8.0 Update – RRM, HDX, HA & Other Enhancements

Jerome Henry

Technical Marketing Engineer
Enterprise Networking Market Strategy

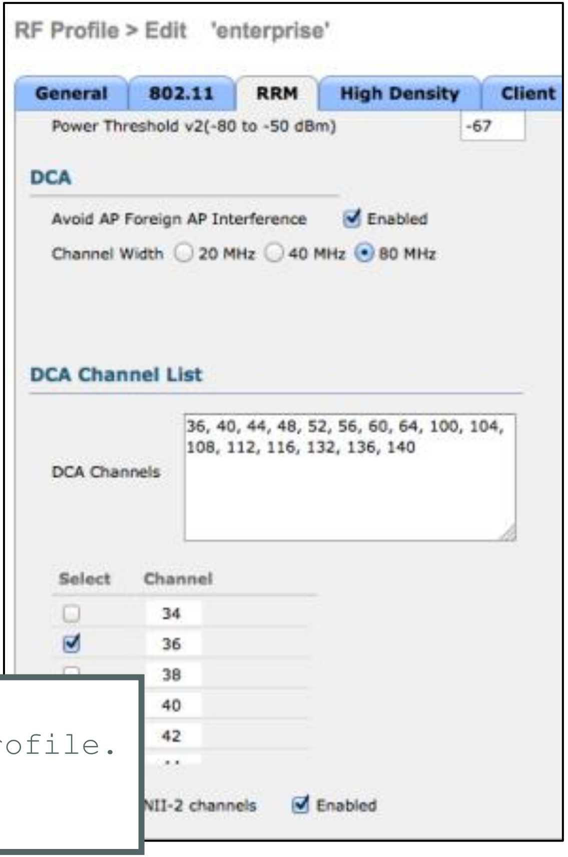
Agenda

- DCA in RF Profiles
- RX_SOP
- Optimized Roaming
- Infrastructure Enhancements
- Client SSO Enhancements
- Qinq Tagging Enhancement

DCA in RF Profiles

WHY DCA in RF Profiles

- Multi Country Support – one AP group per country- each with a defined channel list in RF Profiles
- Managing mixed channel (802.11n/ac 40/80 MHz) environment
- Channel assignment by physical area – engineering on the 2nd floor, accounting on the first floor, you want engineering to limit their impact
- Conference Center – allows the assignment of channel ranges to individual vendors and creation of buffer zones on main network to isolate



RF Profile > Edit 'enterprise'

Power Threshold v2(-80 to -50 dBm) -67

DCA

Avoid AP Foreign AP Interference ☑ Enabled

Channel Width ○ 20 MHz ○ 40 MHz ● 80 MHz

DCA Channel List

DCA Channels: 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140

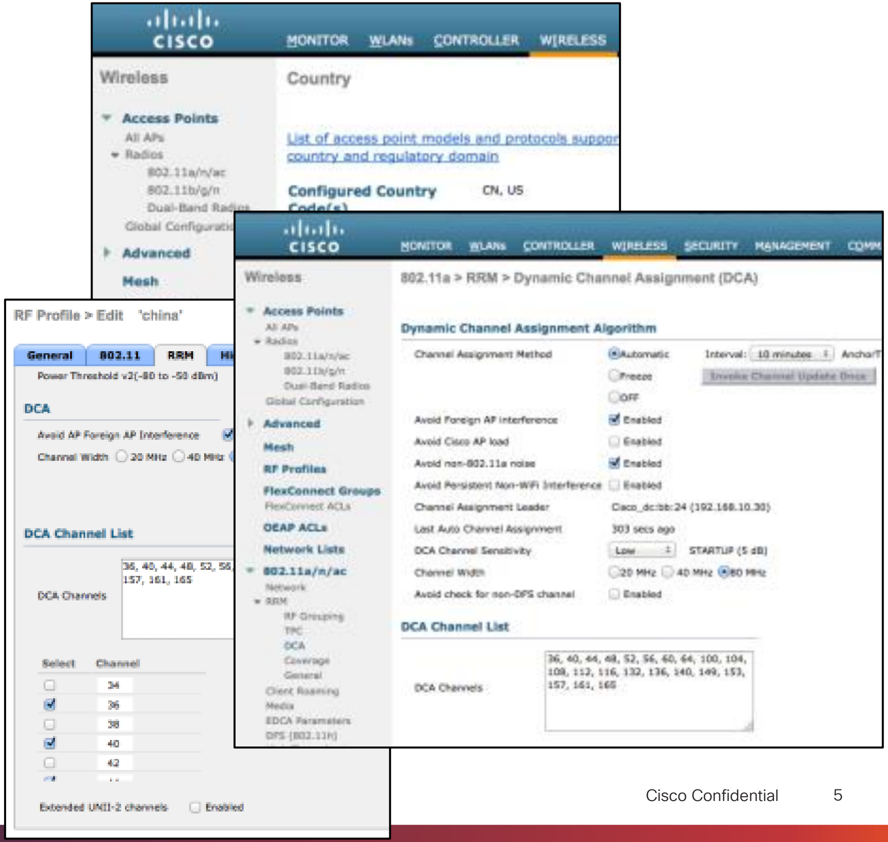
Select	Channel
□	34
☑	36
□	38
	40
	42
	..

NII-2 channels ☑ Enabled

```
(Cisco Controller) >config rf-profile ?
11n-client-only Configures 802.11n-client-only mode of the RF Profile.
channel         Configures the RF Profile DCA settings
coverage        Configures the RF Profile Coverage
```

RRM DCA in RF Profiles – The Rules

- The country code must be set on the controller to allow other reg. domain channels
- Channels must be selected under Global DCA on the controller to be available in profiles
- You must disable 802.11a/b networks to change DCA channels or bandwidth (20/40/80)
- You can have a different assignment for bandwidth in an RF Profile than you have in Global
- RF Profiles and AP groups must be present on every controller that has an AP you want to include in the AP group.



Country

List of access point models and protocols suppor country and regulatory domain

Configured Country Code(s) CN, US

RF Profile > Edit 'china'

Power Threshold v2(-80 to -50 dBm)

DCA

Avoid AP Foreign AP Interference ☑

Channel Width ○ 20 MHz ○ 40 MHz

DCA Channel List

DCA Channels 36, 40, 44, 48, 52, 56, 157, 161, 165

Select	Channel
☐	34
☑	36
☐	38
☑	40
☐	42

Extended UNII-2 channels ☐ Enabled

802.11a > RRM > Dynamic Channel Assignment (DCA)

Dynamic Channel Assignment Algorithm

Channel Assignment Method ● Automatic Interval: 10 minutes Anchor
○ Freeze
○ OFF

Avoid Foreign AP interference ☑ Enabled

Avoid Cisco AP load ☐ Enabled

Avoid non-802.11a noise ☑ Enabled

Avoid Persistent Non-WiFi Interference ☐ Enabled

Channel Assignment Leader Cisco_dc:bb:24 (192.168.10.30)

Last Auto Channel Assignment 303 secs ago

DCA Channel Sensitivity Low STARTUP (5 dB)

Channel Width ○ 20 MHz ○ 40 MHz ● 80 MHz

Avoid check for non-DFS channel ☐ Enabled

DCA Channel List

DCA Channels 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153, 157, 161, 165

RX_SOP

RX_SOP: What is it?

- Receiver Start of Packet Detection Threshold (RX_SOP) determines the Wi-Fi signal level in dBm at which an AP radio will demodulate and decode a packet
- The higher the level, the less sensitive the radio is and the smaller the receiver cell size will be
- By reducing the cell size we can affect everything from the distribution of clients to our perception of channel utilization
- This is for High Density designs – and requires knowledge of the behavior you want to support
- A client needs to have someplace to go if you ignore it on the current cell

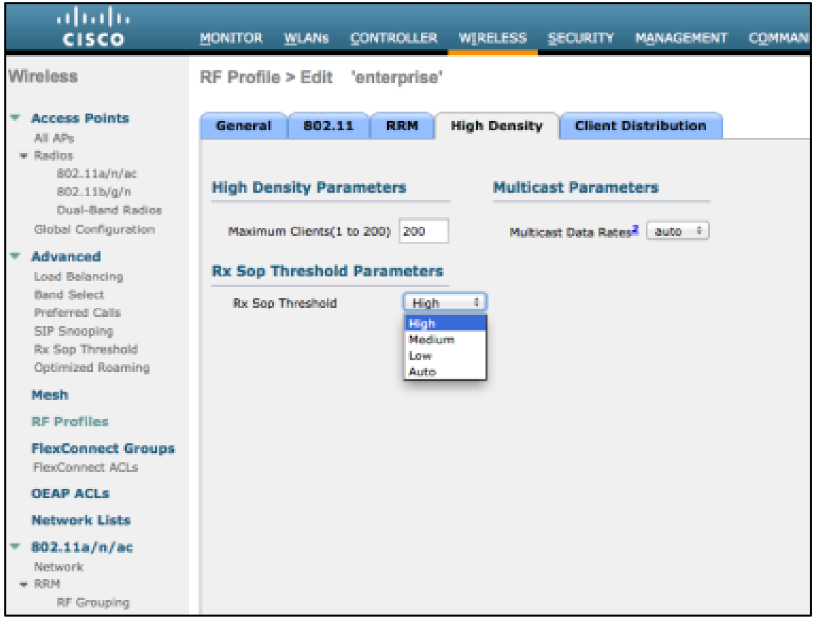
WARNING! This setting is a brick wall – if you set it above where your clients are being heard, they will no longer be heard. Really.

RX_SOP: Why Use It?

- Reduce sensitivity to interference and noise – reduce channel utilization
- It sharpens the cell edge – we will hear what we intend to cover
- Caveats –
  - You can significantly reduce coverage
  - You can make it impossible for intended clients to associate or communicate with your AP
- This feature is to be used in conjunction with a known design to solve a specific problem when you understand the coverage and usage of the network by the users
- RX_SOP is available at the global level as well as in RF profiles – Strongly recommend applying only through profiles – to solve specific problems with HDX

RX_SOP Configuration

- Settings High, Medium, Low, Auto
- Auto is default behavior, and leaves RX_SOP function linked to CCA threshold for automatic adjustment
- Most networks can support a LOW setting and see improvement
- This affects all packets seen at the receiver



RF Profile > Edit 'enterprise'

High Density Parameters

Maximum Clients(1 to 200) 200

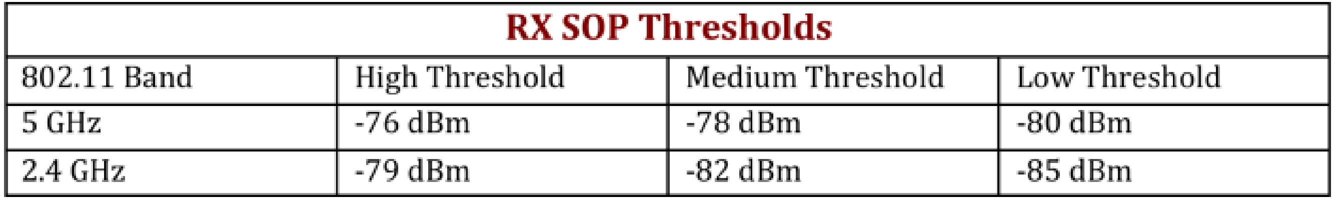
Multicast Parameters

Multicast Data Rates[2] auto

Rx Sop Threshold Parameters

Rx Sop Threshold High

High
Medium
Low
Auto



RX SOP Thresholds			
802.11 Band	High Threshold	Medium Threshold	Low Threshold
5 GHz	-76 dBm	-78 dBm	-80 dBm
2.4 GHz	-79 dBm	-82 dBm	-85 dBm

RX_SOP Configuration

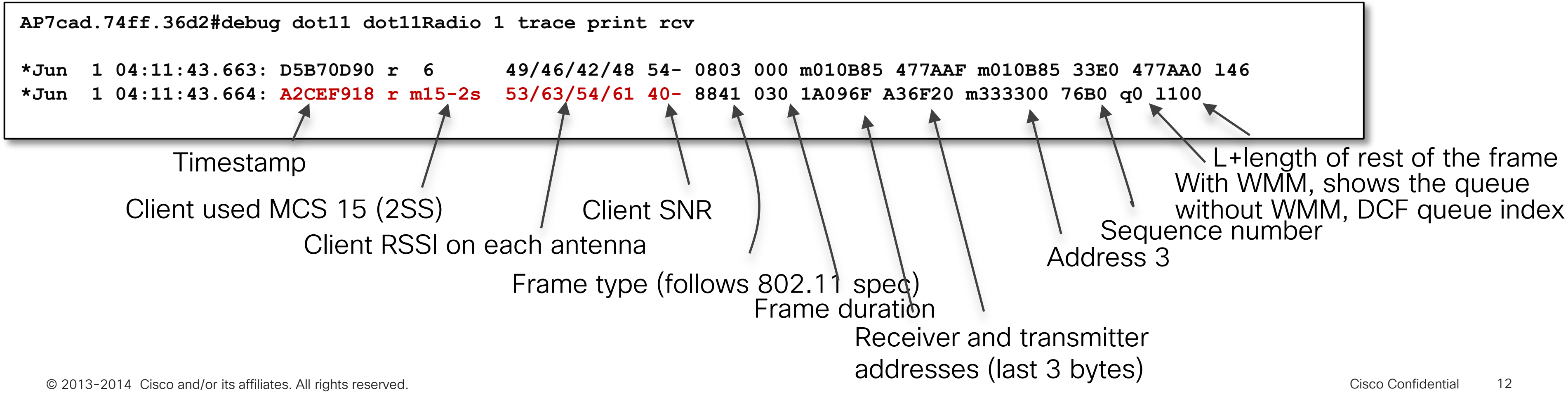
```
(Cisco Controller) >config rf-profile rx-sop threshold ?

auto               Reverts radio receiver SOP to auto.
high               Sets radio receiver SOP to high.
low                Sets radio receiver SOP to low.
medium             Sets radio receiver SOP to medium.

(Cisco Controller) >config rf-profile rx-sop threshold medium ?
<profile name> Specifies the name of the RF Profile.

(Cisco Controller) >show rf-profile details Tryme2
…/…
Rx Sop Threshold................................ Medium
```

RX_SOP Verification

```
((Cisco Controller) >show 802.11a extended

Default 802.11a band Radio Extended Configurations:
    Beacon period: 100, range: 0 (AUTO);
    Multicast buffer: 0 (AUTO), rate: 0 (AUTO);
    RX SOP threshold: 0 (AUTO); CCA threshold: 0 (AUTO);

APa80c.0dd2.218c  a8:0c:0d:db:ce:f0
    Beacon period: 100, range: 0 (AUTO);
    Multicast buffer: 0 (AUTO), rate: 0 (AUTO);
    RX SOP threshold: 0 (AUTO); CCA threshold: 0 (AUTO);
AP7c69.f647.50a8  7c:69:f6:47:7a:a0
    Beacon period: 100, range: 0 (AUTO);
    Multicast buffer: 0 (AUTO), rate: 0 (AUTO);
    RX SOP threshold: 0 (AUTO); CCA threshold: 0 (AUTO);
AP7cad.74ff.36d2  08:cc:68:b4:46:c0
    Beacon period: 100, range: 0 (AUTO);
    Multicast buffer: 0 (AUTO), rate: 0 (AUTO);
    RX SOP threshold: 0 (AUTO); CCA threshold: 0 (AUTO);
```

RX_SOP Troubleshooting

- There are no debug commands for RX_SOP; it is a chipset level tweak and when applied, chipset will not forward *<b>any</b>* frames to the AP receiver.
- Therefore, there is no way to check dot11 frames ignore when RX_SOP is applied. To confirm things are working, you can apply RX_SOP on AP and enable driver debugs (debug dot11 d1 trace print rcv) to ensure no frame is received stronger than the configured Rx_SOP

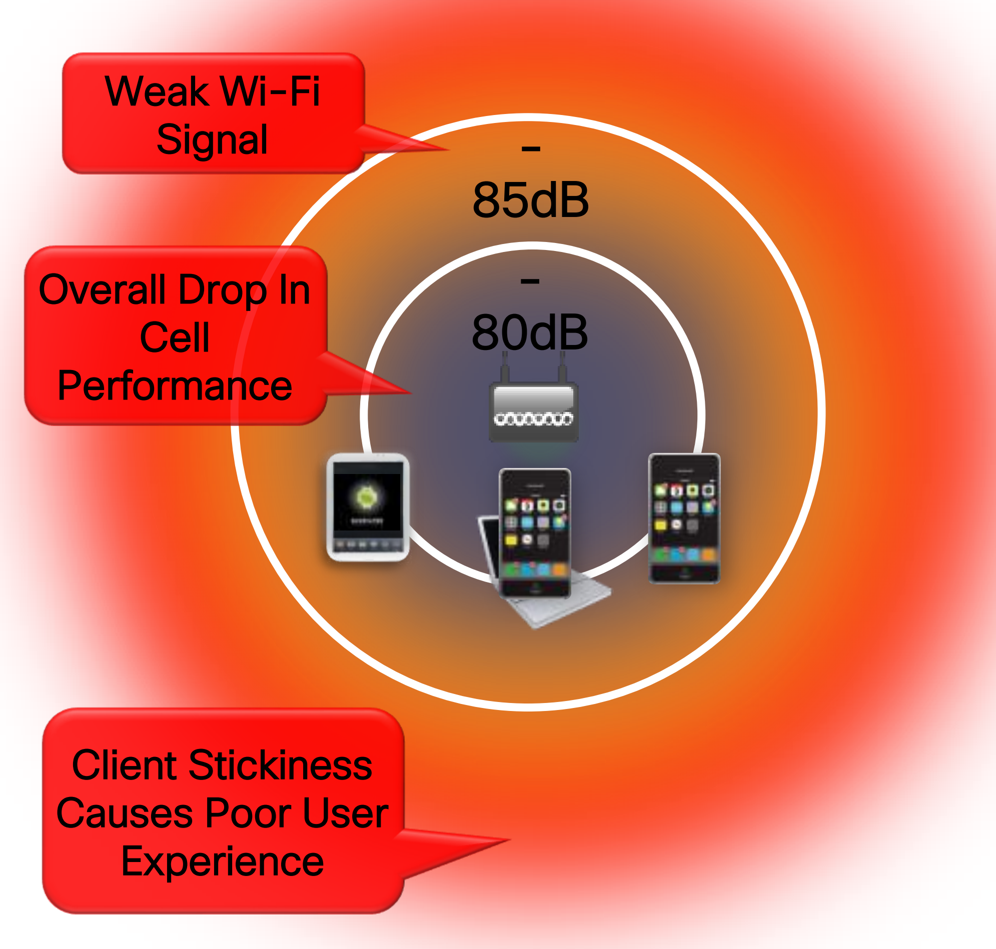


```
AP7cad.74ff.36d2#debug dot11 dot11Radio 1 trace print rcv

*Jun  1 04:11:43.663: D5B70D90 r  6      49/46/42/48 54- 0803 000 m010B85 477AAF m010B85 33E0 477AA0 146
*Jun  1 04:11:43.664: A2CEF918 r m15-2s  53/63/54/61 40- 8841 030 1A096F A36F20 m333300 76B0 q0 1100
```

Timestamp
Client used MCS 15 (2SS)
Client RSSI on each antenna
Client SNR
Frame type (follows 802.11 spec)
Frame duration
Receiver and transmitter addresses (last 3 bytes)
Address 3
Sequence number
L+length of rest of the frame
With WMM, shows the queue without WMM, DCF queue index

Optimized Roaming

Today’s Solution

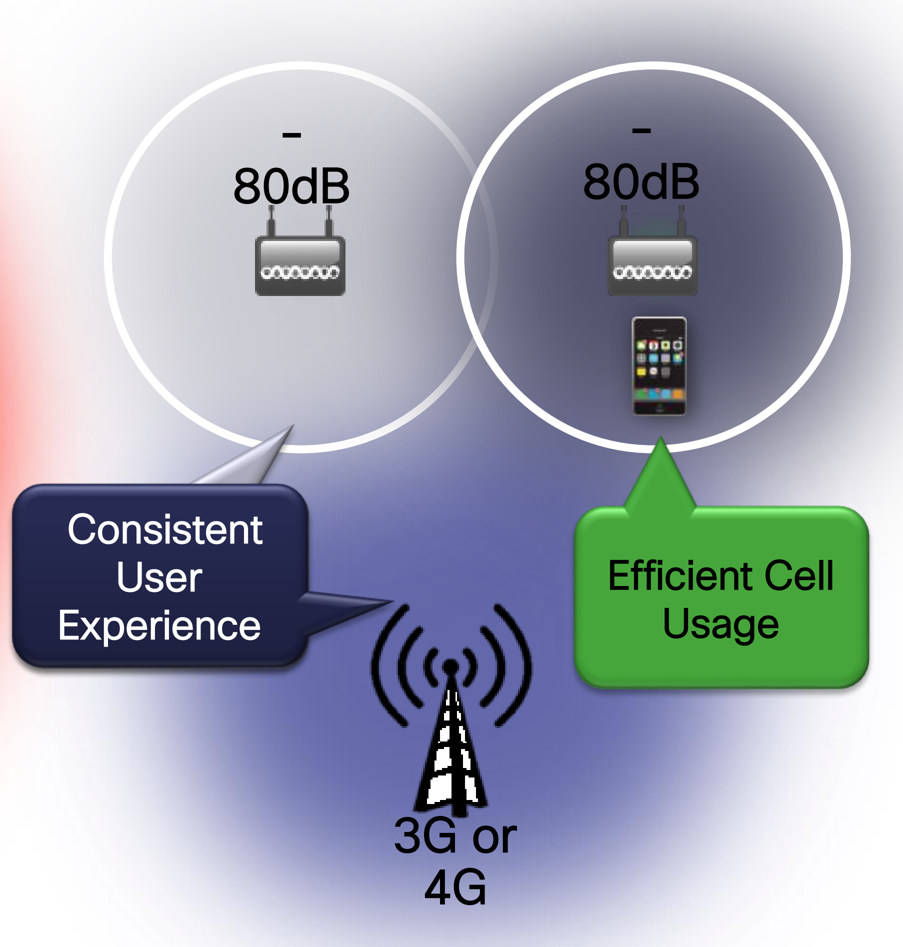


Weak Wi-Fi Signal

Overall Drop In Cell Performance

Client Stickiness Causes Poor User Experience

Cisco “Optimized Roaming”

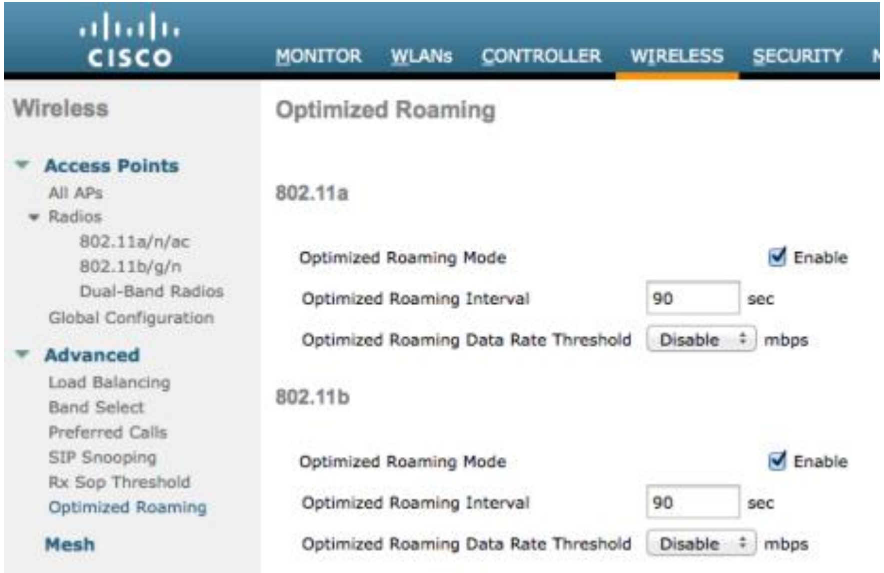


Consistent User Experience

Efficient Cell Usage

Optimized Roaming

- Sets a threshold RSSI value and/or minimum data rate that a client will be sent a **deauth** at
- Developed to support cellular hand-off
- Global configuration of 4 parameters available
  - Enable/Disable
  - Interval (seconds)
  - Data Rate threshold
  - RSSI threshold configured through Data CHD
- Trigger is pre-coverage hole event – set under CHDM config



Optimized Roaming

802.11a

Optimized Roaming Mode ☑ Enable

Optimized Roaming Interval 90 sec

Optimized Roaming Data Rate Threshold Disable mbps

802.11b

Optimized Roaming Mode ☑ Enable

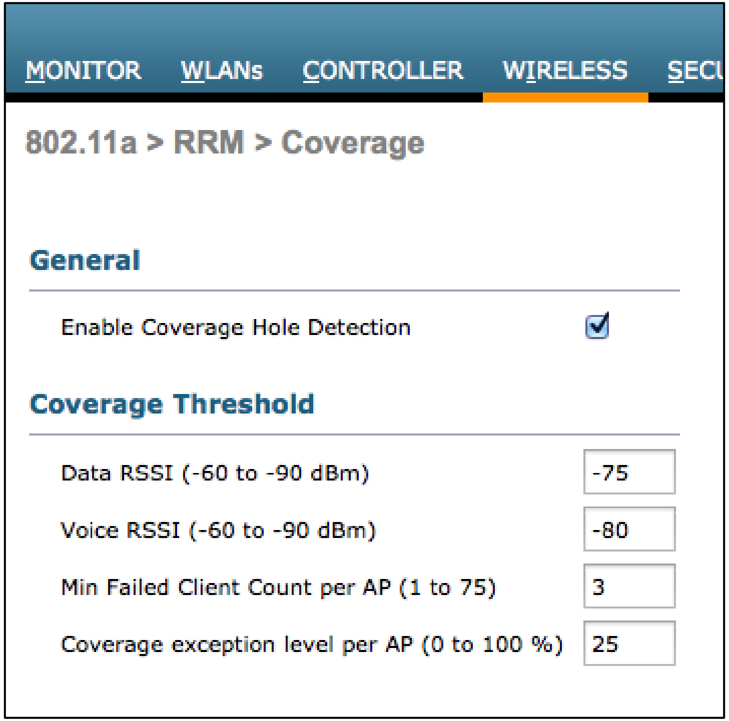
Optimized Roaming Interval 90 sec

Optimized Roaming Data Rate Threshold Disable mbps

```
(Cisco Controller) >config advanced 802.11a optimized-roaming ?
enable          Enable 802.11a OptimizedRoaming
disable         Disable 802.11a OptimizedRoaming
interval        Configure the reporting interval for 802.11a OptimizedRoaming
datarate        Configure the data rate threshold for 802.11a OptimizedRoaming
```

Optimized Roaming Configuration

- Enable/Disable – Global command
- Interval = #seconds between checks at the radio
- Data Rate threshold–
- Used in conjunction with RSSI threshold, if set is a gating function where both data rate and RSSI must be true for action – default is disabled
- RSSI threshold – set through data RSSI config in Coverage at the global level, and under RRM in RF Profile



802.11a > RRM > Coverage

General

Enable Coverage Hole Detection ☑

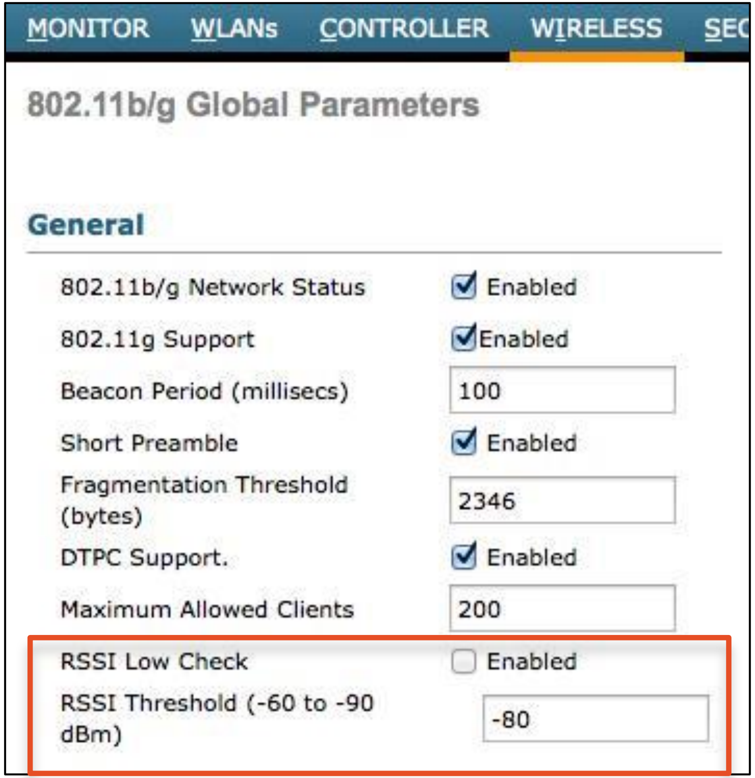
Coverage Threshold

Data RSSI (-60 to -90 dBm)	-75
Voice RSSI (-60 to -90 dBm)	-80
Min Failed Client Count per AP (1 to 75)	3
Coverage exception level per AP (0 to 100 %)	25

Optimized Roaming Logic

- Uses CHDM Data RSSI for trigger
- Alone – decision is based on RSSI seen at the radio
- Combined with Data Rate – provides additional gate for action – and preserves CHDM Function
- If Used with Client Low RSSI check, and the higher of the two values is used (with **6 dB** hysteresis).

Data RSSI	Data Rate	Result
True	Disable (default)	Deauth
True	False	No Action
True	True	Deauth



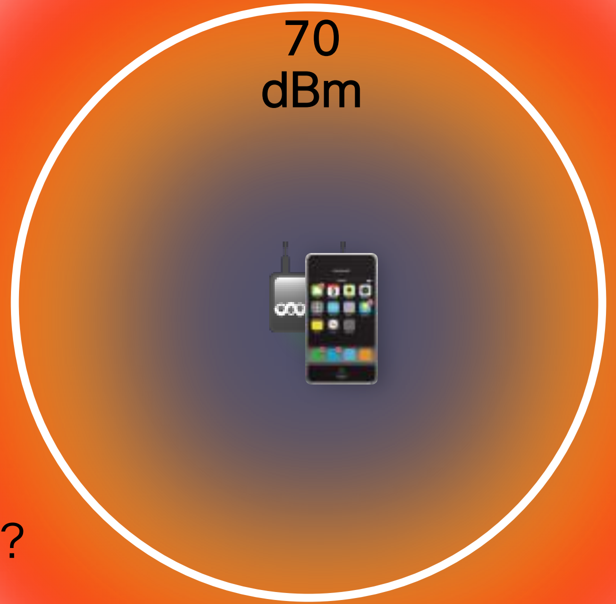
802.11b/g Global Parameters

General

802.11b/g Network Status	☑ Enabled
802.11g Support	☑ Enabled
Beacon Period (millisecs)	100
Short Preamble	☑ Enabled
Fragmentation Threshold (bytes)	2346
DTPC Support.	☑ Enabled
Maximum Allowed Clients	200
RSSI Low Check	□ Enabled
RSSI Threshold (-60 to -90 dBm)	-80

Optimized Roaming Logic

- Your config:
  - Optimized roaming is enabled with rate at 24 Mbps
  - Data RSSI is set to -70 dBm, 1 client
  - Low RSSI disabled



CHDM Data RSSI threshold met?

CHDM quantity met?

Client rate at 24 or below?

Deauth!

