8.0 Update – WLC Enhancements

Jerome Henry
Technical Marketing Engineer
Enterprise Networking Market Strategy

August 2014

Agenda

- AP and Scale Features 1 slider
  - vWLC: 6K clients - 1 slide
  - CAPWAP: Data Tunnel Keep-Alive Support – 1 slide
  - PPPoE Client on FlexConnect - 1 slide
  - Wired Guest Access on 2500 -1 slide
- Security and RADIUS-Related Features
  - Vendor Specific AVPs - simplify
  - HTTPS Support for WebAuth – 1 slide

Agenda

- Ease of Management Features
  - Changes to SSID and WLAN Profile Name 1 slide
  - Ping From Dynamic Interfaces 1 slide
  - show run-config startup-commands 1 slide
  - AP Telnet & SSH Enhancements 1 slide
  - Alternate Color Scheme for the WLC GUI 1slide

Agenda

- Ease of Management Features (Cont.)
  - Local Profiling – Update OUI / Device Profiles list – cover in detail
  - 802.11v Support – Apple – cover in detail
  - 802.11r Mixed WLAN – cover in detail
  - DHCP Relay Sub-Options – 1 slide

AP and Scale Features

vWLC: *100% Increase in the Number of Clients!!*

- ***Service Providers = Large Scale + Cost Awareness***
- There has been an SP movement to offer managed Wi-Fi services to Hospitality and SMB
- Among their top challenges in this business model:
  - Limit of SSIDs per WLC
  - Overlapping IP address space support
- The ***vWLC*** is a very good fit to address those immediate SP needs "***today***"

*And **with 8.0**:*

The ***vWLC*** supports up to ***6,000 wireless clients.*** *That is double the current 3K limit.*

(Note: Maximum AP count supported is still 200)

CAPWAP: Data Tunnel Keep-Alive Support

- SPs looking to provide managed wireless services often face the need to place an AP behind an internet router (or FW) doing Port Address Translation (PAT)
- Routers time out a UDP PAT translation from its table after 5 minutes of inactivity
- Presently, regular keep-alives are sent over the ***CAPWAP Control Tunnel***, but not over the ***CAPWAP Data tunnel***
- This "*can*" lead to a situation where an AP has its ***control*** connection to the WLC active and fresh on the FW, while the ***Data packets are being black-holed.*** The AP assumes the data path is still good, while the internet FW may be dropping those packets because the original source port number is no longer valid! (Ex: Assigned to different flow with the same ephemeral source port number while the original tunnel translation was no longer in the table).
- The AP can remain in this limbo for an unpredictable amount of time. Resetting the AP or the internet connection (the default end-user behavior) will temporarily resolve the issue, which makes the root cause even more illusive.
- ***8.0 is the answer to this problem!***

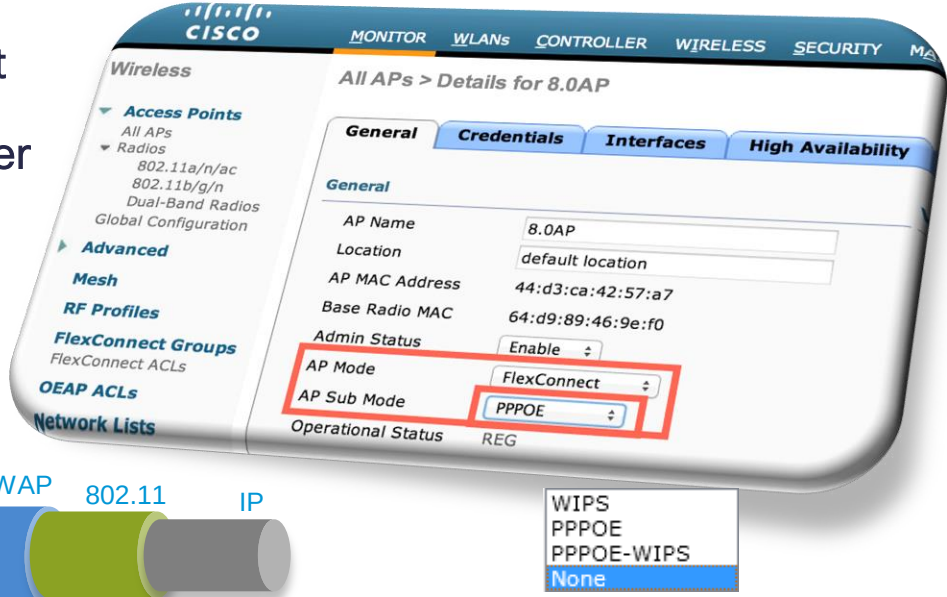
CAPWAP: Data Tunnel Keep-Alive Support

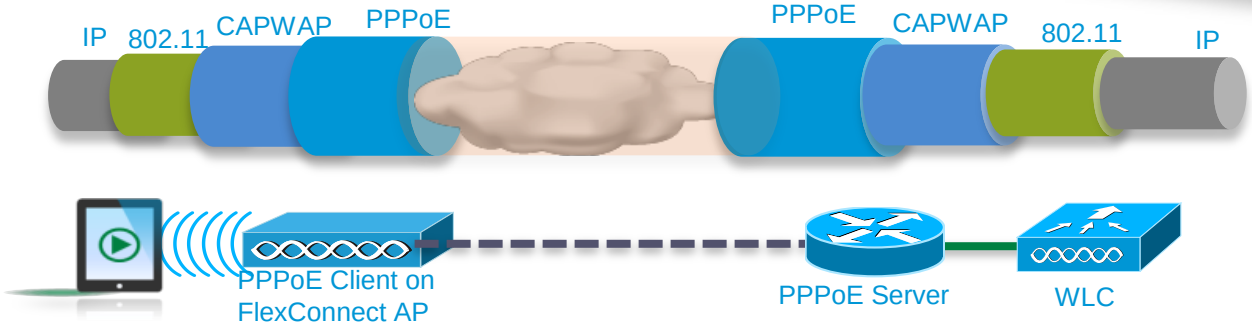
- A workaround was to use CAPWAP DTLS (as it supports keep-alives over the data DTLS tunnel)
- In 8.0 CAPWAP data also has a keep-alive. It is enabled by default and runs every 30 seconds. No configuration is needed or possible.
- You can check the keep-alives (both control and data):

```
(Cisco Controller) >debug capwap dtls-keepalive enable

(Cisco Controller) >*capwapSocketTask: Jun 01 06:21:40.031: 08:cc:68:b4:46:c0 Data
Keepalive received on IP 172.31.255.40, port 5247
*capwapSocketTask: Jun 01 06:21:40.031: 08:cc:68:b4:46:c0 Data Keepalive packet reflected
back to 172.31.255.109:62319

*capwapSocketTask: Jun 01 06:22:01.594: 3c:ce:73:1a:09:60 Data Keepalive received on IP
172.31.255.40, port 5247
*capwapSocketTask: Jun 01 06:22:01.594: 3c:ce:73:1a:09:60 Data Keepalive packet reflected
back to 10.10.21.209:43147
```

The PPPoE Client on FlexConnect APs is back!!

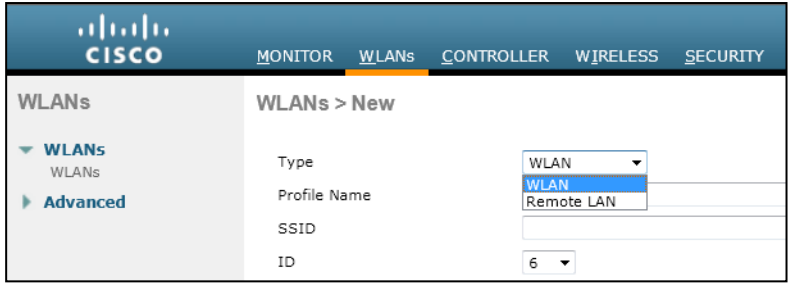
- The FlexConnect AP can act as a PPPoE client
- Eliminates the need of an external PPPoE router
- Introduced in 7.3, then taken out in 7.5
- Back in 8.0, optimized and better then ever!



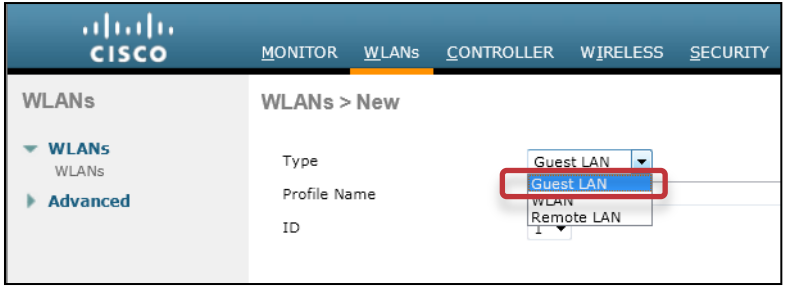


Wired Guest Access on WLC 2500

- You can now create a Guest LAN interface on 2500 to support wired guest access



7.6



8.0

Authentication & RADIUS Enhancements

2.1: We will Send any *Vendor-Specific Attributes* you Want!

A customer wants to add some **VSA**s to **RADIUS Accounting** messages generated by clients on a particular SSID…

Another customer wants to add a different set of VSAs but to both RADIUS Authentication and Accounting messages…

…How can we scale such requests?!

Easy: Allow them to define it for themselves!

In 8.0, the Service Provider can teach the old WLC new VSAs

This is done by importing an XML-like text file that teaches the WLC:

1. The VSAs and their values
2. What to do with them

Vendor Specific AVPs– What Does That File Look Like?

```
<radiusFile>
    <avpList SSID_PROF="SSIDProfileName" incAuth="true" incAcct="false">
        <radiusAttributes>
            <attributeName>SVR-Zip-Code</attributeName>
            <vendorId>14369</vendorId>
          <attributeId>14</attributeId>
            <valueType>STRING</valueType>
            <attributeValue>33612</attributeValue>
        </radiusAttributes>
        <radiusAttributes>
            …
        </radiusAttributes>
    </avpList>
    <avpList SSID_PROF="SSIDProfileName" incAuth="false" incAcct="true">
        <radiusAttributes>
            …
        </radiusAttributes>
    </avpList>
</radiusFile>
```

For more details, see the slide notes

Vendor Specific AVPs- How to get the File to the WLC?

Save Configuration | Ping | Logout | Refresh

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Commands

- Download File
- Upload File
- Reboot
- Config Boot
- Scheduled Reboot
- Reset to Factory Default
- Set Time
- Login Banner

Download file to Controller — Clear | Download

File Type	Radius AVP List
Transfer Mode	TFTP

Server Details

IP Address(Ipv4/Ipv6)	172.20.27.24
Maximum retries (1 to 254)	10
Timeout (1 to 254 seconds)	6
File Path	/
File Name	MyVSAs.txt

Parsed the Radius AVP list successfully from XM

Save Configuration | Ping | Logout | Refresh

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Security

- AAA
  - General
  - RADIUS
    - Authentication
    - Accounting
    - Fallback
    - DNS
    - Downloaded AVP
  - TACACS+
  - LDAP
  - Local Net Users
  - MAC Filtering
  - Disabled Clients
  - User Login Policies
  - AP Policies
  - Password Policies
- Local EAP
- Advanced EAP
- Priority Order
- Certificate
- Access Control Lists
- Wireless Protection Policies
- Web Auth
- Local Policies
- Advanced

DOWNLOADED RADIUS AVP LIST

Wlan SSID Profile Name: SSIDProfileName

Auth AVP | Acct AVP

Auth No	Vendor Id	AttrId	Type	Value
1	557318144	22	STRING	StadiumDirect
2	557318144	14	STRING	75013
3	557318144	19	STRING	33.135774,-96.660483
4	557318144	20	INTEGER	258
5	557318144	21	INTEGER	0
6	3361144832	7	STRING	2001
7	3361144832	8	STRING	EST
8	3361144832	11	STRING	Cisco_Lab
9	3361144832	14	STRING	US
10	3361144832	15	STRING	1
11	3361144832	16	STRING	TX
12	3361144832	17	STRING	Allen
13	3361144832	18	INTEGER	972
14	3361144832	29	STRING	allentxsppoclab
15	3361144832	10	STRING	Standard
16	3361144832	37	STRING	Test_Primary_ISP/Test_Backup_IS

Vendor Specific AVPs- How to get the File to the WLC? (Cont.)

```
(Cisco Controller) >transfer download datatype radius-avplist

(Cisco Controller) >transfer download ?
certpassword   Set a Certificate's private key password
datatype       Set File Type.
filename       Set Filename on Server.
mode           Set transfer mode.
password       Set Server Login Password.
path           Set File Path on Server.
port           Change Default Server Port.
…/…

(Cisco Controller) >show radius avp-list <ssid-profile-name>
```

Example AVP file

Mostattrib.xml

Vendor Specific AVPs- How to get the File to the WLC? (Cont.)

- Debug command to display XML file parsing progress:

```
(Cisco Controller) >debug aaa events enable
(Cisco Controller) >debug aaa detail enable

Radius authentication packets:
*aaaQueueReader: Jul 02 15:53:49.005: NAI-Realm derived from username,
LAB.VTV.BLR.cisco.co.in
*aaaQueueReader: Jul 02 15:53:49.005: NAI-Realm=LAB.VTV.BLR.cisco.co.in comparision with
radius index @ 5 is successful
*aaaQueueReader: Jul 02 15:53:49.005: Found the radius server : 9.9.120.10 from the global
server list
*aaaQueueReader: Jul 02 15:53:49.005: 24:77:03:5c:99:e0 Sending the packet to v4 host
9.9.120.10:1812
*aaaQueueReader: Jul 02 15:53:49.005: 24:77:03:5c:99:e0 Successful transmission of
Authentication Packet (id 112) to 9.9.120.10:1812, proxy state 24:77:03:5c:99:e0-00:01
```

Vendor Specific AVPs- How to get the File to the WLC? (Cont.)

- Debug command to display XML file parsing progress:

```
(Cisco Controller) >debug aaa events enable
(Cisco Controller) >debug aaa detail enable

Accounting packets:
*aaaQueueReader: Jul 02 16:04:41.616: NAI-Realm derived from username,
LAB.VTV.BLR.cisco.co.in
*aaaQueueReader: Jul 02 16:04:41.616: NAI-Realm derived from username,
LAB.VTV.BLR.cisco.co.in
*aaaQueueReader: Jul 02 16:04:41.616: NAI-Realm=LAB.VTV.BLR.cisco.co.in comparision with
radius index @ 17 is successful
*aaaQueueReader: Jul 02 16:04:41.617: Found the radius server : 9.9.120.10 from the global
server list
*aaaQueueReader: Jul 02 16:04:41.617: 24:77:03:5c:99:e0 Sending the packet to v4 host
9.9.120.10:1813
*aaaQueueReader: Jul 02 16:04:41.617: 24:77:03:5c:99:e0 Successful transmission of
Accounting-Start (id 254) to 9.9.120.10:1813, proxy state 24:77:03:5c:99:e0-00:00
*radiusTransportThread: Jul 02 16:04:41.625: ****Enter processIncomingMessages: response
code=5
```

2.2: RADIUS Selection by REALM

*N*etwork *A*ccess *I*dentifier (NAI) is an identifier in the format "Username@Realm"

In dot1x, that *NAI* value is visible to the WLC in the *EAP Identity Response*

In the case of EAP-SIM or EAP-AKA, the NAI looks something like this:

0<IMSI>@wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org†

Anything after the "@" is just the "Realm" value

But, did you notice that the *Realm* value here is unique for an SP?

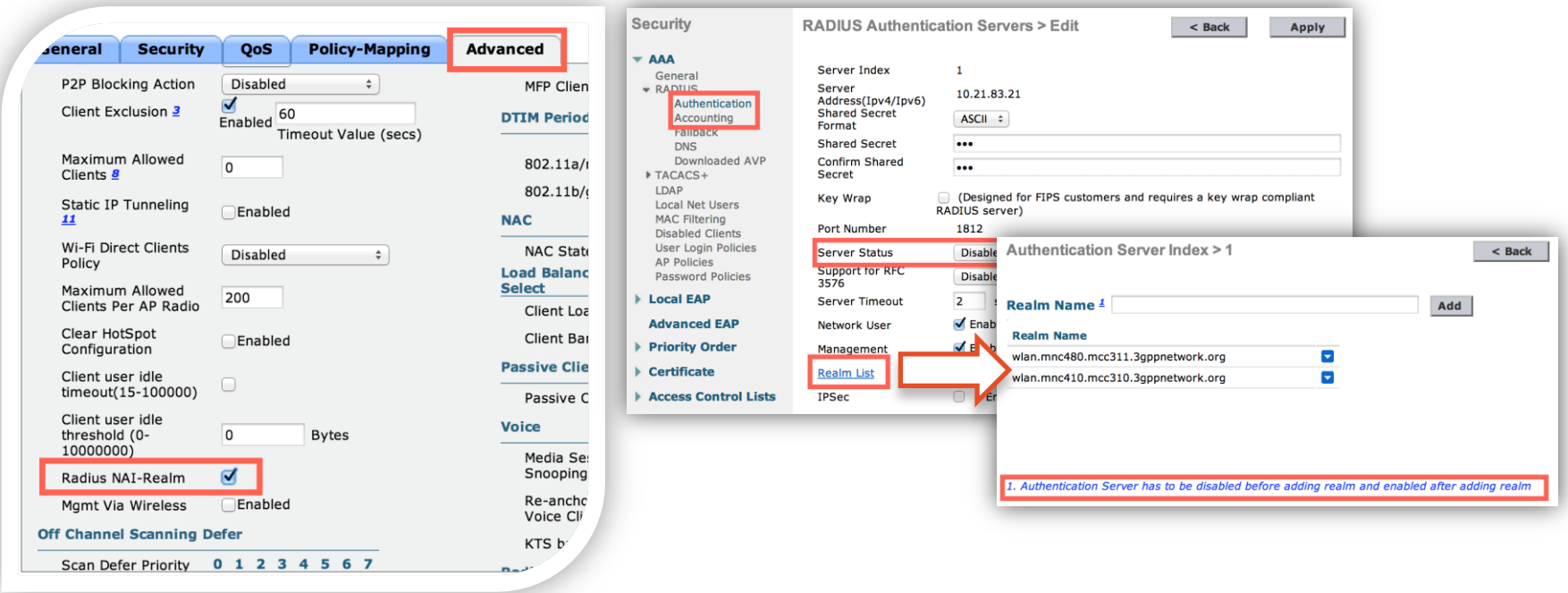
What if the WLC can use this *Realm* as a tag to make a choice on which RADIUS to use for authenticating and/or accounting for that particular wireless client?!

Well that is exactly what this feature is about.

†*More details in the slide notes*

RADIUS Selection by REALM – How to Configure it?

- As Easy as 1-2..:
  1. Enable the feature on the WLAN
  2. Tag the RADIUS servers with the REALM values as needed (up to 30 of them per RADIUS)



RADIUS Selection by REALM – How to Configure it? (Cont.)

