: Mobile Announce
- new-WLC <- old-WLC: Mobile Handoff
- *L3 info transferred from old foreign*
- old-WLC -> anchor : Anchor Xfer
- old-WLC <- anchor : Anchor Xfer Ack
- new-WLC -> anchor : Anchor Req
- new-WLC <- anchor : Anchor grant

Session termination

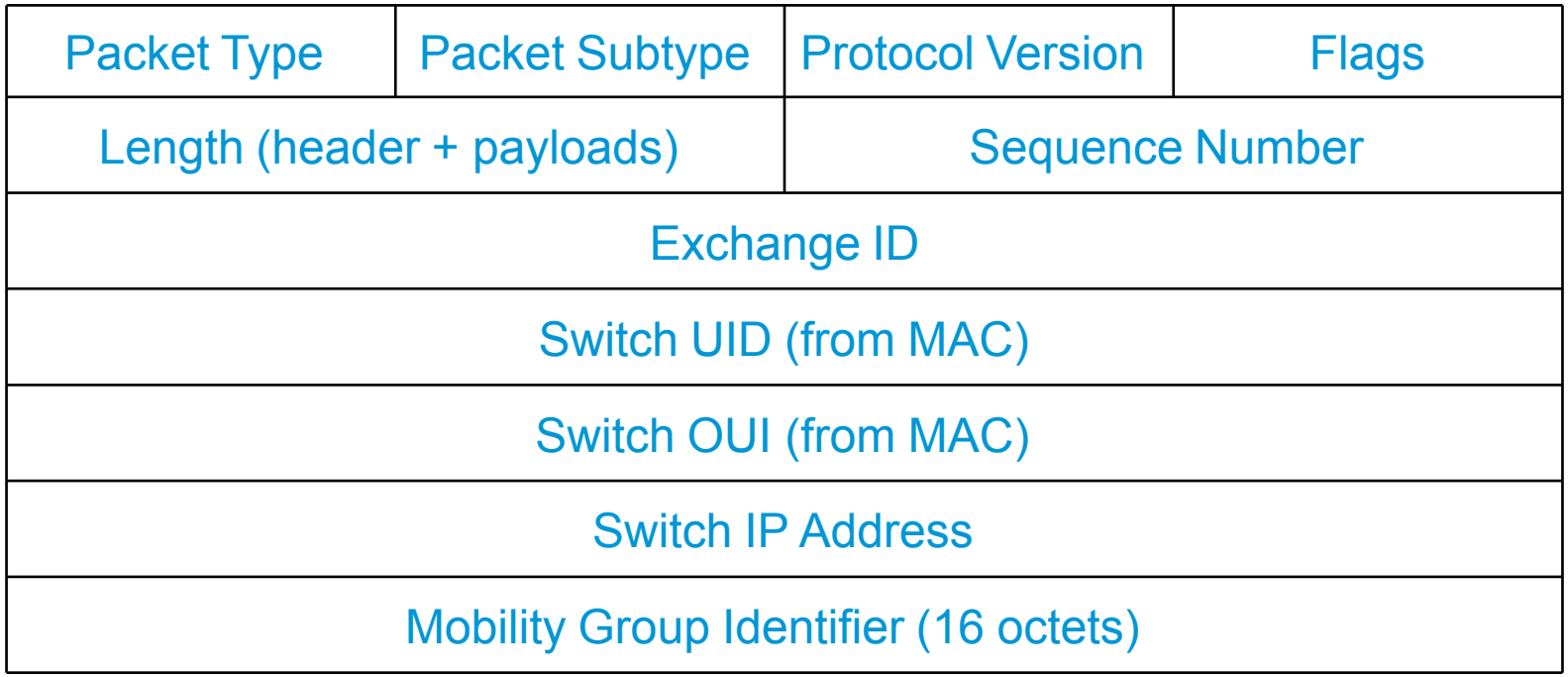


Session termination

- Used to terminate a foreign-anchor relationship

- WLC1 to WLC2 : Mobile Handoff End
- WLC1 to WLC2 : Mobile Handoff End Ack

Packet format



Troubleshooting steps

- Mobility tunnel not coming up:

-Do a ping test to verify connectivity between WLC's.

-If the control path is down try to a mping to check if there are any drops in the path between WLC's. In case data path is down do a eping.

-Re-configure the mobility group between the two controllers (This helps in almost 70% of the scenarios).