Optimized Roaming Verification and Troubleshooting

- No specific debug for optimized roaming; debug client shows the client disconnected with reason 4 (inactivity):

```
(Cisco Controller) >debug client e8:99:c4:8d:10:4c
(Cisco Controller) >debug dot11 mobile enable
(Cisco Controller) >debug dot11 state enable


(Cisco Controller) >*RRM-DCLNT-5_0: Jul 07 12:16:52.294: e8:99:c4:8d:10:4c
apfSendDisAssocMsgDebug (apf_80211.c:3157) Changing state for mobile
e8:99:c4:8d:10:4c on AP a8:0c:0d:db:ce:f0 from Associated to Disassociated

*RRM-DCLNT-5_0: Jul 07 12:16:52.294: e8:99:c4:8d:10:4c Sent Disassociate to mobile
on AP a8:0c:0d:db:ce:f0-1 (reason 4, caller rrmLrad.c:4894)
```

Optimized Roaming Verification and Troubleshooting

- Show optimized roaming shows you the number of clients disconnected due to optimized roaming:

```
(Cisco Controller) >show advanced 802.11a optimized-roaming

OptimizedRoaming
  802.11a OptimizedRoaming Mode................. Enabled
  802.11a OptimizedRoaming Reporting Interval.... 90 seconds
  802.11a OptimizedRoaming Rate Threshold........ 36 mbps

(Cisco Controller) >show advanced 802.11a optimized-roaming stats

OptimizedRoaming Stats
  802.11a OptimizedRoaming Disassociations....... 1
  802.11a OptimizedRoaming Rejections............ 17
```

Optimized Roaming & Low RSSI Feature “WARNING”

- Low RSSI check is a completely separate feature – and sets a low RSSI threshold which a client must be above to associate to the AP
- Optimized Roaming has a 6 dB hysteresis built in to prevent thrashing
- i.e., if Optimized Roaming is set to -75, then to rejoin the AP the client’s signal must improve to -69 dBm
- The logic checks low RSSI – AND Optimized Roaming before allowing a client to join – and both must pass

HA Enhancements

Agenda

- Infrastructure Enhancements
  - Bulk Sync Status
  - Enhanced debugs/ serviceability for HA
  - Configurable keep-alive timer/retries and peer-search timer value
  - Replace peer RMI ICMP ping with UDP message
  - Standby WLC on-the-fly Maintenance mode
  - Default gateway reachability check enhancement
  - Faster HA Pairup
- Client SSO Enhancements
  - SSO support for Internal DHCP server
  - AP Radio CAC statistics sync
  - SSO support for Sleeping Client feature
  - SSO support for OEAP600 APs
  - SSO support for 802.11ac clients

Phase 1 : APSSO 7.3

- Active – Standby 1:1 Redundancy
- Both WLC share IP Address of management interface
- Bulk and Incremental Config Sync
- APs does not go in Discovery state when Active WLC fails
- Supported on 5500 / 7500 / 8500 and WiSM-2 WLC
- Downtime 5 - 1000 msec in case of Box failover , ~3 seconds in case of Network Issues

Phase 2 : Client SSO 7.5

- Active - Standby can be geographically separated over L2 VLAN/Fiber
- Client database is synced to the Standby
  - Client information is synced when client moves to RUN state.
  - Client re-association is avoided on switch over
- Fully authenticated clients(RUN state) are synced to the peer
- Effective service downtime = Detection time + Switch Over Time (Network recovery/convergence)

Phase 3 : Improvements 8.0

- Auto-recovery from maintenance mode once Peer-RP and default gateway reach-ability is restored
- SSO Support for Internal DHCP Server
- SSO support for sleeping clients
- SSO support for 802.11ac clients
- SSO support for OEAP 600
- CAC method Bandwidth allocation parameters for both voice & video and Call Statistics synced to the Standby
- Enhanced GW reachability check mechanism enhanced to avoid false positives
- Peer RMI ICMP ping replaced with UDP messages
- Faster HA Pair-up

Infrastructure Enhancements

High Availability Infrastructure Enhancements

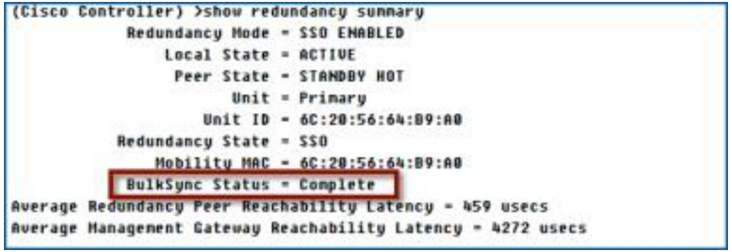
- Bulk Sync Status
- Enhanced debugs/ serviceability for HA
- Configurable keep-alive timer/retries and peer-search timer value
- Replace peer RMI ICMP ping with UDP message
- Standby WLC on-the-fly Maintenance mode
- Default gateway reachability check enhancement
- Faster HA Pairup

Bulk Sync Status

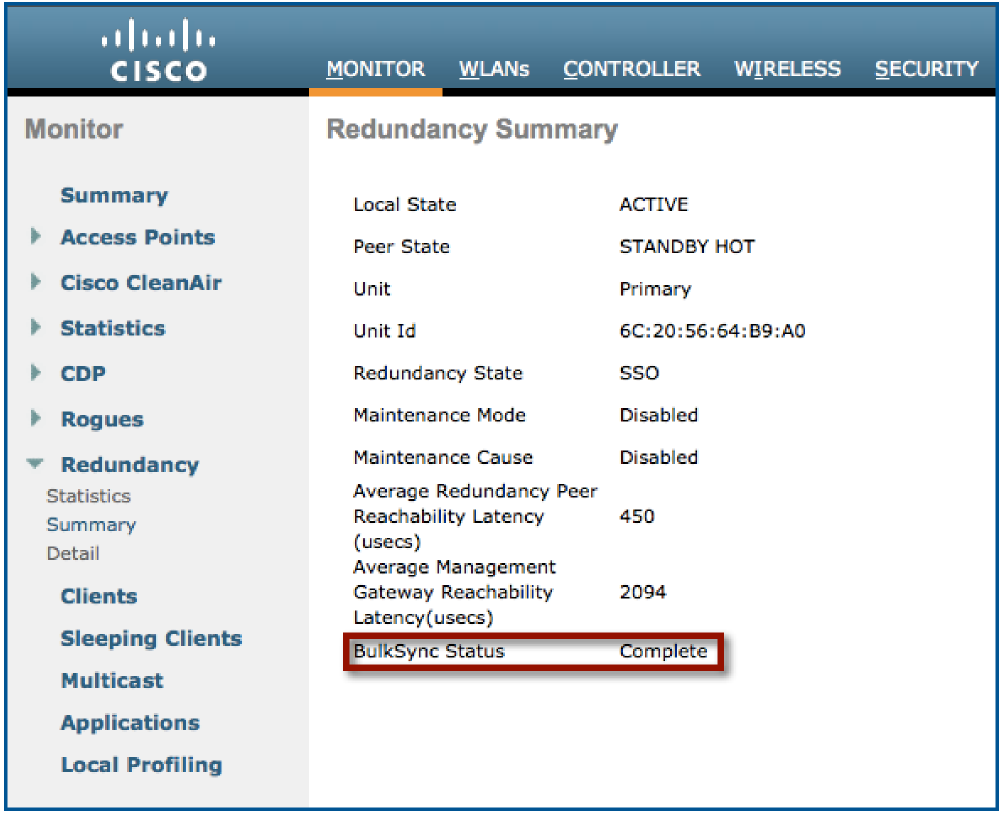
Mechanism to convey the status of Bulk Sync, both AP and Client sync

Status can be Pending/In-progress/Complete

Output of “*show redundancy summary*” will also reflect Bulk Sync status



```
(Cisco Controller) >show redundancy summary
                  Redundancy Mode = SSO ENABLED
                      Local State = ACTIVE
                       Peer State = STANDBY HOT
                             Unit = Primary
                          Unit ID = 6C:20:56:64:B9:A0
                 Redundancy State = SSO
                     Mobility MAC = 6C:20:56:64:B9:A0
                  BulkSync Status = Complete
Average Redundancy Peer Reachability Latency = 459 usecs
Average Management Gateway Reachability Latency = 4272 usecs
```



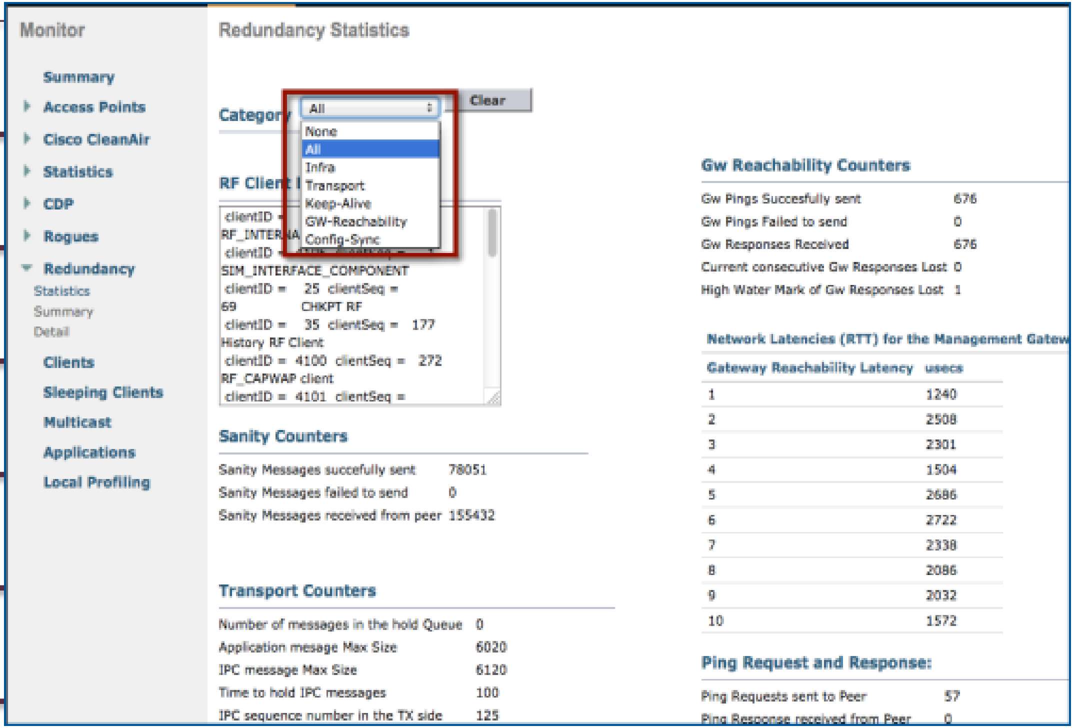
Redundancy Summary

Local State	ACTIVE
Peer State	STANDBY HOT
Unit	Primary
Unit Id	6C:20:56:64:B9:A0
Redundancy State	SSO
Maintenance Mode	Disabled
Maintenance Cause	Disabled
Average Redundancy Peer Reachability Latency (usecs)	450
Average Management Gateway Reachability Latency(usecs)	2094
BulkSync Status	Complete

Enhanced Debugs: Redundancy Statistics

New categories of statistics

- All
- Infra
- Transport
- Keep-Alive
- GW-Reachability
- Config-Sync



Redundancy Statistics

Category All

RF Client I

```
 clientID =
RF_INTERNA
 clientID =
SIM_INTERFACE_COMPONENT
 clientID =    25  clientSeq =
69              CHKPT RF
 clientID =    35  clientSeq =   177
History RF Client
 clientID =  4100  clientSeq =   272
RF_CAPWAP client
 clientID =  4101  clientSeq =
```

Sanity Counters

Sanity Messages succefully sent	78051
Sanity Messages failed to send	0
Sanity Messages received from peer	155432

Transport Counters

Number of messages in the hold Queue	0
Application message Max Size	6020
IPC message Max Size	6120
Time to hold IPC messages	100
IPC sequence number in the TX side	125

Gw Reachability Counters

Gw Pings Succesfully sent	676
Gw Pings Failed to send	0
Gw Responses Received	676
Current consecutive Gw Responses Lost	0
High Water Mark of Gw Responses Lost	1

Network Latencies (RTT) for the Management Gatew

Gateway Reachability Latency	usecs
1	1240
2	2508
3	2301
4	1504
5	2686
6	2722
7	2338
8	2086
9	2032
10	1572

Ping Request and Response:

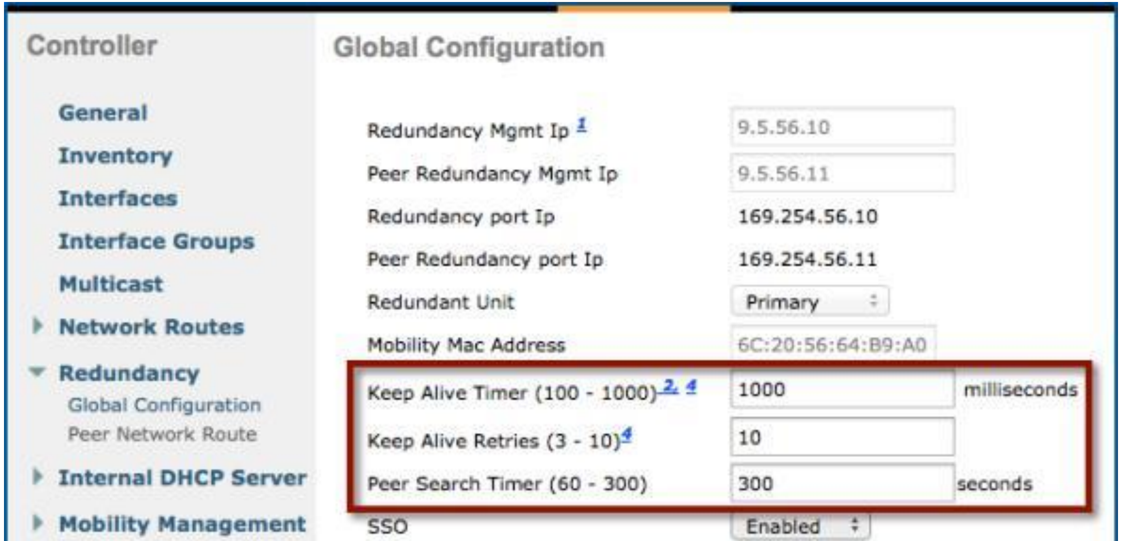
Ping Requests sent to Peer	57
Ping Response received from Peer	0

Configurable Keepalive and Peer Search Parameters

Keep-alive retry
3 to 10

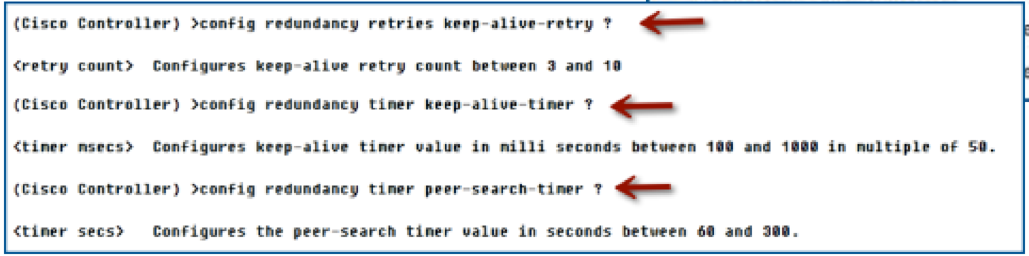
Keep-alive timer
100 to 1000ms

Peer search timer
60-300 s



Global Configuration

Redundancy Mgmt Ip [1]	9.5.56.10	
Peer Redundancy Mgmt Ip	9.5.56.11	
Redundancy port Ip	169.254.56.10	
Peer Redundancy port Ip	169.254.56.11	
Redundant Unit	Primary	
Mobility Mac Address	6C:20:56:64:B9:A0	
Keep Alive Timer (100 - 1000) [2] [4]	1000	milliseconds
Keep Alive Retries (3 - 10) [4]	10	
Peer Search Timer (60 - 300)	300	seconds
SSO	Enabled	
ervice Port Peer Ip	0.0.0.0	
ervice Port Peer Netmask	0.0.0.0	



```
(Cisco Controller) >config redundancy retries keep-alive-retry ?

<retry count>  Configures keep-alive retry count between 3 and 10

(Cisco Controller) >config redundancy timer keep-alive-timer ?

<timer msecs>  Configures keep-alive timer value in milli seconds between 100 and 1000 in multiple of 50.

(Cisco Controller) >config redundancy timer peer-search-timer ?

<timer secs>   Configures the peer-search timer value in seconds between 60 and 300.
```

Additional Infrastructure Enhancements

ICMP ping on RMI is replaced with UDP message

- Beneficial when ICMP pings may get discarded under heavy loads

Default GW reachability enhancement: Upon 6 consecutive ping drops, ARP is sent to GW

- Under heavy loads ICMP may get discarded but not ARPs. An ARP response is considered for GW reachability to avoid false positives, which makes this mechanism more deterministic

Standby WLC enters into MTC mode ‘on-the-fly’ without reboot

- Upon Peer-RP and default gateway reachability, MTC mode auto-recovery will reboot the WLC and pair it with Active WLC (Release 7.6 feature)
- Upon “Peer-RP” and/or default gateway reachability is lost, standby WLC will enter into MTC mode on-the-fly without a reboot (8.0)

Faster HA Pair Up - No comparison of XMLs and no reboot of standby WLC during Pair Up

- XMLs will be sent from the to-be-Active to to-be-Standby at the time of initialization, just before the validation of XMLs . Double reboots avoided.

Client SSO Enhancements

Client SSO Enhancements

SSO support for internal DHCP server

With this support now Internal DHCP Server configuration is allowed with HA enabled

AP radio CAC statistics sync

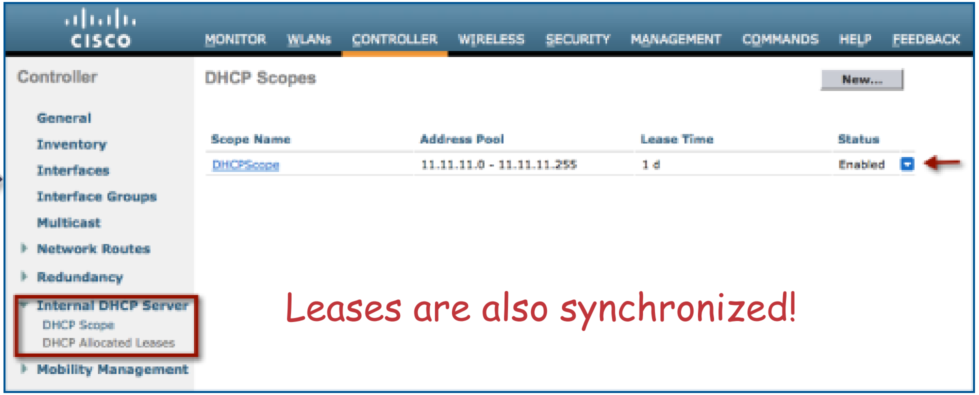
SSO support for Sleeping Client feature

SSO support for OEAP600 APs

SSO support for 802.11ac clients

SSO Support for Internal DHCP Server

‘Internal DHCP Server’ can be configured on HA enabled controllers

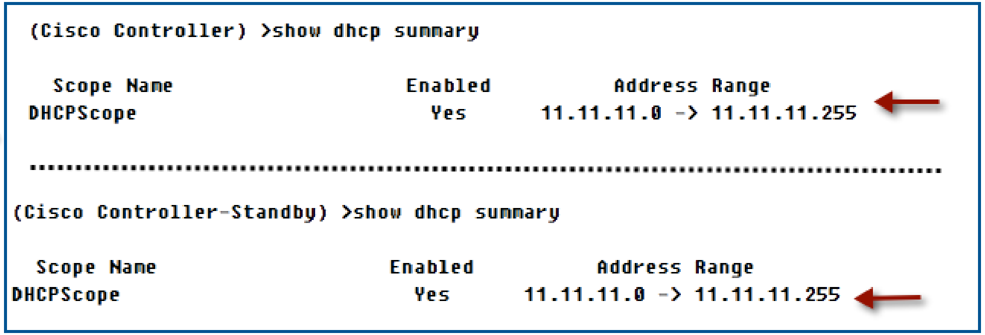


DHCP Scopes

Scope Name	Address Pool	Lease Time	Status
DHCPScope	11.11.11.0 - 11.11.11.255	1 d	Enabled

Leases are also synchronized!

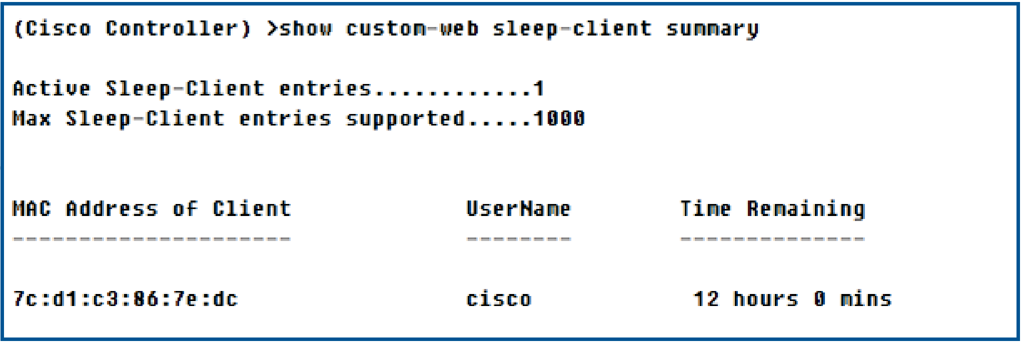
Synced to Standby WLC so that soon after a Switchover the ‘Internal DHCP Server’ on new Active will start serving clients.



```
 (Cisco Controller) >show dhcp summary

   Scope Name                         Enabled          Address Range
 DHCPScope                             Yes       11.11.11.0 -> 11.11.11.255

 ...........................................................................

(Cisco Controller-Standby) >show dhcp summary

  Scope Name                          Enabled          Address Range
DHCPScope                              Yes       11.11.11.0 -> 11.11.11.255
```

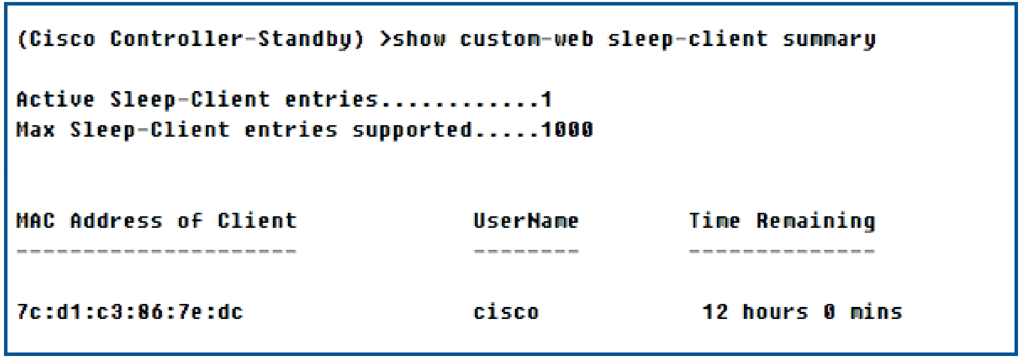
SSO Support for Sleeping Clients

Sleeping Client DB sync between Active and Standby WLC



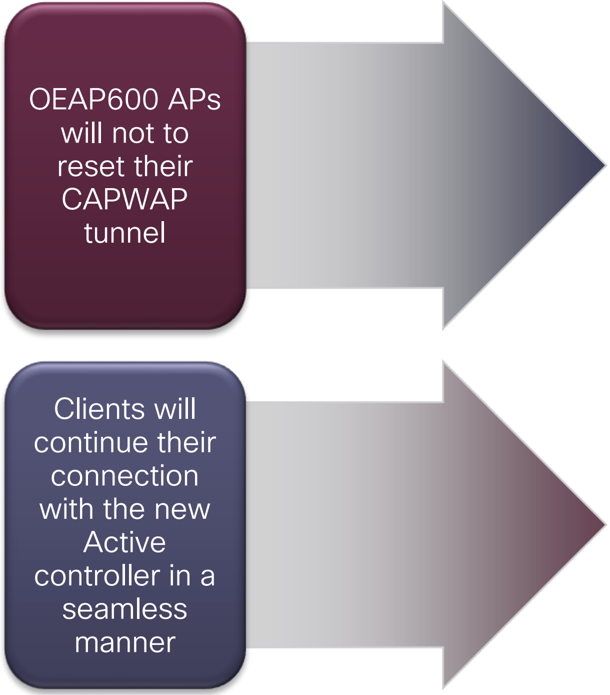
```
(Cisco Controller) >show custom-web sleep-client summary

Active Sleep-Client entries...........1
Max Sleep-Client entries supported.....1000


MAC Address of Client                UserName        Time Remaining
---------------------                --------        --------------

7c:d1:c3:86:7e:dc                    cisco            12 hours 0 mins
```

Sleeping clients avoid web re-authentication if they wake-up within the sleeping client timeout interval post switchover



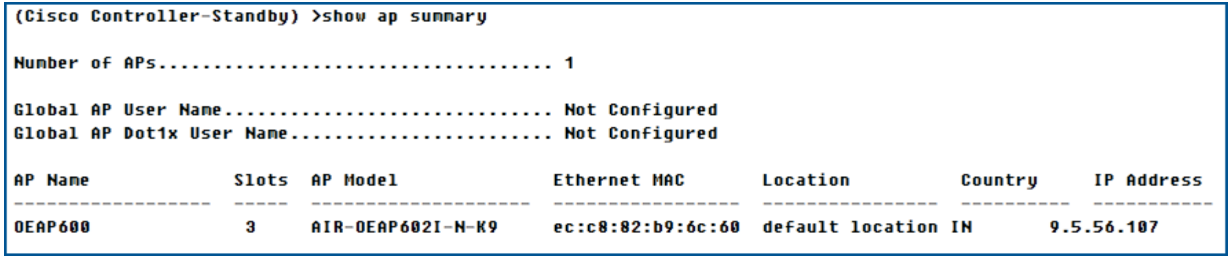
```
(Cisco Controller-Standby) >show custom-web sleep-client summary

Active Sleep-Client entries...........1
Max Sleep-Client entries supported.....1000


MAC Address of Client                UserName        Time Remaining
---------------------                --------        --------------

7c:d1:c3:86:7e:dc                    cisco            12 hours 0 mins
```

SSO Support for OEAP600 APs

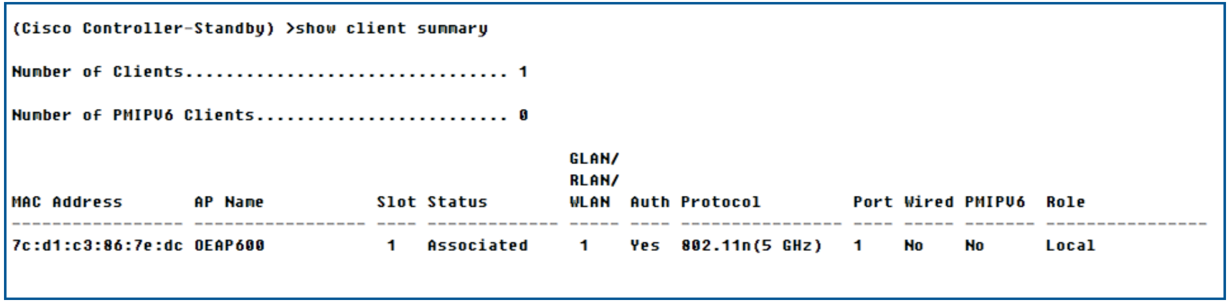


OEAP600 APs will not to reset their CAPWAP tunnel

Clients will continue their connection with the new Active controller in a seamless manner



```
(Cisco Controller-Standby) >show ap summary

Number of APs.................................... 1

Global AP User Name.............................. Not Configured
Global AP Dot1x User Name........................ Not Configured

AP Name             Slots  AP Model              Ethernet MAC       Location          Country      IP Address
------------------  -----  --------------------  -----------------  ----------------  ----------   -----------
OEAP600              3     AIR-OEAP602I-N-K9     ec:c8:82:b9:6c:60  default location  IN       9.5.56.107
```



```
(Cisco Controller-Standby) >show client summary

Number of Clients................................ 1

Number of PMIPV6 Clients......................... 0

                                                       GLAN/
                                                       RLAN/
MAC Address       AP Name           Slot Status        WLAN  Auth Protocol         Port Wired PMIPV6  Role
----------------- ----------------- ---- ------------- ----- ---- ---------------- ---- ----- ------- ----------------
7c:d1:c3:86:7e:dc OEAP600            1   Associated     1    Yes  802.11n(5 GHz)   1    No    No      Local
```

FIPS / CC

Agenda

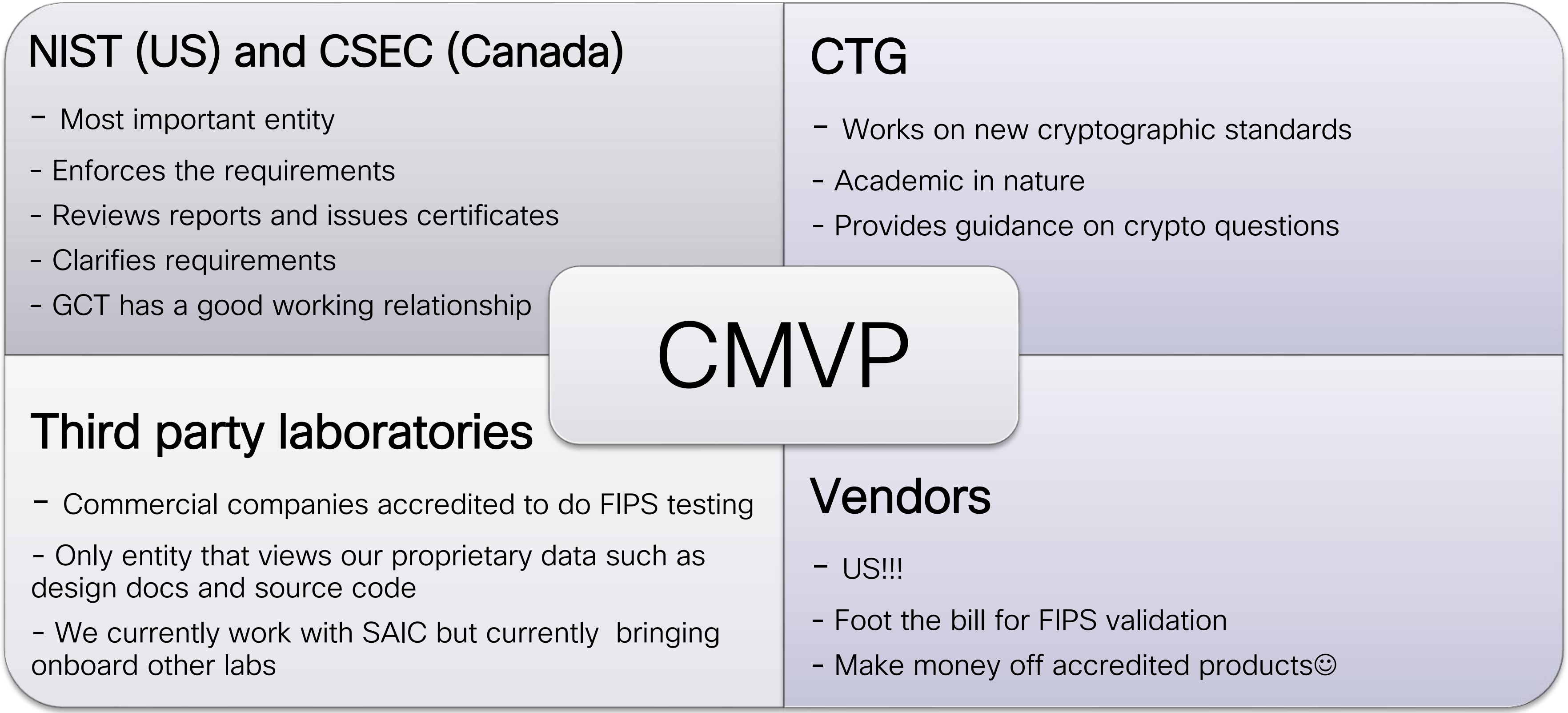
- FIPS / CC Intro
- FIPS / CC on 8.0

FIPS / CC Intro

FIPS Intro

- Federal Information Processing Standard **140-2** is a security standard used to validate cryptographic modules.
- The cryptographic modules are produced by the private sector for use by the U.S. government and other regulated industries (such as financial and health-care institutions) that collect, store, transfer, share and disseminate **sensitive but unclassified** (SBU) **information**.
- Testing against this standard requires documentation, source code review, algorithm, operational, and failure testing
- Overseen by Cryptographic Module Validation Program (CMVP), a joint American and Canadian security accreditation program for cryptographic modules.

FIPS Who's Who and Does What



NIST (US) and CSEC (Canada)

- Most important entity
- Enforces the requirements
- Reviews reports and issues certificates
- Clarifies requirements
- GCT has a good working relationship

CTG

- Works on new cryptographic standards
- Academic in nature
- Provides guidance on crypto questions

CMVP

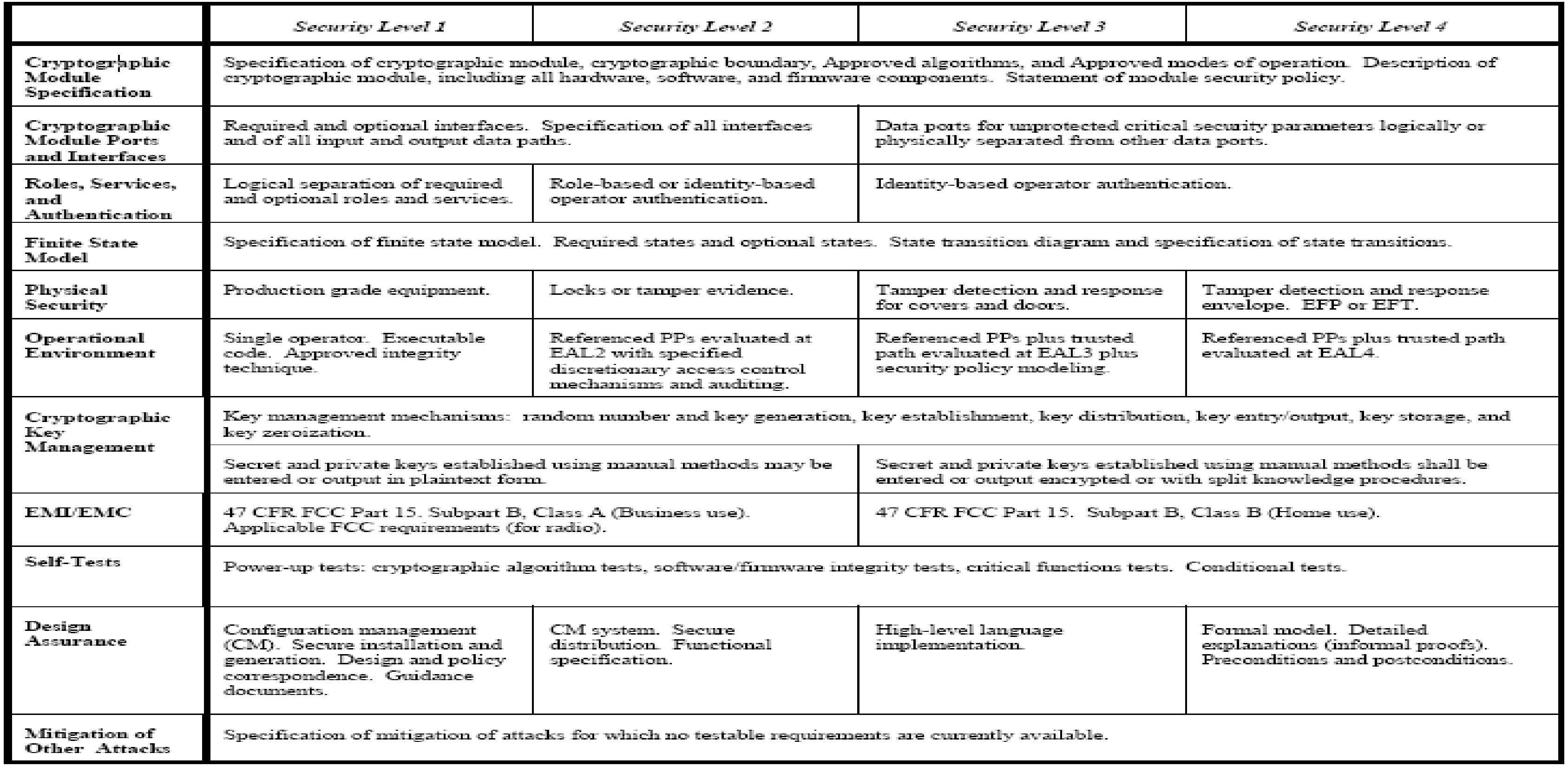
Third party laboratories

- Commercial companies accredited to do FIPS testing
- Only entity that views our proprietary data such as design docs and source code
- We currently work with SAIC but currently bringing onboard other labs

Vendors

- US!!!
- Foot the bill for FIPS validation
- Make money off accredited products☺

FIPS 140-2 Security Levels



	Security Level 1	*Security Level 2*	*Security Level 3*	*Security Level 4*
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. Statement of module security policy.			
Cryptographic Module Ports and Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths.		Data ports for unprotected critical security parameters logically or physically separated from other data ports.	
Roles, Services, and Authentication	Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
Finite State Model	Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions.			
Physical Security	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope. EFP or EFT.
Operational Environment	Single operator. Executable code. Approved integrity technique.	Referenced PPs evaluated at EAL2 with specified discretionary access control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling.	Referenced PPs plus trusted path evaluated at EAL4.
Cryptographic Key Management	Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization.			
	Secret and private keys established using manual methods may be entered or output in plaintext form.		Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures.	
EMI/EMC	47 CFR FCC Part 15. Subpart B, Class A (Business use). Applicable FCC requirements (for radio).		47 CFR FCC Part 15. Subpart B, Class B (Home use).	
Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.			
Design Assurance	Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents.	CM system. Secure distribution. Functional specification.	High-level language implementation.	Formal model. Detailed explanations (informal proofs). Preconditions and postconditions.
Mitigation of Other Attacks	Specification of mitigation of attacks for which no testable requirements are currently available.			

What About CC?

- The Common Criteria (CC) and FIPS 140-2 are **different in** the abstractness and **focus of tests**.
- **FIPS 140-2 testing is against a defined cryptographic module** and provides a suite of conformance tests to four security levels. FIPS 140-2 describes the requirements for cryptographic modules and includes such areas as physical security, key management, self tests, roles and services, etc. The standard was initially developed in 1994 - prior to the development of the CC.
- **Common criteria** is an testing standard the **verifies that the product provides security functionalities that is claimed by its developer**. 24 countries officially recognize CC.
- CC evaluation is against a created protection profile (PP) or security target (ST). Typically, a PP covers a broad range of products. PP are written by people who wish to by a product. ST is written by product developers
- The four security levels in FIPS 140-2 do not map directly to specific CC EALs or to CC functional requirements.