- As Easy as 1-2.. From the CLI:
  - To enable/disable the NAI-realm selectivity on a WLAN:

```
(Cisco Controller) >config wlan radius_server realm ?
enable          Enable realm authentication on the wlan
disable         Disable realm authentication on the wlan

(Cisco Controller) >config wlan radius_server realm enable ?
<WLAN id>       wlan index
```

  - To add/delete a realm on a RADIUS for Authentication:

```
(Cisco Controller) >config radius auth realm ?
add             radius auth realm add
delete          radius auth realm delete

(Cisco Controller) >config radius auth realm add ?
<radius-index> radius index

(Cisco Controller) >config radius auth realm add 1 ?
<realm-string> realm string
```

RADIUS Selection by REALM – How to Configure it? (Cont.)

- As Easy as 1-2.. From the CLI:
  - To add/delete a realm on a RADIUS for accounting purpose:

```
(Cisco Controller) >config radius acct realm ?
add            radius acct realm add
delete         radius acct realm delete

(Cisco Controller) >config radius acct realm add ?
<radius-index> radius index

(Cisco Controller) >config radius acct realm add 1 ?
<realm-string> realm string
```

RADIUS Selection by REALM – Verification

- To check RADIUS configuration:

```
(Cisco Controller) >show radius auth detailed ?
<index>        Displays RADIUS authentication server index details.

(Cisco Controller) >show radius acct detailed ?
<index>        Displays RADIUS accounting server index details.

(Cisco Controller) >show wlan 1
…/…
Radius NAI-Realm.................................. Enabled
```

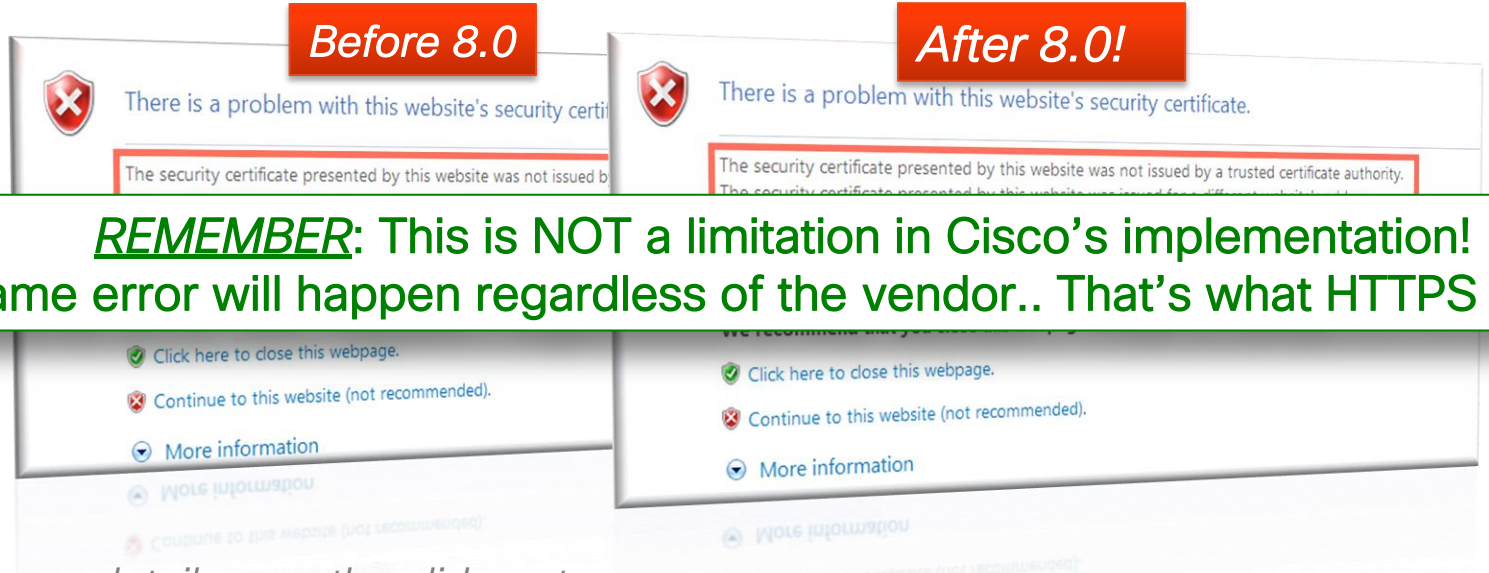
RADIUS Selection by REALM – Design Considerations

- In dot1x, the WLC can only see the user's EAP outer identity.
- If the NAI-realm is enabled on a WLAN, but there was no realm in the outer identity, the behavior is defaulted to no lookup and the usual selection of RADIUS is followed.
- ***<u>However,</u>*** If in that same scenario there was a REALM value in the outer identity - or simply if it contained the character "@", and this Realm value did not match any of the RADIUS servers, ***that wireless client will be disassociated!***
- This works well with EAP-SIM & EAP-AKA, but if this same WLAN will be serving other flavors of EAP, caution should be taken that the outer identity values are considered.†

†*For more details, see the slide notes*

2.3: HTTPS Support for WebAuth

- Great news! *In 8.0*, if a client starts browsing with an ***https://*** webpage, it will be redirected to the WebAuth login page!
- But keep in mind that the *SSL Warning Page* is now here to stay†…



REMEMBER: This is NOT a limitation in Cisco's implementation!
Same error will happen regardless of the vendor.. That's what HTTPS is for!

†*For more details, see the slide notes*

Rejection on Wrong WLAN ID

- When authenticating against RADIUS, WLC can send the WLAN ID – the vendor specific attribute (VSA) of Airespace-WLAN-id
- RADIUS can be configured to allow user connection only from a specific WLAN, and reject authentication from other WLANs
- This rejection works on Webauth WLANs, but not on other 802.1x/EAP WLANs (WLC does not check WLAN-id value returned by RADIUS)
- In 8.0, Dot1X/ Mac filtering is also rejected if Airespace-WLAN-id does not match value returned from AAA
- In addition, an SSID Cisco AVPair is supported that allows WebAuth/Dot1X/Mac filtering to be rejected based on values returned from AAA server

Rejection on Wrong WLAN ID

- On RADIUS, you can set a condition based on the WLAN-ID

Cisco Secure ACS

My Workspace
Network Resources
Users and Identity Stores
Policy Elements
Session Conditions
Date and Time
Custom
Network Conditions
Authorization and Permissions
Network Access
Authorization Profiles
Device Administration
Named Permission Objects
Access Policies
Monitoring and Reports
System Administration

Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: "vinodhk2-1"

General | Common Tasks | RADIUS Attributes

Common Tasks Attributes

Attribute	Type	Value
Tunnel-Type	Tagged Enum	[T:1] VLAN
Tunnel-Medium-Type	Tagged Enum	[T:1] 802
Tunnel-Private-Group-ID	Tagged String	[T:1] 121
Session-Timeout	Unsigned Integer 32	180
Termination-Action	Enumeration	RADIUS-Request

Manually Entered

Attribute	Type	Value
cisco-av-pair	String	avc-profile-name=avc1
cisco-av-pair	String	role=visitor
Airespace-Wlan-Id	Unsigned Integer 32	2

Add Λ | Edit V | Replace Λ | Delete

Dictionary Type: RADIUS-IETF
RADIUS Attribute: Select
Attribute Type:
Attribute Value: Static

= Required fields

Rejection on Wrong WLAN ID

- " debug aaa events enable" and " debug aaa detail enable" show the exchange details:

```
*radiusTransportThread: Jun 24 10:42:12.788: [PA] Done - avpIndex 14, rawOffset 292, rawLeft 0, respOffset
532, respLeft 7560
*radiusTransportThread: Jun 24 10:42:12.788: [PA] 24:77:03:5c:99:e0 Access-Accept received from RADIUS
server 9.1.0.101 for mobile 24:77:03:5c:99:e0 receiveId = 2
*radiusTransportThread: Jun 24 10:42:12.788: [PA] AuthorizationResponse: 0xa119ca0
 *radiusTransportThread: Jun 24 10:42:12.788: [PA]    structureSize.............................532
 *radiusTransportThread: Jun 24 10:42:12.788: [PA]    resultCode................................0
 *radiusTransportThread: Jun 24 10:42:12.788: [PA]
      protocolUsed.............................0x00000001
 *radiusTransportThread: Jun 24 10:42:12.788: [PA]
      proxyState...............................24:77:03:5C:99:E0-02:07
 *radiusTransportThread: Jun 24 10:42:12.788: [PA]    Packet contains 14 AVPs:
  …/…
*radiusTransportThread: Jun 24 10:42:12.788: [PA]         AVP[14] Airespace / WLAN-
Identifier.............0x00000002 (2) (4 bytes)
```

Rejection on Wrong WLAN ID

- " debug aaa events enable" and " debug aaa detail enable" show the exchange details:

```
*Dot1x_NW_MsgTask_0: Jun 24 10:42:12.788: [PA] 24:77:03:5c:99:e0 Processing Access-Accept for mobile
24:77:03:5c:99:e0
*Dot1x_NW_MsgTask_0: Jun 24 10:42:12.788: [PA] 24:77:03:5c:99:e0 Resetting web IPv4 acl from 255 to 255
 *Dot1x_NW_MsgTask_0: Jun 24 10:42:12.788: [PA] 24:77:03:5c:99:e0 Resetting web IPv4 Flex acl from 65535 to
65535
 *Dot1x_NW_MsgTask_0: Jun 24 10:42:12.788: [PA] 24:77:03:5c:99:e0 Username entry (vinodh) created for
mobile, length = 253
*Dot1x_NW_MsgTask_0: Jun 24 10:42:12.788: [PA] 24:77:03:5c:99:e0 Username entry (vinodh) created in mscb for
mobile, length = 253
*Dot1x_NW_MsgTask_0: Jun 24 10:42:12.788: [PA] 24:77:03:5c:99:e0 AAA Override Role-Type 'visitor' set
*Dot1x_NW_MsgTask_0: Jun 24 10:42:12.788: [PA] 24:77:03:5c:99:e0 Entering Backend Auth Failure state (id=25)
for mobile 24:77:03:5c:99:e0
*Dot1x_NW_MsgTask_0: Jun 24 10:42:12.788: [PA] 24:77:03:5c:99:e0 Setting quiet timer for 5 seconds for
mobile 24:77:03:5c:99:e0
```

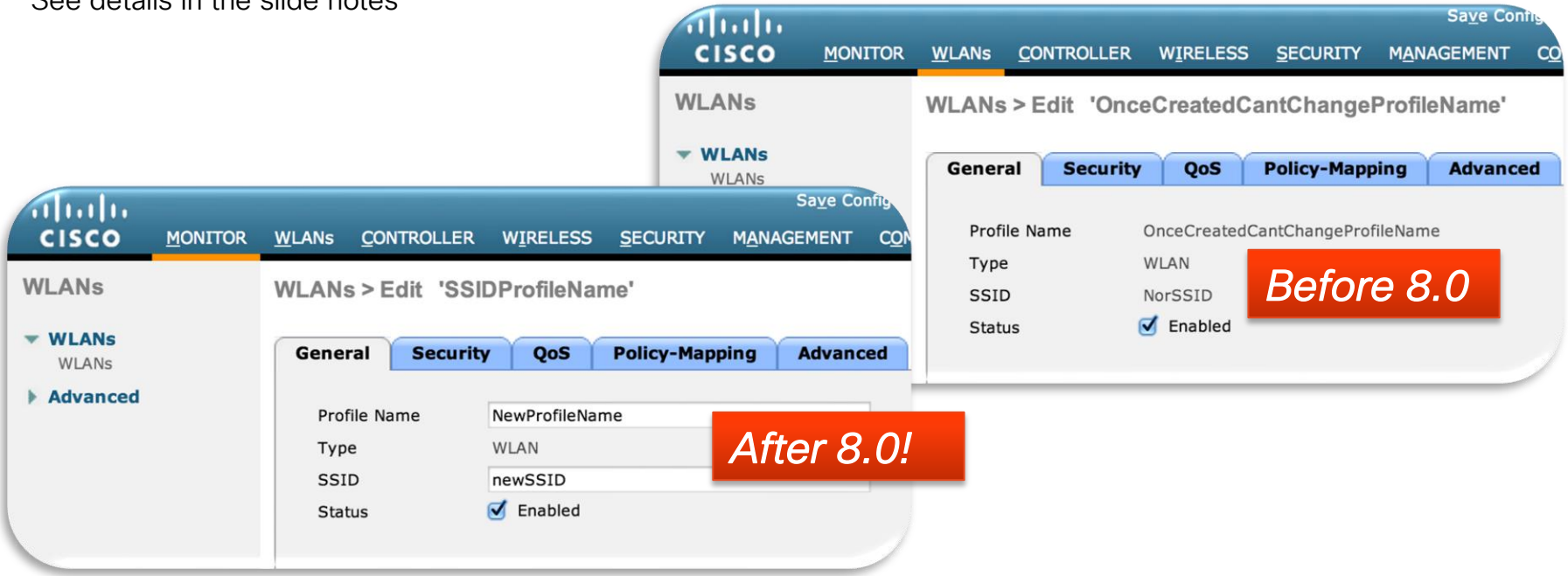
Rejection on Wrong WLAN ID

- Notes:
  - Only one WLAN ID can be sent for Dot1x/Mac filtering. This is consistent with WebAuth behavior today.
  - Multiple SSID attributes may be sent.
  - Mix of WLAN ID/SSID(s) is not supported

Ease of Management

We Will Allow Changes to SSID and WLAN Profile Name

- Before 8.0, customers needed to delete the WLAN and recreate it to change those values
- In 8.0 the change can be done anytime through GUI, CLI or SNMP
  See details in the slide notes



We Will Allow Changes to SSID and WLAN Profile Name

- Anytime the ProfileName or SSID is changed through the GUI or SNMP, internally the WLAN will be disabled and enabled back.
- When done via CLI, the Enable/Disable will have to be performed manually

```
(Cisco Controller) >config wlan ssid 1 newSSID
Please disable the wlan.

(Cisco Controller) >config wlan disable 1

(Cisco Controller) >config wlan ssid 1 newSSID

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

We Will Allow Changes to SSID and WLAN Profile Name

- For ascii-psk wlan, the pre-shared key is computed based on the ssid name and the base key – which is the key fed in “config wlan security wpa akm psk set-psk ascii <key> <wlan-id>” CLI.
- This key is not stored in clear text in the flash for security reasons and it is not possible to restore it from the PSK.
- When the ssid name is changed, the new PSK needs to be generated.
- For this reason, the change ssid config will be modified to query for the base key if the wlan is a psk wlan.

```
(Cisco Controller) >config wlan ssid 2 dhkpsknew2
Please enter PSK: ********
SSID Updated successfully

(Cisco Controller) >show wlan summary
Number of WLANs..................................... 2

WLAN ID  WLAN Profile Name / SSID                Status    Interface Name        PMIPv6 Mobility
-------  -----------------------------------     --------  --------------------  ---------------
2        dhkpsk / dhkpsknew2                     Disabled  management            none

(Cisco Controller) >
```

Ping From Dynamic Interfaces (Extended Ping)

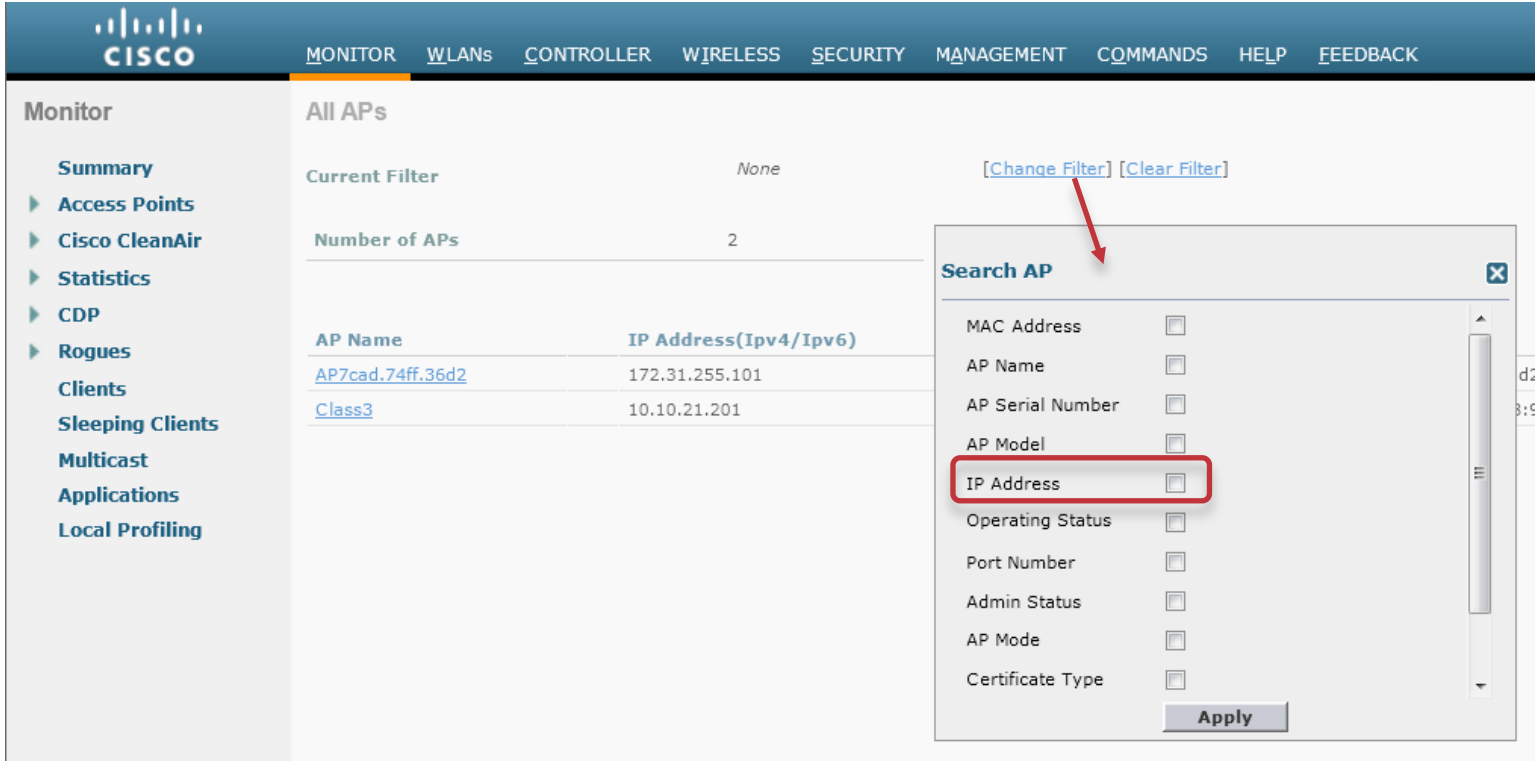
- This is a helpful troubleshooting tool
- Extended Ping options are available only through the CLI.
- The GUI continues to provide basic ping sourced from the management interface
  - In 7.6 you could use the <interface-name> argument only (no repeat count or packet size options)
  - Prior to 7.6, the ping was sourced from the management interface with no options:

```
(Cisco Controller) >ping 10.1.1.254 ?
[<interface-name>] [<repeat count[1-100]>] [<packet size[10-2000]>]
Enter interface name and/or repeat count(1-100) and/or packet size(10-2000).
Example:
(Cisco Controller) > ping 10.1.1.254 MyDynamicInt 10 1000
Send count=10, Receive count=10 from 10.1.1.254, Packet size = 1000
```

IP Address Displayed in the "*show ap summary*" + New Filter for AP IP Address in the GUI

```
(Cisco Controller) >(Cisco Controller) >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   Clients   DSE
Location
---------   ----- -----------------  -----------------  --------  -------  -----------  --------  -----------
8.0AP       2     AIR-CAP3602I-A-K9  44:d3:ca:42:57:a7   MyLab    US       10.40.27.18   0        [0 ,0 ,0 ]
```

IP Address Displayed in the *"show ap summary"* + New Filter for AP IP Address in the GUI



More Hardware & Performance Visibility

- Customers want more visibility into the performance of the WLC
- *Examples:* iowait, cpu, (cpu by system, by user), load per cpu, average load, etc...
- The following set of new "**show system …** " commands are added to 8.0:

```
(Cisco Controller) >show system ?
dmesg          Displays dmesg logs
interfaces     Displays information about the configured network interfaces
interrupts     Displays the number of interrupts
iostat         Displays CPU and input/output statistics for devices
meminfo        Displays system memory information
neighbours     Displays the IPv6 Neighbor Cache
netstat        Display system network stats
process        Displays process related information
route          Displays system routing table
slabs          Displays memory usage on slab level
timers         Display system timer info
top            Displays the cpu usage
vmstat         Displays system virtual memory statistics
```

See sample outputs in the slide notes

"*show run-config startup-commands*" (CSCui39251)

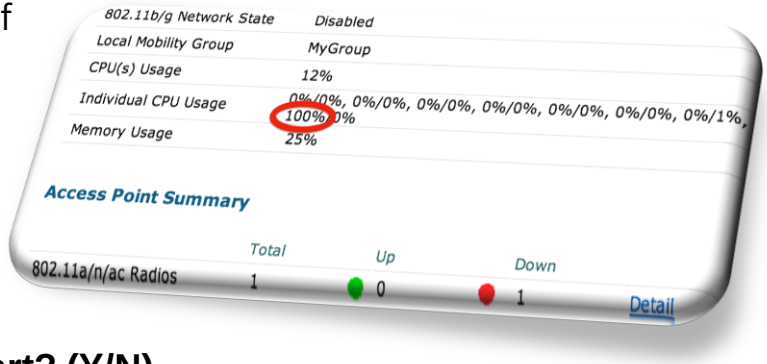
- A method to view the startup configuration
- The output can be used as recovery configuration (copy-and-paste ready)

```
(Cisco Controller) >show run-config ?

commands        Display list of configured commands on WLC.
startup-commands Display list of configured startup commands on WLC.
no-ap           Display running configuration of controller without AP configuration.
<cr>            Display running configuration of controller.

(Cisco Controller) >show run-config startup-commands
# WLC Config Begin <Sun Jun  1 01:44:44 2014>
config network rf-network-name none
config network webmode enable
config network telnet enable
config network multicast mode multicast 239.0.0.4
config network multicast l2mcast disable service-port
config network multicast l2mcast disable virtual
config location expiry tags 5
…/…
```

Here, console pauses for about 60s

"*show run-config startup-commands*"

- Same output as that uploaded using "**`transfer upload datatype config`**"
- Usage considerations:
  - The command is CPU intensive, and will temporarily render both GUI and CLI irresponsive for a brief period of time *(up to 60sec in test lab environment)*
  - However, the impact was localized to one CPU *(out of 8)*, and it did not appear to impact client traffic or ping response time from the WLC (*not an official statement)*
  - The following confirmation message should appear after entering the command:



This may take some time. Are you sure you want to start? (Y/N)

AP CLI to configure mode (mesh, local)

Fun Fact:

5% of the *Indoor* APs that we ship are ordered with the *Mesh* software option

- Also, with our Outdoor APs supporting both ***Local*** and ***Bridge*** *(mesh)* modes, there is a chance that some may inadvertently be configured in the wrong mode
- Traditionally, an AP in Bridge mode needs to first join a WLC that is configured with the proper AP MAC address in its Auth-list before you can change that AP's mode
- *In 8.0 we are introducing 2 new simple, documented, TAC supported AP commands:*

***capwap ap mode local*† & *capwap ap mode bridge*†**

†*This command will cause the AP to reload*

AP CLI to Configure Mode (Cont.) – Usage Considerations

- Local mode APs may ship with a smaller (…-**rcvk9w8**-…) image that does ***Not*** contain radio firmware
- Before switching an AP from Local to Bridge mode ensure that the AP has an image with full radio support (…-**k9w8**-…), and that the AP MAC address has been added to the WLC

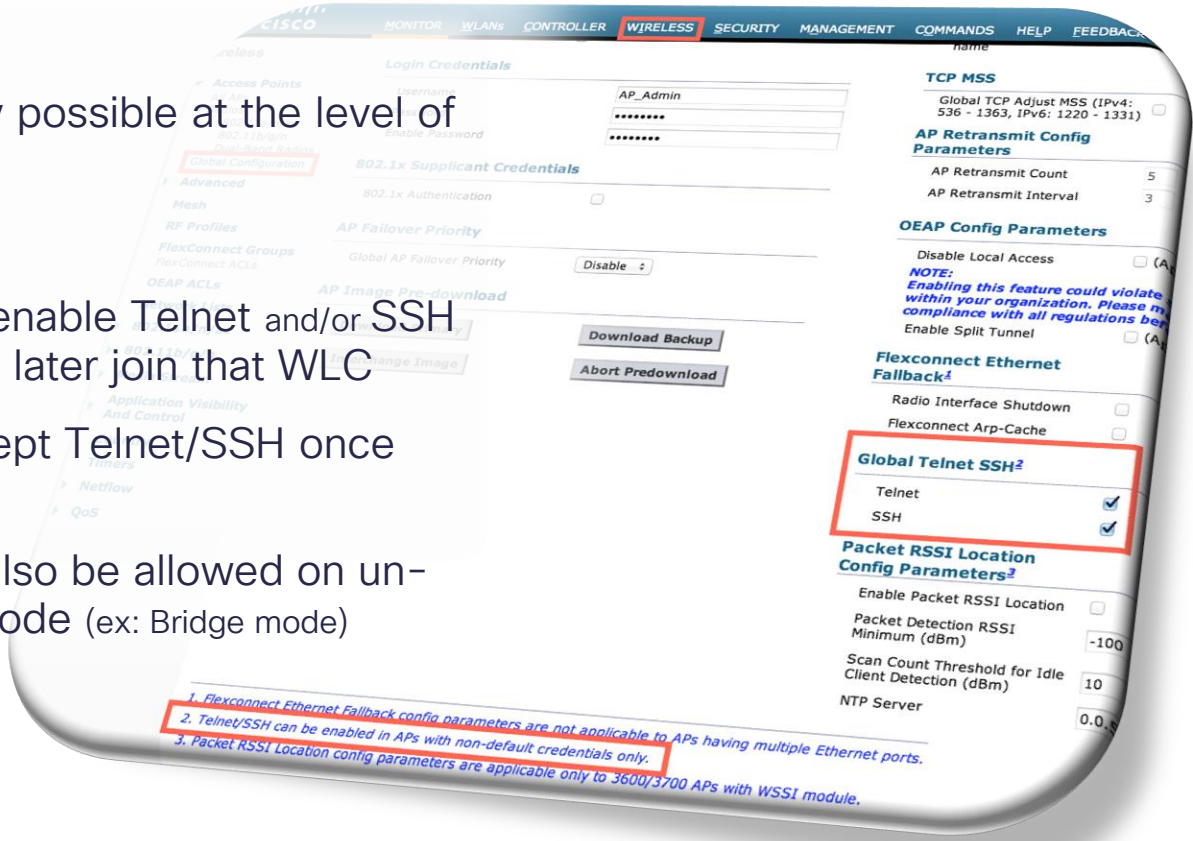
AP Telnet & SSH Enhancements

Before 8.0:

- Enabling Telnet or SSH was only possible at the level of the individual AP

In 8.0:

- You have the option to globally enable Telnet and/or SSH for all APs that are joined, or will later join that WLC
- APs ***out of the box*** will now accept Telnet/SSH once they obtain an IP address
- Once enabled, Telnet/SSH will also be allowed on un-joined APs regardless of their mode (ex: Bridge mode)



AP Telnet & SSH Enhancements – Conditions Apply

- AP code changes will also include accepting telnet/SSH connectivity once mesh AP gets an IP and storing the specifically/globally configured info within the AP (will save that truck roll to access the AP via its console!)
- After joining a WLC, any AP with default credentials (cisco/cisco) would be prevented from enabling telnet/SSH. So it is mandatory to have a non-default credential to enable telnet/SSH.
- A per-AP configured telnet/SSH setting will not be overridden by the controller's global telnet/SSH setting. This is especially when an AP joins a new WLC or when a WLC is configured with a global telnet/SSH setting.
- However, a new provision was added to easily remove this per-AP setting via the CLI "**config ap** [telnet|SSH] **default** <ap_name>". Once this command is executed, now the global config (if any) will be applied on that AP.

AP Telnet & SSH Enhancements – Configuration

- Before 8.0:

```
(Cisco Controller) >config ap [telnet|SSH] [enable|disable] <ap_name>
```

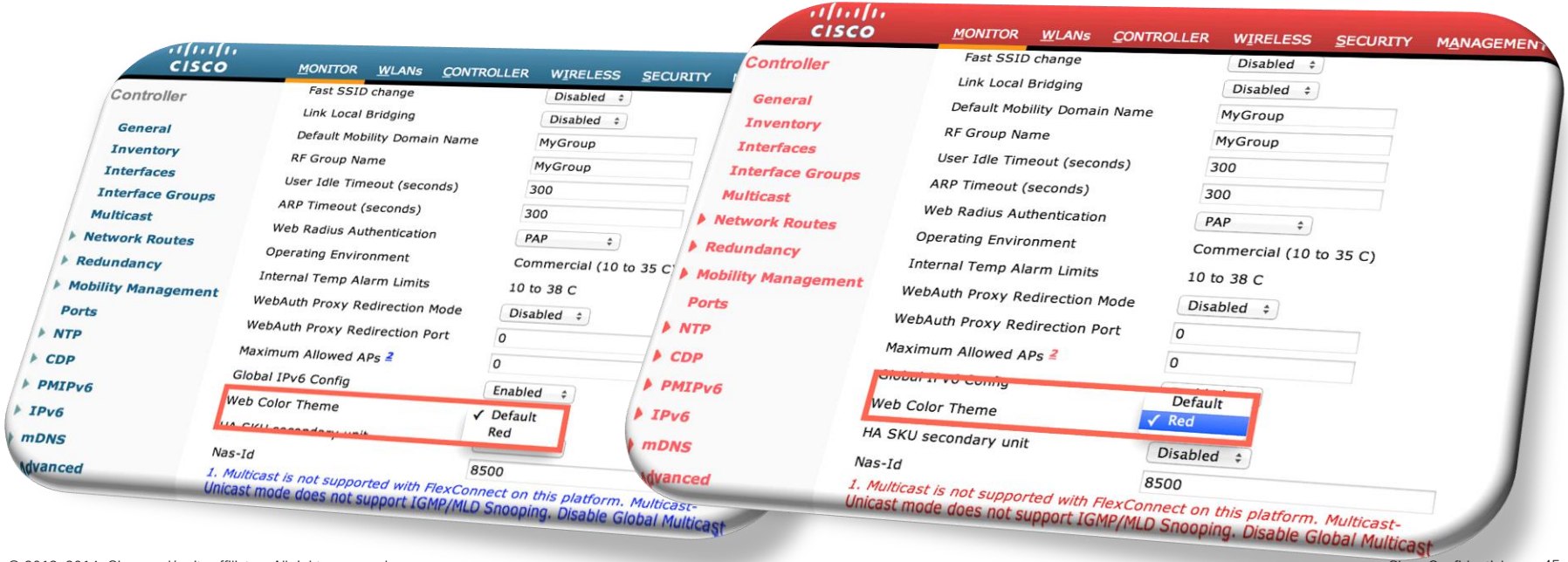
- 8.0:

```
(Cisco Controller) >config ap [telnet|SSH] [enable|disable|default] [all |<ap_name>]
```

  - Keyword “default” is used to reset the Telnet/SSH settings on individual APs (that is, global config configuration is applied to that AP)
  - The Keyword “all” is used to globally alter the Telnet/SSH settings for all APs joined, or will later join that WLC

Alternate Color Scheme for the WLC GUI

- A NOC operator may have multiple GUIs open at the same time
- To minimize human error, some customers standardized on GUI color schemes to drastically identify production vs. lab equipment, and wanted a similar option for the WLC GUI

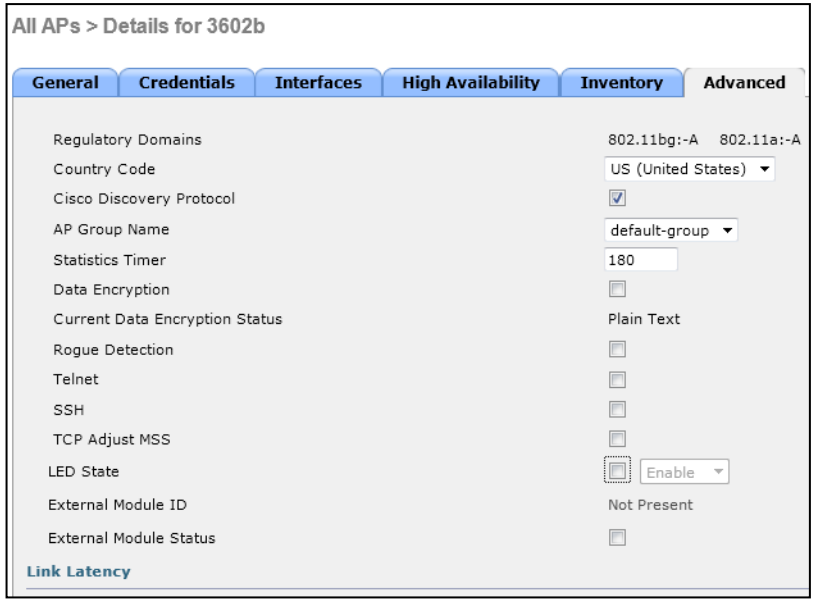


Flash AP LEDs via SNMP and GUI

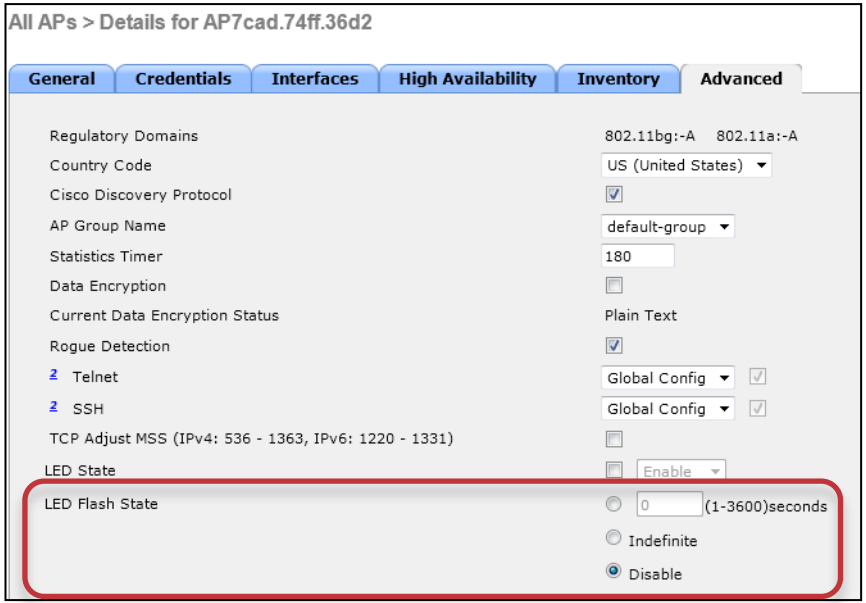
- You can flash the AP LED from the WLC CLI (that is not new)
- New led-flash items are added to the MIB
- You can also flash your AP LEDs from the GUI (see next slide)

Flash AP LEDs via SNMP and GUI, Cont.

- You can also flash your AP LEDs from the GUI



7.6



8.0

show client detail: Will Display WLAN Name & Profile

...Because it will save you referencing a long list of WLAN IDs when troubleshooting a client join problem!

Before 8.0

```
(7.3_WLC) >show client detail 98:fc:

Client MAC Address..............................  98:fc:11:be:69:c1
Client Username ................................  N/A
AP MAC Address..................................  10:bd:18:6b:27:c0
AP Name.........................................  7.3AP
Client State....................................  Associated
Client NAC OOB State............................  Access
Wireless LAN Id.................................  2
Hotspot (802.11u)...............................  Not Supported
BSSID...........................................  10:bd:18:6b:27:c1
Connected For ..................................  39 secs
Channel.........................................  6
IP Address......................................  Unknown
Gateway Address.................................  Unknown
Netmask.........................................  Unknown
Association Id..................................  1
Authentication Algorithm........................  Open System
Reason Code.....................................  1
Status Code.....................................  0
```

After 8.0!