-Take the output of "debug mobility keepalive enable" to see if the keepalive messages are reaching the other side. These debugs will have the sequence number and transfer ID information for each packet. We can compare this with span captures taken at the WLC and compare if all the packets are reaching the WLC. The debugs will look like this:

12:53:24.371: Mobility packet sent to:

12:53:24.371: 192.168.12.2, port 16666

12:53:24.371: type: 3(MobileAnnounce) subtype: 0 version: 1 xid: 1010 seq: 43522 len 116 flags 0

Troubleshooting client handoff

In order to troubleshoot if the client handoff is happening correctly and if all the client parameters are being sent correctly, we will need to take the output of “debug mobility handoff enable” from the WLC. Below is a sample output on the foreign WLC:

***mmListen: May 08 12:10:38.802: 00:17:7c:2f:b8:6e Received Anchor Export Ack for client from Switch IP: 10.105.132.141**

Received a mobility handoff ack for the client.

***mmListen: May 08 12:10:38.802: 00:17:7c:2f:b8:6e Anchor Mac: d0:c2:82:e2:91:60, Old Foreign Mac: 30:e4:db:1b:e0:a0 New Foreign Mac: 30:e4:db:1b:e0:a0**

Updates the new anchor and foreign details for the client.

Troubleshooting client handoff

- On the anchor WLC:

***mmListen: May 08 05:52:50.587: 00:17:7c:2f:b8:6e Received Anchor Export request: from Switch IP: 10.105.132.160**
***mmListen: May 08 05:52:50.587: 00:17:7c:2f:b8:6e Adding mobile on Remote AP 00:00:00:00:00:00(0)**
***mmListen: May 08 05:52:50.587: 00:17:7c:2f:b8:6e mmAnchorExportRcv:, Mobility role is Unassoc**
***mmListen: May 08 05:52:50.587: 00:17:7c:2f:b8:6e mmAnchorExportRcv Ssid=cwa Security Policy=0x42000**
***mmListen: May 08 05:52:50.587: 00:17:7c:2f:b8:6e mmAnchorExportRcv vapId= 5, Ssid=cwa AnchorLocal=0x0**
***mmListen: May 08 05:52:50.588: 00:17:7c:2f:b8:6e mmAnchorExportRcv:Url redirect https://10.106.73.98:8443/guestportal/gateway?sessionId=0a6984a00000004c536bac7b&action=cwa**
***mmListen: May 08 05:52:50.588: 00:17:7c:2f:b8:6e Url redirect ACL REDIRECT**

Show outputs to be used

- Show mobility summary: Gives info about the mobility peer config on the WLC.
- Show mobility statistics: Gives info about packets transmit/receive statistics through the mobility tunnel.
- Show client detail client_mac: This can be used to find out the state of the client (Local/export anchor/export foreign):

Client MAC Address..... 00:17:7c:2f:b8:6e
AP MAC Address..... 00:00:00:00:00:00
Client State..... Associated
Wireless LAN Id..... 5
IP Address..... 10.105.132.254
Mobility State..... Export Anchor
Mobility Foreign IP Address..... 10.105.132.160

Client roaming

- Client roaming is handled seamlessely when roaming between AP's as far as open authentication and webauth is concerned.
- Roaming between controllers is handled as explained above.
- The main issue is with respect to client roaming when using dot1x authentication. The reason for this is that the PMKID info is unavailable at the WLC for the new AP that the client roams to. This will result in the client having to complete full dot1x authentication on every roam which increases the roaming latency.

PMKID generation:

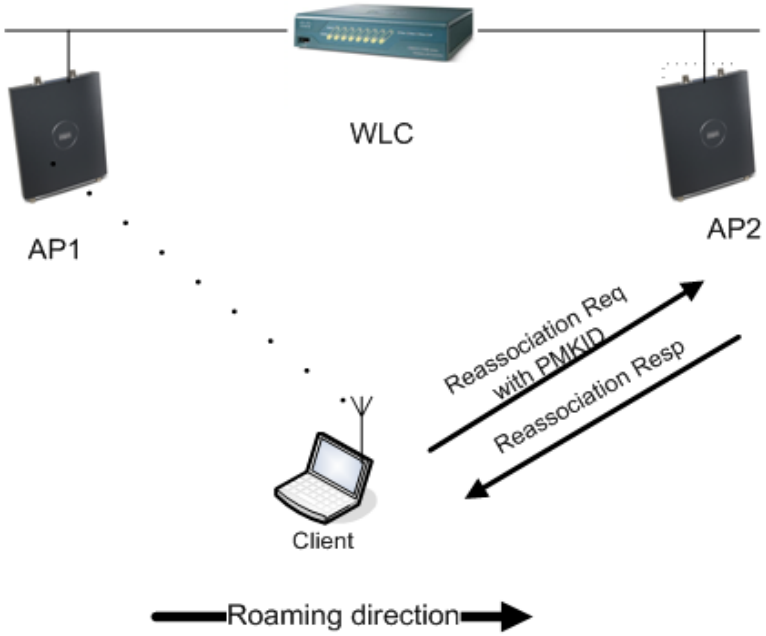
PMKSA contains (from standard point of view)