High Level FIPS Check List for 8.0

- ❑ Any ventilation holes that allow viewing of internal components need to be covered up.
- ❑ Your software module (WLC in our case) has at least one “User” role and One “Crypto-Officer” role.
- ❑ Self-Tests occur when the module is powered on, and transition to an error state on failure
- ❑ While in error state, module cannot be initialized.
- ❑ Module performs conditional Self-Tests
- ❑ Module uses FIPS approved security functions
- ❑ User can zeroize all plaintext secret and private cryptographic keys and CSPs within the module.
- ❑ Code signing has been implemented and any new code loaded is checked for authenticity and integrity

About Roles and Services

AP Role - This role is filled by an access point associated with the controller (mfp, 802.11i, iGTK)

Client Role - This role is filled by a wireless client associated with the controller

User Role - A management user with read-only privileges

Crypto Officer (CO) Role - This role performs the cryptographic initialization and management operations. A management user with read-write privileges.

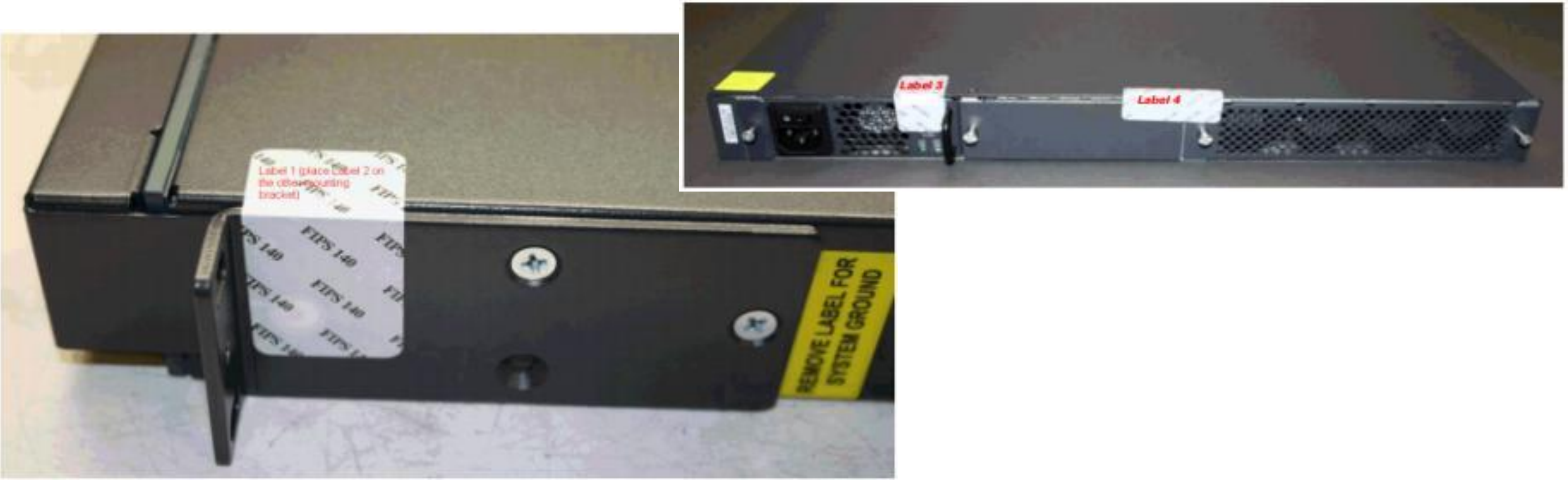
FIPS / CC in 8.0

FIPS and 8.0

- We are targeting FIPS140-2 Level 2 certification and CC (EAL4+) and UCAPL certification. More details here: http://www.cisco.com/web/strategy/government/security_certification/net_business_benefit_seccert_common_criteria.html
- WLC supports AES256/HMAC-SHA256 in DTLS/HTTPS/TLS connections.
- AireOS software implements 128 bit AES-CBC, CTR-DRBG, SHA-1, SHA-2, HMAC-SHA-1 and RSA

FIPS Opacity Testing

- FIPS shields and tamper-evident stickers have to be added to the WLC:


Label 1 (place Label 2 on the other mounting bracket)
FIPS 140
REMOVE LABEL FOR SYSTEM GROUND
Label 3
Label 4

FIPS and Cipher Suites Points of Enforcement

We ensure FIPS approved cipher suites are supported for communication:

- WLC ←→ AP (both data traffic as well as control traffic),
- WLC←→WLC (control traffic),
- WLC←→MSE
- WLC←CIDS sensor
- WLC←→ Management user via HTTPS protocol
- WLC←→ Management user via SSHv2 protocol
- WLC←→ RADIUS, SYSLOG, PI via IPSec

Self Tests

Two types of self-tests

- Power up (POST)
- Conditional

- Consider them as a health check
- POST must be performed at power-up prior to any security relevant services executing and data being output
- Self-tests need to be performed for each crypto implementation e.g. if there are two implementations of AES, each needs a self-test
- Conditional self-tests are initiated when specific triggers execute (e.g. asymmetric key generation, random number generation etc.)
- Upon error specific steps need to be taken

Post Self-Test Failure

- The module must immediately:
  - Output an error
  - Cease cryptographic operations
  - Enter an error state
- Upon encountering a POST failure:
  - Report an error to console
  - Go into an endless reboot until POST passes

FIPS – What Does it Change for the Config / Tshoot?

- Customers not implementing FIPS will not see any difference… but customers implementing FIPS will have new commands:
- Enabling FIPS and creating a FIPS authorization key:

```
((Cisco Controller) >config switchconfig fips-prerequisite enable
```

FIPS – What Does it Change for the Config / Tshoot?

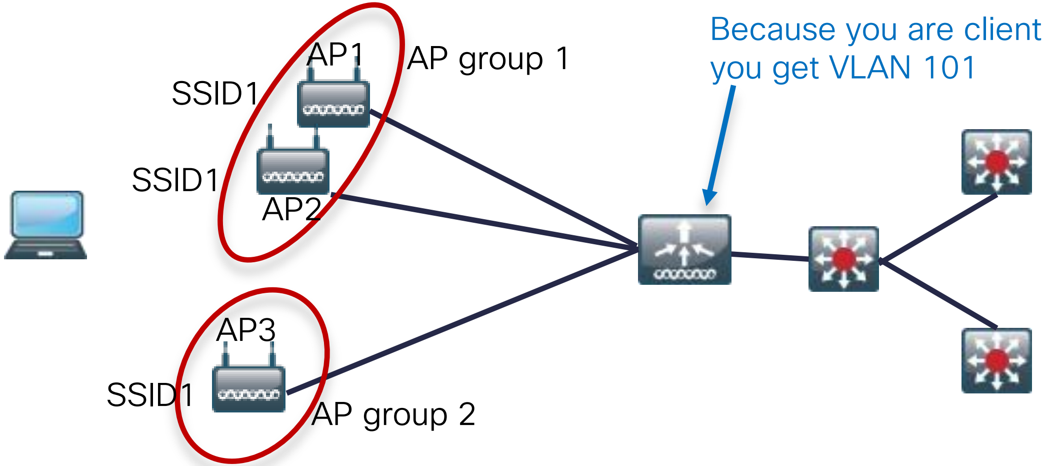
- Verification:

```
(Cisco Controller) >show switchconfig

802.3x Flow Control Mode......................... Disable
FIPS prerequisite features....................... Disabled
WLANCC prerequisite features..................... Disabled
UCAPL prerequisite features...................... Disabled
secret obfuscation............................... Enabled
Strong Password Check Features
   case-check.................................... Enabled
   consecutive-check............................. Enabled
   default-check................................. Enabled
   username-check................................ Enabled
   position-check................................ Disabled
   case-digit-check.............................. Disabled
   Min. Password length.......................... 3
   Min. Upper case chars......................... 0
   Min. Lower case chars......................... 0
   Min. Digits chars............................. 0
   Min. Special chars............................ 0
```

Qinq Tagging Enhancement

Qinq Tagging Enhancement

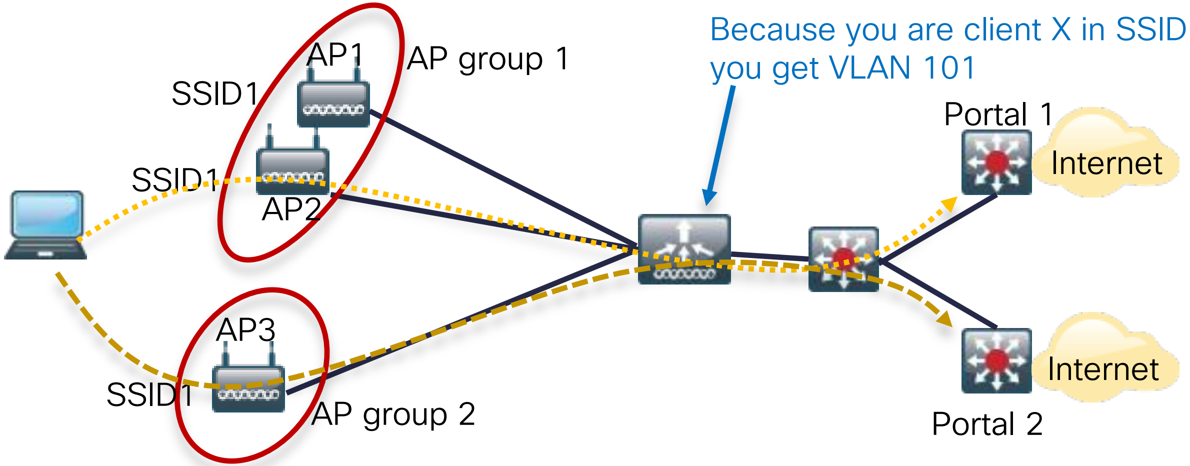
- “Qinq” stands for Q-in-Q, 802.1q tag inside another 802.1q tag
- The request is as follows: In standard solution, client gets the same treatment (VLAN, outgoing interface) regardless of associating through AP1, AP2 or AP3:



Because you are client X in SSID1, you get VLAN 101

Qinq Tagging Enhancement

- How can you make that the client, associating to an AP in group 1, is sent to portal 1, but is sent to portal 2 when associating to an AP in group 2?

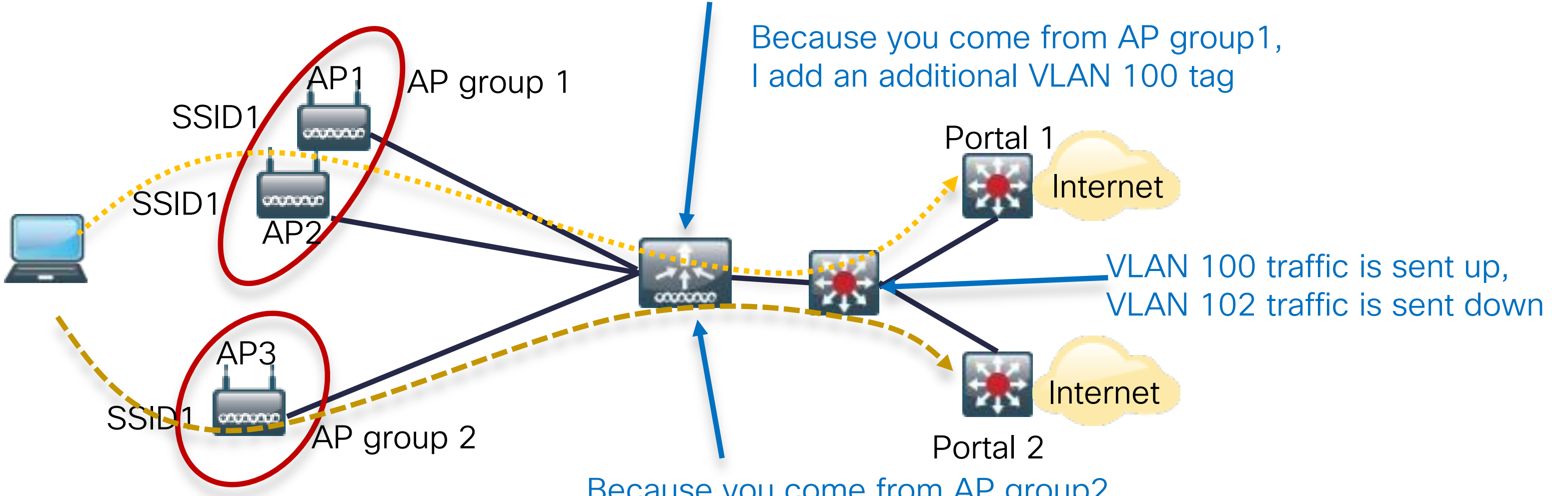


Because you are client X in SSID1, you get VLAN 101

Qinq Tagging Enhancement

- How can you make that the client, associating to an AP in group 1, is sent to portal 1, but is sent to portal 2 when associating to an AP in group 2?

- One solution is to add an additional VLAN tag to the outgoing frames, based on the source AP group



Because you are client X in SSID1, you get VLAN 101

Because you come from AP group1, I add an additional VLAN 100 tag

VLAN 100 traffic is sent up, VLAN 102 traffic is sent down

Because you come from AP group2, I add an additional VLAN 102 tag

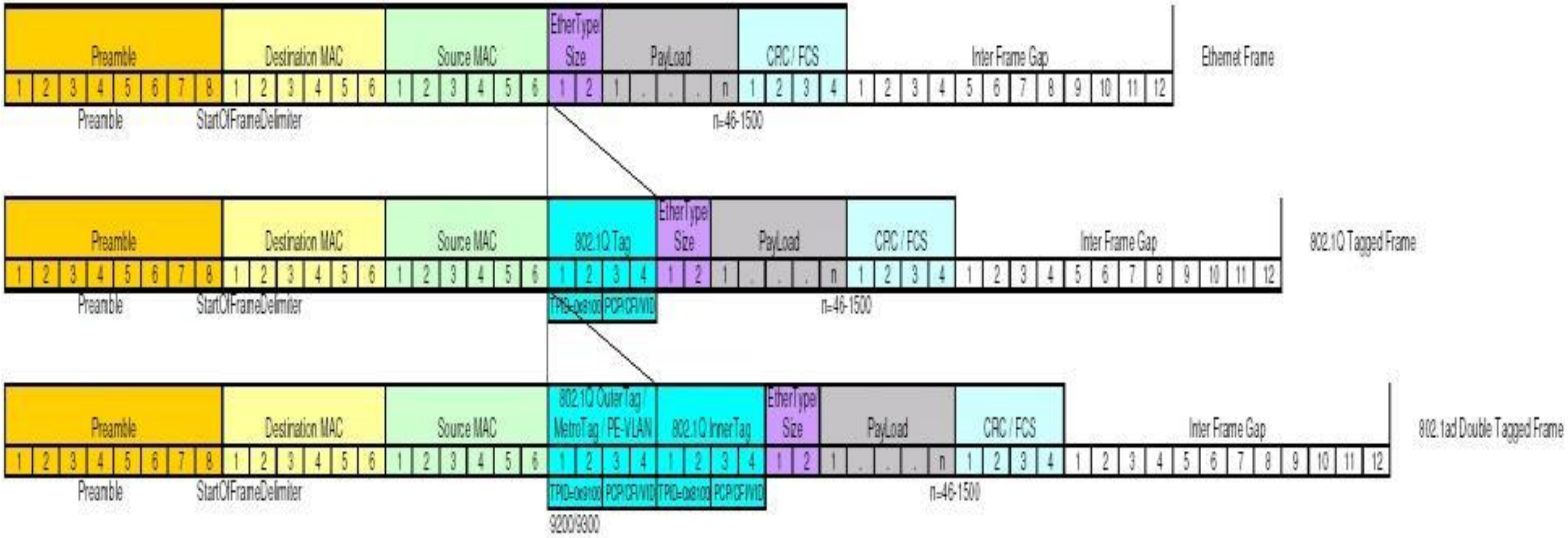
QinQ Switch Example Configuration

- The logic is to block traffic tagged vlan102 (from AP group 2) on the link to Portal 1, only allowing traffic tagged vlan 100 (from AP group 1); also, to remove the vlan 100 (“from AP group 1”) tag that we do not need anymore, and only show the internal tag, vlan 101 (SSID 1 tag):

```
3750_Labjh(config)#interface g1/0/11
3750_Labjh(config-if)#description to Portal 1
3750_Labjh(config-if)#switchport trunk encapsulation dot1q
3750_Labjh(config-if)#switchport mode trunk
3750_Labjh(config-if)#switchport trunk allowed vlan 100,101
<<<<because only vlan 100 and 101 are allowed, traffic from AP group1 will be forwarded here, but
traffic from AP group 2 (vlan 102 tag) will be blocked
3750_Labjh(config-if)#switchport trunk native vlan 100
<<<<because the native vlan is vlan 100, frames tagged vlan100 will be forwarded with their vlan
100 tag removed… only the inner tag (vlan 101) will appear on the frame when reaching portal 1


3750_Labjh(config)#interface g1/0/12
3750_Labjh(config-if)#description to Portal 2
3750_Labjh(config-if)#switchport trunk encapsulation dot1q
3750_Labjh(config-if)#switchport mode trunk
3750_Labjh(config-if)#switchport trunk allowed vlan 102,101
3750_Labjh(config-if)#switchport trunk native vlan 102
```

Qinq Tagging Enhancement

- QinQ tagging adds 4bytes to the 802.1Q tagged frame:



Qinq Tagging Enhancement Notes

- Some customers also need a “special case” (EAP-SIM-AKA) that would have (or not) this outer tag while other traffic would be tagged differently
  - I.e., AKA-SIM-AKA single tagged, PEAP double tagged
- IPv4 DHCP, IGMP and ARP packet from the client in the AP group which QinQ is enabled will be appended with an external VLAN tag which is also configured in AP group
- IPv6 DHCP, Radius and all other control plane packets are always single-tagged
- IPv4 and IPv6 client traffic tagging action is controlled by a single CLI command, and IPv4 DHCP is controlled by another independent CLI command
- To get IPv6 client traffic pass through QinQ tunnel, ICMPv6 NDP packet from the client in the AP group which QinQ is enabled will be appended with an external VLAN tag which is also configured in AP group

Qinq Tagging Enhancement Configuration

- Start by configuring the AP groups.
- Then, for each AP group, configure the service VLAN (the expected outer, double tag for the group):

```
(Cisco Controller) >config wlan apgroup qinq ?
tagging        Enable or disable QinQ tagging for an AP group.
service-vlan   Configures service vlan  for an AP group.

(Cisco Controller) >config wlan apgroup qinq service-vlan ?
<apgroup name> Specify the name of the apgroup to configure.

(Cisco Controller) >config wlan apgroup qinq service-vlan Mygroup ?
<vlan id>      Set service vlan id for an AP group<1~4095>.

(Cisco Controller) >config wlan apgroup qinq service-vlan Mygroup 31
```

  - You MUST configure the service VLAN first, otherwise you get “The Service Vlan Id cannot be 0, configure it first” when configuring the tagging parameters.

Qinq Tagging Enhancement Configuration

- Once service VLAN is configured, decide what should be tagged:

```
(Cisco Controller) >config wlan apgroup qinq tagging ?

client-traffic Enable or disable Client Traffic QinQ tagging for an AP group.
dhcp-v4        Enable or disable DHCPv4 QinQ tagging for an AP group.
eap-sim-aka    Enable or disable EAP-SIM/AKA Client Traffic QinQ tagging for an AP group.

(Cisco Controller) >config wlan apgroup qinq tagging client-traffic ?
<apgroup name> Specify the name of the apgroup to configure.

(Cisco Controller) >config wlan apgroup qinq tagging client-traffic Mygroup ?
enable         Enable QinQ tagging for an AP group.
disable        Disable QinQ tagging for an AP group.

(Cisco Controller) >config wlan apgroup qinq tagging client-traffic Mygroup enable
```

Qinq Tagging Enhancement Configuration

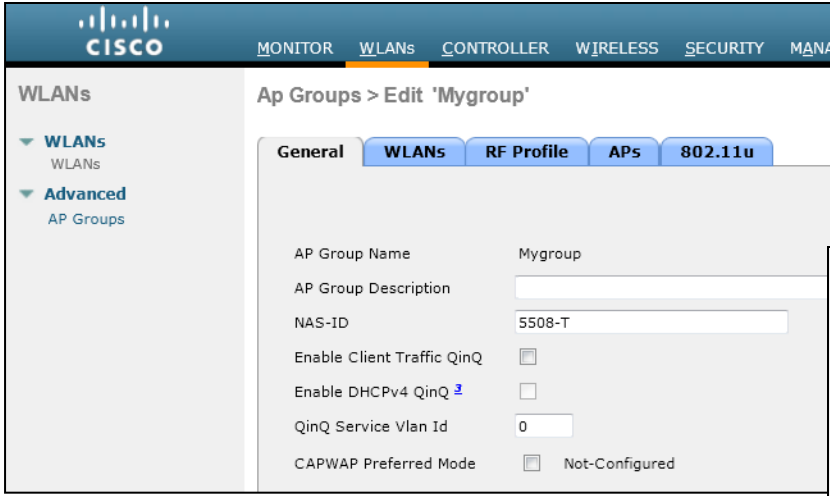
- Once service VLAN is configured, decide what should be tagged:

```
(Cisco Controller) >config wlan apgroup qinq tagging dhcp-v4 ?
<apgroup name> Specify the name of the apgroup to configure.

(Cisco Controller) >config wlan apgroup qinq tagging dhcp-v4 Mygroup ?
enable          Enable QinQ tagging for an AP group.
disable         Disable QinQ tagging for an AP group.

(Cisco Controller) >config wlan apgroup qinq tagging dhcp-v4 Mygroup enable

(Cisco Controller) >config wlan apgroup qinq tagging eap-sim-aka ?
<apgroup name> Specify the name of the apgroup to configure.

(Cisco Controller) >config wlan apgroup qinq tagging eap-sim-aka Mygroup ?
enable          Enable QinQ tagging for an AP group.
disable         Disable QinQ tagging for an AP group.
```

Disable if applicable, when client traffic is double-tagged.
If client traffic is single-tagged, enable if applicable.

Qinq Tagging Enhancement Configuration

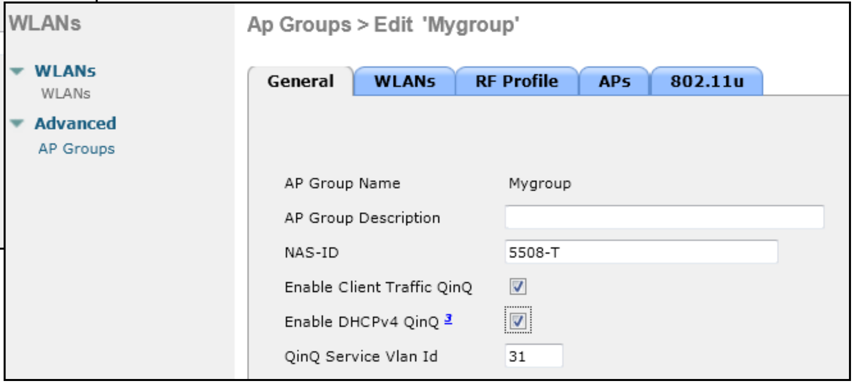
- The GUI offers the config parameters in the AP group section:



Ap Groups > Edit 'Mygroup'

AP Group Name	Mygroup
AP Group Description	
NAS-ID	5508-T
Enable Client Traffic QinQ	□
Enable DHCPv4 QinQ [3]	□
QinQ Service Vlan Id	0
CAPWAP Preferred Mode	□ Not-Configured

Notice that the EAP-SIM-AKA
option is CLI-only (as it is a special case).
By default, client-traffic covers everything,
including EAP-SIM-AKA.



Ap Groups > Edit 'Mygroup'

AP Group Name	Mygroup
AP Group Description	
NAS-ID	5508-T
Enable Client Traffic QinQ	☑
Enable DHCPv4 QinQ [3]	☑
QinQ Service Vlan Id	31

Qinq Tagging Enhancement Verification

- Beyond packet capture, you can check config on the WLC:

```
(Cisco Controller) >show wlan apgroups

Total Number of AP Groups........................ 1

Site Name........................................ Mygroup
Site Description................................. <none>
Venue Group Code................................. Unspecified
Venue Type Code.................................. Unspecified

NAS-identifier................................... 5508-T
Client Traffic QinQ Enable....................... TRUE
EAP-SIM/AKA QinQ Enable.......................... FALSE
DHCPv4 QinQ Enable............................... TRUE
Service Vlan ID.................................. 31
AP Operating Class............................... Not-configured
Capwap Prefer Mode............................... Not-configured
```

PMIPv6

Agenda

- PMIPv6 Review
- MAG on WLC or AP
- PMIPv6 Design Considerations in 8.0

PMIPv6 Review

PMIPv6 Definition

- *PMIPv6 = P*roxy *M*obile *IPv6*
- A **Network based** Mobility Solution (Transparent to the Wireless Client)
- The only network-based mobility management protocol standardized by IETF
- The 3GPP defined the interface for interworking between *Mobile Packet Core* and a trusted *WLAN* access network as S2a *PMIP* and *GTP*

How to Make a Wireless Client Think it Never Changed its Point of Attachment to a Network

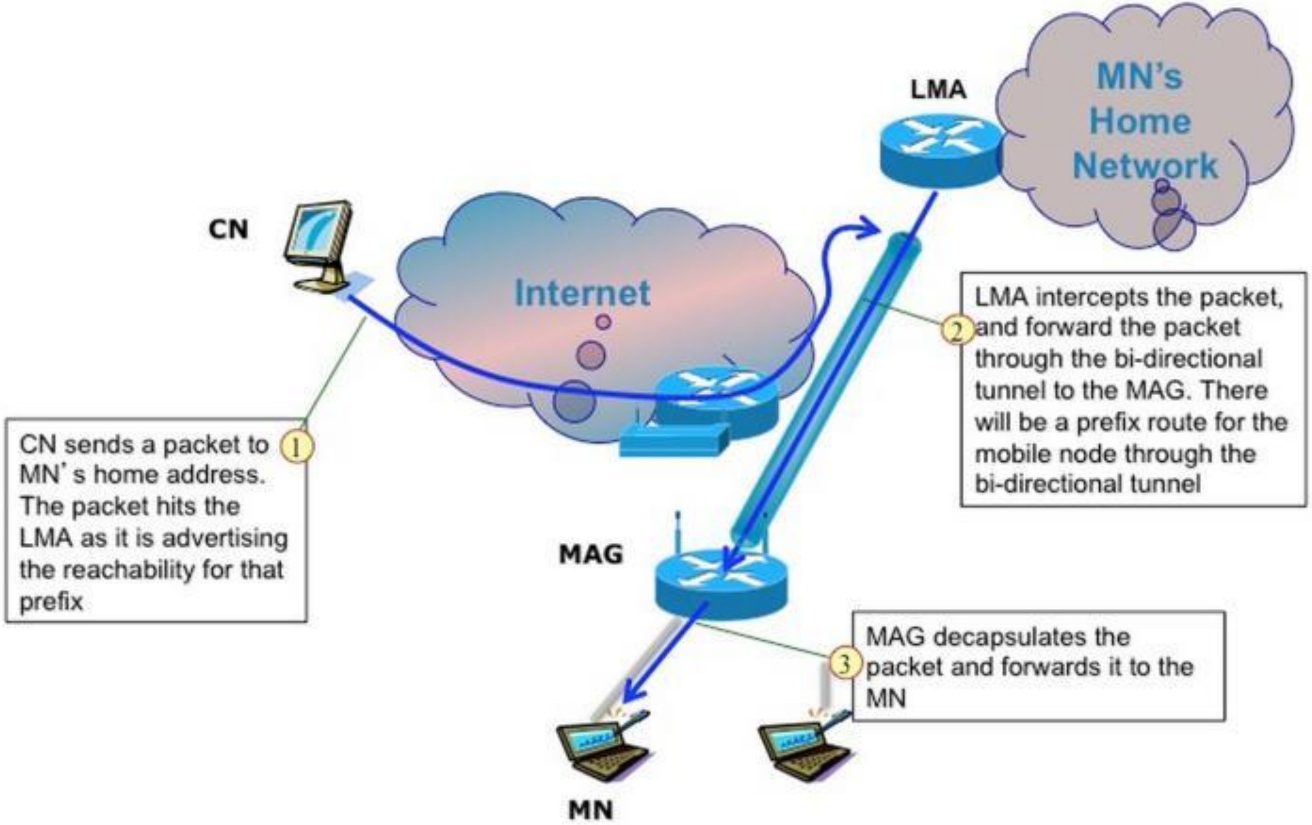
1. Keep the ***Client's IP*** address unchanged
2. Keep its ***Gateway's IP*** address unchanged
3. Keep the ***Gateway's MAC*** address unchanged!
4. Keep its ***DHCP server*** reachable and unchanged
5. Keep its ***Anchor Point*** to the core network unchanged (The anchor point will keep track of the client's movement, and advertise its IP to the world)

The PMIPv6 Lingo

The PMIPv6 architecture defines following functional entities:

- *Mobile Node (**MN**):* This is your ever moving Wireless Client
- *Correspondent Node (**CN**)*: This is some computer sitting somewhere in the world, and trying to communicate with that moving Wireless Client
- *Local Mobility Anchor (**LMA**)*:The LMA is the central core element of the PMIPv6 architecture. The LMA is the point for assigning and advertising the Wireless Client's IP address. The LMA can be the ASR5000 sitting in the Mobile Packet Core
- *Mobile Access Gateway (**MAG**)*:The MAG establishes a bi-directional tunnel to the LMA, and performs the mobility management on behalf of the Wireless Client. In our context, the MAG functionality can be enabled on the ***WLC*** or the ***AP*** *(or even both!)*

How Traffic Finds its Way to That Moving Wireless Client?



CN sends a packet to MN's home address. The packet hits the LMA as it is advertising the reachability for that prefix

LMA intercepts the packet, and forward the packet through the bi-directional tunnel to the MAG. There will be a prefix route for the mobile node through the bi-directional tunnel

MAG decapsulates the packet and forwards it to the MN

PMIPv6 On Wireless Products – The Evolution Since 7.3

- ***7.3***:

  The debut of "***MAG on the WLC***" feature! Back then, the WLAN was statically configured to serve either ***PMIPv6*** or ***Simple IP*** clients *(yep, that's how we now call a normal client in the context of PMIPv6!)*

- ***7.5***:

  In 7.5, the MAG is still only at the WLC, but now we have the option of using AAA override to dynamically define the wireless client's type along with other important variables (ex: which LMA to use, 3GPP charging characteristics,…)

- ***8.0***:

  The MAG function gets pushed all the way out to the AP itself for much greater scalability!

  In 8.0, APs operating in FlexConnect mode with Local Switched, Central Authentication, and *Central Association* WLAN can now act as the MAG.

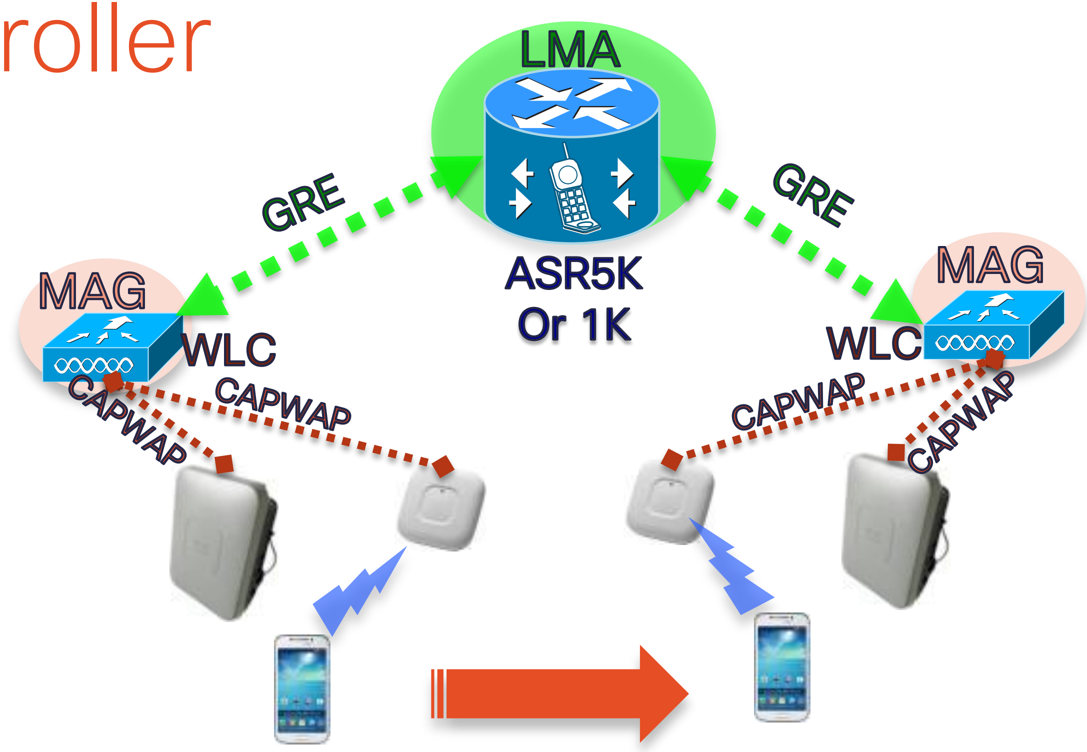
  In that mode PMIPv6 clients' traffic will be tunneled directly from the AP to the LMA; however. the WLC will still handle the FSR, and act as the Authenticator.

  If AAA override is enabled, the WLC dynamically informs the AP through CAPWAP messaging on what to do for that newly associated client.