```
(8.0_WLC) >show client detail 98:fc:

Client MAC Address..............................  98:fc:11:be:69:c1
Client Username ................................  N/A
AP MAC Address..................................  64:d9:89:46:9e:f0
AP Name.........................................  8.0AP
AP radio slot Id................................  0
Client State....................................  Associated
Client User Group...............................
Client NAC OOB State............................  Access
Wireless LAN Id.................................  2
Wireless LAN Network Name (SSID)................  enLight
Wireless LAN Profile Name.......................  enLight_Profile
Hotspot (802.11u)...............................  Not Supported
BSSID...........................................  64:d9:89:46:9e:f1
Connected For ..................................  41 secs
Channel.........................................  1
IP Address......................................  Unknown
Gateway Address.................................  Unknown
Netmask.........................................  Unknown
Association Id..................................  1
Authentication Algorithm........................  Open System
Reason Code.....................................  1
Status Code.....................................  0
```

AP Name Change and Join Stats

- In 7.6 and before, you can change an AP name (okay, nothing new here)
- Issue is that the show ap join stats shows the APs that joined as they were named when they joined
  - So your AP with its new name appears with its old name in the join stats:

```
(Cisco Controller) >config ap name AP3502I-A-K9-1 APGrp-1-AP3502I-A-K9-1
(Cisco Controller) >show ap summary
Number of APs..................................... 1
Global AP User Name............................... Cisco
Global AP Dot1x User Name......................... Not Configured
AP Name             Slots  AP Model              Ethernet MAC      Location      Country  IP Address Clients
------------------  -----  --------------------  -----------------  ----------------
AP3502I-A-K9-1  2     AIR-CAP3502I-A-K9     d4:8c:b5:4e:97:f6  default location  US   9.2.17.100   0

(Cisco Controller) >show ap join stats summary all
Number of APs............................................ 1
Base Mac             AP EthernetMac       AP Name                 IP Address         Status
64:d8:14:6f:42:c0    d4:8c:b5:4e:97:f6    APGrp-1-AP3502I-A-K9-1    9.2.17.100         Joined
```

AP Name Change and Join Stats, Cont.

- This is improved in 8.0, show AP join stats show the new name (and the new name is also sent to the HA WLC if applicable):

```
(Cisco Controller) >config ap name AP3502I-A-K9-1 APGrp-1-AP3502I-A-K9-1
(Cisco Controller) >show ap summary
Number of APs..................................... 1
Global AP User Name............................... Cisco
Global AP Dot1x User Name......................... Not Configured
AP Name             Slots  AP Model              Ethernet MAC      Location      Country  IP Address Clients
------------------  -----  --------------------  -----------------  ----------------
AP3502I-A-K9-1  2     AIR-CAP3502I-A-K9     d4:8c:b5:4e:97:f6  default location  US   9.2.17.100   0

(Cisco Controller) >show ap join stats summary all
Number of APs............................................ 1
Base Mac             AP EthernetMac       AP Name                 IP Address         Status
64:d8:14:6f:42:c0    d4:8c:b5:4e:97:f6    AP3502I-A-K9            9.2.17.100         Joined
```

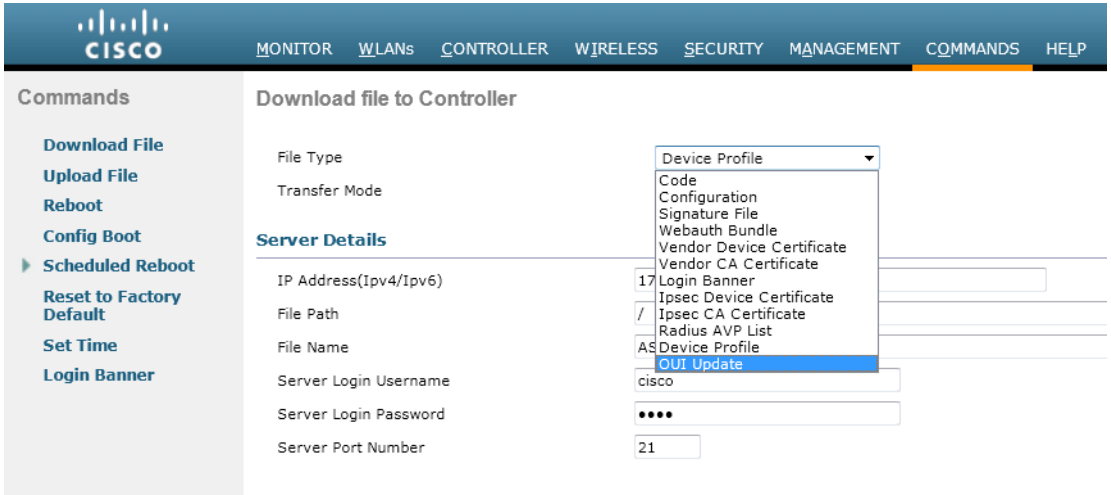
Debug Client Shows AP Name

- In 7.6 and before, debug client shows many things… but not the client AP:
  - AP name is now shown:

```
(5500-1) >*apfMsConnTask_3: Aug 13 11:52:26.374: 00:40:96:b8:d4:b1 Adding mobile on LWAPP AP
58:bc:27:93:4b:c0(1)

*apfMsConnTask_3: Aug 13 11:52:26.374: 00:40:96:b8:d4:b1 Association received from mobile on BSSID
58:bc:27:93:4b:ce AP APf866.f267.7d1b
```

Local Profiling – Update OUI / Device Profiles List

- In 7.6, you can do local profiling…based on client MAC address and behavior (DHCP, HTTP):
- New devices come to the market all the time, and their OUI may not be known to the WLC… and you do not want to wait for the next code release to add them
- In 8.0, you can download an additional OUI list (for local profiling):



Local Profiling – Update OUI List

```
(Cisco Controller) >transfer download datatype ?
…/…
oui-update     Download an OUI Update file to the system.

(Cisco Controller) >transfer download start
Mode..............................................  FTP
Data Type.........................................  OUI Update
FTP Server IP.....................................  9.1.0.150
FTP Server Port...................................  21
FTP Path..........................................  /areef/
FTP Filename......................................  oui.txt
FTP Username......................................  cisco
FTP Password......................................  *********

Starting tranfer of OUI Update
This may take some time.
Are you sure you want to start? (y/N) y

FTP OUI Update transfer starting.
FTP receive complete... Loading OUI Update.
Transferring file to the Standby Controller
Transfer Download complete on Active & Standby
```

Local Profiling – Update OUI List

```
(Cisco Controller) >show profiling oui-string summary

Number of OUI Strings Available: 573
OUI            OUI-String
==========     ==================================================================
 0x00000003    XEROX CORPORATION
 0x00000009    XEROX CORPORATION
 0x000002ba    CISCO SYSTEMS, INC.
 0x000006d6    CISCO SYSTEMS, INC.
 0x00000831    CISCO SYSTEMS, INC.
 0x000008a4    CISCO SYSTEMS, INC.
 0x00000b6b    WISTRON NEWEB CORP.
 0x000015e8    NORTEL
 0x000016b8    SONY ERICSSON MOBILE COMMUNICATIONS
 0x000016c7    CISCO SYSTEMS, INC.
 0x00001956    CISCO SYSTEMS, INC.
 0x00001b7a    NINTENDO CO., LTD.
 0x00001b90    CISCO SYSTEMS, INC.
 0x00001d45    CISCO SYSTEMS, INC.
 0x00001d4f    APPLE
 0x00001daf    NORTEL
 0x00001e1f    NORTEL
 0x000007eb    CISCO SYSTEMS, INC.
--More-- or (q)uit
```

Local Profiling – Update OUI List

```
(Cisco Controller) >show profiling oui-string sum

Number of OUI Strings Available: 573
OUI           OUI-String
==========    ==================================
 0x00000003   XEROX CORPORATION
 0x00000009   XEROX CORPORATION
 0x000002ba   CISCO SYSTEMS, INC.
 0x000006d6   CISCO SYSTEMS, INC.
 0x00000831   CISCO SYSTEMS, INC.
 0x000008a4   CISCO SYSTEMS, INC.
 0x00000b6b   WISTRON NEWEB CORP.
 0x000015e8   NORTEL
 0x000016b8   SONY ERICSSON MOBILE COMMUNICATIONS
 0x000016c7   CISCO SYSTEMS, INC.
 0x00001956   CISCO SYSTEMS, INC.
 0x00001b7a   NINTENDO CO., LTD.
 0x00001b90   CISCO SYSTEMS, INC.
 0x00001d45   CISCO SYSTEMS, INC.
 0x00001d4f   APPLE
 0x00001daf   NORTEL
 0x00001e1f   NORTEL
 0x000007eb   CISCO SYSTEMS, INC.
--More-- or (q)uit
```

Before

```
(Cisco Controller-Standby) >show profiling oui-string summary

Number of OUI Strings Available: 2064
OUI           OUI-String
==========    ==========================================================
 0x00000003   XEROX CORPORATION
 0x00000009   XEROX CORPORATION
 0x000002ba   CISCO SYSTEMS, INC.
 0x000006d6   CISCO SYSTEMS, INC.
 0x00000831   CISCO SYSTEMS, INC.
 0x000008a4   CISCO SYSTEMS, INC.
 0x00000b6b   WISTRON NEWEB CORP.
 0x000015e8   NORTEL
 0x000016b8   SONY ERICSSON MOBILE COMMUNICATIONS
 0x000016c7   CISCO SYSTEMS, INC.
 0x00001956   CISCO SYSTEMS, INC.
 0x00001b7a   NINTENDO CO., LTD.
 0x00001b90   CISCO SYSTEMS, INC.
 0x00001d45   CISCO SYSTEMS, INC.
 0x00001d4f   APPLE
 0x00001daf   NORTEL
 0x00001e1f   NORTEL
 0x00001f16   WISTRON CORPORATION
--More-- or (q)uit
```

After

Local Profiling – Update OUI List

- OUI file is provided by the BU, based on http://standards.ieee.org/develop/regauth/oui/oui.txt

```
Generated: Mon, 09 Jun 2014 05:00:03 -0400

OUI/MA-L            Organization
company_id                Organization
                    Address


00-00-00    (hex)         XEROX CORPORATION
000000      (base 16)           XEROX CORPORATION
                    M/S 105-50C
                    800 PHILLIPS ROAD
                    WEBSTER NY 14580
                    UNITED STATES

00-00-01    (hex)         XEROX CORPORATION
000001      (base 16)           XEROX CORPORATION
                    ZEROX SYSTEMS INSTITUTE
                    M/S 105-50C 800 PHILLIPS ROAD
                    WEBSTER NY 14580
                    UNITED STATES

00-00-02    (hex)         XEROX CORPORATION
000002      (base 16)           XEROX CORPORATION
                    XEROX SYSTEMS INSTITUTE
                    M/S 105-50C 800 PHILLIPS ROAD
                    WEBSTER NY 14580
                    UNITED STATES
```

Latest OUI (early June 2014)

oui.txt

Local Profiling – Update Profile List

```
(Cisco Controller) >transfer download datatype device-profile

(Cisco Controller) >transfer download filename dc_embedded_profiles.xml
(Cisco Controller) >transfer download start
Mode..............................................  FTP
Data Type.........................................  Device Profile
FTP Server IP.....................................  9.1.0.150
FTP Server Port...................................  21
FTP Path..........................................  /areef/
FTP Filename......................................  dc_embedded_profiles.xml
FTP Username......................................  cisco
FTP Password......................................  *********

Starting tranfer of Device profiles
This may take some time.
Are you sure you want to start? (y/N) y
FTP Device Profile transfer starting.
FTP receive complete... Loading Device profiles.
Transferring file to the Standby Controller
Standby - Standby receive complete... Loading Device profiles.
Standby - Updated the Device Profiles successfully.
```

Local Profiling – Update Profile List

```
(Cisco Controller) >show profiling policy summary

Number of Builtin Classification Profiles: 88
ID   Name
==== ==============================================
   0 Android
   1 Apple-Device
   2 Apple-MacBook
   3 Apple-iPad
   4 Apple-iPhone
   5 Apple-iPod
   6 Aruba-Device
   7 Avaya-Device
   8 Avaya-IP-Phone
   9 BlackBerry
  10 Brother-Device
  11 Canon-Device
  12 Cisco-Device
  13 Cisco-IP-Phone
  14 Cisco-IP-Phone-7945G
  15 Cisco-IP-Phone-7975
  16 Cisco-IP-Phone-9971
  17 Cisco-DMP
--More-- or (q)uit
```

Before

```
(Cisco Controller) >show profiling policy summary

Number of Builtin Classification Profiles: 156
ID   Name                                                Parent Min CM Valid
==== ================================================== ====== ====== =====
   0 Android                                              None     30   Yes
   1 Android-Amazon-Kindle                                   0     40   Yes
   2 Android-Asus                                            0     30   Yes
   3 Android-Google                                          0     40   Yes
   4 Android-HTC                                             0     40   Yes
   5 Android-LG                                              0     40   Yes
   6 Android-Micromax                                        0     40   Yes
   7 Android-Motorola                                        0     40   Yes
   8 Android-Motorola-Tablet                                 7     40   Yes
   9 Android-Nook                                            0     40   Yes
  10 Android-Samsung                                         0     40   Yes
  11 Android-Samsung-Galaxy-Note                            10     40   Yes
  12 Android-Samsung-Galaxy-Phone                           10     40   Yes
  13 Android-Samsung-Galaxy-Tablet                          10     40   Yes
  14 Android-Sony-Ericsson                                   0     40   Yes
  15 Android-Sony-Ericsson-Phone                            14     40   Yes
  16 Android-Sony-Ericsson-Tablet                           14     40   Yes
  17 Apple-Device                                         None     10   Yes
--More-- or (q)uit
```

After

Local Profiling – Update Profile List

- Profile list file is provided by the BU, based on new profiles available (for new products):

```
<Policy description="Policy for 3Com-Device" isEnabled="true"
matchingIdentityGroup="false" minimumCertaintyMetric="5"
name="3Com-Device" version="0">
<PolicyRules>
<PolicyRule certaintyFactor="5" name="3Com-DeviceRule1"/>
</PolicyRules>
</Policy>
<Policy description="Policy for Aerohive-Device" isEnabled="true"
matchingIdentityGroup="false" minimumCertaintyMetric="10"
name="Aerohive-Device" version="0">
<PolicyRules>
<PolicyRule certaintyFactor="10" name="Aerohive-DeviceRule1"/>
</PolicyRules>
</Policy>
```

Example profile file

profiler_policies.xml

Local Profiling – Update OUI / Profile Troubleshooting

```
(Cisco Controller-Standby) >debug transfer all enable

(Cisco Controller-Standby) >*HAPeerToPeerCommTask: May 15 14:29:06.335: [SS] Started receiving file on
Standby
*TransferTask: May 15 14:29:07.809: [SS] Memory overcommit policy changed from 0 to 1

*TransferTask: May 15 14:29:07.809: [SS] RESULT_STRING: Standby receive complete... Loading OUI Update.

*TransferTask: May 15 14:29:07.809: [SS] RESULT_CODE:24


(Cisco Controller-Standby) >sh*TransferTask: May 15 14:29:25.290: [SS] RESULT_STRING: Updated the OUI List
successfully.


*TransferTask: May 15 14:29:25.290: [SS] RESULT_STRING: OUI Update installed.


*TransferTask: May 15 14:29:25.291: [SS] RESULT_CODE:11

*TransferTask: May 15 14:29:25.291: [SS] Memory overcommit policy restored from 1 to 0
```

802.11v Support – Apple

- When the iOS device (iPhone, iPad) is put to sleep (either because the user clicks the ON/OFF button on the device or the device is idle for some time), processors are also put to sleep. But the radio needs to wake up periodically:
  1. Beacon Frame Processing: device periodically wakes up to receive an 802.11 beacon so that it can remain in time synchronization with the AP.
  2. DTIM Multicast: device needs to wake up every DTIM period to check if there are any multicast frames buffered at the AP and if so, wait to receive these frames.
  3. Sending keep-alives to the AP: The Cisco WLC maintains an idle timer for each associated client. The Apple device periodically needs to send a NULL frame to the WLC to ensure the WLC does not time it out and disconnect the client.
  4. Other proprietary reasons to do with Apple protocols like Bonjour and iTunes Sync Over Wi-Fi.

802.11v Support – Apple

- Three activities consume considerably more energy than periodic Beacon and DTIM frame decoding done by the radio alone:
  a) Transmitting the NULL frame;
  b) PR1 staying awake to receive buffered multicast frames; and
  c) Turning on the CPU to process the application payload of a received packet.
- Activity (a) needs to be done by the device to maintain its association with the AP. Apple devices typically use some conservative idle period to ensure that they remain connected to a wide variety of access points by different manufacturers. Activities (b) and (c) need to be done if there is considerable multicast traffic in the air.

802.11v Support – Apple

- The goal of 802.11v in 8.0 is to develop algorithms that minimize the amount of time the device does the above three activities, thereby extending its battery life.
- The IEEE Standard 802.11v-2011 outlines several mechanisms for saving power for battery-operated devices.
- 8.0 implements two of them:
  - **Directed Multicast Service (DMS):** Ensures that an iOS device does not need to wake up to receive the iTunes Magic Packet (sent as a multicast)
  - **BSS Max Idle Period:** Ensures that the device does not wake up as often to unnecessarily send the keep-alive NULL frames.

802.11v Support – Apple – DMS

- In standard 802.11, in order to receive broadcast and multicast frames a station must wake up every DTIM interval and stay awake until all broadcast/multicast frames have been received. In particular for Apple devices, the host processor must be woken up to process the payload of the multicast frame.
- DMS allows a client to request the AP to convert multicast frames that match a certain traffic classifier into unicast frames for the client. This request can be sent either as a DMS Request Information Element in the Association/Reassociation Request frame or explicitly via a DMS Request Action Frame after the client has completed association.
- If the AP accepts the DMS Request, all multicast frames matching the traffic classifier specified in the DMS Request will be unicasted directly to the client as an AMSDU. The original multicast frame will still be transmitted as described in the preceding paragraph for the benefit of those clients that do not support or request for DMS.
- With DMS, the device need not wake up to process any multicast packet, as it will get the unicast copy upon waking up.

802.11v Support – Apple – BSS MAX Idle Period

- The BSS Max Idle period is a time period during which the access point does not disassociate a station (STA) due to non-receipt of frames from that STA.
  - Prior to 11v, this client idle timeout was a parameter configured on a per WLAN basis by the network administrator on the WLC. The client had no standardized way of knowing this value, and hence client driver manufacturers typically assume conservative (low) values of this timer and make sure to send NULL frames to maintain their association status with the AP.
  - With BSS Max Idle and 11v, the value of this timer is now advertised as an Information Element in the Association/Reassociation Response frame. This allows a client to immediately know the maximum time it can remain idle without transmitting any frame to the AP.
  - Protected Keep-Alive mode: With this mode, only authenticated frames (encrypted with RSN information) are accepted from the client to reset the BSS Max Idle period counter. Without protected mode, any data or management frame (encrypted or unencrypted) sent by the client will reset the idle timer for the client.

802.11v Support – Apple – BSS MAX Idle Period

- The BSS Max Idle period is seen in the AP association and reassociation responses:

```
⊟ IEEE 802.11 Association Response, Flags: ........C
    Type/Subtype: Association Response (0x01)
  ⊞ Frame Control Field: 0x1000
    .000 0000 0011 1100 = Duration: 60 microseconds
    Receiver address: Apple_cc:e6:2e (e0:b9:ba:cc:e6:2e)
    Destination address: Apple_cc:e6:2e (e0:b9:ba:cc:e6:2e)
    Transmitter address: Cisco_db:ce:fc (a8:0c:0d:db:ce:fc)
    Source address: Cisco_db:ce:fc (a8:0c:0d:db:ce:fc)
    BSS Id: Cisco_db:ce:fc (a8:0c:0d:db:ce:fc)
    Fragment number: 0
    Sequence number: 2945
  ⊞ Frame check sequence: 0xdf680018 [correct]
⊟ IEEE 802.11 wireless LAN management frame
  ⊟ Fixed parameters (6 bytes)
    ⊞ Capabilities Information: 0x0011
      Status code: Successful (0x0000)
      ..00 0000 0000 0001 = Association ID: 0x0001
  ⊟ Tagged parameters (93 bytes)
    ⊞ Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    ⊞ Tag: HT Capabilities (802.11n D1.10)
    ⊞ Tag: HT Information (802.11n D1.10)
    ⊟ Tag: BSS Max Idle Period
        Tag Number: BSS Max Idle Period (90)
        Tag length: 3
        BSS Max Idle Period (1000 TUs): 300
        .... ...0 = BSS Max Idle Period Options: Protected Keep-Alive Required: 0
    ⊞ Tag: Vendor Specific: Microsof: WMM/WME: Parameter Element
```

802.11v Support – Apple – BSS MAX Idle Period

- The BSS Max Idle period is configurable from the CLI or GUI:

WLANs > Edit 'Mynet'

General | Security | QoS | Policy-Mapping | Advanced

Client Exclusion [2] — Enabled — 60 Timeout Value (secs)

Maximum Allowed Clients [8] — 0

Static IP Tunneling [11] — Enabled

Wi-Fi Direct Clients Policy — Disabled

Maximum Allowed Clients Per AP Radio — 200

Clear HotSpot Configuration — Enabled

Client user idle timeout(15-100000) —

Client user idle threshold (0-10000000) — 0 Bytes

Radius NAI-Realm —

default

WLANs > Edit 'Mynet'

General | Security | QoS | Policy-Mapping | Advanced

Client Exclusion [2] — Enabled — 60 Timeout Value (secs)

Maximum Allowed Clients [8] — 0

Static IP Tunneling [11] — Enabled

Wi-Fi Direct Clients Policy — Disabled

Maximum Allowed Clients Per AP Radio — 200

Clear HotSpot Configuration — Enabled

Client user idle timeout(15-100000) — 300 Timeout Value (secs)

802.11v Support – Apple – BSS MAX Idle Period

- The BSS Max Idle period is configurable from the CLI or GUI:

```
(Cisco Controller) >config wlan bssmaxidle ?

disable        Disables BSS Max Idle Processing on a WLAN.
enable         Enables BSS Max Idle Processing on a WLAN.
protected-mode Configures Protected Mode for BSS Max Idle Processing on a WLAN.