- PMK (32 bytes)

- BSSID (6 bytes)

- Client's MAC (6 bytes)

- any supporting data structure to handle these cache



Dot1x Fast roaming techniques:

The Cisco WLC supports the following main techniques for fast secure roaming:

1. Sticky (PKC) PMKID caching: In this method the client stores each PMKID against a PMKSA. When client finds an AP for which it has PMKSA, it will send the PMKID in the association request in RSN IE in hope that AP remembered the client and kept his PMKSA is alive. If both has the PMKSA alive, then AP will directly go to 4-Way handshake rather than full auth. The command to enable this on the WLC is: “config wlan security wpa wpa2 cache sticky enable wlan_id”

2. Opportunistic PMKID caching (OKC) : In this case, client/AP stores only one PMKSA. Now, when client roams, it dynamically calculates PMKID. Since PMKSA is same so client and AP's PMKID matches and AP starts 4-Way handshake rather than full 802.1x auth. This solution works good, where PMKSA can be transferred from old AP to new AP using some communication like over DS.

Dot1x Fast roaming techniques (continued):

3. 802.11r

4. CCKM

Thank you.

Agenda (Session 16 – 2nd July)

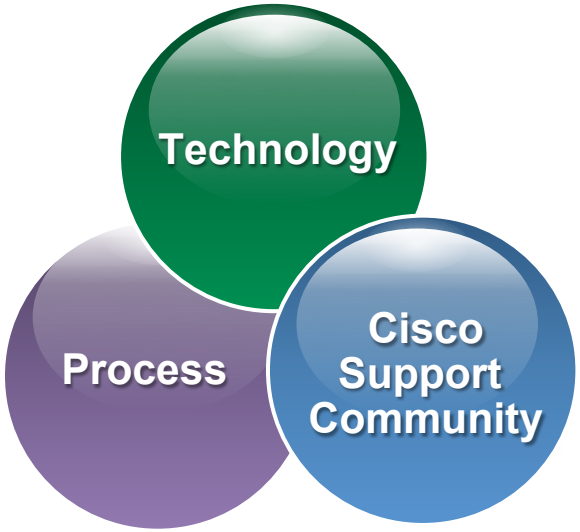
Technology

FlexConnect/HREAP

- FlexConnect AP modes of operation
- Latest feature in FlexConnect

AP Join Troubleshooting

- AP join process through WLC
- Live troubleshooting on debug and show commands
- Case studies which can cause an AP join failure

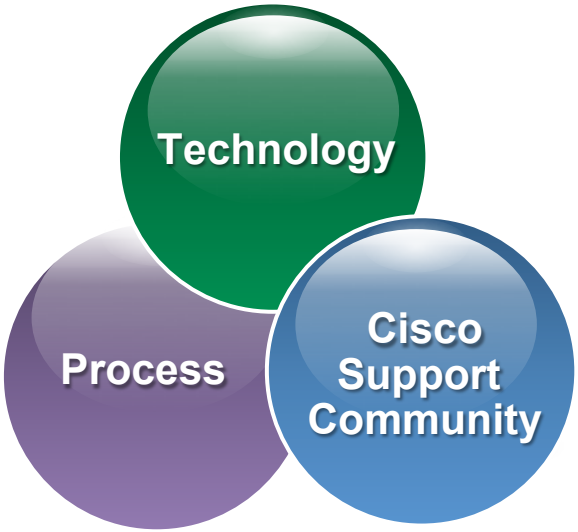


Q&A

Upcoming Sessions…..

June “Month of Wireless Technology”

- Session 16 – 2nd July 2014



And many more……Months and Technologies

Thank you.