MAG on WLC or AP

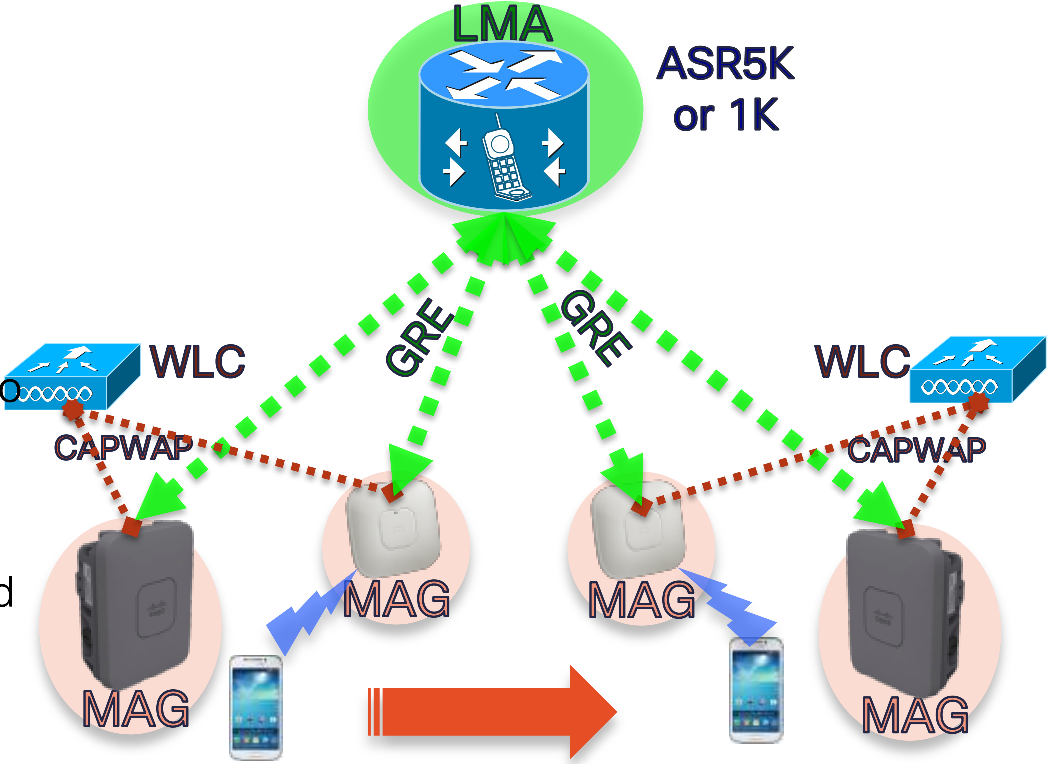
MAG on the Controller

- The WLC builds static bidirectional tunnels to the LMAs
- The client traffic is mapped to the appropriate tunnel as configured on the WLAN, or as dynamically assigned by AAA
- The client's IP address and traffic routing are handled by the LMA
- From the AP's perspective, it is business as usual



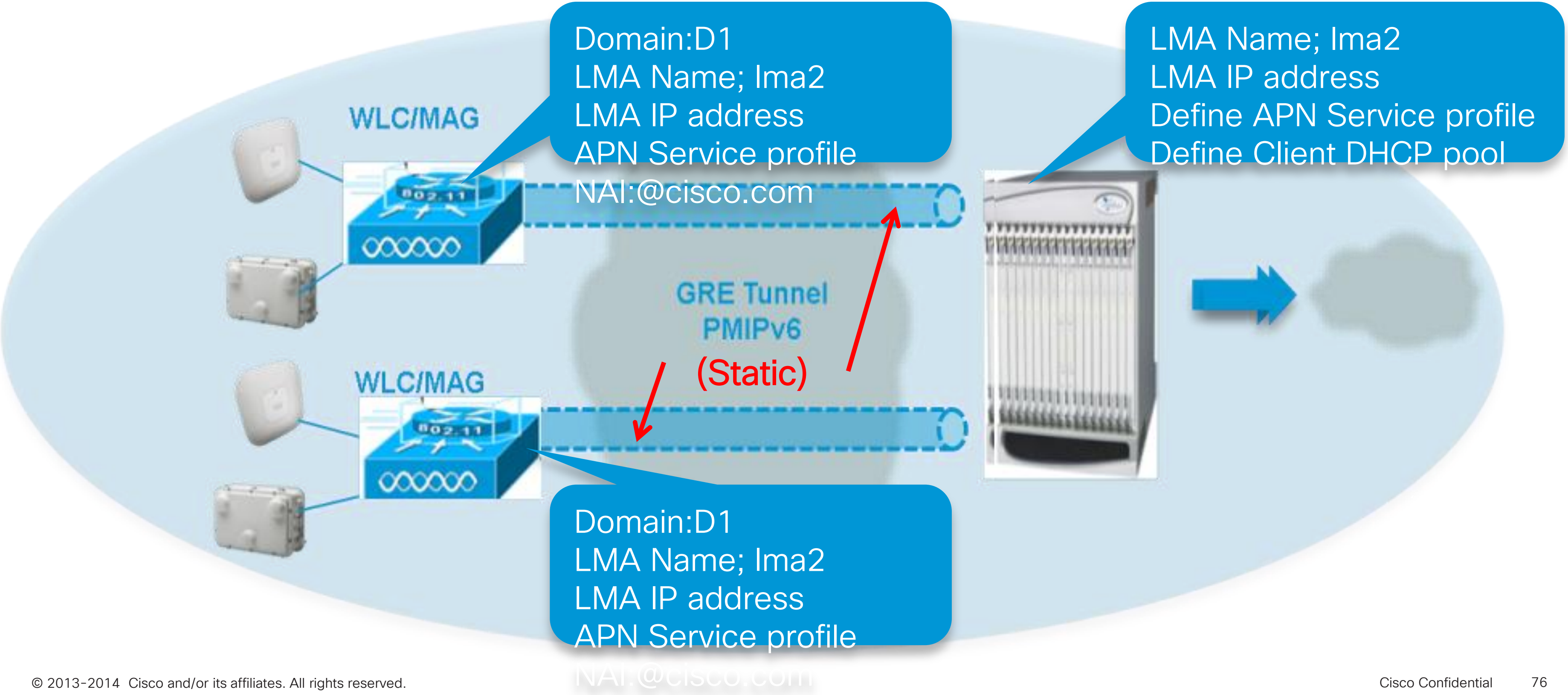
MAG on the AP

- AP must be in FlexConnect mode
- The WLAN Requirements:
  - Local Switching
  - Central Authentication
  - Central Association ←NEW!!
- As instructed by the WLC via CAPWAP, the AP dynamically builds the tunnel to the LMA(s) as needed
- The client traffic is mapped to the appropriate tunnel as configured on the WLAN, or as dynamically assigned by AAA
- FSR is handled centrally at the WLC
- Centrally switched WLANs can also serve PMIPv6 clients, but the MAG will be on the WLC (see previous slide)



For more details, and the CLI command, see the slide notes

PMIPv6 Architecture

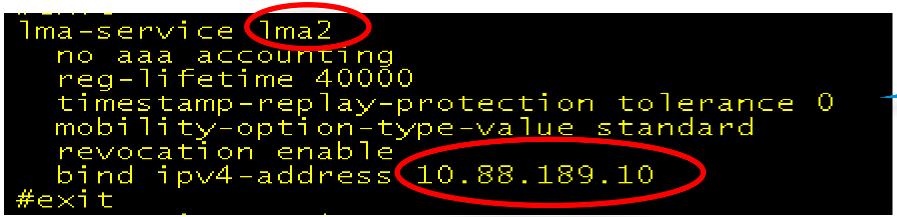


Domain:D1
LMA Name; lma2
LMA IP address
APN Service profile
NAI:@cisco.com

LMA Name; lma2
LMA IP address
Define APN Service profile
Define Client DHCP pool

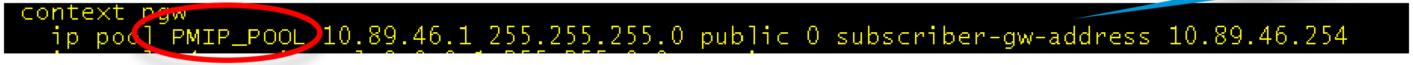
Domain:D1
LMA Name; lma2
LMA IP address
APN Service profile
NAI:@cisco.com

PMIPv6 Provisioning - LMA



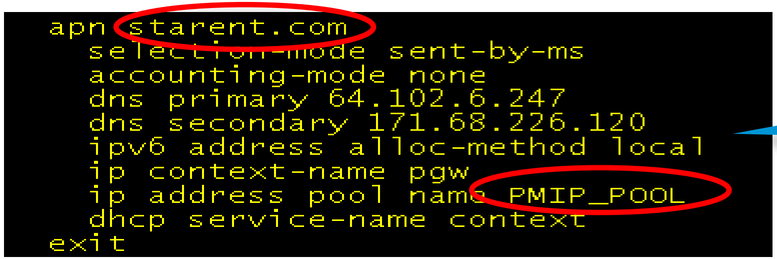
```
lma-service lma2
  no aaa accounting
  reg-lifetime 40000
  timestamp-replay-protection tolerance 0
  mobility-option-type-value standard
  revocation enable
  bind ipv4-address 10.88.189.10
#exit
```

Define LMA name and IP address



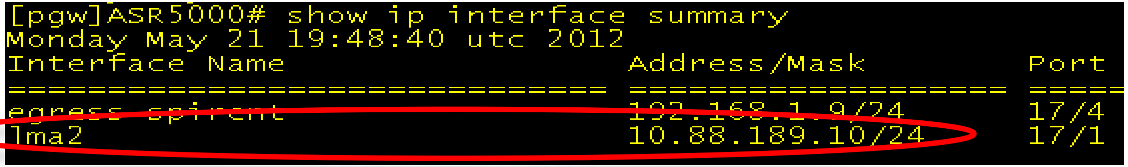
```
context pgw
  ip pool PMIP_POOL 10.89.46.1 255.255.255.0 public 0 subscriber-gw-address 10.89.46.254
```

Define DHCP Pool for APN



```
  apn starent.com
    selection-mode sent-by-ms
    accounting-mode none
    dns primary 64.102.6.247
    dns secondary 171.68.226.120
    ipv6 address alloc-method local
    ip context-name pgw
    ip address pool name PMIP_POOL
    dhcp service-name context
  exit
```

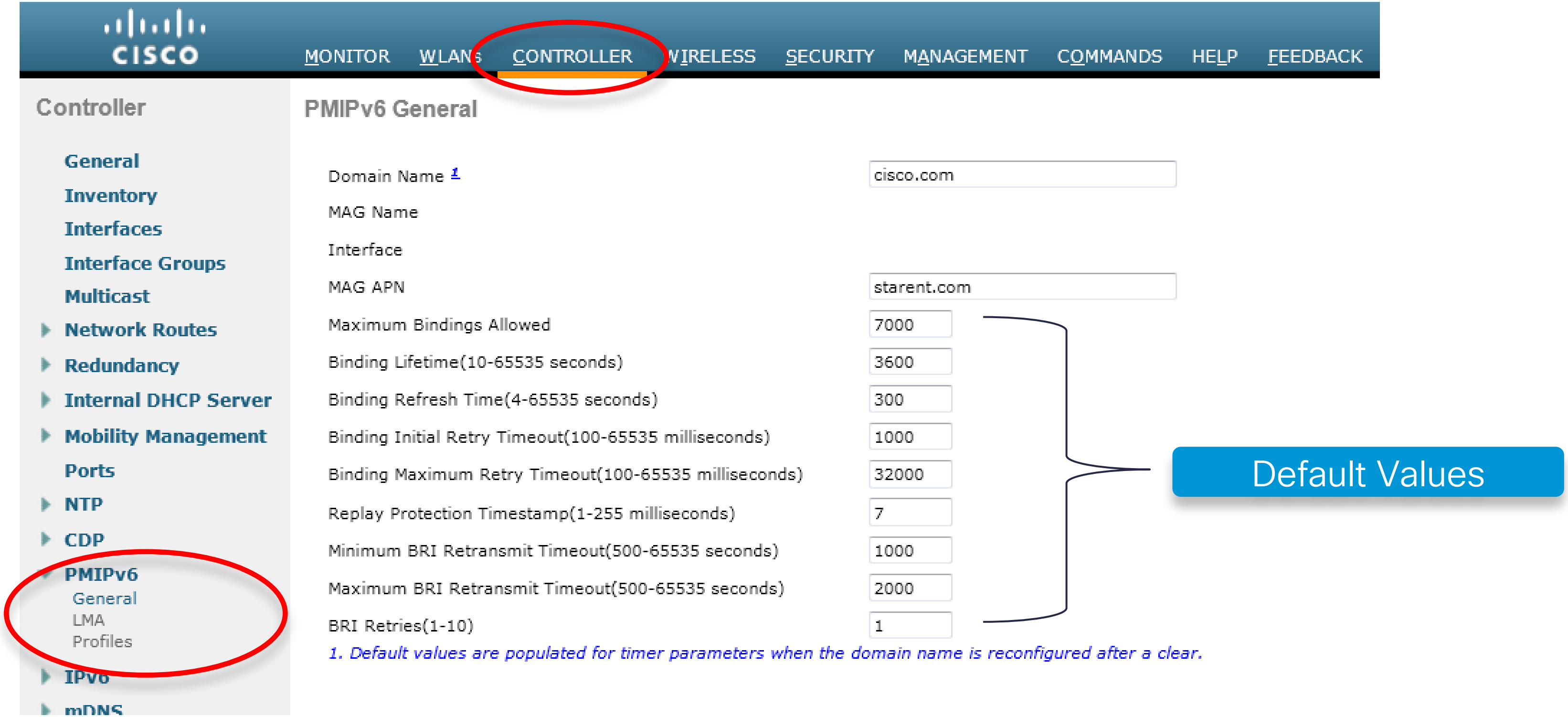
Define APN and properties to be used.



```
[pgw]ASR5000# show ip interface summary
Monday May 21 19:48:40 utc 2012
Interface Name                 Address/Mask         Port
============================== ==================== =====
egress_spirent                 192.168.1.9/24       17/4
lma2                           10.88.189.10/24      17/1
```

Verify LMA name and IP binding.

PMIPv6 Provisioning - WLC / MAG



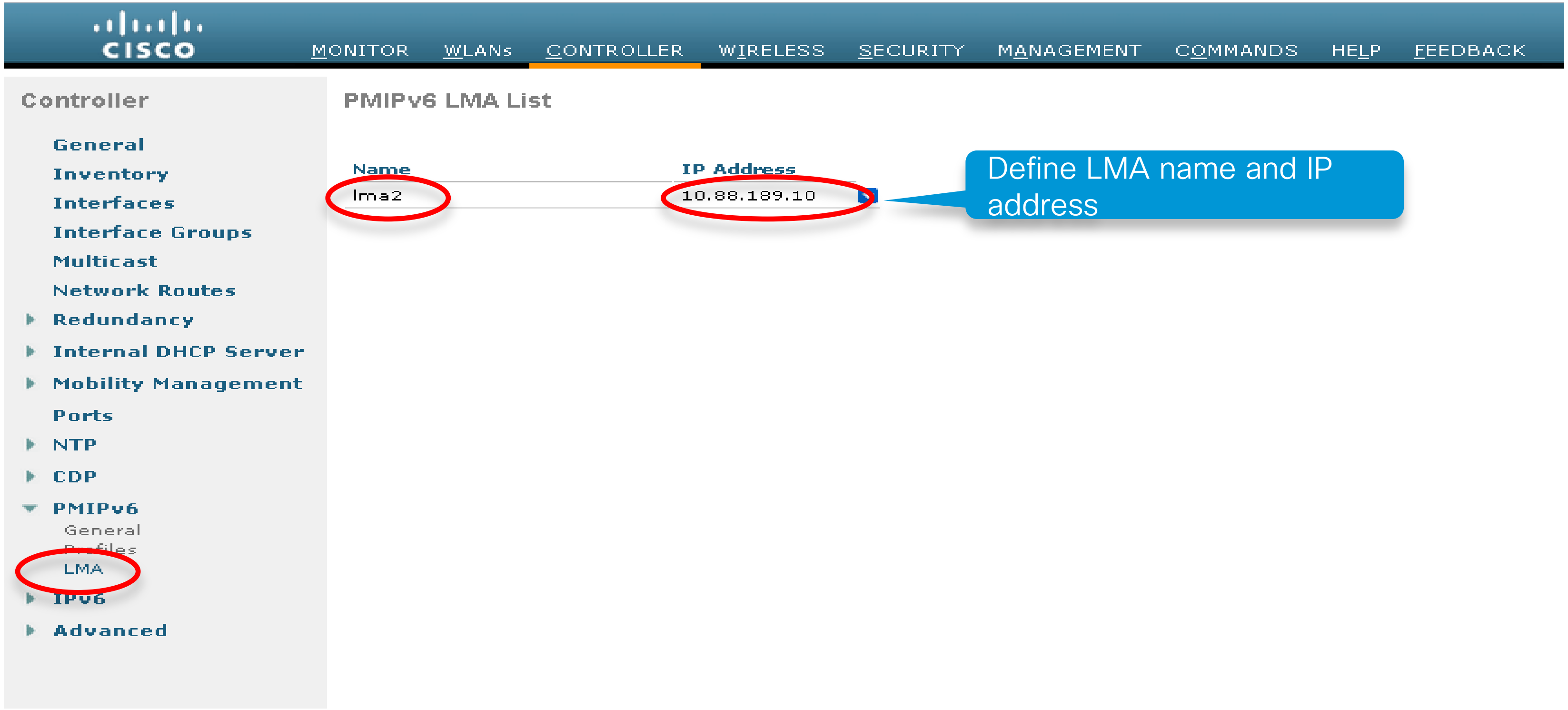
PMIPv6 General

Domain Name [1]	cisco.com
MAG Name	
Interface	
MAG APN	starent.com
Maximum Bindings Allowed	7000
Binding Lifetime(10-65535 seconds)	3600
Binding Refresh Time(4-65535 seconds)	300
Binding Initial Retry Timeout(100-65535 milliseconds)	1000
Binding Maximum Retry Timeout(100-65535 milliseconds)	32000
Replay Protection Timestamp(1-255 milliseconds)	7
Minimum BRI Retransmit Timeout(500-65535 seconds)	1000
Maximum BRI Retransmit Timeout(500-65535 seconds)	2000
BRI Retries(1-10)	1

1. Default values are populated for timer parameters when the domain name is reconfigured after a clear.

Default Values

PMIPv6 Provisioning - WLC / MAG – (cont’d)

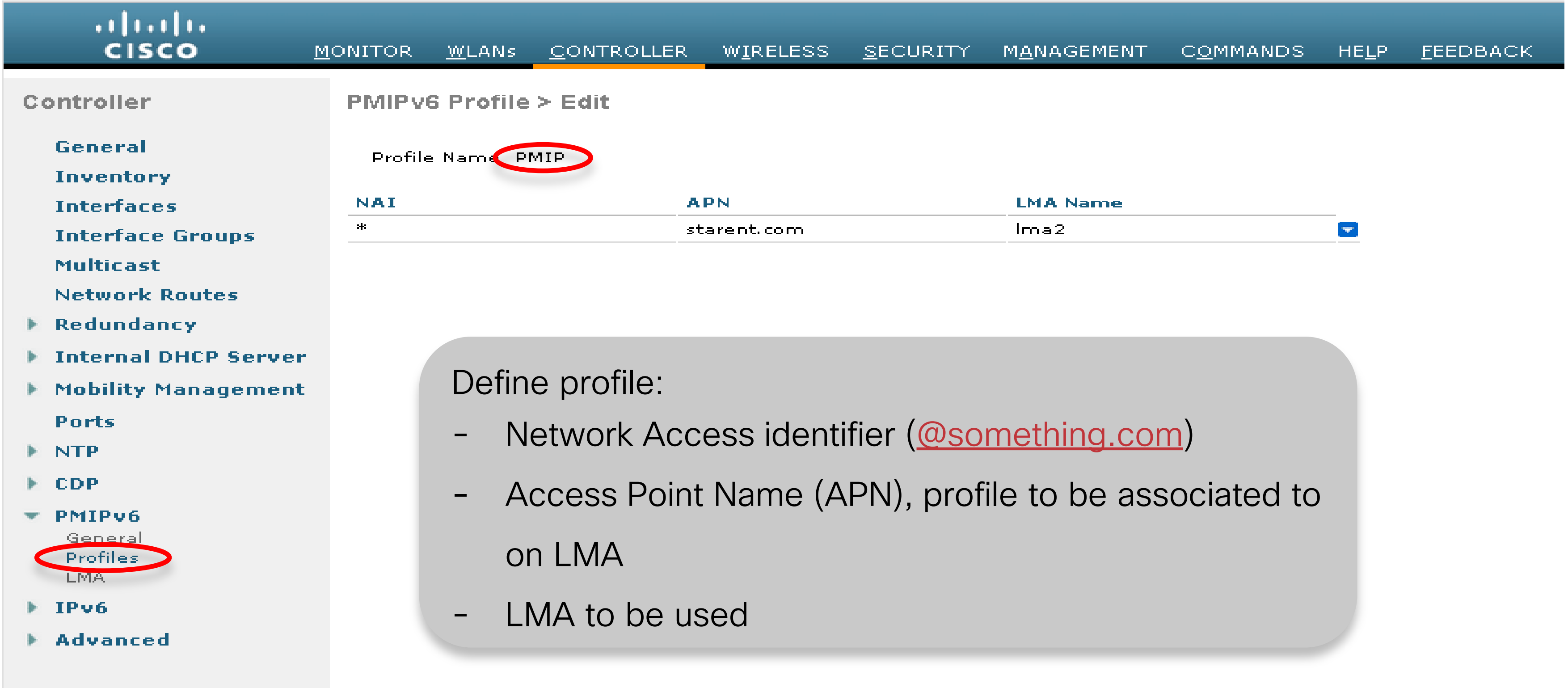


PMIPv6 LMA List

Name	IP Address
lma2	10.88.189.10

Define LMA name and IP address

PMIPv6 Provisioning - WLC / MAG – (cont'd)



PMIPv6 Profile > Edit

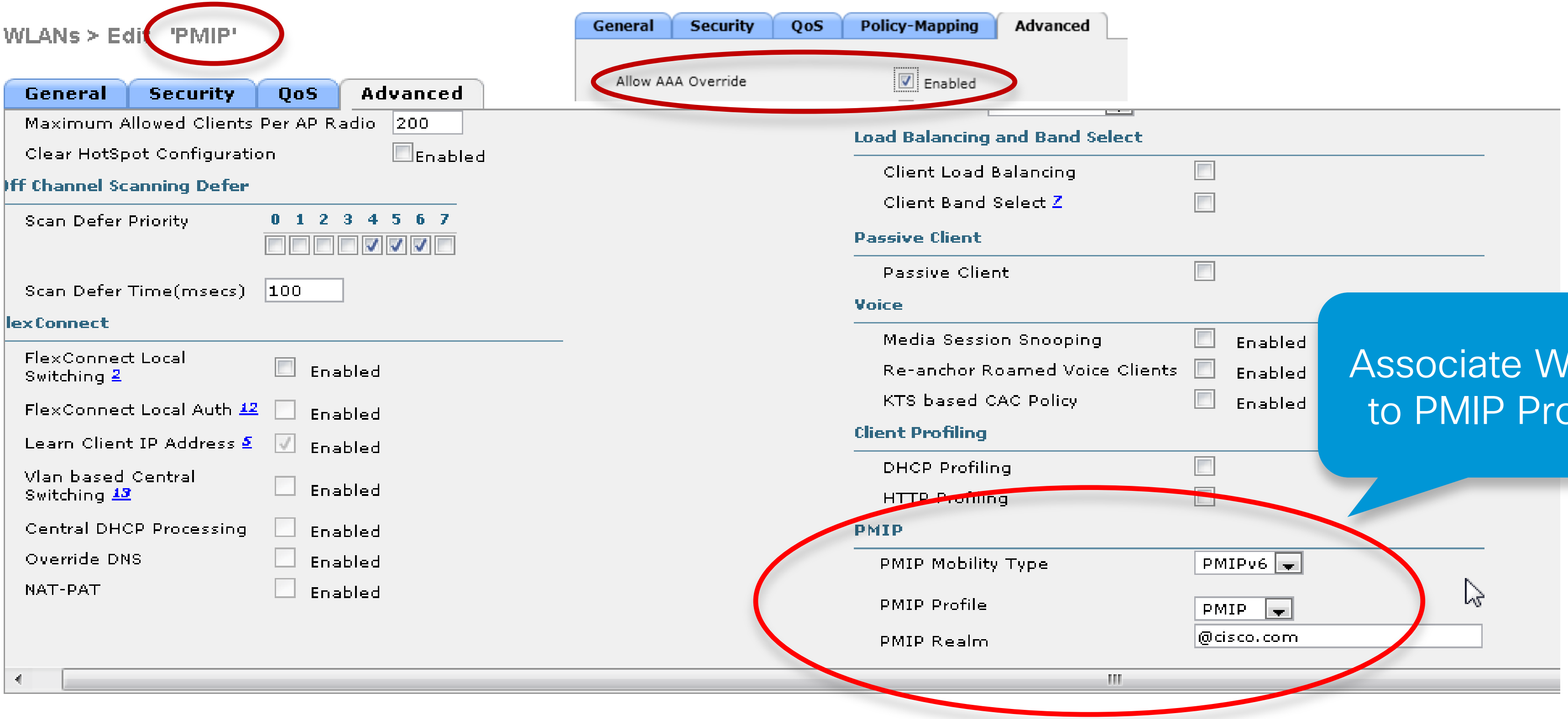
Profile Name PMIP

NAI	APN	LMA Name
*	starent.com	lma2

Define profile:

- Network Access identifier (@something.com)
- Access Point Name (APN), profile to be associated to on LMA
- LMA to be used

PMIPv6 Provisioning - WLC / MAG – (cont’d)



WLANs > Edit 'PMIP'

General | Security | QoS | Policy-Mapping | Advanced

Allow AAA Override ☑ Enabled

General | Security | QoS | Advanced

Maximum Allowed Clients Per AP Radio 200

Clear HotSpot Configuration □ Enabled

ff Channel Scanning Defer

Scan Defer Priority

0	1	2	3	4	5	6	7
□	□	□	□	☑	☑	☑	□

Scan Defer Time(msecs) 100

lexConnect

FlexConnect Local Switching 2 □ Enabled

FlexConnect Local Auth 12 □ Enabled

Learn Client IP Address 5 ☑ Enabled

Vlan based Central Switching 13 □ Enabled

Central DHCP Processing □ Enabled

Override DNS □ Enabled

NAT-PAT □ Enabled

Load Balancing and Band Select

Client Load Balancing □

Client Band Select 7 □

Passive Client

Passive Client □

Voice

Media Session Snooping □ Enabled

Re-anchor Roamed Voice Clients □ Enabled

KTS based CAC Policy □ Enabled

Client Profiling

DHCP Profiling □

HTTP Profiling □

PMIP

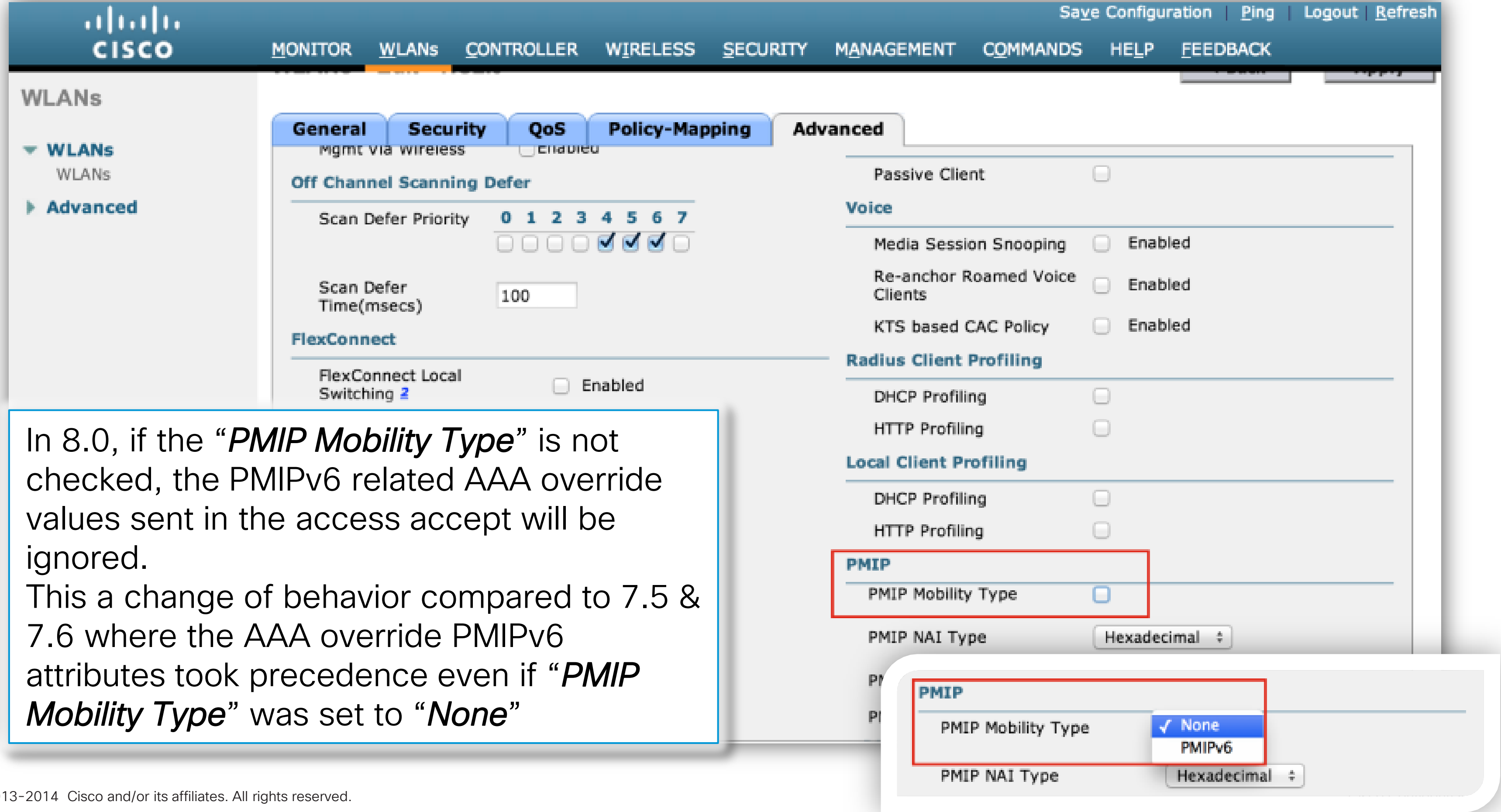
PMIP Mobility Type PMIPv6

PMIP Profile PMIP

PMIP Realm @cisco.com

Associate WLAN to PMIP Profile

Configurations Gotchas



Mgmt via Wireless □ Enabled

Off Channel Scanning Defer

Scan Defer Priority

0	1	2	3	4	5	6	7
□	□	□	□	☑	☑	☑	□

Scan Defer Time(msecs) 100

FlexConnect

FlexConnect Local Switching 2 □ Enabled

Passive Client □

Voice

Media Session Snooping □ Enabled

Re-anchor Roamed Voice Clients □ Enabled

KTS based CAC Policy □ Enabled

Radius Client Profiling

DHCP Profiling □

HTTP Profiling □

Local Client Profiling

DHCP Profiling □

HTTP Profiling □

PMIP

PMIP Mobility Type □

PMIP NAI Type Hexadecimal

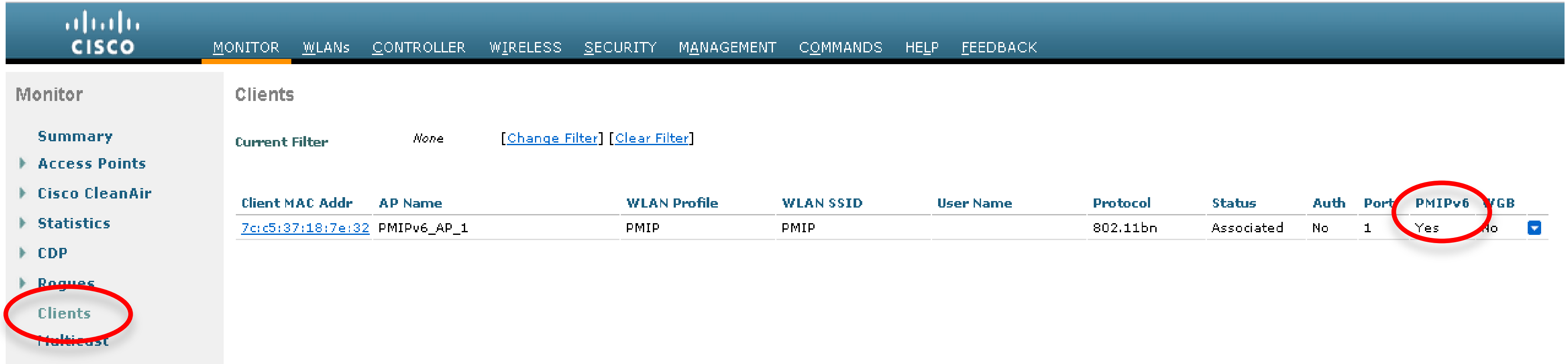
PMIP

PMIP Mobility Type ✓ None / PMIPv6

PMIP NAI Type Hexadecimal

In 8.0, if the “*PMIP Mobility Type*” is not checked, the PMIPv6 related AAA override values sent in the access accept will be ignored.
This a change of behavior compared to 7.5 & 7.6 where the AAA override PMIPv6 attributes took precedence even if “*PMIP Mobility Type*” was set to “*None*”

PMIPv6 Provisioning - WLC / MAG – (cont'd)

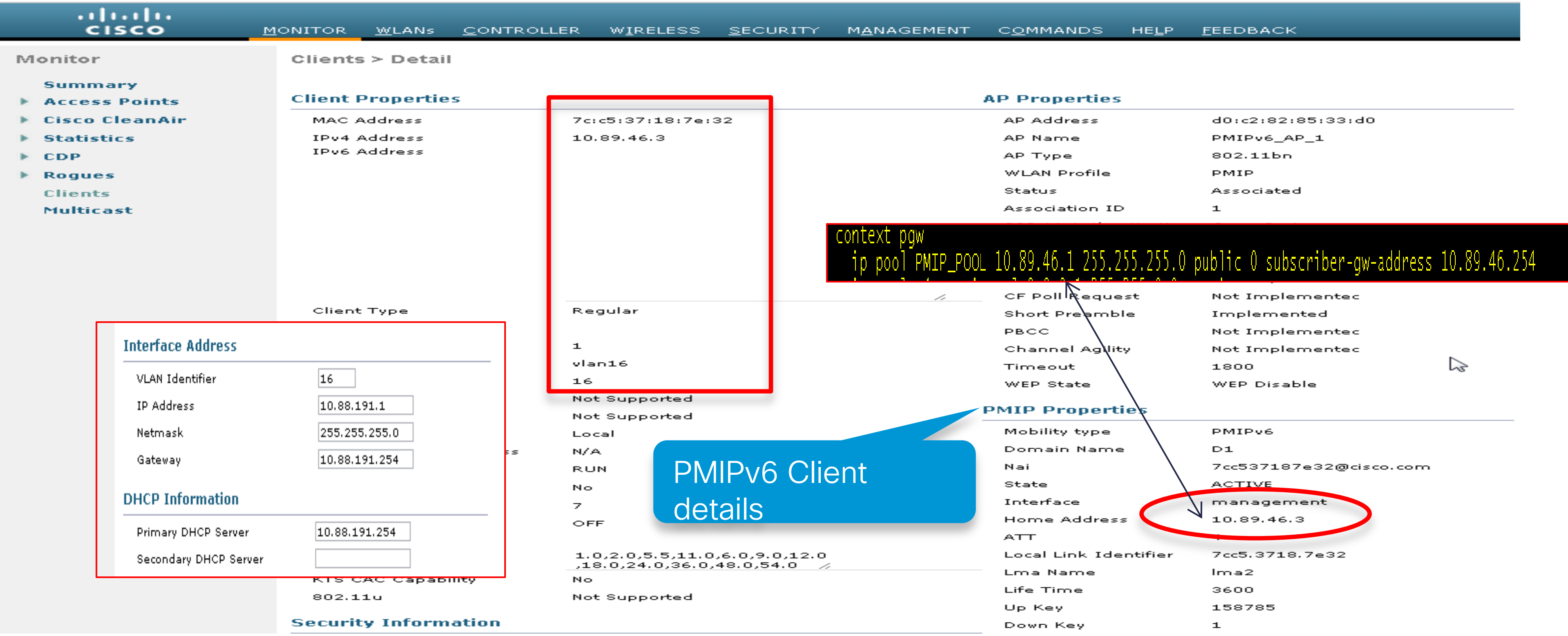


Clients

Current Filter None [Change Filter] [Clear Filter]