(Cisco Controller) >config wlan bssmaxidle protected-mode ?

disable        Disables Protected Mode for BSS Max Idle processing on a WLAN.
enable         Enables Protected Mode for BSS Max Idle processing on a WLAN.
(Cisco Controller) >config wlan bssmaxidle enable ?

<WLAN id>      Enter WLAN Identifier between 1 and 16.

(Cisco Controller) >config wlan bssmaxidle enable 3
```

802.11v Support – Apple - DMS

- The DMS exchange can be seen in Association request/response exchanges, or in action frames post-association
- The i-device sends a DMS add request action frame a few seconds after it goes to sleep and a DMS delete (remove) just after it wakes up
- IOS 7 devices (and later) support DMS

1	0.000000	c0:63:94:9f:30:da	34:a8:4e:3a:4a:30	802.11	62	-56	-56	dBm	1.0	DMS Request
2	0.000019	34:a8:4e:3a:4a:30	c0:63:94:9f:30:da	802.11	64	-49	-49	dBm	5.5	DMS Response
3	24.056879	c0:63:94:9f:30:da	34:a8:4e:3a:4a:30	802.11	83	-56	-56	dBm	1.0	DMS Request
4	438.147666	c0:63:94:9f:30:da	34:a8:4e:3a:4a:30	802.11	83	-54	-54	dBm	1.0	DMS Request
5	438.149546	c0:63:94:9f:30:da	34:a8:4e:3a:4a:30	802.11	83	-55	-55	dBm	1.0	DMS Request
6	438.150804	34:a8:4e:3a:4a:30	c0:63:94:9f:30:da	802.11	64	-50	-50	dBm	5.5	DMS Response
7	522.743138	c0:63:94:9f:30:da	34:a8:4e:3a:4a:30	802.11	62	-49	-49	dBm	1.0	DMS Request
8	522.744191	34:a8:4e:3a:4a:30	c0:63:94:9f:30:da	802.11	64	-50	-50	dBm	5.5	DMS Response

802.11v Support – Apple - DMS

- The DMS behavior is configurable from the CLI (no GUI):

```
(Cisco Controller) >config wlan disable 3

(Cisco Controller) >config wlan dms ?

disable         Disables DMS Processing on a WLAN.
enable          Enables DMS Processing on a WLAN.

(Cisco Controller) >config wlan dms enable 3

(Cisco Controller) >config wlan enable 3
```

802.11v Support – Apple – Verification

- Both BSS Max Idle period and DMS Multicast are visible from *show wlan <id>*:

```
(Cisco Controller) >show wlan 4


WLAN Identifier.................................. 4
Profile Name..................................... Mynet
…/…
802.11v Directed Multicast Service............... Disabled
802.11v BSS Max Idle Service..................... Enabled
802.11v BSS Max Idle Protected Mode.............. Disabled
DMS DB is empty
```

Default values

802.11v Support – Apple - Troubleshooting

- 802.11v introduces new debug commands:

```
(Cisco Controller) >debug 11v ?

all             Configures debug of all 802.11v events
detail          Configures debug of 802.11v detail
errors          Configures debug of 802.11v errors
events          Configures debug of 802.11v events
optimization    Configures debug of 802.11v Optimizations
simulation      Configures debug of 802.11v for simulation data


(Cisco Controller) >*apfReceiveTask: Jun 30 22:14:04.568: Sent Deauthenticate to STA:
e0:b9:ba:cc:e6:2e on BSSID: a8:0c:0d:db:ce:f0, slotId: 1, vapId: 4
*apfReceiveTask: Jun 30 22:14:04.569: apfMsExpireMobileStation: Calling Delete STA from
DMS DB by MAC Address
```

Client disconnected

802.11v Support – Apple - Limitation

- 2500 and vWLC are NOT supported

802.11r Mixed-Mode Support

- Remove the restriction of creating separate WLAN for 802.11r support
  - Enable FT and AKM as 802.1x <<< for 802.1x Client
  - Enable FT and AKM as PSK <<< for non-802.1x Client
- Clients
  - iPhone, iPad, Android, iPod, Linksys, AnyConnect, IntelPro, 7921, 9971, D-Link supported
  - Netgear, ADU, Juniper Odyssey not supported
- OS
  - Windows XP - AnyConnect, Win7 – default and AnyConnect, Win8 – default and AnyConnect supported
  - MAC OS X - version 10.7, 10.8, 10.9 not supported

802.11r Mixed-Mode Support

Make/NIC model	Driver Version	Support
iPad	iOS 6	✔
iPad Air	iOS 7.0	✔
iPod	iOS 6.1.3	✔
Android	Samsung Galaxy S4	✔
D Link		✔
Linksys AE2500	5.100.68.46 (6/10/2011)	✔
MAC	OS X 10.9.2	✔
Cisco 7921		✔
Cisco 9971		✔
MAC	OS X 10.9	✗
MAC	OS X 10.7.4	✗
Netgear	6.30.145.30 (03/26/2013)	✗
ADU	4.3.0.305	✗
Juniper Odyssey		✗

Removing the restriction of creating separate WLAN for 802.11r support

Specified non-11r clients can join 802.11r enabled SSID

Worksheet

Why are Some Clients “Not Supported”

```
⊟ Tag: RSN Information
    Tag Number: RSN Information (48)
    Tag length: 20
    RSN Version: 1
  ⊞ Group Cipher Suite: 00-0f-ac (Ieee8021) AES (CCM)
    Pairwise Cipher Suite Count: 1
  ⊞ Pairwise Cipher Suite List 00-0f-ac (Ieee8021) AES (CCM)
    Auth Key Management (AKM) Suite Count: 1
  ⊞ Auth Key Management (AKM) List 00-0f-ac (Ieee8021) PSK
  ⊟ RSN Capabilities: 0x0028
      .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
      .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
      .... .... .... 10.. = RSN PTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GTKSA/STAKeySA (0x0002)
      .... .... ..10 .... = RSN GTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GTKSA/STAKeySA (0x0002)
      .... .... .0.. .... = Management Frame Protection Required: False
      .... .... 0... .... = Management Frame Protection Capable: False
      .... ..0. .... .... = PeerKey Enabled: False
```

Standard WPA2 PSK WLAN

Standard FT (WPA2 PSK) WLAN

```
⊟ Tag: RSN Information
    Tag Number: RSN Information (48)
    Tag length: 24
    RSN Version: 1
  ⊞ Group Cipher Suite: 00-0f-ac (Ieee8021) AES (CCM)
    Pairwise Cipher Suite Count: 1
  ⊞ Pairwise Cipher Suite List 00-0f-ac (Ieee8021) AES (CCM)
    Auth Key Management (AKM) Suite Count: 2
  ⊞ Auth Key Management (AKM) List 00-0f-ac (Ieee8021) PSK 00-0f-ac (Ieee8021) FT using PSK
  ⊟ RSN Capabilities: 0x0028
      .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
      .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
      .... .... .... 10.. = RSN PTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GTKSA/STAKeySA (0x0002)
      .... .... ..10 .... = RSN GTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GTKSA/STAKeySA (0x0002)
      .... .... .0.. .... = Management Frame Protection Required: False
      .... .... 0... .... = Management Frame Protection Capable: False
      .... ..0. .... .... = PeerKey Enabled: False
```

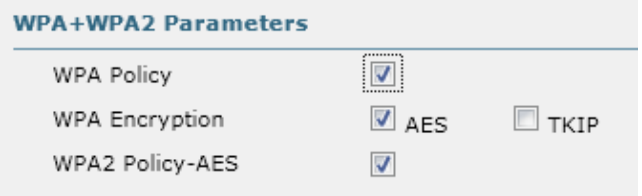
Why are Some Clients “Not Supported”

```
⊟ IEEE 802.11 wireless LAN management frame
  ⊞ Fixed parameters (12 bytes)
  ⊟ Tagged parameters (238 bytes)
    ⊞ Tag: SSID parameter set: Mixed
    ⊞ Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    ⊞ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    ⊞ Tag: Country Information: Country Code US, Environment Any
    ⊞ Tag: QBSS Load Element 802.11e CCA Version
    ⊞ Tag: Power Constraint: 3
    ⊞ Tag: HT Capabilities (802.11n D1.10)
    ⊟ Tag: RSN Information
        Tag Number: RSN Information (48)
        Tag length: 24
        RSN Version: 1
      ⊞ Group Cipher Suite: 00-0f-ac (Ieee8021) AES (CCM)
        Pairwise Cipher Suite Count: 1
      ⊞ Pairwise Cipher Suite List 00-0f-ac (Ieee8021) AES (CCM)
        Auth Key Management (AKM) Suite Count: 2
      ⊟ Auth Key Management (AKM) List 00-0f-ac (Ieee8021) PSK 00-0f-ac (Ieee8021) FT using PSK
        ⊞ Auth Key Management (AKM) Suite: 00-0f-ac (Ieee8021) PSK
        ⊞ Auth Key Management (AKM) Suite: 00-0f-ac (Ieee8021) FT using PSK
      ⊟ RSN Capabilities: 0x0028
          .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
          .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
          .... .... .... 10.. = RSN PTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GTKSA/STAKeySA (0x0002)
          .... .... ..10 .... = RSN GTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GTKSA/STAKeySA (0x0002)
          .... .... .0.. .... = Management Frame Protection Required: False
          .... .... 0... .... = Management Frame Protection Capable: False
          .... ..0. .... .... = PeerKey Enabled: False
```

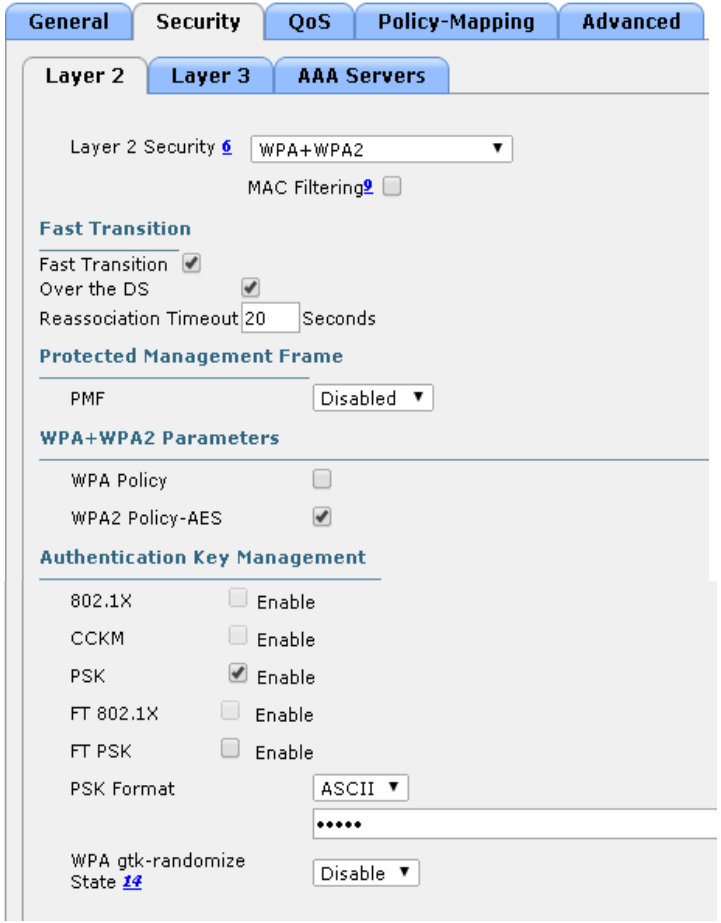
New Hybrid mode
Some client simply refuse to join a WLAN that shows FT… for those old misbehaving clients, you need to create a FT WLAN… and another, non-FT-only WLAN

Mixed-Mode Configuration

- Interface did not change, but no “or” logic anymore; you can set WPA2+FT in single WLAN



Notice that, in compliance with WFA new guidance, you cannot set WPA2/TKIP anymore



DHCP Relay SubOptions

(LinkSelect & VPNSelect)

DHCP Relay SubOptions Introduction

DHCP servers can hand out addresses on multiple subnets.

How do they know which subnet a client belongs to?

The DHCP server finds out about the client's subnet because the Relay Agent (ex: WLC) puts its own IP address facing that client into the "**GIADDR**" field of the DHCP packet.

Now the DHCP server uses that one **GIADDR** to do *TWO* things:

1. Determine the subnet of allocation
2. Use it to unicast the DHCP reply back to the **GIADDR**

Obviously this implies that the DHCP server <u>needs to have a route back</u> to the GIADDR

DHCP Relay *SubOption 5* – Why Do We Need It?

Sometimes it is not practical to make every dynamic interface network reachable from the DHCP server. Life would be easier if we had a way to send a subnet selection information separate from WLC's **GIADDR.**

That's where the '*Link/Subnet Selection Sub-Option*" – RFC 3527 comes in.

In 8.0, we are adding support for the WLC to include *Option 82*, **SubOption 5** when relaying the DHCPDiscover message from the client.

SubOption 5 defines the subnet, hence allowing the *GIADDR* to have only one job, being just the relay source! .... the address that the relay agent can be reached at.

We can also use SubOption *151* to tell the DHCP the *VPN-id* <u>*or*</u> the *VRF name* of that subnet.

Great, why *SubOption 152* then? Well, it tells us if the DHCP understood *SubOption 151*

DHCP Relay *SubOptions 151/152* – What is That for?

If knowing the subnet from Sub-Option 5 was not enough…

We can also use SubOption *151* to tell the DHCP the *VPN-id* *or* the *VRF name* of that subnet.

Cisco Network Registrar (CNR) supports multiple IP pools based on VPN-ids or VRF names.

The WLC can send the *VPN-id* or *VRF name* of the pool from which address has to be assigned.

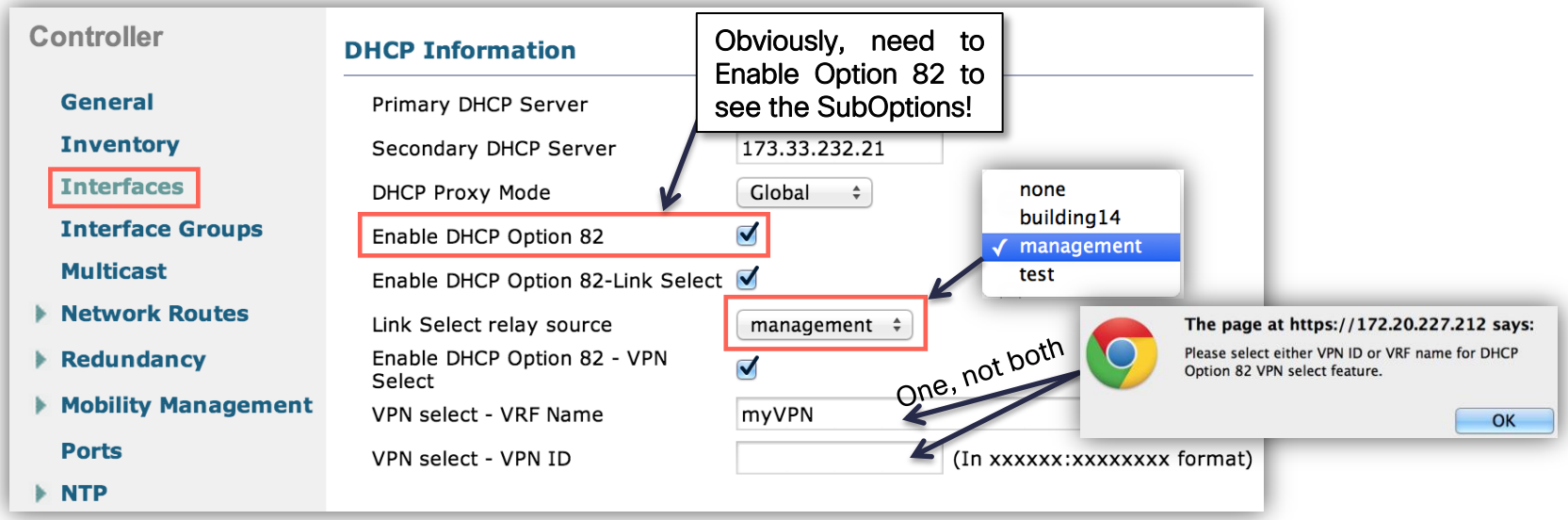
Great, why *SubOption 152* then? Well, it tells us if the DHCP understood *SubOption 151*†

Supporting The *DHCP Relay Agent Information SubOptions* will enable easy to operate, shared usage of a centralized DHCP server and result in cost savings.

†*More details in the slide notes*

Configuring *SubOptions 5, 151/152*

In the GUI, the configuration is done at the Interface level



Configuring *SubOptions 5, 151/152*

Linkselect

```
config interface dhcp dynamic-interface <intf-name> option-82  linkselect relaysrc <intf-name>
config interface dhcp dynamic-interface <intf-name> option-82  linkselect enable/disable
```

- <intf-name> is the name of a configured interface with an IP address.
- **linkselect enable** will be allowed only if **relaysrc** is set by a previous command

VPNselect:

```
config interface dhcp dynamic-interface <intf-name> option-82 vpnselect  vpnid <vpn-id>
-OR-
config interface dhcp dynamic-interface <intf-name> option-82  vpnselect  vrfname <vrf-name>
config interface dhcp dynamic-interface <intf-name> option-82 vpnselect enable/disable
```

- <vpn-id> is of the format oui:index … oui is between 0-7, index is between 0-15
- <vrf-name> is a string of length 7 octets
- Only one of **vrfname** OR **vpnid** is allowed to be configured. Configuring one will automatically clear the other only when vpnselect is disabled.

SubOptions 5, 151/152 Verification

```
(8500-1) >show interface detailed building14

…/…
DHCP Option 82..................................... Enabled
Remote ID format................................... apmac:ssid
Link Select Suboption.............................. Enabled
Relay Src Intf..................................... management
VPN Select Suboption............................... Enabled
VRF Name........................................... myVPN
IPv4 ACL........................................... Unconfigured
mDNS Profile Name.................................. Unconfigured
AP Manager......................................... No
Guest Interface.................................... No
L2 Multicast....................................... Enabled
```

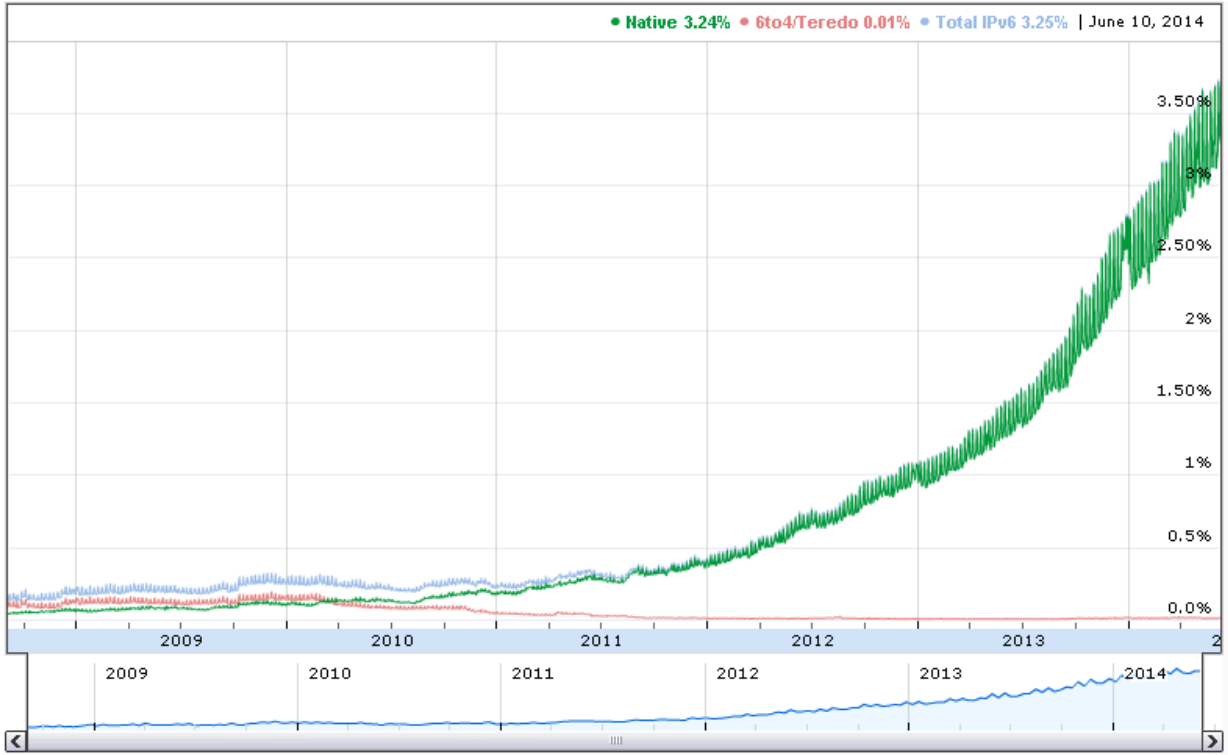
IPv6

Agenda

- Why Now?
- Ipv6 Review
- IPv6 in the 8.0 Release: What is Supported and not Supported?
- Monitoring and Troubleshooting Commands

Why Now?

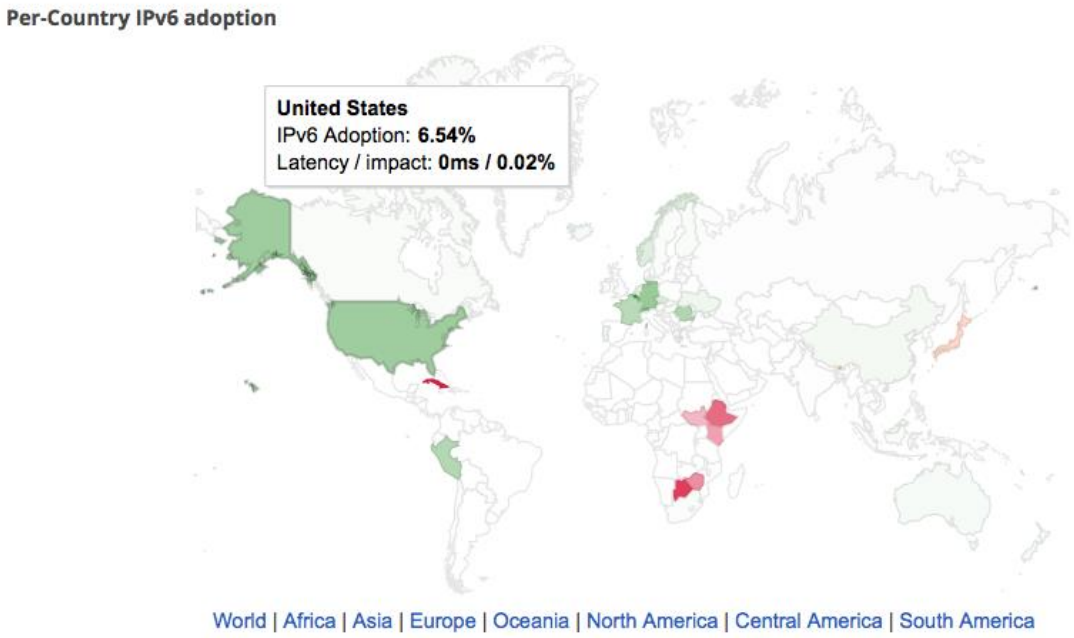
IPv6 Adoption Rate



Actual Data Source: Google, 2014 https://www.google.com/intl/en/ipv6/statistics.html

IPv6 Adoption Rate Per Country

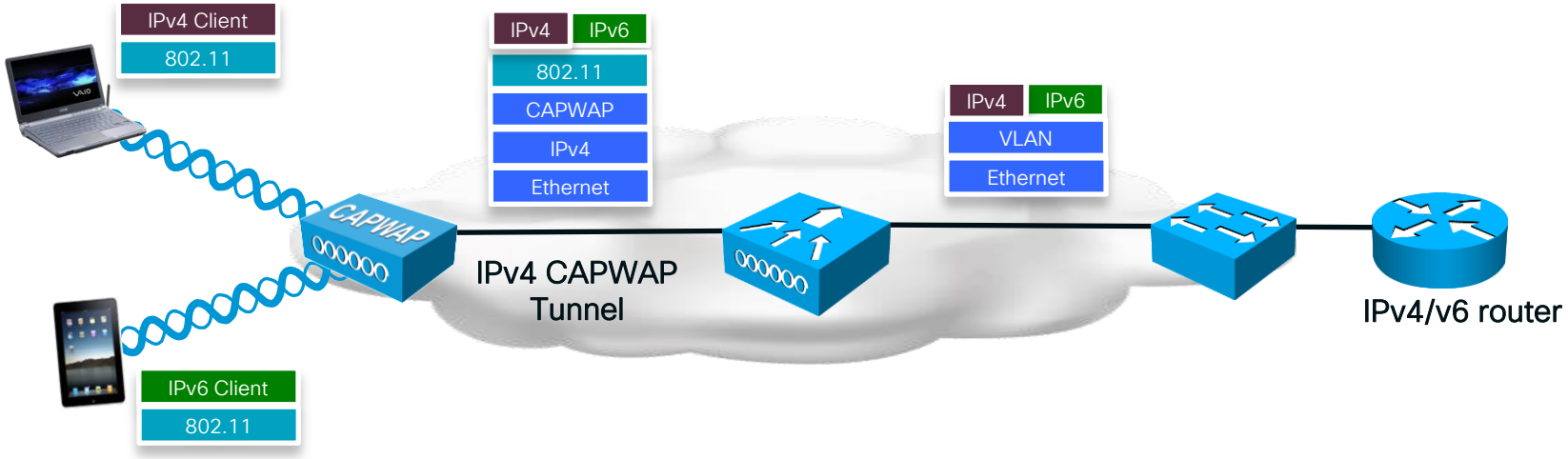
- Belgium 15.29%
- Switzerland 9.53%
- Germany 6.9%
- US 6.54%
- Peru 5.17%
- Japan 3.61%
- China 0.76%
- Total IPv6 3.34%



Actual Data Source: Google, March 25, 2014
https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption

IPv6 Review

Client IPv6 Solution Introduced in 7.2

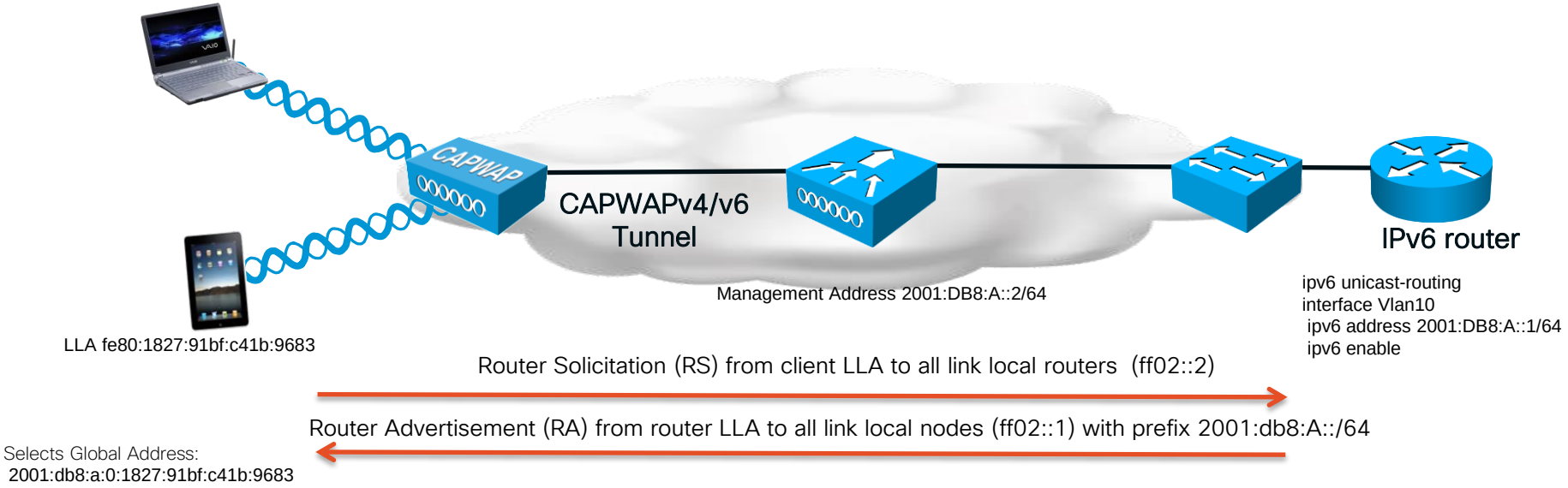


WLC bridges all IPv6 client traffic

IPv6 Addressing Used by WLC

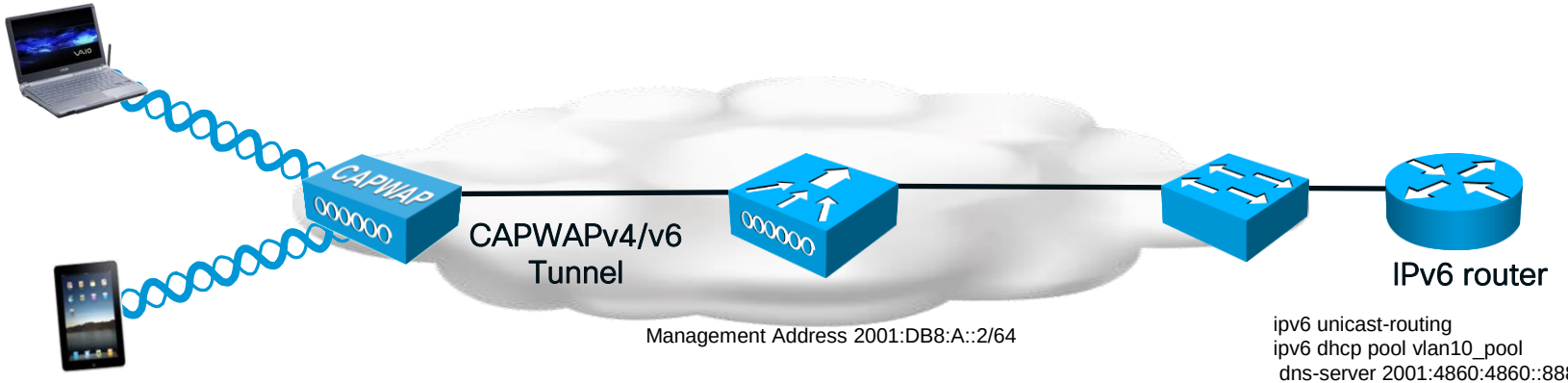
- ::/128 – Unspecified: Used as a source address until an address is assigned
- ::1/128 – Loopback address
- fd09::/8 – Unique local: Private network 10.0.0.0, 172.16.0.0, 192.168.0.0
- fe80::/64 – Link-local: non-routed, self-generated addresses that do not exist outside the layer 3 link
- ff00::/8 – Multicast: Used to identify multicast groups
- 2000::/3 – Global Unicast: Assigned using stateful/stateless DHCPv6 or SLAAC
- ::ffff/96 – IPv4-Mapped: Used to embed an IPv4 address in IPv6

SLAAC (Stateless Address Auto-configuration)



SLAAC uses EUI-64 to select an IPv6 address

Stateless DHCPv6



LLA fe80:1827:91bf:c41b:9683

```
ipv6 unicast-routing
ipv6 dhcp pool vlan10_pool
 dns-server 2001:4860:4860::8888
 domain-name ipv6.rf-demo.com

interface Vlan10
 ipv6 address 2001:DB8:A::1/64
 ipv6 enable
 ipv6 nd prefix 2001:DB8:A::/64
 ipv6 nd other-config-flag
 ipv6 dhcp server vlan10_pool rapid-commit
```

RS from client LLA to all link local routers (ff02::2)

Select Global Address:
2001:db8:a:0:1827:91bf:c41b:9683

RA from router to client's LLA with prefix 2001:db8:A::/64

DHCPv6 Solicit from client LLA to all DHCP servers/relays agents (ff02::1:2)

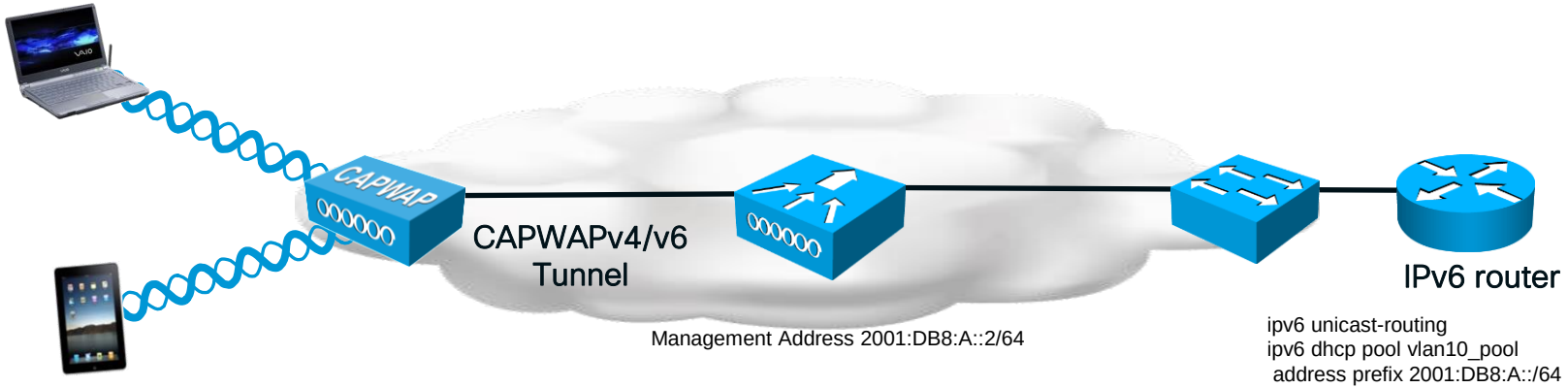
DHCPv6 Advertisement from DHCPv6 server to client's LLA

DHCPv6 Request from client LLA to all DHCP servers/relays agents (ff02::1:2)

DHCPv6 Reply from DHCPv6 server to client's LLA with DNSv6 and domain

Receive DNS and host:
IPv6: 2001:db8:a:0:1827:91bf:c41b:9683
DNS: 2001:4860:4680::8888
domain: ipv6.rf-demo.com

Stateful DHCPv6



LLA fe80:1827:91bf:c41b:9683