Client MAC Addr	AP Name	WLAN Profile	WLAN SSID	User Name	Protocol	Status	Auth	Port	PMIPv6	WGB
7c:c5:37:18:7e:32	PMIPv6_AP_1	PMIP	PMIP		802.11bn	Associated	No	1	Yes	No

PMIPv6 Provisioning – WLC / MAG – (cont’d)



Clients > Detail

Client Properties

MAC Address	7c:c5:37:18:7e:32
IPv4 Address	10.89.46.3
IPv6 Address	
Client Type	Regular
	1
	vlan16
	16
	Not Supported
	Not Supported
	Local
ss	N/A
	RUN
	No
	7
	OFF
	1.0,2.0,5.5,11.0,6.0,9.0,12.0 ,18.0,24.0,36.0,48.0,54.0
KTS CAC Capability	No
802.11u	Not Supported

Security Information

Interface Address

VLAN Identifier	16
IP Address	10.88.191.1
Netmask	255.255.255.0
Gateway	10.88.191.254

DHCP Information

Primary DHCP Server	10.88.191.254
Secondary DHCP Server	

AP Properties

AP Address	d0:c2:82:85:33:d0
AP Name	PMIPv6_AP_1
AP Type	802.11bn
WLAN Profile	PMIP
Status	Associated
Association ID	1
CF Poll Request	Not Implementec
Short Preamble	Implemented
PBCC	Not Implementec
Channel Agility	Not Implementec
Timeout	1800
WEP State	WEP Disable

```
context pgw
  ip pool PMIP_POOL 10.89.46.1 255.255.255.0 public 0 subscriber-gw-address 10.89.46.254
```

PMIP Properties

Mobility type	PMIPv6
Domain Name	D1
Nai	7cc537187e32@cisco.com
State	ACTIVE
Interface	management
Home Address	10.89.46.3
ATT	
Local Link Identifier	7cc5.3718.7e32
Lma Name	lma2
Life Time	3600
Up Key	158785
Down Key	1

PMIPv6 Client details

CLI Configuration

- CLI configuration is mostly similar to 7.3, difference being that config is pushed to the APs. The WLC command to AP map is as follows:

These commands exist since 7.3

When you enter the command to the WLC, this is what is pushed to the AP (you can type the command on the AP directly if you debug capwap con cli first)

CLI on WLC	IOS CLI on AP
config pmipv6 domain <dom-name>	AP_3600(config)#ipv6 mobile pmipv6-domain <dom-name>
config pmipv6 delete domain <name>	AP_3600(config)#no ipv6 mobile pmipv6-domain <dom-name>
config pmipv6 add profile <prof-name> nai <user@realm> lma <lma-name> apn <apn-name>	AP_3600(config)#ipv6 mobile pmipv6-domain <dom-name> AP_3600(config-ipv6-pmipv6-domain)#nai <nai-name> AP_3600(config-ipv6-pmipv6-domain-mn)#lma <lma-id> AP_3600(config-ipv6-pmipv6-domain-mn)#apn <apn-name>
config pmipv6 delete profile <name> nai <user>	AP_3600(config)#ipv6 mobile pmipv6-domain <dom-name> AP_3600(config-ipv6-pmipv6-domain)#no nai <nai-name>
config pmipv6 mag binding maximum <num>	AP_3600(config)#ipv6 mobile pmipv6-mag <mag-name> domain <dom-name> AP_3600(config-ipv6-pmipv6-mag)#binding maximum <num>
config pmipv6 mag binding lifetime <num>	AP_3600(config)#ipv6 mobile pmipv6-mag <mag-name> domain <dom-name> AP_3600(config-ipv6-pmipv6-mag)#binding lifetime <num>
config pmipv6 mag binding refresh-time <num>	AP_3600(config)#ipv6 mobile pmipv6-mag <mag-name> domain <dom-name> AP_3600(config-ipv6-pmipv6-mag)#binding refresh-time 100

CLI Configuration

- CLI configuration is mostly similar to 7.3, difference being that config is pushed to the APs. The WLC command to AP map is as follows:

These commands exist since 7.3

When you enter the command to the WLC, this is what is pushed to the AP
(you can type the command on the AP directly if you debug capwap con cli first)

CLI on WLC	IOS CLI on AP
config pmipv6 mag binding init-retx-time <num>	AP_3600(config)#ipv6 mobile pmipv6-mag <mag-name> domain <dom-name> AP_3600(config-ipv6-pmipv6-mag)#binding init-retx-time <num>
config pmipv6 mag binding max-retx-time <num>	AP_3600(config)#ipv6 mobile pmipv6-mag <mag-name> domain <dom-name> AP_3600(config-ipv6-pmipv6-mag)#binding max-retx-time <num>
config pmipv6 mag replay-protection timestamp window <num>	AP_3600(config)#ipv6 mobile pmipv6-mag <mag-name> domain <dom-name> AP_3600(config-ipv6-pmipv6-mag)#replay-protection timestamp window <num>
config pmipv6 mag bri delay min <num>	AP_3600(config)#ipv6 mobile pmipv6-mag <mag-name> domain <dom-name> AP_3600(config-ipv6-pmipv6-mag)#bri delay min <num>
config pmipv6 mag bri delay max <num>	AP_3600(config)#ipv6 mobile pmipv6-mag <mag-name> domain <dom-name> AP_3600(config-ipv6-pmipv6-mag)#bri delay max <num>
config pmipv6 mag bri retries <num>	AP_3600(config)#ipv6 mobile pmipv6-mag <mag-name> domain <dom-name> AP_3600(config-ipv6-pmipv6-mag)#bri retries <num>

CLI Configuration

- CLI configuration is mostly similar to 7.3, difference being that config is pushed to the APs. The WLC command to AP map is as follows:

These commands exist since 7.3

When you enter the command to the WLC, this is what is pushed to the AP (you can type the command on the AP directly if you debug capwap con cli first)

CLI on WLC	IOS CLI on AP
config pmipv6 mag lma <name> ipv4-address <ip>	AP_3600(config)#ipv6 mobile pmipv6-mag <mag-name> domain <dom-name> AP_3600(config-ipv6-pmipv6-mag)# AP_3600(config-ipv6-pmipv6-mag)#lma <lma-name> <dom-name> AP_3600(config-ipv6-pmipv6mag-lma)# ipv4-address <ipv4-addr> 600(config-ipv6-pmipv6mag-lma)#encap gre-ipv4
config pmipv6 delete lma <name>	AP_3600(config)#ipv6 mobile pmipv6-mag <mag-name> domain <dom-name> AP_3600(config-ipv6-pmipv6-mag)# AP_3600(config-ipv6-pmipv6-mag)#no lma <lma-name> <dom-name>
config wlan pmipv6 default-realm <realm-string> <wlan-id>	There is no IOS CLI for this. This information will be stored in WLAN structure and used as default for clients in this WLAN.
config wlan pmipv6 default-realm NONE <wlan-id>	There is no IOS CLI for this.
config wlan pmipv6 mobility-type {pmipv6| none} {<wlan-id> | all}	There is no IOS CLI for this. This information will be stored in WLAN structure and used for clients in this WLAN to be considered as PMIPv6.
config wlan pmipv6 profile-name <name> <wlan-id>	There is no IOS CLI for this.

CLI Configuration

- New CLI commands are as follows:

```
(Cisco Controller) >config pmipv6 mag apn ?
<apn>          MAG APN

(Cisco Controller) >config pmipv6 delete mag apn ?
<apn>          MAG APN
```

- The above CLI is introduced to specify the APN name for the MAG. When the MAG role is 3GPP, it is mandatory to specify the APN name for the MAG. In WLC, we use the MAG role as WLAN. In IOS AP, we use the MAG role as 3GPP as per the recommendation from PMIPv6 team.
- This command sets the APN used by MAG for a pmipv6 client if APN is not specified for the client. For MAG on AP, since APN information is specified by AAA server or through static profile configuration, this command for MAG APN will never be used.

CLI Configuration

- New CLI commands are as follows:

```
(Cisco Controller) >config wlan flexconnect central-assoc ?
<WLAN id>      Enter WLAN Identifier between 1 and 512.

(Cisco Controller) >config wlan flexconnect central-assoc 1 ?
enable         Enables central association on the WLAN.
disable        Disables central association on the WLAN.
```

- The above CLI is applicable only for Flex mode of APs. When the above CLI is used to enable, all management messages from the clients on this WLAN will be handled by the WLC. Flex-mode AP will not respond to association messages from Client, but it will be forwarded to WLC.
- The association response from the WLC will be forwarded by the AP to the wireless client, as in the case of local mode AP. Apart from this the key caching for clients on this WLAN will be handled by the WLC. WLC will not distribute the keys to APs for clients in this WLAN. WLC will distribute the keys for all WLCs in the mobility domain when this CLI is enabled.
- By default, this CLI is disabled

PMIPv6 Verification

- Same commands as in 7.3:

```
(Cisco Controller) >show pmipv6 mag globals
 Domain  : DOM-1
 MAG Identifier  : Srini-Talwar-3
 MAG APN  : starent.com
        MAG Interface  : management
        Max Bindings  : 7000
        Registration Lifetime  : 3600
        BRI Init-delay time  : 1000
        BRI Max-delay time  : 2000
        BRI Max retries  : 1
        Refresh time  : 300
        Refresh RetxInit time  : 1000
        Refresh RetxMax time  : 32000
        Timestamp option : Enabled
        Validity window  : 7
        Peer#1:
                LMA Name: lma1   LMA IP: 9.7.53.201
```

PMIPv6 Verification

- Same commands as in 7.3:

```
(Cisco Controller) >show pmipv6 mag stats
----------------------------------------
[Srini-Talwar-3]: Total Bindings        : 0
[Srini-Talwar-3]: PBU Sent              : 0
[Srini-Talwar-3]: PBA Rcvd              : 0
[Srini-Talwar-3]: PBRI Sent             : 0
[Srini-Talwar-3]: PBRI Rcvd             : 0
[Srini-Talwar-3]: PBRA Sent             : 0
[Srini-Talwar-3]: PBRA Rcvd             : 0
[Srini-Talwar-3]: No Of handoff : 0


(Cisco Controller) >show pmipv6 domain DOM-1 profile prof-1
 NAI: *
 APN: starent.com
 LMA: lma1
```

PMIPv6 Verification

- Same commands as in 7.3:

```
(Cisco Controller) >show wlan summary

Number of WLANs.................................. 14

WLAN ID  WLAN Profile Name / SSID                  Status    Interface Name          PMIPv6
Mobility
-------  ----------------------------------  --------  --------------------  -------------
--
1        anj_ktsriniv_1 / anj_ktsriniv_1     Disabled  management            pmipv6 WLC
2        anj_ktsriniv_3 / anj_ktsriniv_3     Disabled  management            none
…/…
8        ktsriniv_pmip_1 / ktsriniv_pmip_1   Enabled   management            pmipv6 AP
9        ktsriniv_pmip_2 / ktsriniv_pmip_2   Enabled   management            pmipv6 WLC
10       ktsriniv_pmip_3 / ktsriniv_pmip_3   Disabled  management            pmipv6 AP
11       ktsriniv_pmip_4 / ktsriniv_pmip_4   Disabled  management            pmipv6 AP
```

PMIPv6 Verification

Complete output

pmipv6showwlan.txt

- Same commands as in 7.3:

```
(Cisco Controller) >show wlan 8
WLAN Identifier.................................. 8
Profile Name..................................... ktsriniv_pmip_1
…/…
PMIPv6 Mobility Type............................. PMIPv6 MAG
Profile.......................................... prof-1
PMIPv6 Default Realm............................. starent.com PMIPv6 NAI
Type............................................. Hexadecimal
PMIPv6 MAG location.............................. AP
…/…
 FlexConnect Local Switching..................... Enabled FlexConnect Central
Association....................................... Enabled
FlexConnect Learn IP Address...................... Enabled
```

PMIPv6 Verification

Complete output

pmipv6showwlan.txt

- Same commands as in 7.3:

```
(Cisco Controller) >show pmipv6 profile summary
Profile Name    WLAN IDs (Mapped)
        ------------    -----------------
        prof-1          8, 9, 11, 12



(Cisco Controller) >show client summary
Number of Clients................................ 1
Number of PMIPV6 Clients......................... 1
                                                       RLAN/
MAC Address       AP Name           Slot Status        WLAN  Auth Protocol         Port Wired PMIPV6  Role
----------------- ----------------- ---- ------------- ----- ---- ---------------- ---- ----- ------- ------
----------
00:21:6a:9b:32:d6 AP6c20.560e.1a30   1   Associated      8   Yes  802.11n(5 GHz)   13   No    Yes-AP  Local
```

PMIPv6 Verification

Complete output

pmipv6showclient.txt

- Same commands as in 7.3:

```
(Cisco Controller) >show client detail 00:21:6a:9b:32:d6
Client MAC Address............................... 00:21:6a:9b:32:d6
Client Username ................................. Srini
…/…
Client Type...................................... PMIPv6
PMIPv6 State..................................... Complete
PMIPv6 MAG location.............................. AP
PMIPv6 AAA MN Service............................ Unavailable
PMIPv6 AAA NAI................................... Unavailable
PMIPv6 AAA LMA................................... Unavailable
PMIPv6 AAA APN................................... Unavailable
PMIPv6 AAA MSISDN................................ Unavailable
PMIPv6 AAA 3gpp Charging Characteristics......... Unavailable
…/…
FlexConnect Data Switching....................... Local
FlexConnect Dhcp Status.......................... Local
FlexConnect Vlan Based Central Switching......... No
FlexConnect Authentication....................... Central
FlexConnect Central Association.................. Yes
```

PMIPv6 Verification

- show commands on AP for the PMIPv6 feature:

```
AP7cad.74ff.36d2#show ipv6 mobile pmipv6 mag binding
AP7cad.74ff.36d2#show  ipv6 mobile pmipv6 mag globals
AP7cad.74ff.36d2#show  ipv6 mobile pmipv6 mag stats
AP7cad.74ff.36d2#show ipv6 mobile pmipv6 mag heartbeat
AP7cad.74ff.36d2#show ipv6 mobile pmipv6 mag logical-mn
AP7cad.74ff.36d2#show  ip access-lists dynamic
AP7cad.74ff.36d2#show  route-map dynamic detail
Current active dynamic routemaps = 0
AP7cad.74ff.36d2#show ip cef
%IPv4 CEF not running
AP7cad.74ff.36d2#show  ip route
Default gateway is 172.31.255.1

Host                   Gateway                 Last Use    Total Uses  Interface
ICMP redirect cache is empty
AP7cad.74ff.36d2#show  ip policy
Interface      Route map
AP7cad.74ff.36d2#show running-config brief
```

PMIPv6 Verification

- show commands on AP for the PMIPv6 feature:

```
AP_2600#show running-config | beg ipv6 mobile
ipv6 mobile pmipv6-domain wnbu
encap gre-ipv4
lma wnbu-lma
  ipv4-address 9.6.84.60

ipv6 mobile pmipv6-mag AP_2600 domain wnbu
no discover-mn-detach
role 3GPP
apn starent.com
address ipv4 9.6.81.152
interface BVI3
lma wnbu-lma wnbu
  ipv4-address 9.6.84.60
  encap gre-ipv4
```

PMIPv6 Verification

- show commands on AP for the PMIPv6 feature:

```
AP6c20.560e.1a30#show ipv6 mobile pmipv6 mag binding
Total number of bindings: 1
----------------------------------------
[Binding][MN]: Domain: DOM-1, Nai: srini
        [Binding][MN]: State: ACTIVE
        [Binding][MN]: Interface: BVI3
        [Binding][MN]: Hoa: 20.10.0.2, Att: 4, llid: 0021.6a9b.32d6
        [Binding][MN]: HNP: 0
        [Binding][MN]: APN: starent.com
        [Binding][MN][LMA]: Id: lma1
        [Binding][MN][LMA]: Lifetime: 3600
        [Binding][MN]: No
        [Binding][MN][PATH]:
                State: PATH_ACTIVE
                Tunnel: Tunnel0
                Refresh time: 300(sec), Refresh time Remaining: 288(sec)
                [Binding][MN][PATH][GREKEY]: Upstream: 1, Downstream: 1
```

PMIPv6 Verification

- show commands on AP for the PMIPv6 feature:

```
AP6c20.560e.1a30#show ipv6 mobile pmipv6 mag globals
---------------------------------------------------
Domain  : DOM-1
Mag Identifier  : AP6c20.560e.1a30
        MN's detach discover            : disabled
        Heartbeat                       : disabled
        Local routing                   : disabled
        Session Manager                 : disabled
        Mag is enabled on interface     : BVI3
        Max Bindings                    : 10000
        AuthOption                      : disabled
        RegistrationLifeTime            : 3600 (sec)
        BRI InitDelayTime               : 1000 (msec)
        BRI MaxDelayTime                : 2000 (msec)
        BRI MaxRetries                  : 1
        EncapType                       : GRE in IPV4
        Fixed Link address is           : enabled
        Fixed Link address              : 0000.5e00.5213
        Fixed Link Local address is     : enabled
        Fixed Link local address        : 0xFE800000 0x0 0x2005EFF 0xFE005213
        RefreshTime                     : 300 (sec)
        Refresh RetxInit time           : 1000 (msec)
        Refresh RetxMax time            : 32000 (msec)
        Timestamp option                : enabled
        Validity Window                 : 7
Peer :  lma1
        AuthOption                      : disabled
        EncapType                       : GRE in IPV4
```

PMIPv6 Verification

Complete output

pmipv6showapmagstats.txt

- show commands on AP for the PMIPv6 feature:

```
AP6c20.560e.1a30#show ipv6 mobile pmipv6 mag stats
----------------------------------------
[AP6c20.560e.1a30]: Total Bindings      : 1
[AP6c20.560e.1a30]: PBU Sent            : 3
[AP6c20.560e.1a30]: PBA Rcvd            : 3
[AP6c20.560e.1a30]: PBRI Sent           : 0
[AP6c20.560e.1a30]: PBRI Rcvd           : 0
[AP6c20.560e.1a30]: PBRA Sent           : 0
[AP6c20.560e.1a30]: PBRA Rcvd           : 0
[AP6c20.560e.1a30]: No Of handoff       : 0
Detailed Statistics Information
[AP6c20.560e.1a30]: PBU Dropped         : 0
-------------------------------------------------
Proxy Binding Acknowledgment Received Stats
Total                         : 3       Drop                          : 0
BA_ACCEPTED                   : 3       BA_UNKNOWN                    : 0
BA_UNSPEC_FAIL                : 0       BA_ADMIN_FAIL                 : 0
…/…
```

PMIPv6 Verification

Complete output

pmipv6showapmagstatsdomain.txt

- show commands on AP for the PMIPv6 feature:

```
AP6c20.560e.1a30#show ipv6 mobile pmipv6 mag stats domain DOM-1 peer lma1
----------------------------------------
[AP6c20.560e.1a30]: PBU Sent              : 3
[AP6c20.560e.1a30]: PBA Rcvd              : 3
[AP6c20.560e.1a30]: PBRI Sent             : 0
[AP6c20.560e.1a30]: PBRI Rcvd             : 0
[AP6c20.560e.1a30]: PBRA Sent             : 0
[AP6c20.560e.1a30]: PBRA Rcvd             : 0
[AP6c20.560e.1a30]: No Of handoff         : 0
Detailed Statistics Information
[AP6c20.560e.1a30]: PBU Dropped           : 0
-------------------------------------------------
Proxy Binding Acknowledgment Received Stats
Total                            : 3       Drop                           : 0
BA_ACCEPTED                      : 3       BA_UNKNOWN                     : 0
…/…
```

PMIPv6 Verification

- show commands on AP for the PMIPv6 feature:

```
AP6c20.560e.1a30#show ipv6 mobile pmipv6 mag tunnel
----------------------------------------------------
[AP6c20.560e.1a30] Tunnel Information
Peer [lma1] : Tunnel Bindings 1
  Tunnel0:
        src 9.19.14.224, dest 9.7.53.201
        encap GRE/IP, mode reverse-allowed
        Outbound Interface BVI1
    3 packets input, 376 bytes, 0 drops
    6 packets output, 536 bytes
```

PMIPv6 Troubleshooting

- Debug commands on WLC for the PMIPv6 feature:

```
(Cisco Controller) >debug proxy-mobility events enable
PMIPv6 MAG Event debug is turned on
PMIPv6 MAG Event debug is turned on
PMIPv6 MAG Event debug is turned on
PMIPv6 MAG Event debug is turned on

(Cisco Controller) >debug proxy-mobility errors enable

(Cisco Controller) >debug proxy-mobility detail enable
PMIPv6 MAG INFO debug is turned on
PMIPv6 MAG INFO debug is turned on
PMIPv6 MAG INFO debug is turned on
PMIPv6 MAG INFO debug is turned on
PMIPv6 PKT debug is turned on
PMIPv6 PKT debug is turned on
PMIPv6 PKT debug is turned on
PMIPv6 PKT debug is turned on
```

PMIPv6 Troubleshooting

- Debug commands on WLC for the PMIPv6 feature:

```
(Cisco Controller) >debug proxy-mobility detail enable
[PMIPV6_MAG_EVENT]: Trigger request received (L2 Detach trigger) from (srini1)
*PMIPV6_Thread_2: Jun 27 23:32:48.413: [PA]
[PMIPV6_PDB_INFO]: MN entry srini1:prof-1 found in hashset
*PMIPV6_Thread_2: Jun 27 23:32:48.413: [PA]
[PMIPV6_BINDING_API]: pmipv6_get_binding API called
*PMIPV6_Thread_2: Jun 27 23:32:48.413: [PA]
[PMIPV6_BINDING_INFO_KEY]: Keytype as NAI. NAI: srini1
*PMIPV6_Thread_2: Jun 27 23:32:48.413: [PA]
[PMIPV6_BINDING_INFO]: binding found on NAI tree
*PMIPV6_Thread_2: Jun 27 23:32:48.413: [PA]
[PMIPV6_MAG_EVENT]: Trigger detach request received
*PMIPV6_Thread_2: Jun 27 23:32:48.413: [PA]
[PMIPV6_MAG_API]: mag_bul_do_state_transition API called
*PMIPV6_Thread_2: Jun 27 23:32:48.413: [PA]
[PMIPV6_MAG_EVENT]: Event received Old MN intf detached in state: ACTIVE, new state:
Disconnecting
```

PMIPv6 Troubleshooting

Complete output

pmipv6debugwlc1.txt

- Debug commands on WLC for the PMIPv6 feature:

```
(Cisco Controller) >debug client 7c:d1:c3:7f:1f:24
*apfMsConnTask_2: Jun 27 23:30:34.933: [PA] 7c:d1:c3:7f:1f:24 apfApplyWlanPolicy: Apply WLAN Policy over
PMIPv6 Client
Mobility Type
*apfMsConnTask_2: Jun 27 23:30:34.933: [PA] 7c:d1:c3:7f:1f:24 In processSsidIE:5679 setting Central switched
to TRUE
*apfMsConnTask_2: Jun 27 23:30:34.933: [PA] 7c:d1:c3:7f:1f:24 In processSsidIE:5682 apVapId = 3 and Split
Acl Id = 65535
*apfMsConnTask_2: Jun 27 23:30:34.933: [PA] 7c:d1:c3:7f:1f:24 Applying site-specific Local Bridging override
for station

7c:d1:c3:7f:1f:24 - vapId 3, site 'Flex', interface 'management`
…/…
```

PMIPv6 Troubleshooting

- Debug commands on WLC for the PMIPv6 feature:

```
*PMIPV6_Thread_2: Jun 27 23:30:37.845: [PA] 7c:d1:c3:7f:1f:24 Pmip mag config, ip = 20.10.0.135, mask =
0.0.0.16, dflt-
gw = 20.10.0.1, dns = 64.72.88.90, lease-time = 3600, upstream-key = 134, downstream-key = 131 tunnel-index
= (ni
*PMIPV6_Thread_2: Jun 27 23:30:37.845: [PA] 7c:d1:c3:7f:1f:24 20.10.0.135 DHCP_REQD (7) Replacing Fast Path
rule type = Airespace AP - Learn IP address on AP 34:a8:4e:ba:02:f0, slot 1, interface = 13, QOS = 0
  IPv4 ACL ID =
*PMIPV6_Thread_2: Jun 27 23:30:37.845: [PA] 7c:d1:c3:7f:1f:24 20.10.0.135 DHCP_REQD (7) Fast Path rule
(contd...) 802.1P
= 0, DSCP = 0, TokenID = 15206, IntfId = 0  Local Bridging Vlan = 91, Local Bridging intf id = 0
*PMIPV6_Thread_2: Jun 27 23:30:37.845: [PA] 7c:d1:c3:7f:1f:24 20.10.0.135 DHCP_REQD (7) Fast Path rule
(contd...) AVC  Ratelimit:  AppID = 0 ,AppAction = 0, AppToken = 15206  AverageRate = 0, BurstRate = 0
*PMIPV6_Thread_2: Jun 27 23:30:37.845: [PA] 7c:d1:c3:7f:1f:24 20.10.0.135 DHCP_REQD (7) Fast Path rule
(contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 0, AppToken = 15206  AverageRate = 0, BurstRate = 0
*PMIPV6_Thread_2: Jun 27 23:30:37.845: [PA] 7c:d1:c3:7f:1f:24 20.10.0.135 DHCP_REQD (7) Fast Path rule
(contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 0, AppToken = 15206  AverageRate = 0, BurstRate = 0
*PMIPV6_Thread_2: Jun 27 23:30:37.845: [PA] 7c:d1:c3:7f:1f:24 20.10.0.135 DHCP_REQD (7) Successfully plumbed
mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
…/…
*DHCP Server: Jun 27 23:30:39.006: [PA] 7c:d1:c3:7f:1f:24 Accounting NAI-Realm: srini1, from Mscb username :
srini1
*DHCP Proxy Task: Jun 27 23:30:39.007: [PA] 7c:d1:c3:7f:1f:24 Assigning Address 20.10.0.135 to PMIP client
```

PMIPv6 Troubleshooting

- Debug commands on WLC for the PMIPv6 feature:

```
*PMIPV6_Thread_2: Jun 27 23:32:45.359: [PA]
[PMIPV6_PDB_API]:pmipv6_pdb_clear_dynamic_mn
<Srini> this is for clearing the mobile node from the pmip database when the client leaves

[PMIPv6_MM] L2 Attach: MN nai:srini1 llid:7cd1.c37f.1f24 formatted_nai:srini1:prof-1
<Srini> L2 Attach is when a client joins, a unique GRE Key allocated for the client and session is
established between the client and LMA and all client traffic is tunnelled to LMA
[Durga] L2 Attach is a keyword in case of WLC MAG for sending the PBU message to LMA.
It is called L2 Attach here since the PBU is triggered when the L2 Authentication is completed for the
wireless client. In case of wired world, PBU is triggered as part of DHCP Discover message.

*PMIPV6_Thread_2: Jun 27 23:32:48.413: [PA]
[PMIPV6_MAG_EVENT]: Trigger request received (L2 Detach trigger) from (srini1)
 <Srini> L2 Detach is triggered when a client leaves/LMA clears the entry in its database
[Durga] L2 Detach is a keyword in WLC MAG for PBU de-registration message. WLC sends a (L2 Detach or) PBU
De-registration message to LMA when the client is removed from WLC in following cases –
Idle timeout for client  2) WLAN disable  3) Client de-authentication from WLC CLI.

*PMIPV6_Thread_2: Jun 27 23:32:48.413: [PA]
[PMIPV6_PDB_INFO]: MN entry srini1:prof-1 found in hashset
[Durga] This is internal to code, to make sure pmip profile exists in database.
```

PMIPv6 Troubleshooting

- Debug commands on WLC for the PMIPv6 feature:

```
*PMIPV6_Thread_2: Jun 27 23:32:48.413: [PA]
[PMIPV6_MAG_EVENT]: Trigger detach request received
<Srini> L2 Detach is triggered when a client leaves/LMA clears the entry in its database

PMIPV6_Thread_2: Jun 27 23:32:48.413: [PA]
[PMIPV6_MAG_API]: mag_bul_do_state_transition API called
[Durga] This is an internal MAG API to handle PMIPv6 client state machine.

*PMIPV6_Thread_2: Jun 27 23:32:48.413: [PA]
[PMIPV6_MAG_EVENT]: Event received Old MN intf detached in state: ACTIVE, new state: Disconnecting
[Durga] This is a debug message within the state machine to indicate the client is moving from ACTIVE state
to Disconnecting state.

*PMIPV6_Thread_2: Jun 27 23:32:48.413: [PA]
[PMIPV6_MAG_INFO]: PBU message nai(srini1.starent.com), nai len: 7, hoa(336199815), att(4)
llid(7cd1.c37f.1f24) , ll len: 16 seqNo:285
<Srini> This is PBU message sent from WLC to LMA on client successful authentication. It has the NAI, Realm,
Home Address and Local Link ID.
```

PMIPv6 Troubleshooting

- Debug commands on AP for the PMIPv6 feature:

```
AP7cad.74ff.36d2#debug  capwap flexconnect pmipv6
Capwap REAP PMIPv6 debugging is on
AP7cad.74ff.36d2#debug  ipv6 mobile packets
AP7cad.74ff.36d2#debug  ipv6 mobile mag ?
  all     all debug message (event and info)
  api     api Debugging
  events  event Debugging
  info    info Debugging
  <cr>
AP7cad.74ff.36d2#debug ip access-list internal
AP7cad.74ff.36d2#debug ip access-list dynamic
AP7cad.74ff.36d2#debug  route-map api
Routemap related API debugging is on
AP7cad.74ff.36d2#debug  ip policy
Policy routing debugging is on
```

PMIPv6 Design Considerations in 8.0

PMIPv6 Design Considerations in 8.0

- MAG on AP is supported on:

  WLC 5500, 7500, 8500, WiSM2 and **AP** 1140, 3500, 3600, 3700, 2600, 1600, CAPRI, 1530, 1550 (128MB RAM)
- Client SSO is supported
  - Client session is maintained on the AP when controller switches over
- MAG on AP is only available for FlexConnect Local Switching/Central Authentication
  - No support on mesh/bridge, local mode, or flex with central switching and local auth
- FSR with MAG on AP only possible in Central Association mode
- IPv4 only support (both clients and transport) – no IPv6 support
- No Multicast or Broadcast support (ARP, DHCP get special treatment)
- MAG-LMA tunnels are static when the WLC is the MAG
- Dynamic MAG-LMA tunnel establishment is supported with MAG on the AP
- No overlapping IP address support in MAG on the AP

PMIPv6 Design Considerations in 8.0

- PMIPv6 is supported with web-Auth clients
- PMIPv6 is supported for clients with Dot1x Authentication. Once the Dot1x Authentication is complete, AP will start the PMIPv6 signaling for the client
- Fast roaming is supported when central association is enabled on the WLAN.
  - When central association is enabled, all key caching will happen on the WLC. When the PMIPv6 client is roamed from one AP to another on the same mobility domain, WLC will send the client PMIPv6 parameters to the new AP in PMIPv6 Tunnel payload to start PMIPv6 signaling. Also, the WLC will send the PMIPv6 Tunnel payload to the old AP to tear-down the GRE tunnel for the client with the LMA. Fast roaming will be supported in both Intra and Inter-WLC roaming scenarios and mobility messages will be added to send PMIPv6 parameters from one WLC to another during roam.
- Fast roaming will not be supported when central association is disabled. In this case, association is handled by the AP and the key caching happens within the AP group.

PMIPv6 Design Considerations in 8.0

- When the Flex-connect AP moves from CAPWAP connected to Stand-alone mode, all existing PMIPv6 clients will continue to pass data traffic, till they are getting de-auth or dis-associated. In stand-alone mode, no new clients will be associated to the AP in PMIPv6 enabled WLAN. AP does not send a L2-Detach message to the LMA irrespective of the AP state (connected/standalone), , if a PMIPv6 client moves away from the Flex AP.

- When the AP connectivity to WLC is restored, AP moves to connected mode. At this time AP will inform WLC about all of the existing wireless clients including PMIPv6 clients. Existing PMIPv6 clients will not be dis-connected when the AP moves to connected mode again and traffic from/to PMIPv6 clients will not be disturbed.

- If the AP gets dis-connected from the LMA, all existing PMIPv6 sessions will be broken and all the traffic from the PMIPv6 clients will be dropped on the AP. The PMIPv6 clients will still be associated on the AP and the bindings will be removed from the AP after timeout due to failure during binding refresh.