```
ipv6 unicast-routing
ipv6 dhcp pool vlan10_pool
 address prefix 2001:DB8:A::/64 lifetime
86400 43200
 dns-server 2001:4860:4860::8888
 domain-name ipv6.rf-demo.com

interface Vlan10
 ipv6 address 2001:DB8:A::1/64
 ipv6 enable
 ipv6 nd prefix 2001:DB8:A::/64
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
 ipv6 dhcp server vlan10_pool rapid-commit
```

RS from client LLA to all link local routers (ff02::2) →

← RA from router to client's LLA

DHCPv6 Solicit from client LLA to all DHCP servers/relays agents (ff02::1:2) →

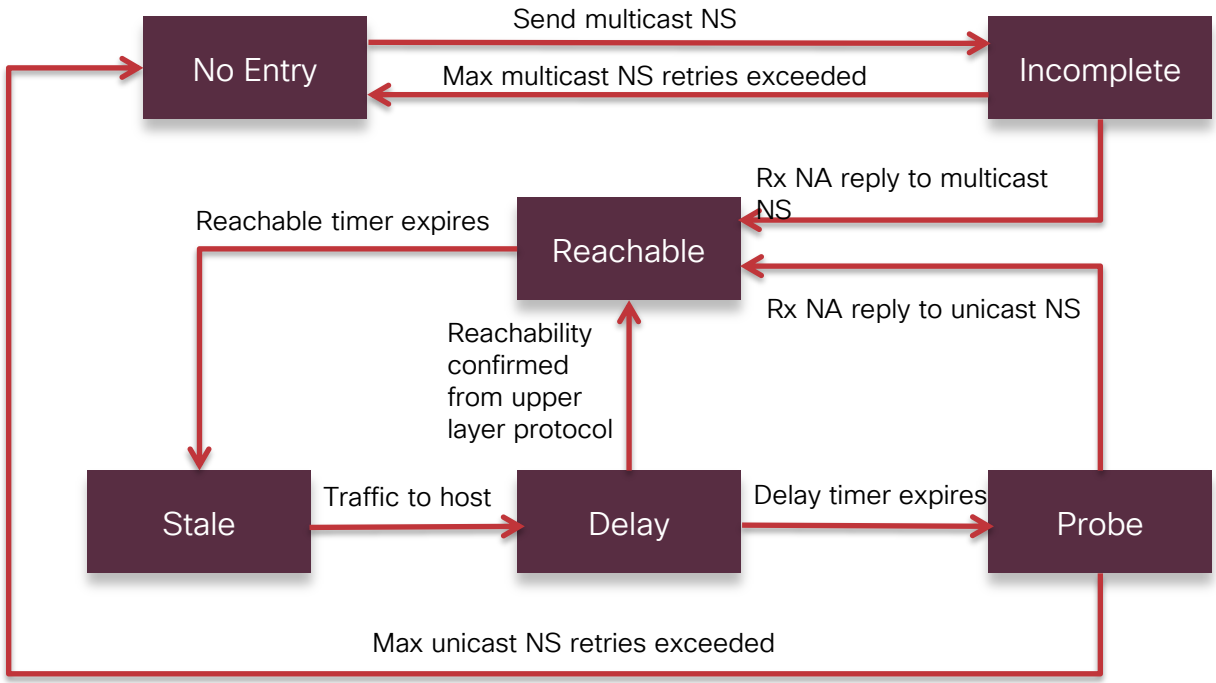
← DHCPv6 Advertisement from DHCPv6 server to client's LLA

DHCPv6 Request from client LLA to all DHCP servers/relays agents (ff02::1:2) →

← DHCPv6 Reply from DHCPv6 server to client's LLA with DNSv6 and domain

Receive Global Address:
IPv6: 2001:db8:a:0:C840:1620:FD66:69B1
DNS: 2001:4860:4680::8888
domain: ipv6.rf-demo.com

IPv6 Neighbor Binding



NS = Neighbor Solicitation
NA = Neighbor Advertisement

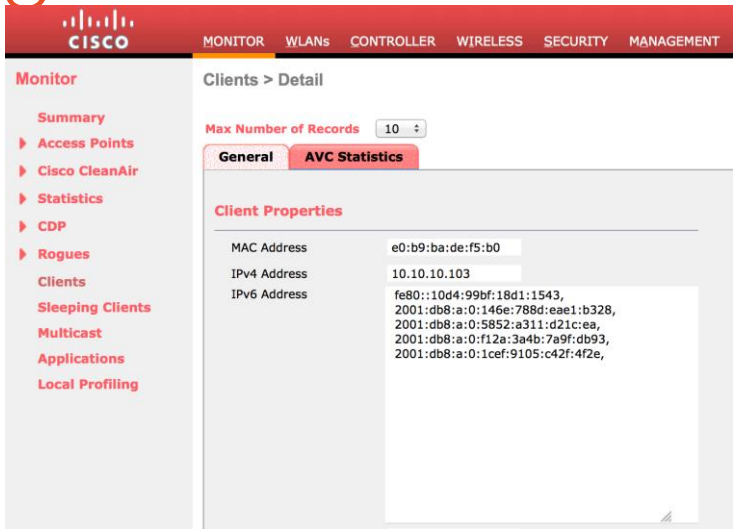
Source: RFC 4861, Cisco Live BRKEWN 2666

IPv6 Neighbor Binding

Controller → IPv6 →Neighbor Binding

Neighbor Binding

Down Lifetime (0-86400 seconds)	30
Reachable Lifetime (0-86400 seconds)	300
Stale Lifetime (0-86400 seconds)	86400
Unknown Address Multicast NS Forwarding	Disable
NA Multicast Forwarding	Enable

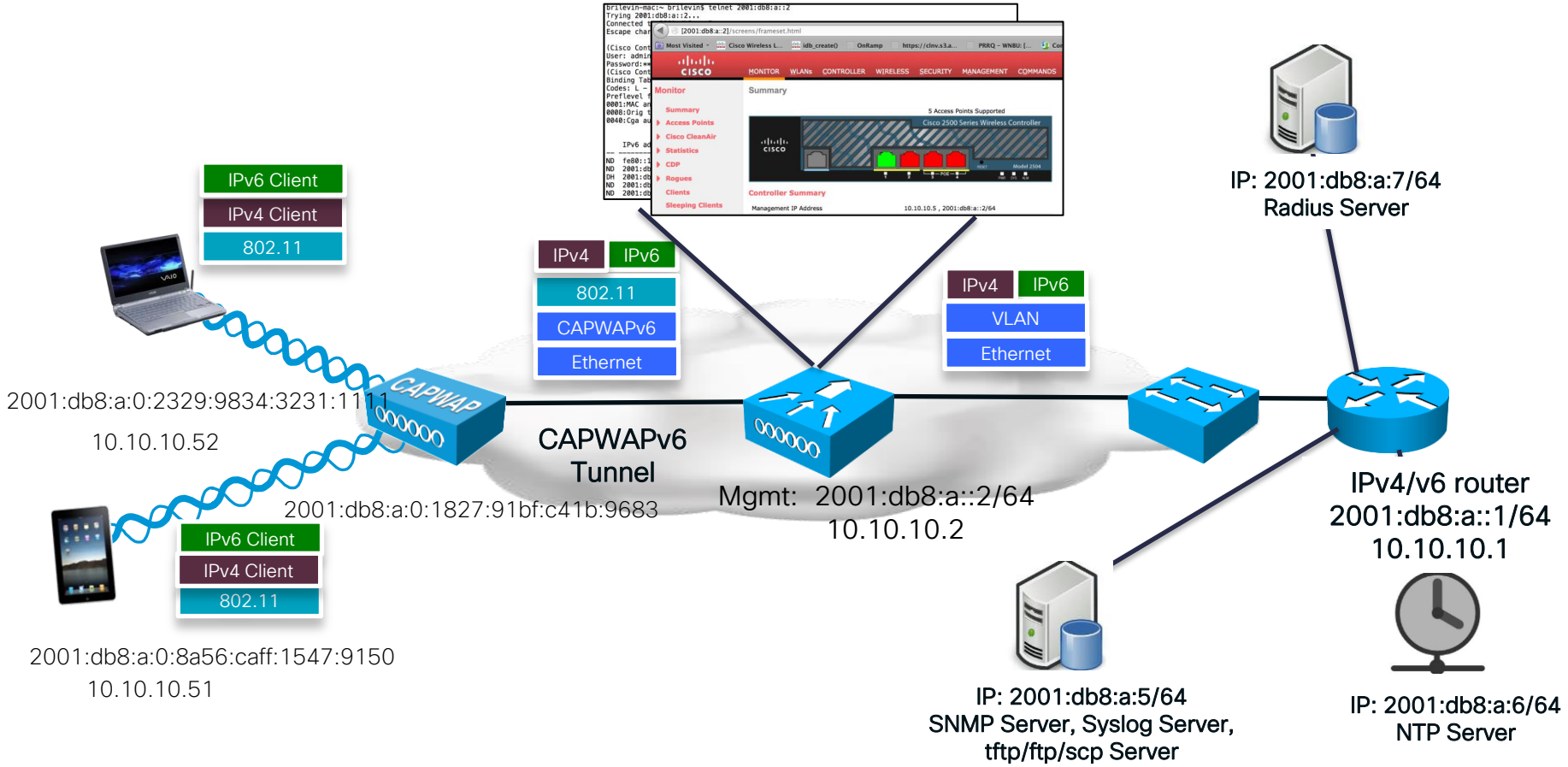



```
(Cisco Controller) >show ipv6 neighbor-binding summary
Binding Table has 6 entries, 6 dynamic (limit 1000)
Codes: L - Local, S - Static, ND - Neighbor Discovery, DH - DHCP
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned


    IPv6 address                              MAC Address       Port  VLAN Type     prlvl age  state     Time left
-- ----------------------------------------  ----------------- ----- ---- --------- ----- ---- --------- ----------
ND  fe80::1827:91bf:c41b:9683                 7c:fa:df:a1:31:c4    AP   20 wireless  0005    0 REACHABLE  278
ND  fe80::10d4:99bf:18d1:1543                 e0:b9:ba:de:f5:b0    AP   10 wireless  0005    1 REACHABLE  213
ND  2001:db8:a:0:f12a:3a4b:7a9f:db93          e0:b9:ba:de:f5:b0    AP   10 wireless  0005    8 STALE      90349
DH  2001:db8:a:0:5852:a311:d21c:ea            e0:b9:ba:de:f5:b0    AP   10 wireless  0024    1 REACHABLE  199(89281)
ND  2001:db8:a:0:1cef:9105:c42f:4f2e          e0:b9:ba:de:f5:b0    AP   10 wireless  0005    1 REACHABLE  207
ND  2001:db8:a:0:146e:788d:eae1:b328          e0:b9:ba:de:f5:b0    AP   10 wireless  0005    1 REACHABLE  202
```

- 8 IPv6 addresses are supported per client
- Upon the 9th, the WLC removes oldest stale entry
- Reachable, stale, and down lifetimes can be different across WLCs, routers, and switches but Best practices is keep them the same
- Neighbor Binding is very chatty, which is very bad over a wireless network

IPv6 in the 8.0 Release: What is Supported and not Supported?

8.0 IPv6 Overview



WLC IPv6 Address Overview

Controller

- General
- Inventory
- Interfaces
- Interface Groups
- Multicast
- Network Routes

Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
management	10	10.10.10.8	Static	Enabled	2001:a:a::2/64
redundancy-management	10	10.10.10.15	Static	Not Supported	
redundancy-port	untagged	169.254.10.15	Static	Not Supported	
service-port	N/A	0.0.0.0	DHCP	Disabled	::/128
virtual	N/A	1.1.1.1	Static	Not Supported	

- ONE IPv6 address (+ LLA address) management solution
- Only IPv4 address support on Dynamic interfaces
- Only IPv4 Dynamic AP manager support
- Only IPv4 Redundancy-management/Redundancy port (HA interfaces are IPv4 only)
- Service-port can get an IPv6 address statically or using SLAAC (only SLAAC interface on WLC)
- LAG needed for IPv6 AP load balancing
- DHCPv6 Proxy not supported (ONLY IPv6 DHCP bridging support - like 7.6 legacy)

IPv6 Management Address Assignment

- Management default is the unspecified IPv6 address (::/128)
- Gateway must be the Link-Local address of the next hop router
- Management Link Local is assigned automatically but Primary must be a globally unique address or a Unique Local Address (fc00::/7)

General Information

Interface Name	management
MAC Address	6c:20:56:b8:f0:8f

Configuration

Quarantine	☐
Quarantine Vlan Id	0

NAT Address

Enable NAT Address	☐

Interface Address

VLAN Identifier	10
IP Address	10.10.10.5
Netmask	255.255.255.0
Gateway	10.10.10.1
Primary IPv6 Address	2001:db8:a::2
Prefix Length	64
Primary IPv6 Gateway	fe80::c267:afff:fe51:85e0
Link Local IPv6 Address	fe80::6e20:56ff:feb8:f08f/64

Statically assigned IPv6 address

Link Local Address of the next hop

Dynamic Interface

- No IPv6 address
- Traffic will be bridged on the VLAN so an IPv6 address can exist on an IPv6 enabled switch/router
- A DHCPv6 server or relay can exist on the VLAN interface at the switch/router

General Information

Interface Name	employee
MAC Address	6c:20:56:b8:f0:8f

Configuration

Guest Lan	☐
Quarantine	☐
Quarantine Vlan Id	0
NAS-ID	

Physical Information

The interface is attached to a LAG.

Enable Dynamic AP Management	☐

Interface Address

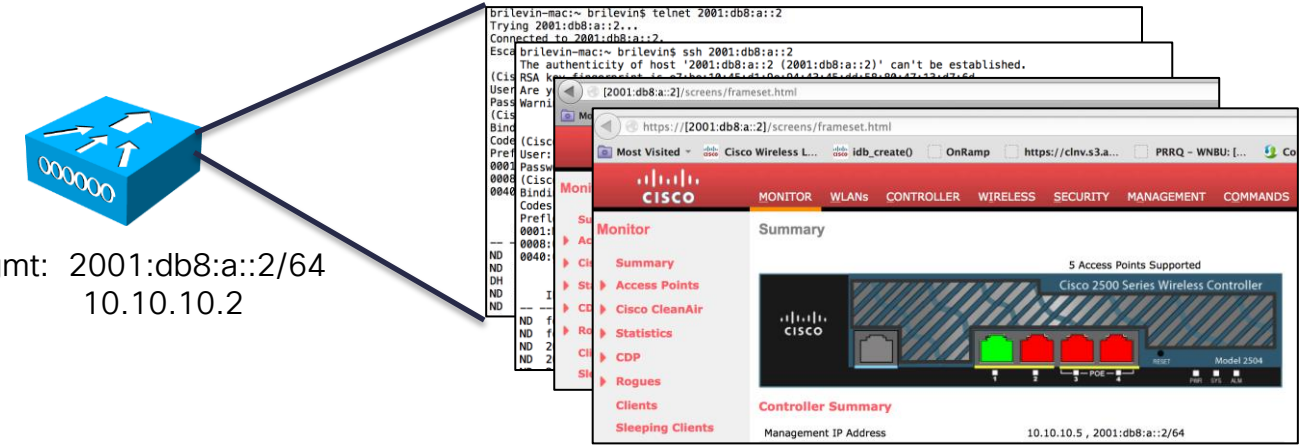
VLAN Identifier	20
IP Address	10.10.20.5
Netmask	255.255.255.0
Gateway	10.10.20.1

Router/Switch Configuration

```
ipv6 dhcp pool vlan20_pool
 address prefix 2001:DB8:B::/64 lifetime 1800 60
 dns-server 2001:DB8:B::1
 domain-name ipv6.rf-demo.com
!
interface Vlan20
 ip address 10.10.20.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 ipv6 address 2001:DB8:B::1/64
 ipv6 enable
 ipv6 nd prefix 2001:DB8:B::/64
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
 ipv6 dhcp server vlan20_pool rapid-commit
!
```

Dynamic Interfaces support IPv4 only

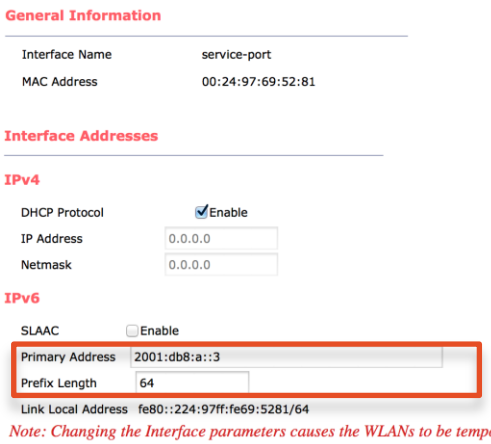
Management Access (telnet, SSH, HTTP, HTTPS)

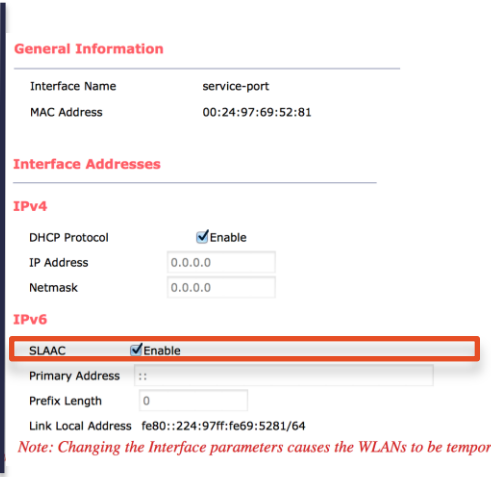


Mgmt: 2001:db8:a::2/64
10.10.10.2

- WLC can be accessed from wired/wireless via its IPv4 or IPv6 Management Interface using:
  - telnet
  - SSH
  - HTTP
  - HTTPS

WLC Service Port





IOS Router Config

```
ipv6 unicast-routing
interface Vlan10
 ipv6 address 2001:DB8:A::1/64
 ipv6 enable
```

- Service Port can be statically assigned an address or select an address via SLAAC
- This is the only SLAAC interface on the WLC, all other interfaces must be statically assigned (just like for IPv4), for the same reasons

IPv6 CLI Configuration

- IPv6 has its own set of commands family:

```
(Cisco Controller) >config ipv6 ?

acl             Configures IPv6 Access Control Lists.
capwap          Configure IPv6 Capwap
disable         Disables IPv6 globally.
enable          Enables IPv6 globally.
interface       Configures system interfaces.
multicast       Configures Ipv6 Multicast.
na-mcast-fwd    Configures NA Multicast forwarding.
neighbor-binding Configures Neighbor binding table options.
ns-mcast-fwd    Configures NS Multicast CacheMiss forwarding.
ra-guard        Configures filter for Router Advertisement packets originating from
client.
route           Add/Delete an IPv6 network route
```

IPv6 CLI Configuration

- CLI error messages help get the right syntax:

```
(Cisco Controller) >config ipv6 interface ?
acl             Configures an interface's Access Control List.
address         Configures an interface's address information.
slaac           Configures SLAAC options on an interface.

(Cisco Controller) >config ipv6 interface address ?
management      Configures the management interface.
service-port    Configures the out-of-band service Port.

(Cisco Controller) >config ipv6 interface address management ?
primary         Configures the primary IPv6  Address for an interface

(Cisco Controller) >config ipv6 interface address management primary ?
<IPv6 Address> Configures an interface with IPv6 address information.