- MAG on WLC GRE tunnel is initiated with Management Interface only

- When the client is de-authenticated from WLC, PMIPv6 binding is cleared in WLC and vice-versa

8.0 Update – Bonjour, AVC Phase 3; IPv6

Jerome Henry
Technical Marketing Engineer
Enterprise Networking Market Strategy

August 2014

Agenda

- Bonjour Phase 3 Introduction cover in detail
  - Bonjour Policies and ISE
  - Profiles Enhancements
  - My Device Bonjour Portal
  - PI Portal for Instant Services

Agenda

- AVC Phase 3 introduction cover in detail
- AVC AAA Override
- Directional DSCP Configuration
- Integration of AVC Profiles to the Local Policy Classification per User and per Device
- NBAR Engine

Agenda

- IPv6 cover in detail
- Why Now?
- IPv6 Review
- IPv6 in the 8.0 Release: What is Supported and not Supported?
- Monitoring and Troubleshooting Commands

Bonjour Phase 3 – Introduction

Bonjour - 7.4
Phase 1

- Bonjour service with mDNS gateway for wired and wireless services
- Bonjour Service policy applied per Interface, group of interfaces, or per WLAN
- mDNS services cached on the controller
- Bonjour services available on all Controller seen L2 domains
- Bonjour services supported on the Anchor controller
- Bonjour services supported with L2 and L3 roaming
- 100 services and 64 service-providers per service type
- Support of Flex Connect APs in central switching
- Support of mDNS services across L3 domains

Bonjour - 7.5
Phase 2

- Introduction of mDNS AP for Bonjour service snooping on 10 Wired VLANs
- LSS – Location Specific Services
- Priority MAC of Bonjour service
- Origin Based service discovery
- 6400 services and service-providers per service type

Bonjour – 8.0
Phase 3

- Bonjour GW with access policy controlled service discovery
- Device service mapping to access policy
- Bonjour Group and single access policy management
- Bonjour profile control by local policy
- Bonjour Device management from ISE portal
- Introduction of Bonjour admin to manage specific Bonjour services from Cisco Prime

Bonjour Services Enhancements - Phases 1-2

- mDNS Gateway and Bonjour Services snooping
- mDNS -AP
- LSS – Location Specific Services
- Priority MAC of Bonjour service
- Origin Based service discovery

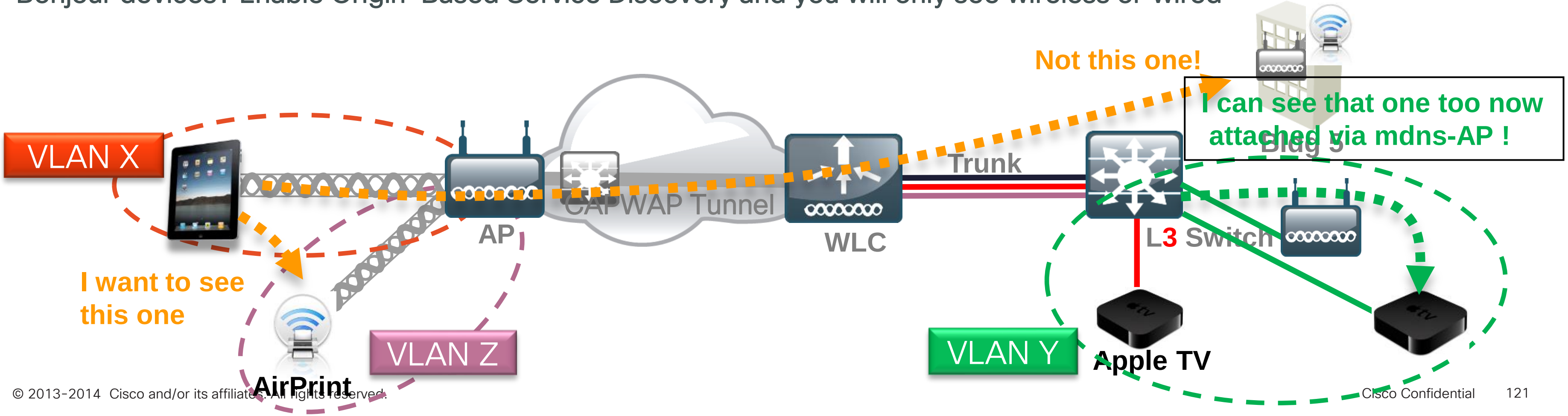
Scaling and Expanding Services

- In 7.4, Cisco worked on mDNS GW on the controller, Service snooping and Unicast responds to Service requests
- In 7.5, Cisco worked on scaling and expanding services:

1. Location Specific Services (LSS): tired of seeing all wireless Apple TVs in the entire campus? Enable “LSS”, and only see the Bonjour devices on the AP you are associated to

2. mDNS AP: In 7.4, wired devices must be on WLC trunk to be seen. In 7.5, Bonjour devices on mdns-AP switch are also listed

3. Origin-Based Service Discovery: only want to see wired Bonjour Devices (including mDNS AP)? Or only wireless Bonjour devices? Enable Origin-Based Service Discovery and you will only see wireless or wired



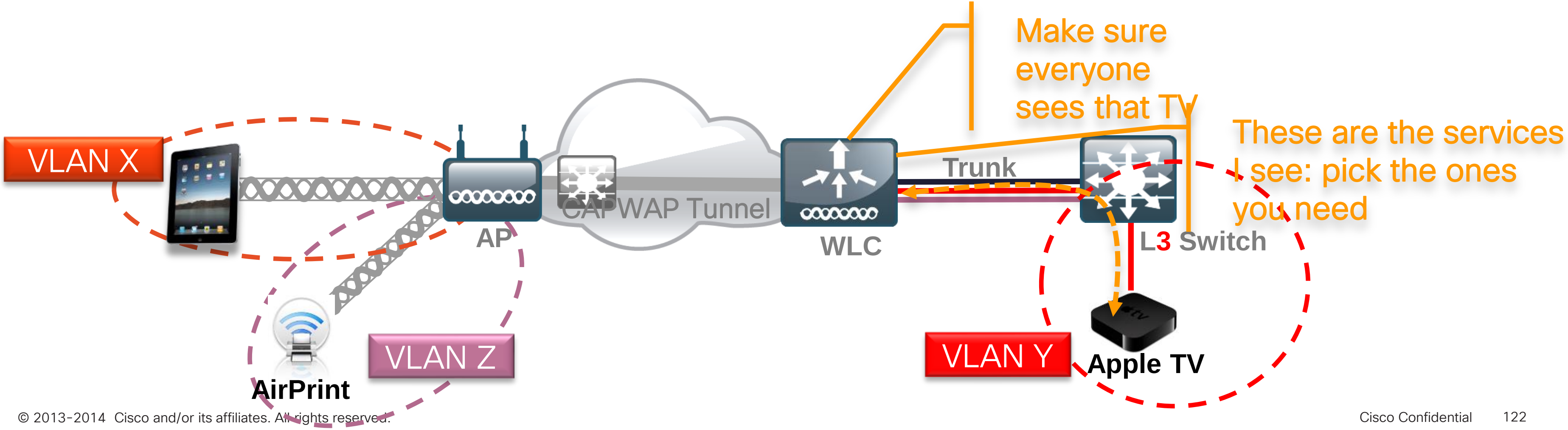
Scaling and Expanding Services (Cont.)

- In 7.5, Cisco worked on scaling and expanding services:

4. Service limit: extended from 100 devices / 64 services to 6400 on 2500,5508,WiSM2 and vWLC and 16000 services on 7510 and 8510 UC Controllers.

5. Priority MAC: (in large campuses), ensures that up to 50 MAC per Service Instance addresses are always listed, even if network contains more than 6400 / 16000 services

6. Bonjour Browser: WLC lists all discovered services, even if you did not configure them (easier to add to the WLC service list)



Make sure everyone sees that TV

These are the services I see: pick the ones you need

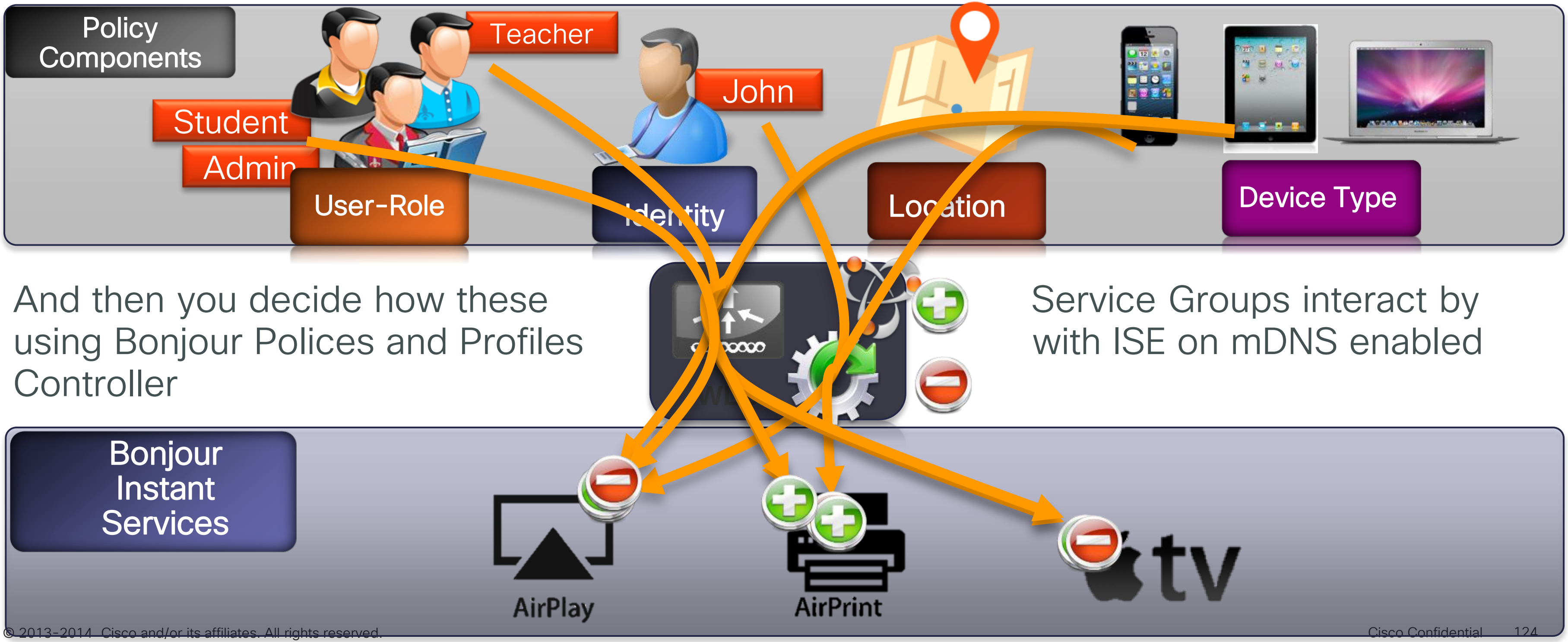
Bonjour Phase 3

- Bonjour Policies and ISE
- Profiles Enhancements

8.0 Bonjour Service Control

Organize by using policies

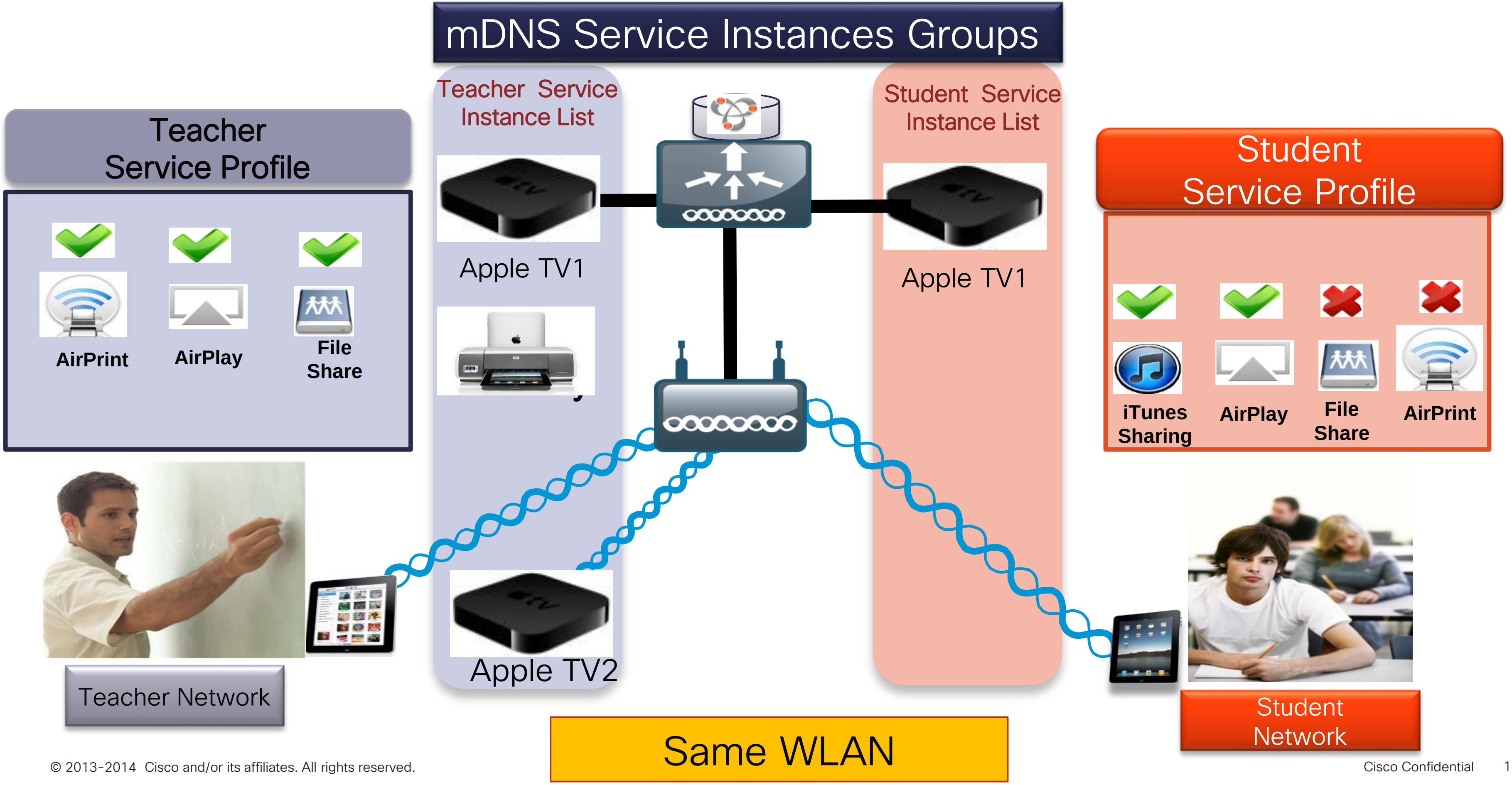
- In 8.0 you can create Service Groups: Users (roles and identity), Devices, Service



- And then you decide how these using Bonjour Polices and Profiles Controller

Service Groups interact by with ISE on mDNS enabled

Bonjour Policy Example for Education



mDNS Service Instances Groups

Teacher Service Instance List

Apple TV1

Apple TV2

Student Service Instance List

Apple TV1

Teacher Service Profile

✓ AirPrint

✓ AirPlay

✓ File Share

Student Service Profile

✓ iTunes Sharing

✓ AirPlay

✗ File Share

✗ AirPrint

Teacher Network

Student Network

Same WLAN

Bonjour Policy Enhancements in 8.0

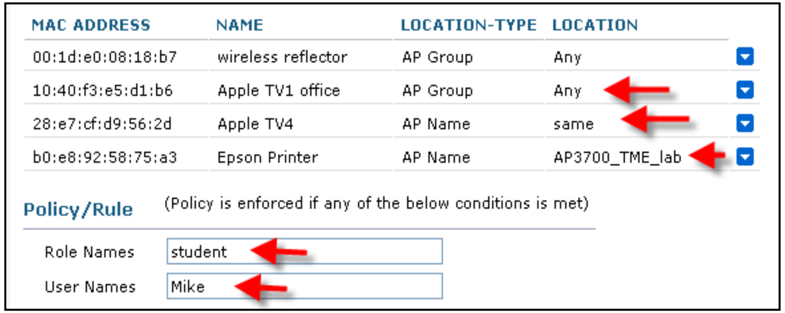
- Location and role filtering in release 8.0
- Bonjour policies allow creation of the mDNS Service Groups and Service Instances within the Group
- Service Instance mandates how the service instance is shared by configuring
  - **MAC address** of the Service Instance
  - **Name** of the Service Instance
  - **Location Type** Of the Services Instance by **AP Group, AP Name** or **AP Location**
  - **Location configuration** allows access the "service instance" i.e. client location
    - *Location configuration applied to wired and wireless instances of all services and printers as in **Any, Same** or one **AP Name.***
    - *This allows selective sharing of service instances based on the location and rule (=user-id and role) on the **Same WLAN***

Bonjour Policy Enhancements in 8.0

- Service Instance associated with mac address can be configured in multiple service groups
  - Currently we support a maximum of 5 service groups for a single mac address.
  - Service group configurations can be done even when mDNS snooping is disabled
  - Number of Service instances per Service group is limited 100 and maximum of 100 service-group can be created

- Location Filtering of Service instance can be limited by following attributes:

- "any" –clients from any location can access the service subject to **role** or **user-id** credentials being allowed by the policy associated with the service group for the said mac address.
- "same" - only clients from the SAME location (same AP-GROUP or AP-NAME or AP-LOCATION as per config) as that of the device can access that Service Instance publishing the service can access the service. Applicable for wireless only.
- "ap-name" – only clients associated to that AP can access the Service Instance



MAC ADDRESS	NAME	LOCATION-TYPE	LOCATION
00:1d:e0:08:18:b7	wireless reflector	AP Group	Any
10:40:f3:e5:d1:b6	Apple TV1 office	AP Group	Any
28:e7:cf:d9:56:2d	Apple TV4	AP Name	same
b0:e8:92:58:75:a3	Epson Printer	AP Name	AP3700_TME_lab

Policy/Rule (Policy is enforced if any of the below conditions is met)

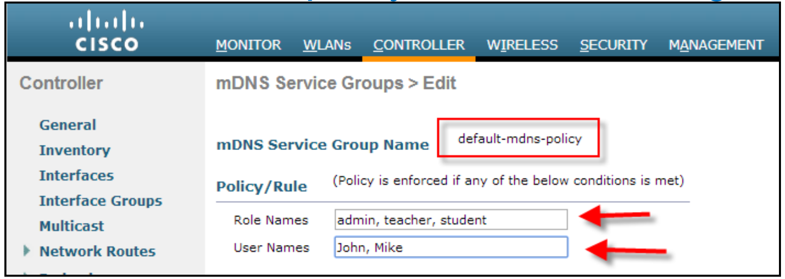
Role Names: student

User Names: Mike

Bonjour Policy Enhancements in 8.0

- Allows articulation as "**service instance**" is shared with whom, i.e., **user-id**, "service instance is shared with which **role**/s", i.e., teacher or student
- With Bonjour access policy there will now be two levels of filtering client queries
  1. At the service type level by using the mDNS profile
     - ➢ mDNS profile can be user specific and be overridden with ISE "**av-pair** "returned to WLC that overrides default profile
  2. At the Service Instance level using the access policy associated with each Service Instance.

Note: Service instances which are not configured with any access policy will be mapped to the default access policy that allows configured <roles/names> to receive the service instances



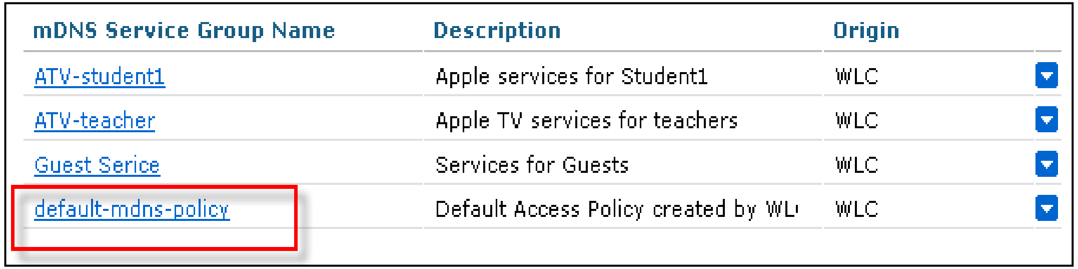
mDNS Service Groups > Edit

mDNS Service Group Name: default-mdns-policy

Policy/Rule (Policy is enforced if any of the below conditions is met)

Role Names: admin, teacher, student

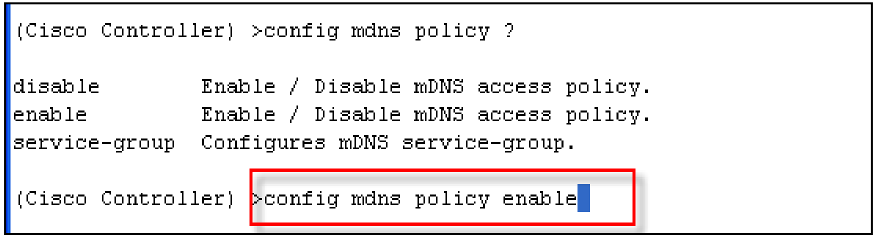
User Names: John, Mike



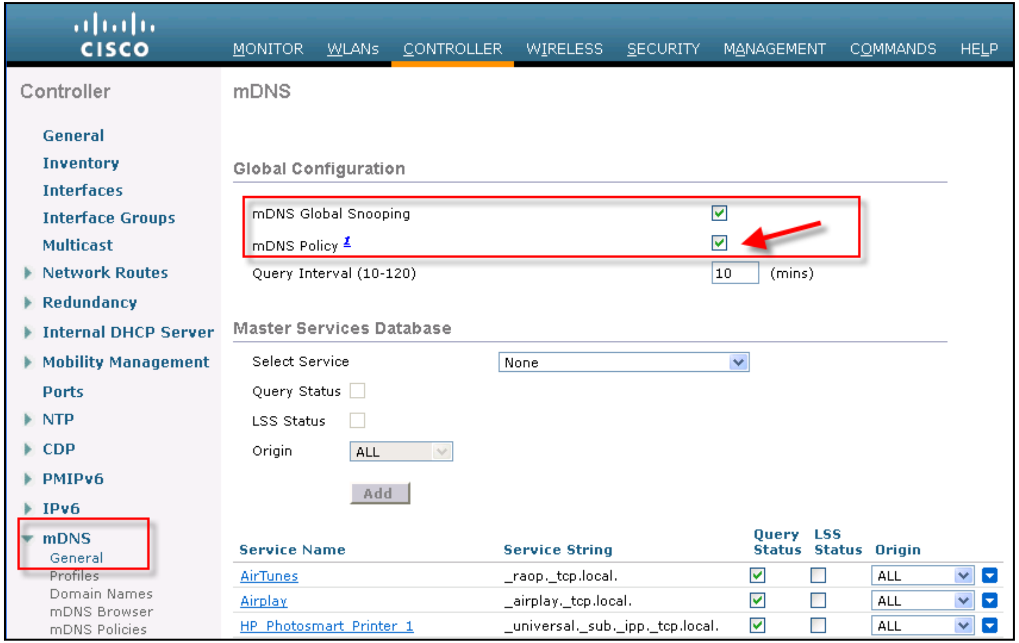
mDNS Service Group Name	Description	Origin	
ATV-student1	Apple services for Student1	WLC	▼
ATV-teacher	Apple TV services for teachers	WLC	▼
Guest Serice	Services for Guests	WLC	▼
default-mdns-policy	Default Access Policy created by WL	WLC	▼

Bonjour Policy Configuration

1. Enable mDNS policy on the controller from GUI or CLI



```
(Cisco Controller) >config mdns policy ?

disable        Enable / Disable mDNS access policy.
enable         Enable / Disable mDNS access policy.
service-group  Configures mDNS service-group.

(Cisco Controller) >config mdns policy enable
```



mDNS

Global Configuration

mDNS Global Snooping ☑

mDNS Policy [1] ☑

Query Interval (10-120) 10 (mins)

Master Services Database

Select Service None

Query Status □

LSS Status □

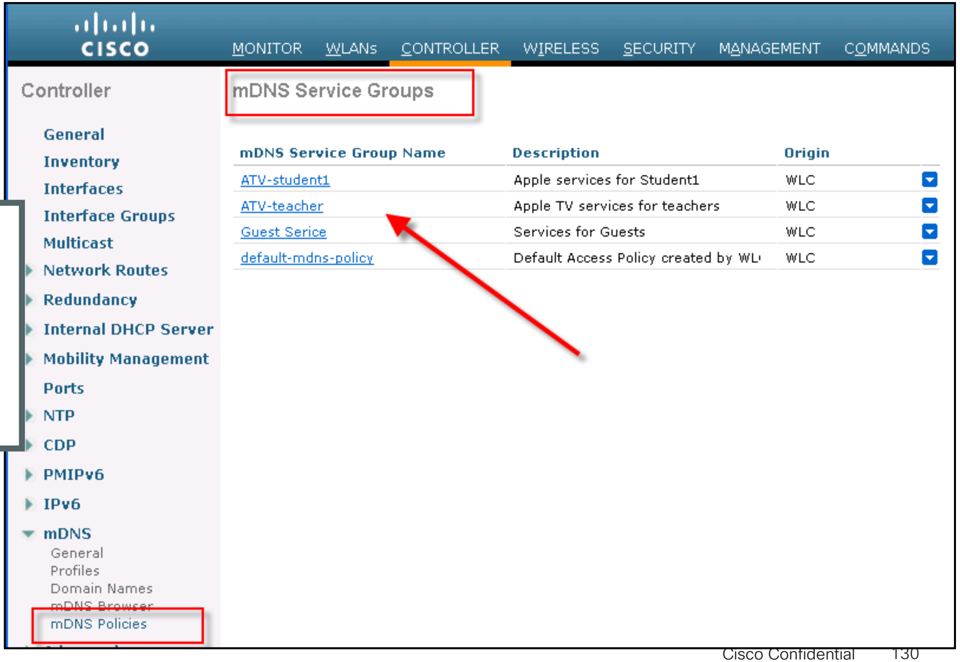
Origin ALL

Service Name	Service String	Query Status	LSS Status	Origin
AirTunes	_raop._tcp.local.	☑	□	ALL
Airplay	_airplay._tcp.local.	☑	□	ALL
HP_Photosmart_Printer_1	_universal._sub._ipp._tcp.local.	☑	□	ALL

Bonjour Policy Configuration

2. Create mDNS Service Group

```
(Cisco Controller) >config mdns policy service-group ?

create          Creates a mDNS service-group.
delete          Deletes a mDNS service-group.
device-mac      Add/Delete device-mac to service-group.
user-name       Add/Delete user name to service-group.
user-role       Add/Delete user role to service-group.
```

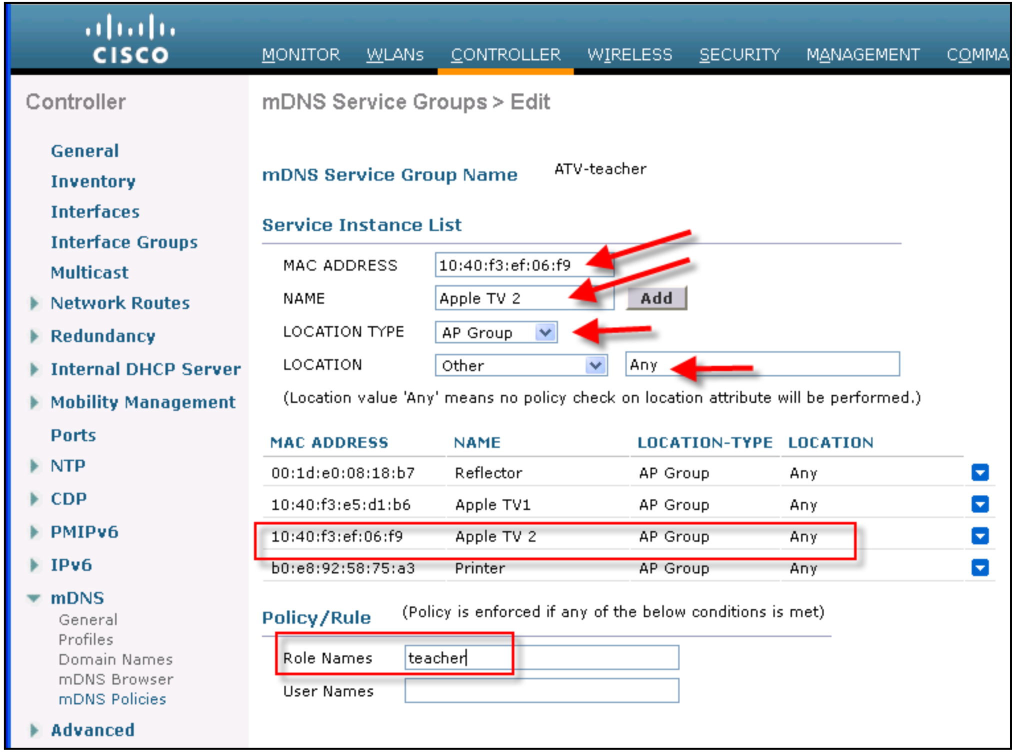


mDNS Service Groups

mDNS Service Group Name	Description	Origin
ATV-student1	Apple services for Student1	WLC
ATV-teacher	Apple TV services for teachers	WLC
Guest Serice	Services for Guests	WLC
default-mdns-policy	Default Access Policy created by WL	WLC

Bonjour Policy Configuration

3. Configure Service Instances in the mDNS group, and role



mDNS Service Groups > Edit

mDNS Service Group Name ATV-teacher

Service Instance List

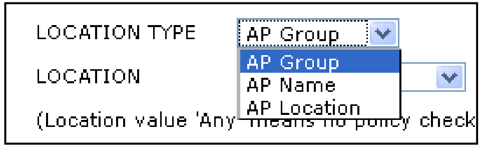
MAC ADDRESS	10:40:f3:ef:06:f9	
NAME	Apple TV 2	
LOCATION TYPE	AP Group	
LOCATION	Other	Any

(Location value 'Any' means no policy check on location attribute will be performed.)

MAC ADDRESS	NAME	LOCATION-TYPE	LOCATION
00:1d:e0:08:18:b7	Reflector	AP Group	Any
10:40:f3:e5:d1:b6	Apple TV1	AP Group	Any
10:40:f3:ef:06:f9	Apple TV 2	AP Group	Any
b0:e8:92:58:75:a3	Printer	AP Group	Any

Policy/Rule (Policy is enforced if any of the below conditions is met)

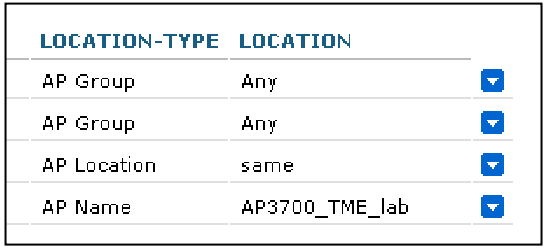
Role Names	teacher
User Names	



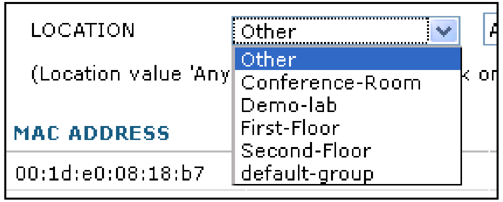
LOCATION TYPE AP Group

LOCATION

(Location value 'Any' means no policy check



LOCATION-TYPE	LOCATION
AP Group	Any
AP Group	Any
AP Location	same
AP Name	AP3700_TME_lab



LOCATION Other

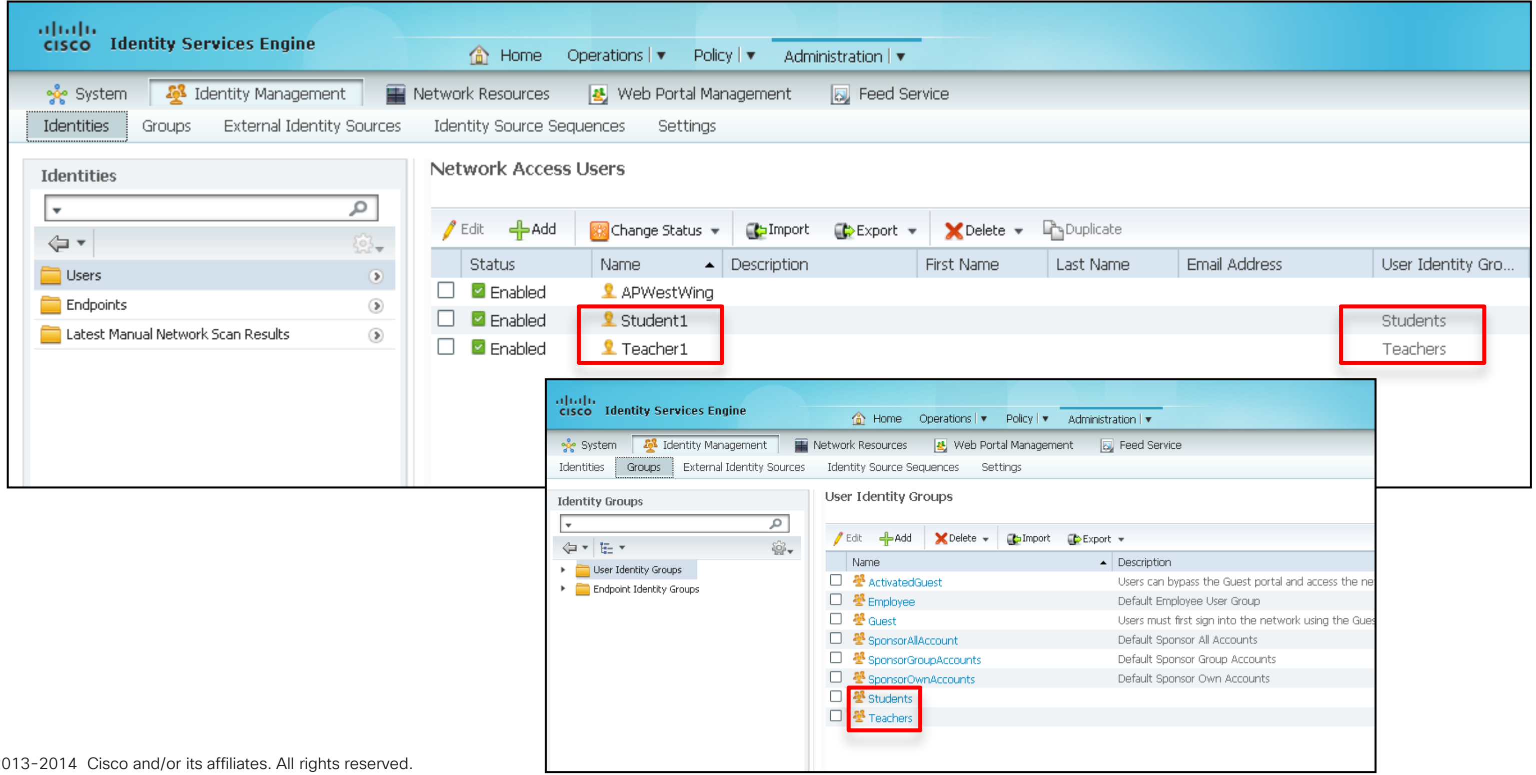
(Location value 'Any

MAC ADDRESS

00:1d:e0:08:18:b7

Bonjour Policy Configuration

4. On ISE, define users and group



Network Access Users

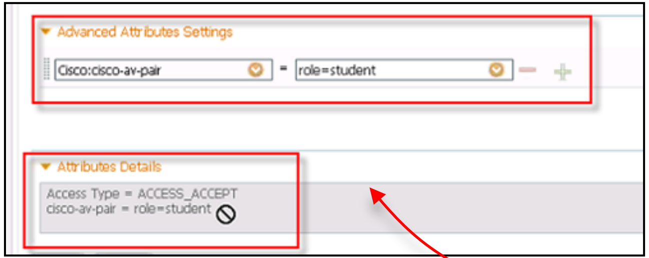
	Status	Name	Description	First Name	Last Name	Email Address	User Identity Gro...
☐	☑ Enabled	APWestWing					
☐	☑ Enabled	Student1					Students
☐	☑ Enabled	Teacher1					Teachers

User Identity Groups

	Name	Description
☐	ActivatedGuest	Users can bypass the Guest portal and access the ne
☐	Employee	Default Employee User Group
☐	Guest	Users must first sign into the network using the Gues
☐	SponsorAllAccount	Default Sponsor All Accounts
☐	SponsorGroupAccounts	Default Sponsor Group Accounts
☐	SponsorOwnAccounts	Default Sponsor Own Accounts
☐	Students	
☐	Teachers	

Bonjour Policy Configuration

5. On AAA server, create authorization profiles that send back and AV-pair, that is the mDNS role.

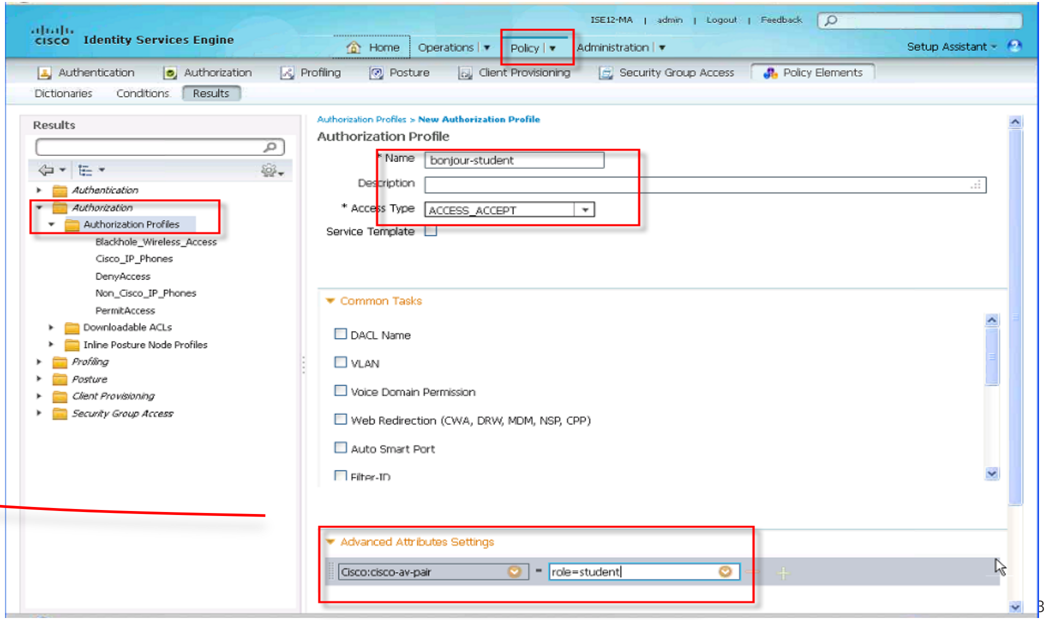


Advanced Attributes Settings

Cisco:cisco-av-pair = role=student

Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = role=student



Authorization Profiles > New Authorization Profile

Authorization Profile

* Name: bonjour-student

Description:

* Access Type: ACCESS_ACCEPT

Service Template □

Common Tasks

□ DACL Name
□ VLAN
□ Voice Domain Permission
□ Web Redirection (CWA, DRW, MDM, NSP, CPP)
□ Auto Smart Port
□ Filter-ID

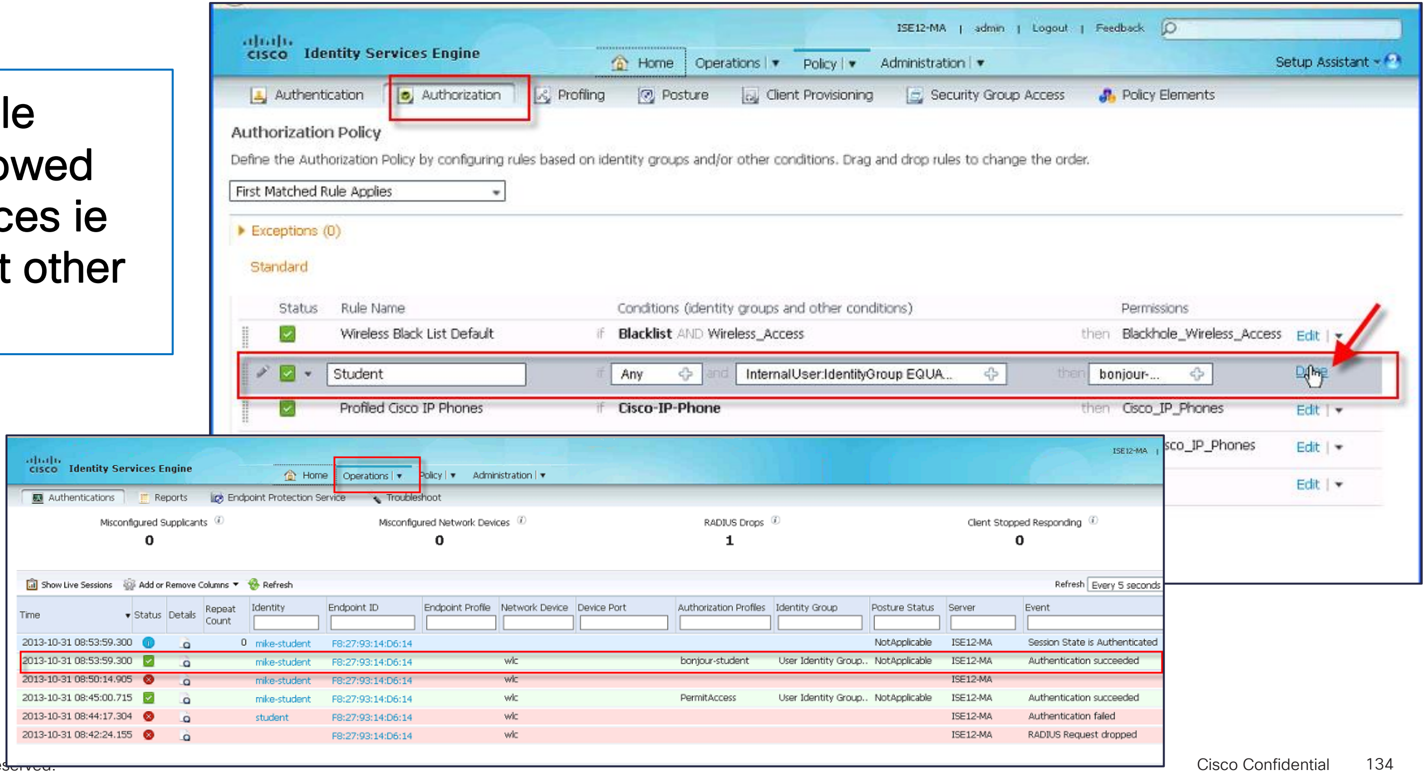
Advanced Attributes Settings

Cisco:cisco-av-pair = role=student

Bonjour Policy Configuration

5. On AAA server, associate user/group IDs to Permissions

Result: User with “role =Student “ will be allowed to use Instance Services ie “bonjour-student” but other won’t



cisco Identity Services Engine
ISE12-MA | admin | Logout | Feedback
Home | Operations ▾ | Policy ▾ | Administration ▾
Setup Assistant ▾
Authentication | Authorization | Profiling | Posture | Client Provisioning | Security Group Access | Policy Elements

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

▸ Exceptions (0)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
✓	Wireless Black List Default	if	Blacklist AND Wireless_Access	then	Blackhole_Wireless_Access	Edit ▾
✓	Student	if	Any and InternalUser:IdentityGroup EQUA...	then	bonjour-...	Done
✓	Profiled Cisco IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phones	Edit ▾
					sco_IP_Phones	Edit ▾
						Edit ▾

cisco Identity Services Engine
ISE12-MA
Home | Operations ▾ | Policy ▾ | Administration ▾
Authentications | Reports | Endpoint Protection Service | Troubleshoot

Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding
0	0	1	0

Show Live Sessions | Add or Remove Columns ▾ | Refresh — Refresh: Every 5 seconds

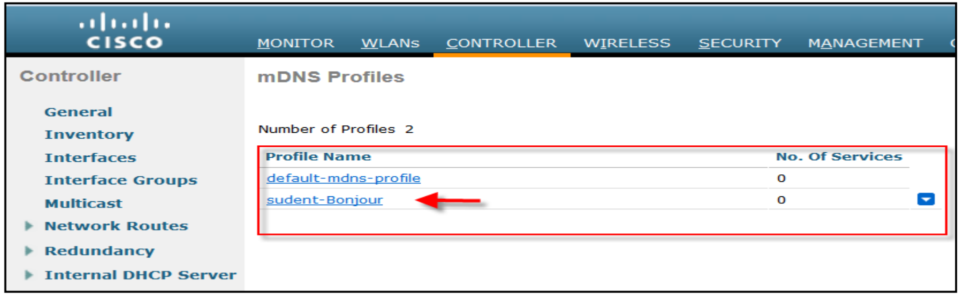
Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status	Server	Event
2013-10-31 08:53:59.300	●		0	mike-student	F8:27:93:14:D6:14						NotApplicable	ISE12-MA	Session State is Authenticated
2013-10-31 08:53:59.300	✓			mike-student	F8:27:93:14:D6:14		wlc		bonjour-student	User Identity Group..	NotApplicable	ISE12-MA	Authentication succeeded
2013-10-31 08:50:14.905	☒			mike-student	F8:27:93:14:D6:14		wlc					ISE12-MA	
2013-10-31 08:45:00.715	✓			mike-student	F8:27:93:14:D6:14		wlc		PermitAccess	User Identity Group..	NotApplicable	ISE12-MA	Authentication succeeded
2013-10-31 08:44:17.304	☒			student	F8:27:93:14:D6:14		wlc					ISE12-MA	Authentication failed
2013-10-31 08:42:24.155	☒				F8:27:93:14:D6:14		wlc					ISE12-MA	RADIUS Request dropped

Bonjour Phase 3

- Bonjour Policies and ISE
- Profiles Enhancements

Bonjour Profile Configuration

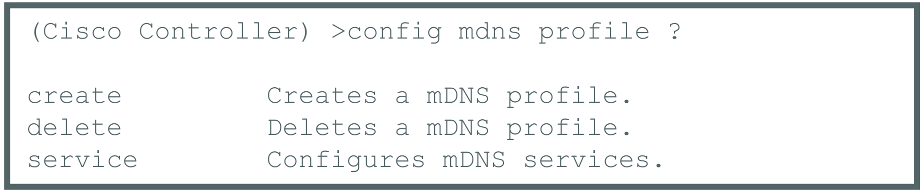
1. You can also create multiple mDNS Profiles on the WLC and override them



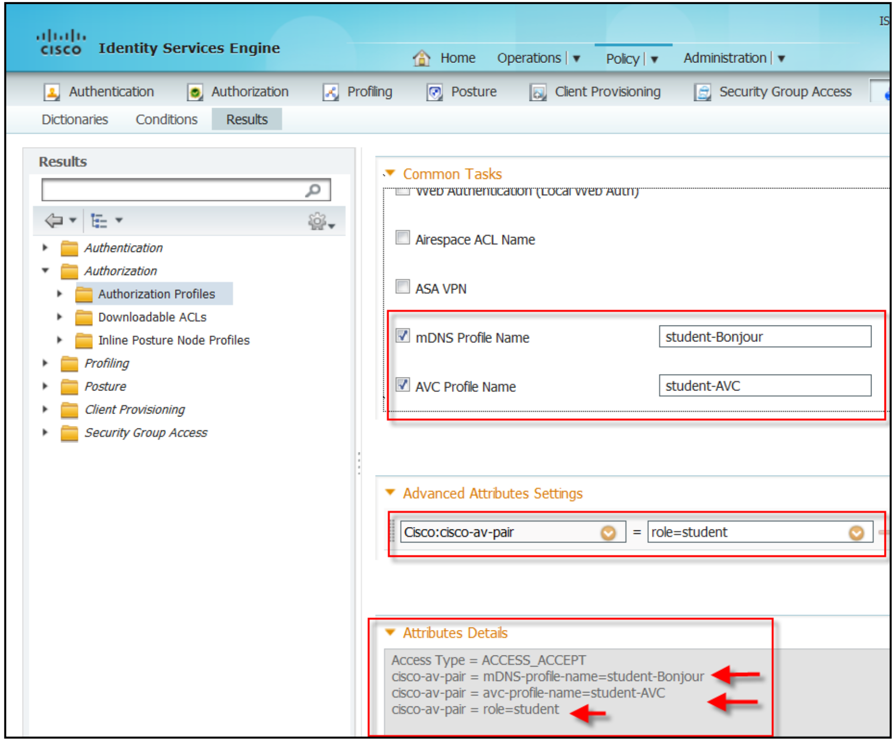
mDNS Profiles

Number of Profiles 2

Profile Name	No. Of Services
default-mdns-profile	0
sudent-Bonjour	0



```
(Cisco Controller) >config mdns profile ?

create         Creates a mDNS profile.
delete         Deletes a mDNS profile.
service        Configures mDNS services.
```



□ Airespace ACL Name

□ ASA VPN

☑ mDNS Profile Name student-Bonjour

☑ AVC Profile Name student-AVC

Advanced Attributes Settings

Cisco:cisco-av-pair = role=student

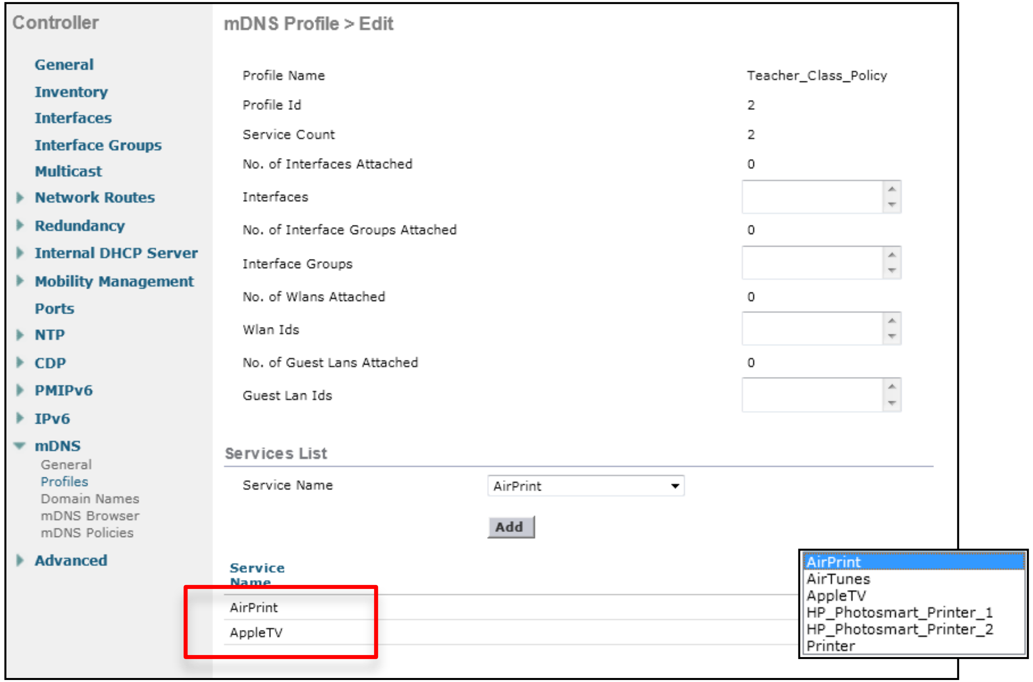
Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = mDNS-profile-name=student-Bonjour
cisco-av-pair = avc-profile-name=student-AVC
cisco-av-pair = role=student

Note: mDNS profile can be user specific and be overridden with AAA "av-pair=mDNS-profile-name" returned to WLC from AAA Server that overrides default profile

Bonjour Profile Configuration

2. Decide what services should be available in this profile



mDNS Profile > Edit

Profile Name	Teacher_Class_Policy
Profile Id	2
Service Count	2
No. of Interfaces Attached	0
Interfaces	
No. of Interface Groups Attached	0
Interface Groups	
No. of Wlans Attached	0
Wlan Ids	
No. of Guest Lans Attached	0
Guest Lan Ids	

Services List

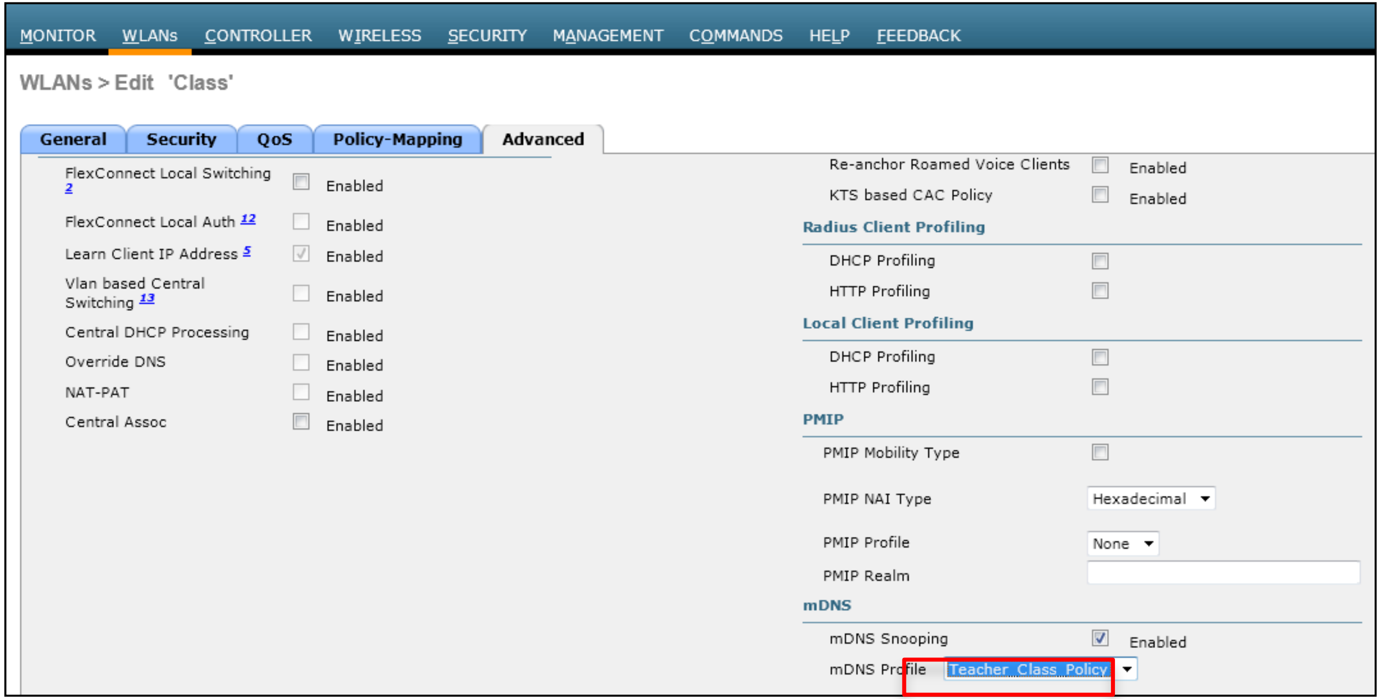
Service Name: AirPrint

Service Name
AirPrint
AppleTV

Bonjour Profile Configuration

3. Attach the profile to your SSID

- This already limits the services that will be available (and visible) to users on this SSID
- Initial filtering function, when some services should be blocked for all on a given SSID



WLANs > Edit 'Class'

FlexConnect Local Switching 2 □ Enabled

FlexConnect Local Auth 12 □ Enabled

Learn Client IP Address 5 ☑ Enabled

Vlan based Central Switching 13 □ Enabled

Central DHCP Processing □ Enabled

Override DNS □ Enabled

NAT-PAT □ Enabled

Central Assoc □ Enabled

Re-anchor Roamed Voice Clients □ Enabled

KTS based CAC Policy □ Enabled

Radius Client Profiling

DHCP Profiling □

HTTP Profiling □

Local Client Profiling

DHCP Profiling □

HTTP Profiling □

PMIP

PMIP Mobility Type □

PMIP NAI Type: Hexadecimal

PMIP Profile: None

PMIP Realm:

mDNS

mDNS Snooping ☑ Enabled

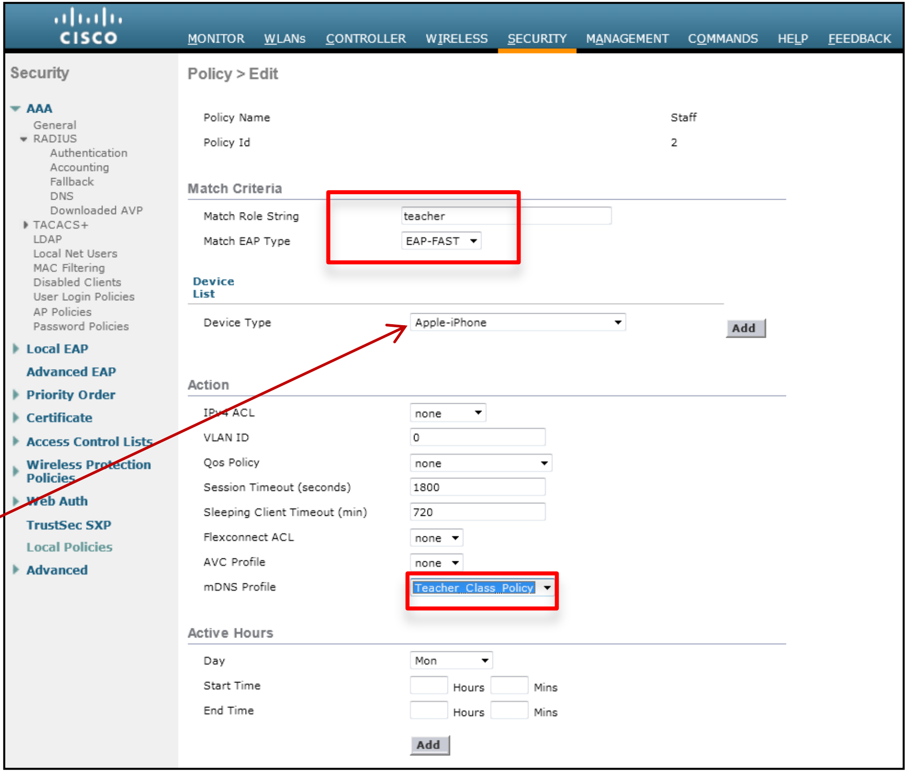
mDNS Profile: Teacher_Class_Policy

Bonjour Profile Enhancements in 8.0

3. You also have an option to attach the profile to a local policy

- Bonjour profile could be attached to a local policy for a client with a particular device type
- This ensures each policy can be configured with a different mDNS profile name and to restrict the user from being able to use the services allowed by the profile

In the example shown – Local Policy limits users with role "teacher" to using Service Group instances on the Apple iPhone devices



Policy > Edit

Policy Name: Staff
Policy Id: 2

Match Criteria

Match Role String: teacher
Match EAP Type: EAP-FAST

Device List

Device Type: Apple-iPhone

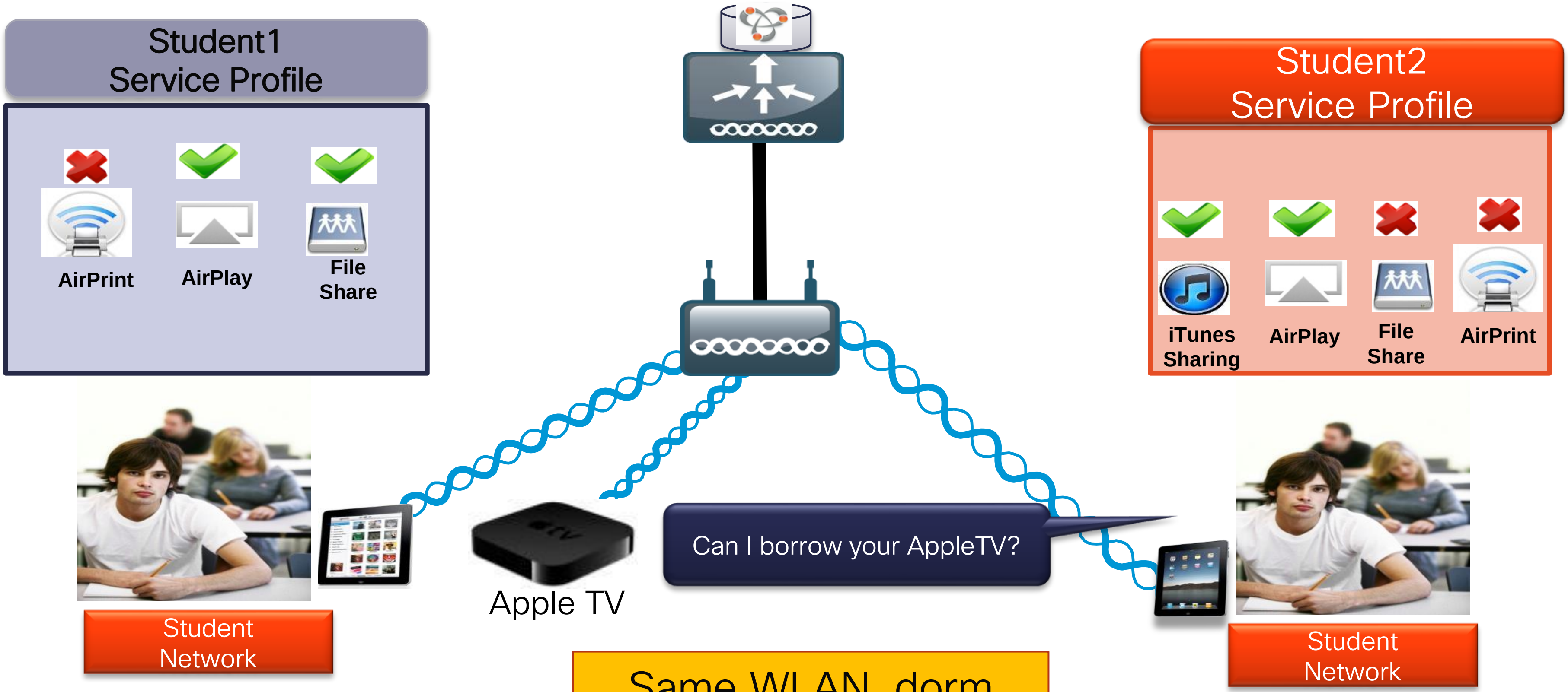
Action

IPv4 ACL: none
VLAN ID: 0
Qos Policy: none
Session Timeout (seconds): 1800
Sleeping Client Timeout (min): 720
Flexconnect ACL: none
AVC Profile: none
mDNS Profile: Teacher_Class_Policy

Active Hours

Day: Mon
Start Time: Hours Mins
End Time: Hours Mins

Bonjour Policy Example for Education



Student1 Service Profile

- ✗ AirPrint
- ✓ AirPlay
- ✓ File Share

Student2 Service Profile

- ✓ iTunes Sharing
- ✓ AirPlay
- ✗ File Share
- ✗ AirPrint

Student Network

Apple TV

Can I borrow your AppleTV?

Student Network

Same WLAN, dorm

AVC Phase 3

Agenda

- AVC Phase 3 introduction
- AVC AAA Override
- Directional DSCP Configuration
- Integration of AVC Profiles to the Local Policy Classification per User and per Device
- NBAR Engine

AVC - 7.4
Phase 1

- Application classification and Control of 1039 applications with NBAR2 engine
- Support of 16 AVC profiles with 32 rules per profile
- One AVC profiles support per WLAN; same profile support on multiple WLANs
- AVC profile mapped to WLAN has a rule for MARK or DROP action
- Graphical presentation on the controller of all classified applications
- One NetFlow exporter and monitor can be configured on WLC
- AVC NetFlow monitoring on PI with PAM license

AVC – 7.5
Phase 2

- Protocol Pack 4.1 Support in AVC phase 2
- Additional application support – total of 1056
- Protocol Pack dynamic load to update applications support

AVC – 8.0
Phase 3

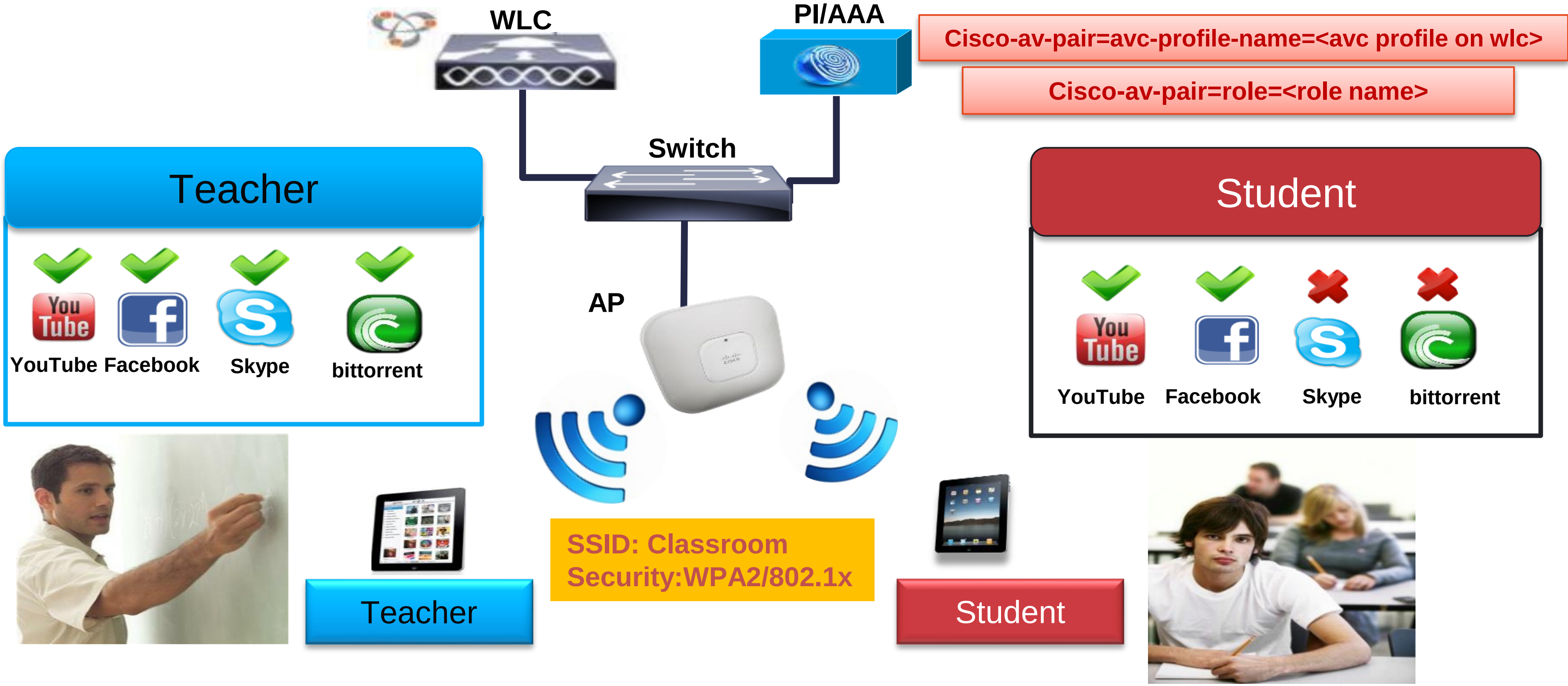
- Protocol Pack 9.0
- NBAR Engine rel 3.1
- AAA AVC Profile over-ride for clients
- AVC Per Application, Per Client based Rate limiting on WLAN
- Integration of AVC profiles to the Local Policy classification per user and per device
- AVC Directional QoS DSCP Marking for Upstream and Downstream traffic
- Support for 1088 applications

AAA AVC Override

AAA AVC Profile Override for Clients

Prior to rel 8.0 AVC Profile is configured on a WLAN and all clients connected to that WLAN would inherit the same AVC profile.

- In Rel 8.0 AAA AVC profile override per clients to obtain different AVC profiles even though they are connected to the same WLAN.
- AAA attribute for client or for a user profile can be configured on AAA servers, e.g. Open Radius/Cisco ACS/ISE.
- The AAA attribute is defined as a generic Cisco “AV-Pair” and can be defined as a string and value pair in AAA.
- The AAA AVC Profile is defined as a Cisco AV Pair. The string is defined as “avc-profile-name” . This has to be configured for any AVC profile existing on the WLC.



WLC

PI/AAA

Cisco-av-pair=avc-profile-name=<avc profile on wlc>

Cisco-av-pair=role=<role name>

Switch

AP

Teacher

✓	✓	✓	✓
YouTube	Facebook	Skype	bittorrent

Student

✓	✓	✗	✗
YouTube	Facebook	Skype	bittorrent

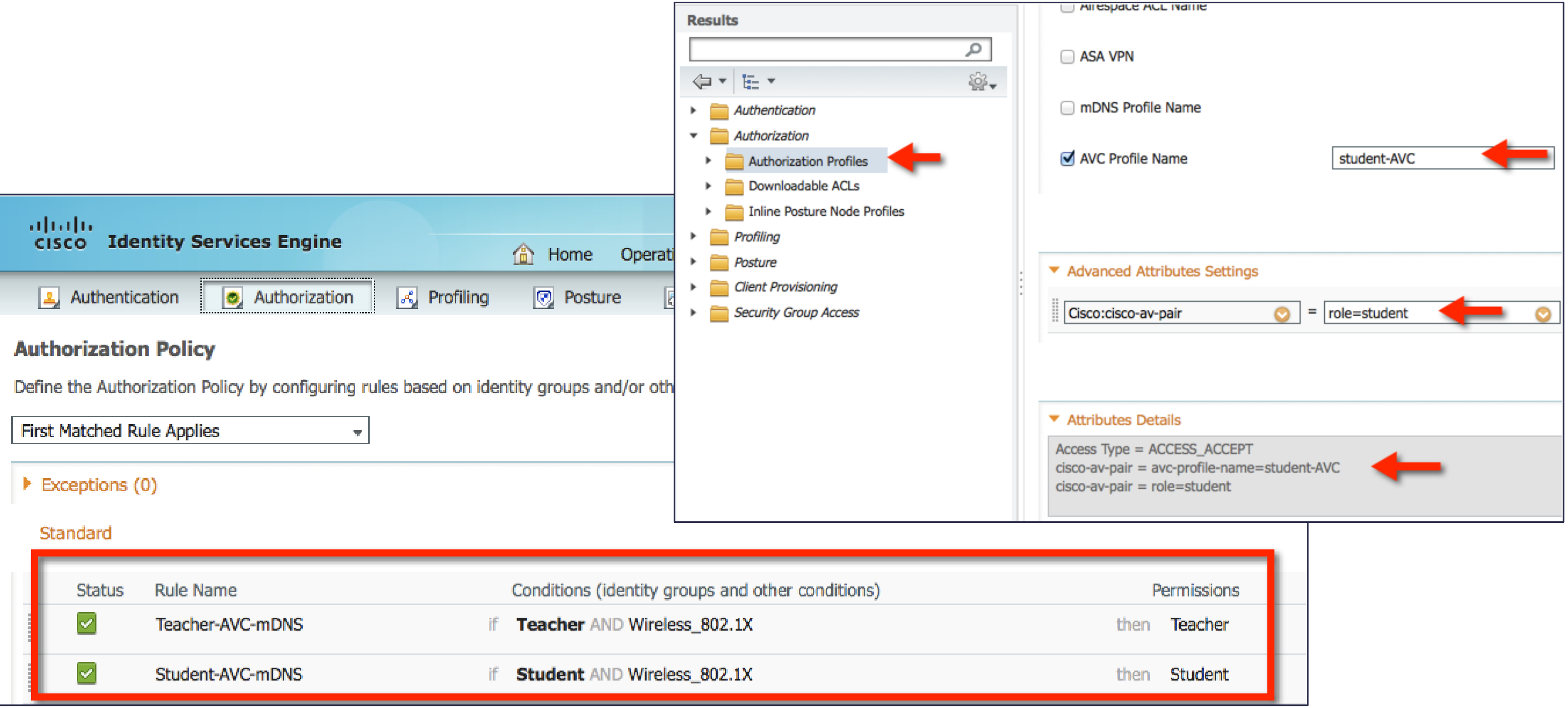
Teacher

SSID: Classroom
Security:WPA2/802.1x

Student

AAA profile enables different users /clients to obtain different mDNS/AVC profiles even though they are connected to same SSID which is tied to the same VLAN

ISE Configuration for AVC



Results

□ Airespace ACL Name

□ ASA VPN

□ mDNS Profile Name

☑ AVC Profile Name: student-AVC

Advanced Attributes Settings

Cisco:cisco-av-pair = role=student

Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = avc-profile-name=student-AVC
cisco-av-pair = role=student
```

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or oth

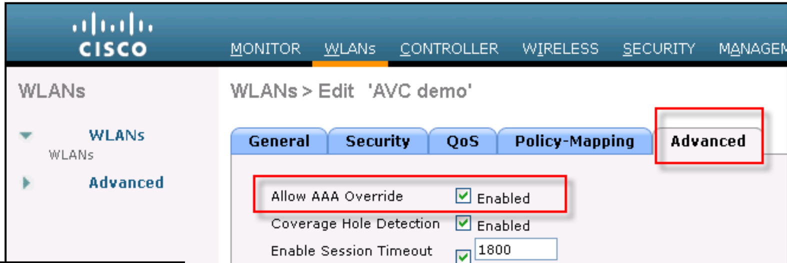
First Matched Rule Applies

Exceptions (0)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	Teacher-AVC-mDNS	if	**Teacher** AND Wireless_802.1X	then	Teacher
✓	Student-AVC-mDNS	if	**Student** AND Wireless_802.1X	then	Student

AVC Configuration for AAA Override Example – Teacher, Student

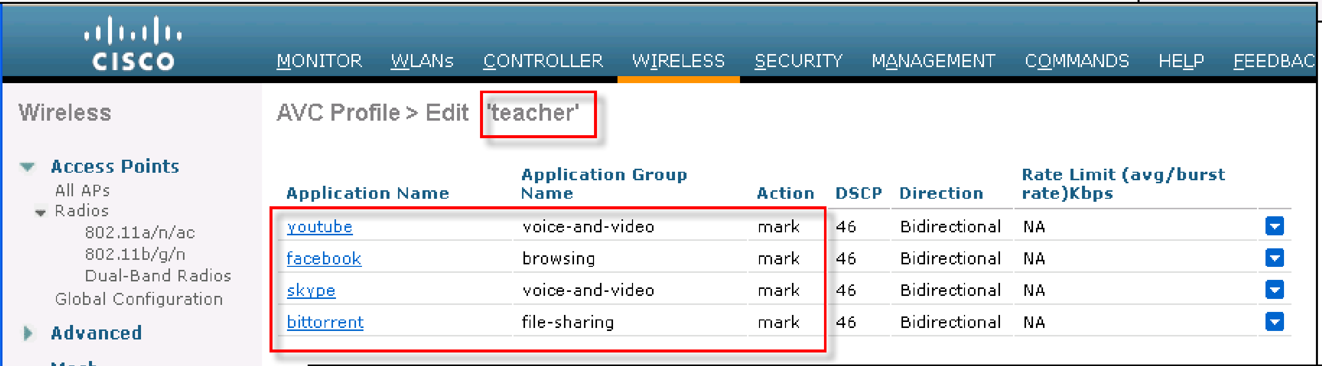


WLANs > Edit 'AVC demo'

Allow AAA Override ☑ Enabled

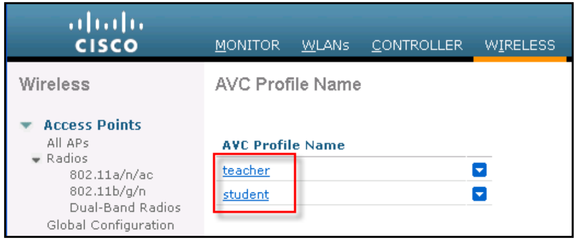
Coverage Hole Detection ☑ Enabled

Enable Session Timeout ☑ 1800 Session Timeout (secs)



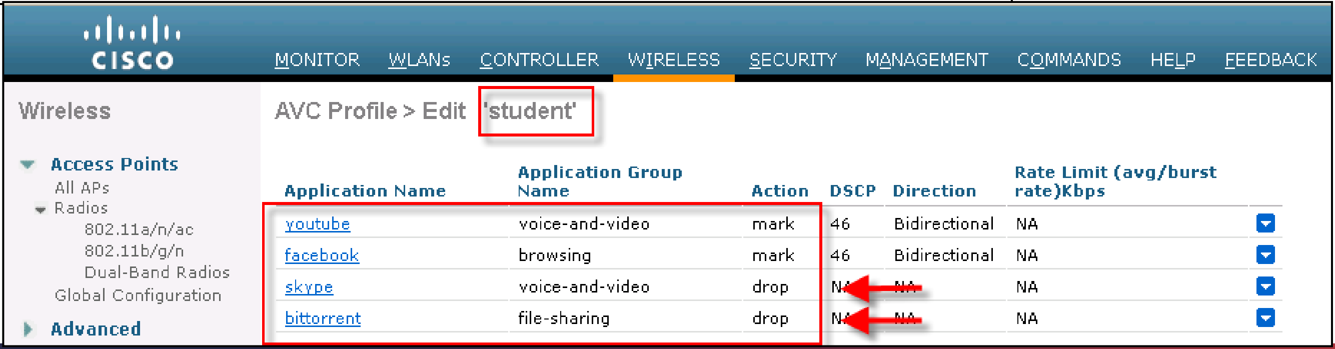
AVC Profile > Edit 'teacher'

Application Name	Application Group Name	Action	DSCP	Direction	Rate Limit (avg/burst rate)Kbps
youtube	voice-and-video	mark	46	Bidirectional	NA
facebook	browsing	mark	46	Bidirectional	NA
skype	voice-and-video	mark	46	Bidirectional	NA
bittorrent	file-sharing	mark	46	Bidirectional	NA



AVC Profile Name

AVC Profile Name
teacher
student



AVC Profile > Edit 'student'

Application Name	Application Group Name	Action	DSCP	Direction	Rate Limit (avg/burst rate)Kbps
youtube	voice-and-video	mark	46	Bidirectional	NA
facebook	browsing	mark	46	Bidirectional	NA
skype	voice-and-video	drop	NA	NA	NA
bittorrent	file-sharing	drop	NA	NA	NA

CLI AVC Client Configuration

```
(Cisco Controller) >config avc profile ?
<Profile Name> Enter AVC Profile Name up to 32 alphanumeric characters.

(Cisco Controller) >config avc profile Myprofile4 ?
create         Create an AVC Profile.
delete         Delete an AVC Profile.
rule           Configure a Rule for AVC Profile.

(Cisco Controller) >config avc profile Myprofile4 create

(Cisco Controller) >config avc profile Myprofile4 rule ?
add            Add a Rule for AVC Profile.
remove         Configure a Rule for AVC Profile.

(Cisco Controller) >config avc profile Myprofile4 rule add ?
application    Application Protocol name.

(Cisco Controller) >config avc profile Myprofile4 rule add application ?
<Appl Name>    Enter Application Name up to 32 alphanumeric characters.

(Cisco Controller) >config avc profile Myprofile4 rule add application facebook ?
drop           Rule to Drop packets.
mark           Rule to Mark Packets with specific DSCP.
ratelimit      Rule to Ratelimit Packets per app.
```

CLI AVC Client Configuration

```
(Cisco Controller) >config avc profile ?
<Profile Name> Enter AVC Profile Name up to 32 alphanumeric characters.

(Cisco Controller) >config avc profile Myprofile4 ?
create          Create an AVC Profile.
delete          Delete an AVC Profile.
rule            Configure a Rule for AVC Profile.

(Cisco Controller) >config avc profile Myprofile4 create

(Cisco Controller) >config avc profile Myprofile4 rule ?
add             Add a Rule for AVC Profile.
remove          Configure a Rule for AVC Profile.

(Cisco Controller) >config avc profile Myprofile4 rule add ?
application     Application Protocol name.

(Cisco Controller) >config avc profile Myprofile4 rule add application ?
<Appl Name>     Enter Application Name up to 32 alphanumeric characters.

(Cisco Controller) >config avc profile Myprofile4 rule add application facebook ?
drop            Rule to Drop packets.
mark            Rule to Mark Packets with specific DSCP.
ratelimit       Rule to Ratelimit Packets per app.
```

Show avc applications
for list of supported applications

CLI AVC Client Configuration

```
(Cisco Controller) >show avc profile ?
summary        Display Summary of AVC Profiles.
detailed       Display Details of an AVC Profile.

(Cisco Controller) >show avc profile summary
Profile-Name                      Number of Rules
  ============                      ==============
  Myprofile4                                1

(Cisco Controller) >show avc profile detailed ?
<Profile Name> Enter AVC Profile Name up to 32 alphanumeric characters.

(Cisco Controller) >show avc profile detailed Myprofile4
Application-Name          Application-Group-Name            Action     DSCP   DIR  AVG-RATELIMIT BURST-
RATELIMIT
  ================          =======================           ======     ====   ===== =============
=============
  facebook                  browsing                           Drop       -

  Associated WLAN IDs        :
  Associated Remote LAN IDs :
  Associated Guest LAN IDs   :
```

CLI AVC Client Configuration

```
(Cisco Controller) >config wlan avc ?
<WLAN id>      Enter WLAN Identifier between 1 and 16.

(Cisco Controller) >config wlan avc 1 ?
profile        AVC profile configuration.
visibility     Application Visibility configuration.

(Cisco Controller) >config wlan avc 1 profile ?
<Profile Name> Enter AVC Profile Name up to 32 alphanumeric characters.

(Cisco Controller) >config wlan avc 1 profile Myprofile4 ?
enable         Associate an AVC Profile.
disable        Remove an AVC Profile.

(Cisco Controller) >config wlan avc 1 profile Myprofile4 enable

(Cisco Controller) >config wlan avc 1 visibility ?
enable         Enable Application Visibility.
disable        Disable Application Visibility.

(Cisco Controller) >config wlan avc 1 visibility enable
```

CLI AVC Client Configuration

> show client detail

```
(WLC) >show client detail 18:20:32:bd:52:b7
Client MAC Address............................... 18:20:32:bd:52:b7
Client Username ................................. student1
Client State..................................... Associated
Client User Group................................ student
Client NAC OOB State............................. Access
Wireless LAN Id.................................. 2
Wireless LAN Network Name (SSID)................. ClassroomAVC
Wireless LAN Profile Name........................ ClassroomAVC
Policy Manager State............................. RUN
Policy Manager Rule Created...................... Yes
Audit Session ID................................. 0a0a0a0500000061533434e9
AAA Role Type.................................... student
Local Policy Applied............................. None
AVC Profile Name: ............................... student-AVC
```

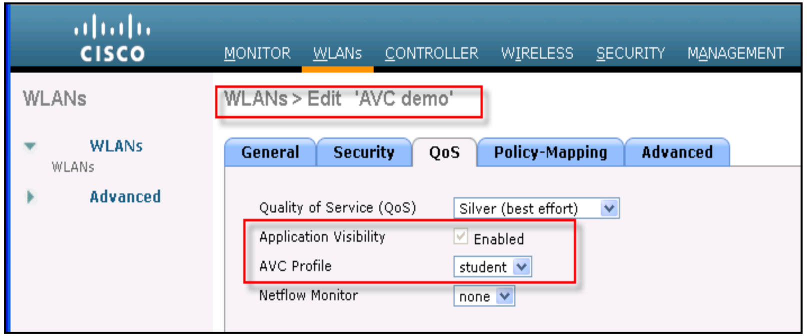
CLI AVC Client Troubleshooting

> debug aaa events enable and debug aaa detail enable

avc_debug_logs1.txt

```
*Dot1x_NW_MsgTask_0: Jun 24 05:59:28.194: [PA] 24:77:03:5c:99:e0 Override values for station 24:77:03:5c:99:e0
       source: 4, valid bits: 0x20000
       qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1

*Dot1x_NW_MsgTask_0: Jun 24 05:59:28.194: [PA] 24:77:03:5c:99:e0 Override values (cont..) dataAvgC: -1, rTAvgC: -1,
dataBurstC: -1, rTimeBurstC: -1
       vlanIfName: '', vlanId:0, aclName: ', ipv6AclName: , avcProfileName: avc1'

*Dot1x_NW_MsgTask_0: Jun 24 05:59:28.194: [PA] 24:77:03:5c:99:e0 Inserting new RADIUS override into chain for station
24:77:03:5c:99:e0
*Dot1x_NW_MsgTask_0: Jun 24 05:59:28.194: [PA] 24:77:03:5c:99:e0 Override values for station 24:77:03:5c:99:e0
       source: 4, valid bits: 0x20000
       qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1

*Dot1x_NW_MsgTask_0: Jun 24 05:59:28.194: [PA] 24:77:03:5c:99:e0 Override values (cont..) dataAvgC: -1, rTAvgC: -1,
dataBurstC: -1, rTimeBurstC: -1
       vlanIfName: '', vlanId:0, aclName: ', ipv6AclName: , avcProfileName: avc1'

*Dot1x_NW_MsgTask_0: Jun 24 05:59:28.194: [PA] 24:77:03:5c:99:e0 Applying override policy from source Override Summation:
with value 20000

*Dot1x_NW_MsgTask_0: Jun 24 05:59:28.194: [PA] 24:77:03:5c:99:e0 Override values for station 24:77:03:5c:99:e0
       source: 256, valid bits: 0x20000
       qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1

*Dot1x_NW_MsgTask_0: Jun 24 05:59:28.194: [PA] 24:77:03:5c:99:e0 Override values (cont..) dataAvgC: -1, rTAvgC: -1,
dataBurstC: -1, rTimeBurstC: -1
       vlanIfName: '', vlanId:0, aclName: ', ipv6AclName: , avcProfileName: avc1'
```

AVC Profile Applied on the WLAN



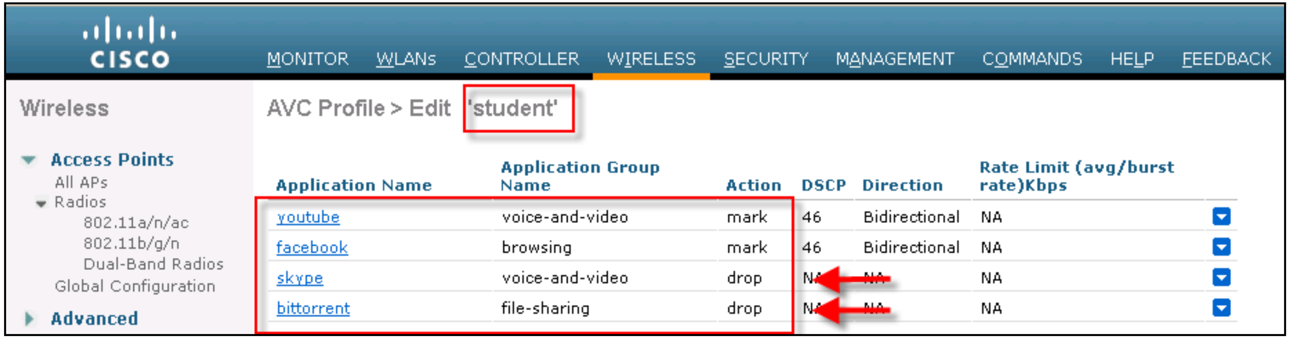
WLANs > Edit 'AVC demo'

Quality of Service (QoS): Silver (best effort)

Application Visibility: ☑ Enabled

AVC Profile: student

Netflow Monitor: none



AVC Profile > Edit 'student'

Application Name	Application Group Name	Action	DSCP	Direction	Rate Limit (avg/burst rate)Kbps
youtube	voice-and-video	mark	46	Bidirectional	NA
facebook	browsing	mark	46	Bidirectional	NA
skype	voice-and-video	drop	NA	NA	NA
bittorrent	file-sharing	drop	NA	NA	NA

Granular Policy for AVC – Use Cases

User and Device specific Application Policies

ROLE BASED APPLICATION POLICY

- Alice(Nurse) and Bob(IT Admin) are both employees in a hospital
- Both Alice and connected to same SSID.
- Bob can access certain applications (for e.g. YouTube), Alice cannot

ROLE BASED + DEVICE TYPE APPLICATION POLICY

- Alice can access EMR info on an IT provisioned Windows Laptop
- Alice cannot access EMR info on her personal iPAD

ROLE BASED + DEVICE TYPE + APPLICATION SPECIFIC POLICY

- Alice has limited access (rate limit) to Skype on her iPhone and limited download (directional) for Bittorrent

AVC Directional QoS

AVC Directional QoS DSCP Marking for Upstream/Downstream Traffic

- Prior to rel 8.0 QOS marking can be configured as an application rule on the AVC profile. The marking configured is a DSCP Marking and is applied bi-directionally for upstream **and** downstream.

- In rel 8.0 new feature provides an extra configuration parameter of direction where the marking can be specified with respect to direction – Upstream **or** Downstream.

- An extra configuration parameter will specify the direction attribute. This will be plumbed in as an AVC rule

AVC Per-Application Per-Client Rate Limiting on WLAN

- Prior to Rel 8.0, only bi-directional per client bandwidth control.
  - The downstream rate-limiting per client is performed at the WLC and upstream is performed at the AP.

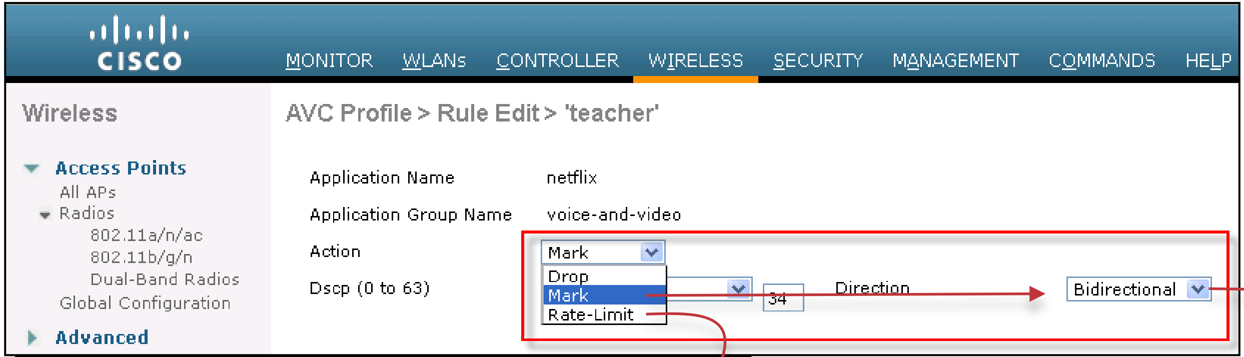
- In rel 8.0 - **per-Client** and **per-Application** based bidirectional rate-limiting available.
- This feature proposes to have per application based bandwidth control per client.
  - This will be above the per client bandwidth contracts
  - The bandwidth contracts will co-exist with per-client downstream rate-limiting taking precedence over the per-application rate limits.

Note: Rate Limiting is not supported on 2500 controllers; AVC is not supported on vWLC controllers

AVC Per Application Per Client Based Rate Limiting on WLAN - Limitation

- The number of rate limit applications is limited currently to 3. This limit is enforced during configuration.
- Only one rule can be configured per application.
  - An application cannot have both a rate-limit as well as a mark rule.
- The same rates are used for both upstream and downstream.
  - So the rates shall apply bi-directionally as a collective amount and not individually.
- The rate-limit rules will not be applied dynamically to the clients. The clients will inherit the rules only when they are re-authenticated.

Directional DSCP Configuration



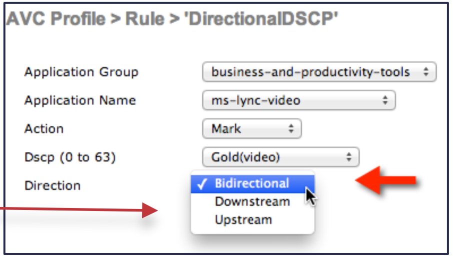
AVC Profile > Rule Edit > 'teacher'

Application Name netflix

Application Group Name voice-and-video

Action Mark

Dscp (0 to 63) 34 Direction Bidirectional



AVC Profile > Rule > 'DirectionalDSCP'

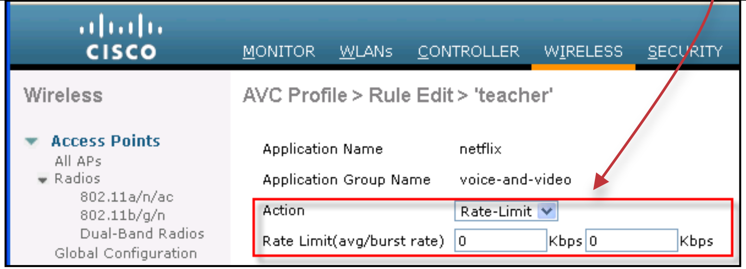
Application Group business-and-productivity-tools

Application Name ms-lync-video

Action Mark

Dscp (0 to 63) Gold(video)

Direction ✓ Bidirectional



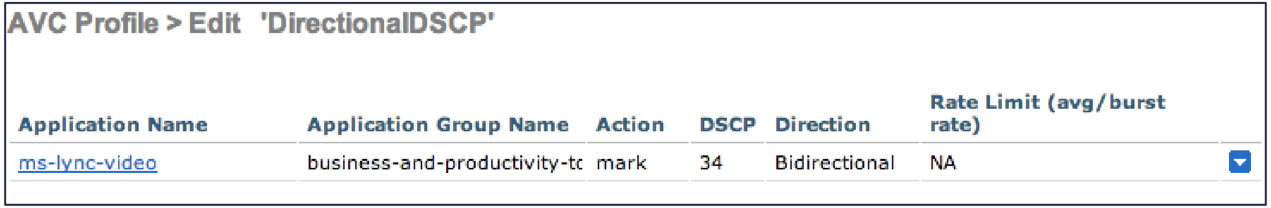
AVC Profile > Rule Edit > 'teacher'

Application Name netflix

Application Group Name voice-and-video

Action Rate-Limit

Rate Limit(avg/burst rate) 0 Kbps 0 Kbps



AVC Profile > Edit 'DirectionalDSCP'

Application Name	Application Group Name	Action	DSCP	Direction	Rate Limit (avg/burst rate)
ms-lync-video	business-and-productivity-tc	mark	34	Bidirectional	NA

Directional DSCP Configuration

```
(Cisco Controller) >config avc profile ?
<Profile Name> Enter AVC Profile Name up to 32 alphanumeric characters.

(Cisco Controller) >config avc profile Myprofile ?
create         Create an AVC Profile.
delete         Delete an AVC Profile.
rule           Configure a Rule for AVC Profile.

(Cisco Controller) >config avc profile Myprofile rule ?
add            Add a Rule for AVC Profile.
remove         Configure a Rule for AVC Profile.

(Cisco Controller) >config avc profile Myprofile rule add application ?
<Appl Name>    Enter Application Name up to 32 alphanumeric characters.

(Cisco Controller) >config avc profile Myprofile rule add application Netflix ?
drop           Rule to Drop packets.
mark           Rule to Mark Packets with specific DSCP.
ratelimit      Rule to Ratelimit Packets per app.
```

Directional DSCP Configuration

```
(Cisco Controller) >config avc profile Myprofile rule add application Netflix drop ?

(Cisco Controller) >config avc profile Myprofile rule add application Netflix mark 46 ?
upstream       DSCP Direction for Marking packets. Default is Bidirectional.
downstream     DSCP Direction for Marking packets. Default is Bidirectional.

(Cisco Controller) >config avc profile Myprofile rule add application Netflix ratelimit ?
<Average Ratelimit value> Configure ratelimit in kbps.
(Cisco Controller) >config avc profile Myprofile rule add application Netflix ratelimit
200 ?
<Burst Ratelimit value> Configure ratelimit in kbps.

(Cisco Controller) >config avc profile Myprofile rule add application Netflix ratelimit
200 600 ?

(Cisco Controller) >
```

CLI DSCP Verification

```
(Cisco Controller) >show avc profile detailed avc1

  Application-Name      Application-Group-Name        Action     DSCP   DIR  AVG-RATELIMIT BURST-RATELIMIT
  ================      =======================       ======     ====  ===== ============= =============
  youtube               voice-and-video               Ratelimit     -    -        70              70
  video-over-http       voice-and-video               Drop          -
  http                  browsing                      Ratelimit     -    -        70              70
  ssl                   internet-privacy              Drop          -
  binary-over-http      file-sharing                  Ratelimit     -    -        10              10

  Associated WLAN IDs       : 58,61,62,63
  Associated Remote LAN IDs :
  Associated Guest LAN IDs  :
```

CLI DSCP Troubleshooting

> debug client aa:bb:cc:dd:ee:ff

debug_logs-ratelimit.txt

```
*apfReceiveTask: Jun 24 06:18:37.742: [PA] 24:77:03:5c:99:e0 9.9.120.118 RUN (20) Fast
Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 64206, IntfId = 0  Local Bridging
Vlan = 121, Local Bridging intf id = 6
*apfReceiveTask: Jun 24 06:18:37.742: [PA] 24:77:03:5c:99:e0 9.9.120.118 RUN (20) Fast
Path rule (contd...) AVC Ratelimit:  AppID = 82 ,AppAction = 4, AppToken =
64206  AverageRate = 70, BurstRate = 70

*apfReceiveTask: Jun 24 06:18:37.742: [PA] 24:77:03:5c:99:e0 9.9.120.118 RUN (20) Fast
Path rule (contd...) AVC Ratelimit:  AppID = 3 ,AppAction = 4, AppToken =
64206  AverageRate = 70, BurstRate = 70

*apfReceiveTask: Jun 24 06:18:37.742: [PA] 24:77:03:5c:99:e0 9.9.120.118 RUN (20) Fast
Path rule (contd...) AVC Ratelimit:  AppID = 121 ,AppAction = 4, AppToken =
64206  AverageRate = 10, BurstRate = 10
```

AVC Integration with Local Profiling

Integration of AVC Profiles to the Local Policy Classification per User and per Device

- Provides the capability to apply the AVC profiles (used to control the applications) based on the role defined on AAA

  1. Per user-group basis
  2. Per-user basis
  3. Per-user and per-device(defined on the policy, including device type, EAP type) basis

Integration of AVC Profiles to the Local Policy Classification per User and per Device

- An AVC profile is defined as a part of Local policy.
- Any client/user when authenticates with the AAA server will receive the role defined per User or User group as a part of the AAA response.
  - The received role is used to match the role defined on the policies defined per WLAN
- On successful policy matching, a particular policy gets selected and the AVC profile defined under the policy is applied on to the client/user.
- Device type defined the policy can also be a deciding factor in the policy matching if AVC profile needs to be selected on a per user per specific device type.

Policy tie-in with AVC

User-aware and Device-aware

WLC rel 7.5 and 7.6

Application-based Policies

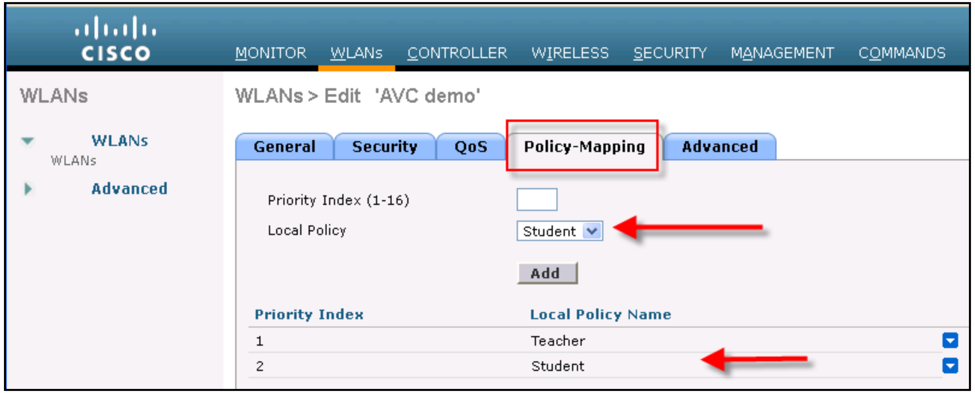
WLC rel 8.0

User-role aware

Device-aware

Alice cannot access Netflix but Bob can even though both are employees connecting to same SSID
Alice can access EHS records on (IT provisioned) Windows Laptop but cannot on personal (unsecure)

AVC Profile and Local Policy Configuration

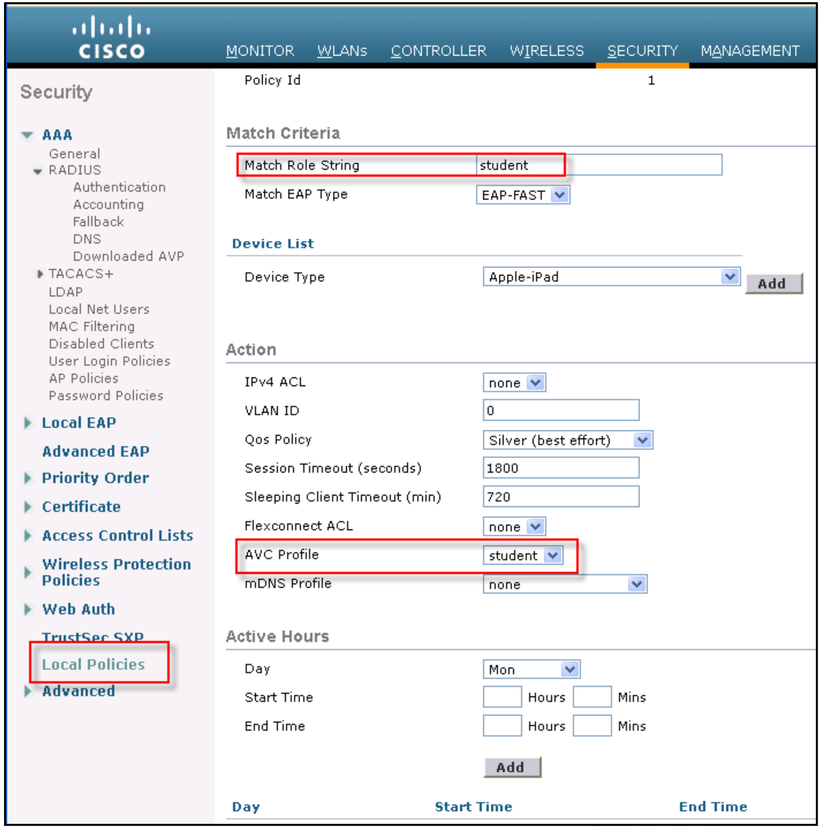


WLANs > Edit 'AVC demo'

Priority Index (1-16)

Local Policy: Student

Priority Index	Local Policy Name
1	Teacher
2	Student



Policy Id 1

Match Criteria

Match Role String: student

Match EAP Type: EAP-FAST

Device List

Device Type: Apple-iPad

Action

IPv4 ACL: none

VLAN ID: 0

Qos Policy: Silver (best effort)

Session Timeout (seconds): 1800

Sleeping Client Timeout (min): 720

Flexconnect ACL: none

AVC Profile: student

mDNS Profile: none

Active Hours

Day: Mon

Start Time: Hours Mins

End Time: Hours Mins

Day	Start Time	End Time

Protocol Pack

AVC Protocol Pack 9.0 in Release 8.0

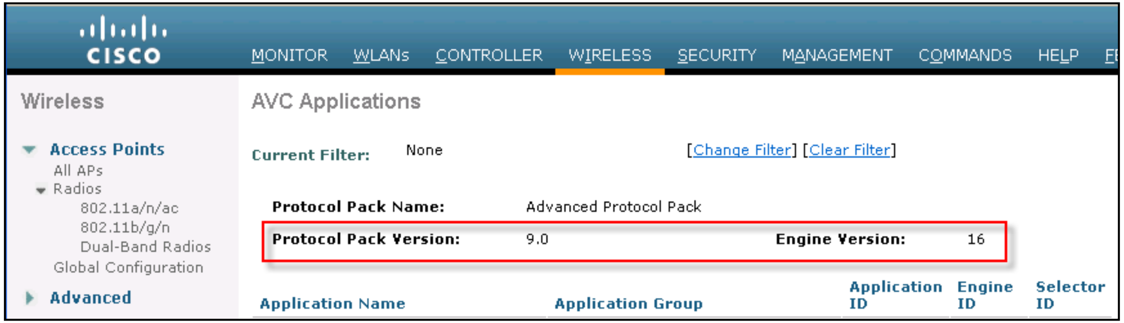
Updated Signatures

- Chinese Top Apps
- iTunes Update
- Web Video Services
- Web Audio Services

Enhancement Highlights

- Microsoft Lync Audio/Video Separately
- Non-Encrypted Cisco-Jabber Support

```
(WLC) >show avc protocol-pack version

 AVC Protocol Pack Name: Advanced Protocol Pack
 AVC Protocol Pack Version: 9.0
```



AVC Applications

Current Filter: None

Protocol Pack Name: Advanced Protocol Pack

Protocol Pack Version: 9.0 Engine Version: 16

Application Name	Application Group	Application ID	Engine ID	Selector ID

http://www.cisco.com/c/en/us/td/docs/wireless/controller/nbar2_prot_pack/6-3-0/b_nbar2_prot_pack_630/b_nbar2_prot_pack_630_chapter_01.html

AVC Protocol Pack in Release 8.0

- 8.0 release ships with 9.0 as default protocol pack and we are recommending 11.0 protocol pack.”
- In 8.0 the engine version will be changed from 13 (3.7) in 7.6 to 16(3.10)… and the protocol packs are tightly coupled with engine version.
- Consequence: If customer is on 7.6 release with 6.4 protocol pack installed, and upgrades to 8.0 he will have 9.0 as protocol pack, and then he downgrades to 7.6 he will have 6.4 protocol pack. This is not the case with 7.5 to 7.6 upgrade/downgrade scenario.

NBAR Engine in Release 8.0

- NBAR2 engine ver 3.10/3.7 is tightly coupled with WLC code
- Update engine for new protocol packs
- Code for the engine will be maintained by the NBAR team
- Provides easier upgrades to future engine

Note: Newer AVC protocol packs are tied with engine

Older AVC PP will not work with new engine.

Custom applications are not supported.

AVC Features in 8.0 – Summary

- NBAR2 engine will be ver 3.7 and will be ported as library for smoother upgrades
- A new Protocol Pack ver 9.0 will be released for the new engine – not backward compatible
- Local Policy can be applied to the same WLAN to allow access on certain devices for certain applications
- In rel 7.5 and 7.6 all users on the same WLAN inherit the same AVC profile
- In 8.0 the value proposition is to allow for AAA AVC profile over-ride is to enable different clients to have different AVC profiles on the same WLAN
- In 7.5 and in 7.6 we support bidirectional per client bandwidth control
  - ➢ The downstream rate-limiting per client is performed at the WLC and upstream is performed at the AP.
- In rel 8.0 AVC per application and per client/SSID bidirectional Rate-Limiting supported
  - ➢ This feature proposes to have per application based bandwidth control per client.
  - ➢ This will be above the *Per-User* and *per-SSID* bandwidth contracts.
  - ➢ The number of rate limit applications is limited currently to 3
  - ➢ The rate limit rules will not be applied dynamically to all clients – they have to de-authenticate to inherit new rules
  - ➢ Same or Different rates can be applied for upstream and downstream.

Thank you.