(Cisco Controller) >config ipv6 interface address management primary 2001:15::1/64
Incorrect input! Use 'config ipv6 interface address management <primary> <IPv6 Address> <Prefix Length>
<IPv6 Gateway Address>'

(Cisco Controller) >config ipv6 interface address management primary 2001:15::1 64 2001:15::17

 Request failed - Ipv6 Gateway Address should be of Link Local Scope (FE80::/64).
(Cisco Controller) >config ipv6 interface address management primary 2001:15::1 64 fe80::7
```

CAPWAP – Prefer Mode

All APs

Current Filter: *None* [Change Filter] [Clear Filter]

Number of APs: 1

AP Name	IP Address(Ipv4/Ipv6)	AP Model	AP MAC	AP Up Time
AP0022.bdf7.5594	2001:db8:a:0:222:bdff:fef7:5594	AIR-CAP2702I-A-K9	00:22:bd:f7:55:94	0 d, 00 h 12 m 27 s

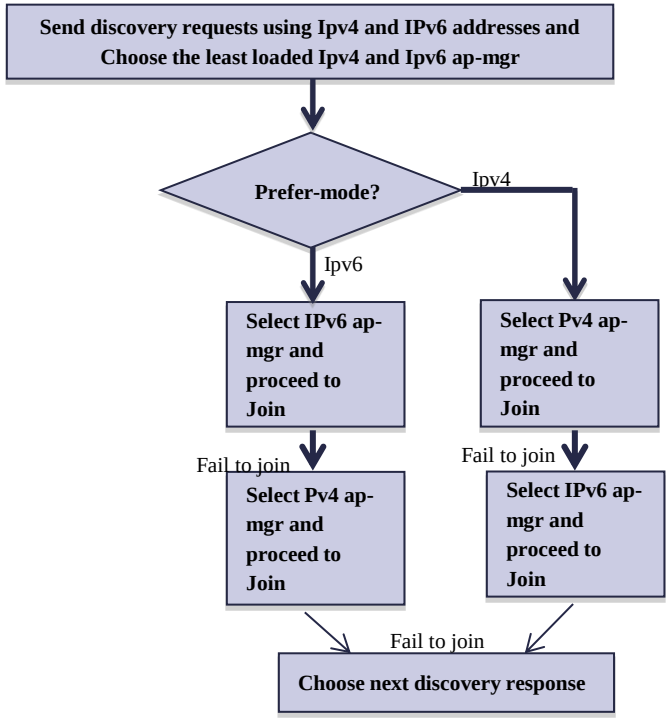
- Prefer-mode is to allow administrator to configure capwap L3 transport (ipv4 and ipv6) through which APs will join to WLC (based on its primary/secondary/tertiary configuration).
- There are two level of prefer-mode
  - 1)ApGroup Specific
  - 2)Global

CAPWAP – Prefer Mode Sequence

- ApGroup specific prefer-mode will be pushed to the AP if prefer-mode of ApGroup is configured to which Ap belongs
- Global prefer-mode will be pushed to default-group Aps and to those ApGroups who do not have prefer-mode configured
- By-default values of prefer-mode for ApGroup and Global will be un-configured and IPv4 respectively
- Static ip configuration will take precedence over prefer mode.
  - Example:
    - Preferred mode configured as Ipv4
    - Static IPv6 configuration on AP using CLI or GUI
    - AP will join WLC using IPv6 transport mode

CAPWAP – Prefer Mode Sequence

- If AP tries to join WLC with configured prefer-mode and it fails to join, then it will fall back to choose ap-manager of the other transport and joins the same WLC. When both transports fail, AP will move to next discovery response.



CAPWAP – Prefer Mode Configuration

- To configure the prefer mode, issue the command:

```
(Cisco Controller) >config ap preferred-mode ?
ipv4            configures preferred mode ipv4
ipv6            configures preferred mode ipv6
disable         Disable preferred mode of ApGroup

(Cisco Controller) >config ap preferred-mode ipv6 ?
<Ap-group name> configures preferred mode to AP group members
all             configures preferred mode to all APs
```

- Global ("all") prefer-mode will not be applied to Aps whose ApGroup prefer-mode is configured. On success, AP will restart capwap to join with configured prefer-mode after choosing WLC based on its primary/secondary/tertiary configuration.

CAPWAP – Prefer Mode Configuration

- To disable the prefer mode for an AP group, issue the command:

```
(Cisco Controller) >config ap preferred-mode disable ?
<Ap-group name> configures preferred mode to AP group members
```

  - Aps belonging to <apgroup> will restart capwap and join back with global prefer-mode.

- To show statistics for prefer-mode configuration CLIs. Stats are not cumulative but will be updated for last executed config CLI of prefer-mode:

```
(Cisco Controller) >show ap prefer-mode stats

Number of APs..................................... 2

Prefer-mode of Global/ApGroups      Total  Success  Unsupported   Already Configured   perApGroup Configured   Failure
------------------------------      -----  -------  -----------   ------------------   ----------------------   -------
Global (ALL APs)                    0      0        0             0                    0                        0

ApGroups :
==========
Mygroup                             0      0        0             0                    0                        0
```

CAPWAP – Prefer Mode Configuration

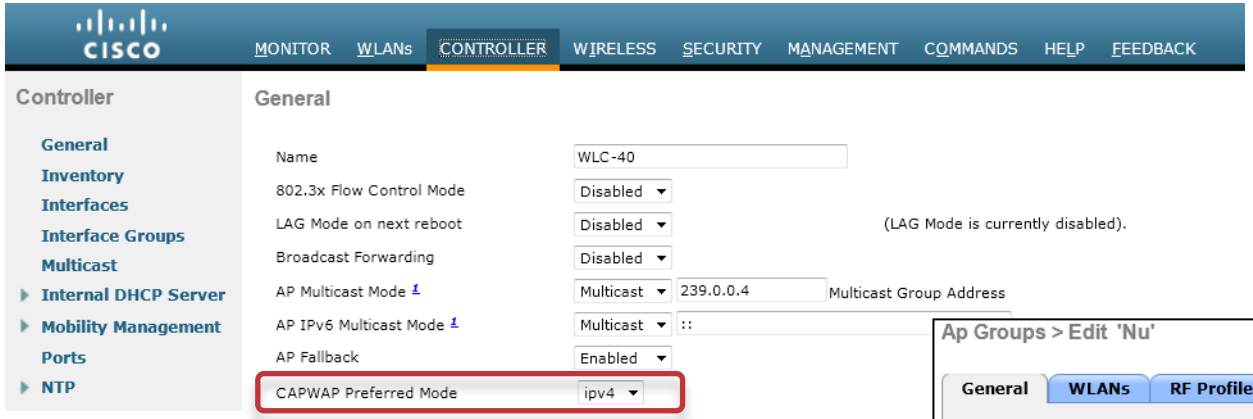
- To show prefer-mode configured for all apgroups:

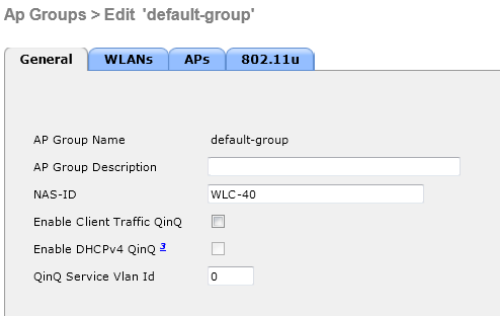
```
Cisco Controller) >show wlan apgroups
Total Number of AP Groups..................... 1
Site Name..................................... Mygroup
Site Description.............................. <none>
Venue Group Code.............................. Unspecified
Venue Type Code............................... Unspecified
NAS-identifier................................ WLC-40
Client Traffic QinQ Enable.................... FALSE
DHCPv4 QinQ Enable............................ FALSE
AP Operating Class............................ Not-configured
Capwap Prefer Mode............................ IPv6
```

- To show global prefer-mode configured:

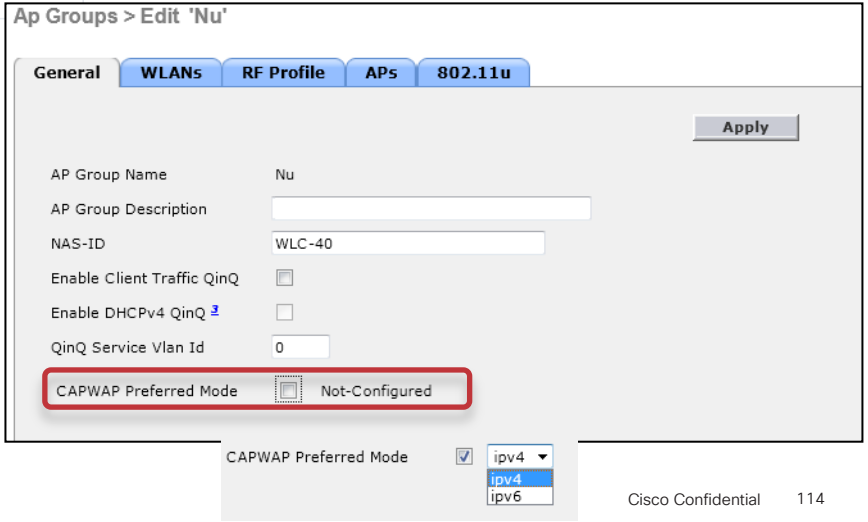
```
(Cisco Controller) >show network summary
…/…
Capwap Prefer Mode....................... IPv4
```

CAPWAP – Prefer Mode Configuration



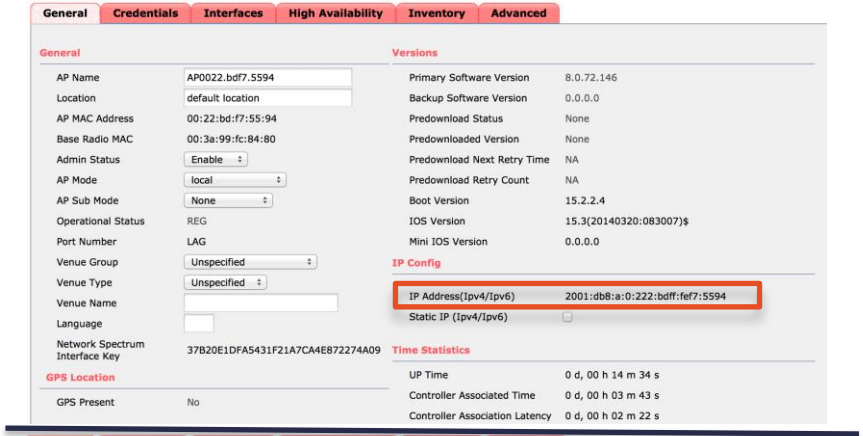


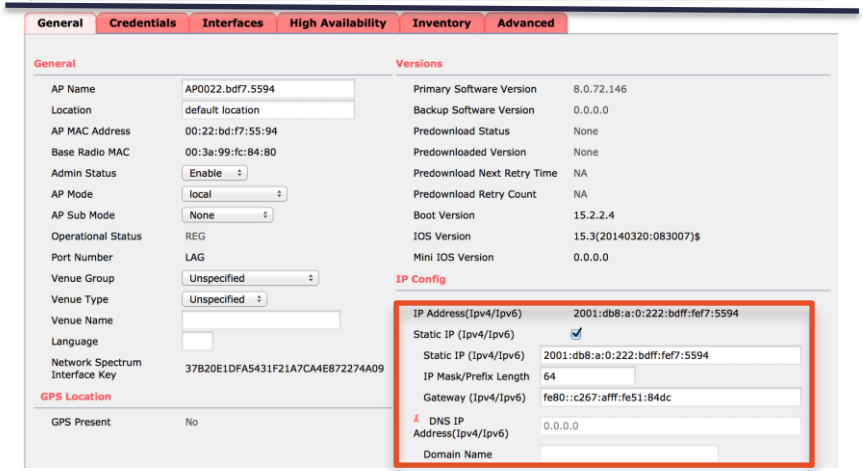
"default-group" does not have the option



CAPWAP

- AP can get IPv6 addresses from state-full DHCPv6/SLAAC or static assignment
- If statically assigned, the gateway can be the unique global or Link-Local address of the router
- Either ‘CAPWAPv4’ or ‘CAPWAPv6’ can be used, but not both
- APs in bridge mode do not support CAPWAPv6



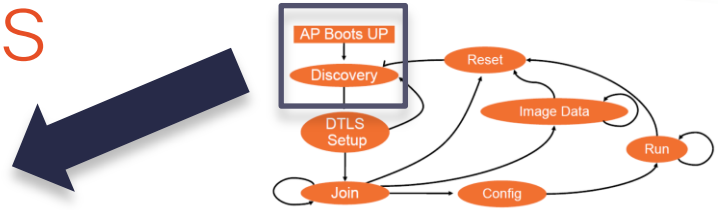


DTLS

- Like CAPWAP, DTLS also uses the access point's IPv6 address

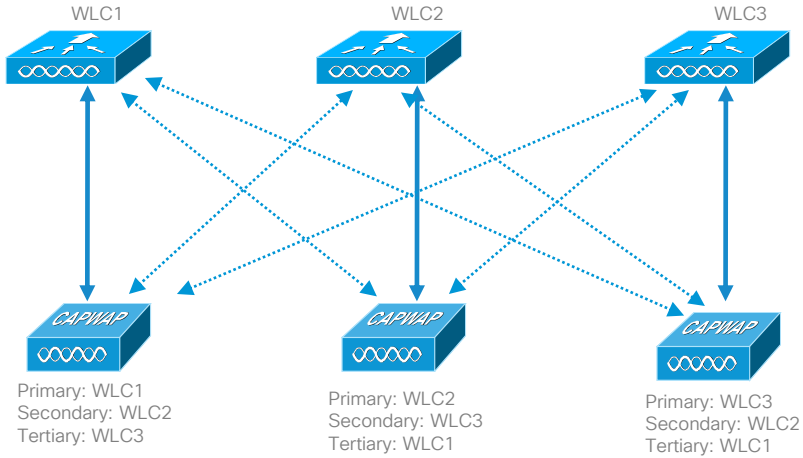
```
(Cisco Controller) >show dtls connections

 AP Name          Local Port   Peer IP                       Peer Port  Ciphersuite
---------------- ------------ ----------------                -------  ----------------------------
AP0022.bdf7.5594  Capwap_Ctrl 2001:db8:a:0:222:bdff:fef7:5594   30043  TLS_RSA_WITH_AES_128_CBC_SHA
AP0022.bdf7.5594  Capwap_Data 2001:db8:a:0:222:bdff:fef7:5594   30043  TLS_RSA_WITH_AES_128_CBC_SHA
CAP3702           Capwap_Ctrl 10.10.10.105                       62195  TLS_RSA_WITH_AES_128_CBC_SHA
CAP3702           Capwap_Data 10.10.10.105                       62195  TLS_RSA_WITH_AES_128_CBC_SHA
```

AP Discovery Mechanisms



- DHCPv6 Option 52
  - OPTION_CAPWAP_AC_V6 (52) RFC 5417
  - As part of the DHCPv6 Reply, the server will provide the IPv6 WLC management IPv6 address
  - AP will begin unicast CAPWAP discovery
- Multicast discovery
  - Broadcast does not exist in IPv6
  - Send CAPWAP discovery messages to " All ACs multicast address" (FF01::18C)
- Using DNS
  - Configure DNS server to resolve cisco-capwap-controller.domain-name
  - domain-name should be returned from DHCPv6 server
- AP Priming
  - Preconfiguring the AP with a Primary, secondary, and tertiary IPv6 managed WLC

AP Failover



All APs > Details for AP0022.bdf7.5594

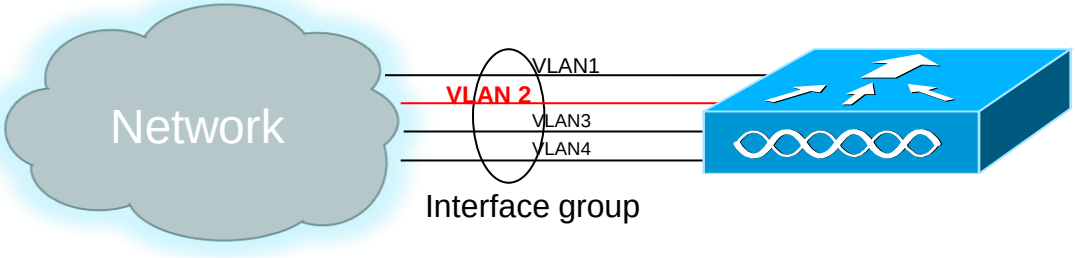
General | Credentials | Interfaces | High Availability | Inventory | Advanced

	Name	Management IP Address
Primary Controller	WLC1	2001:db8:a::2
Secondary Controller	WLC2	10.10.10.5
Tertiary Controller	WLC3	2001:db8:a::4

AP Failover Priority: Critical

- Management IP address must be reachable
- One entry per WLC
- The AP will join either IPv4 or IPv6 address of the WLC (regardless of management IP listed)
- All other AP Failover behavior is the same as previous versions

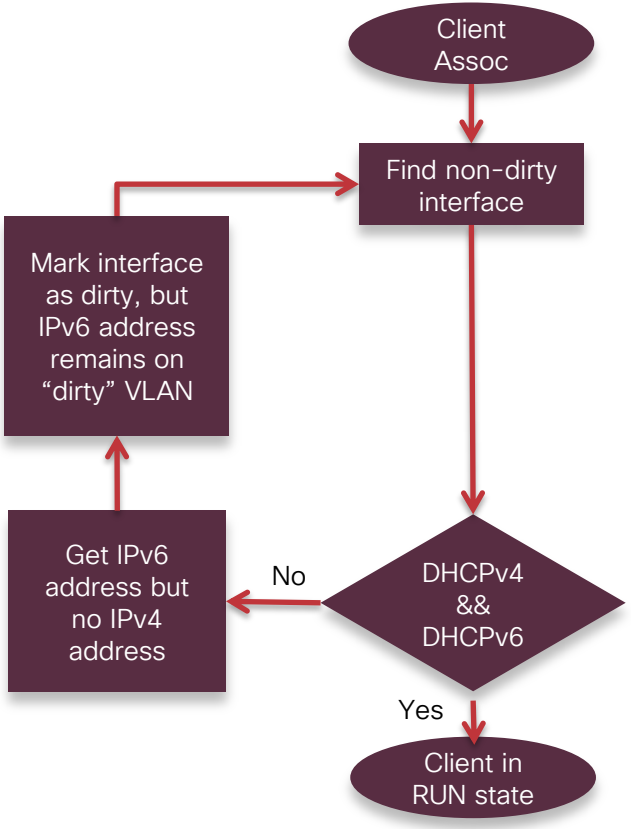
VLAN Select / Interface Groups Review



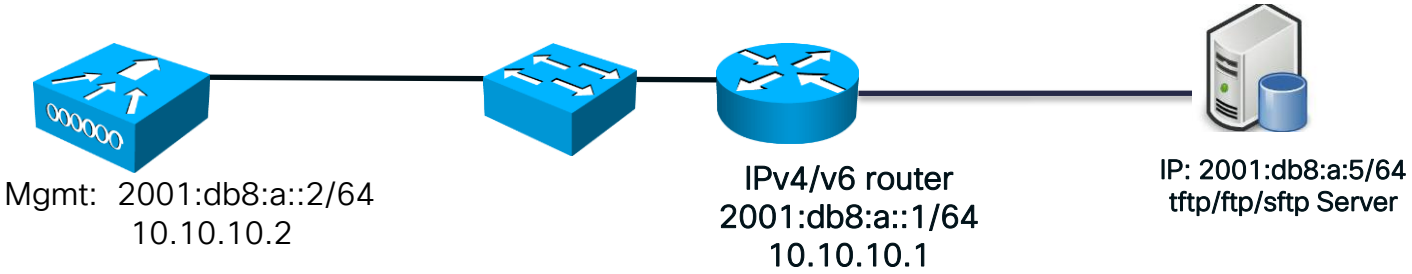
- Map a WLAN to multiple VLANs
- Based on DHCP address pool availability select client's VLAN
- If DHCP address space is exhausted, mark VLAN "dirty" move to the next
- This is based on IPv4 DHCP

VLAN Select / Interface Groups with IPv6

- VLAN Select should not be used in a dual-stack environment
- VLAN Select only works on the IPv4 address
- Client can get an IPv4 address from one VLAN and IPv6 address from another
- VLAN mismatch causes problems

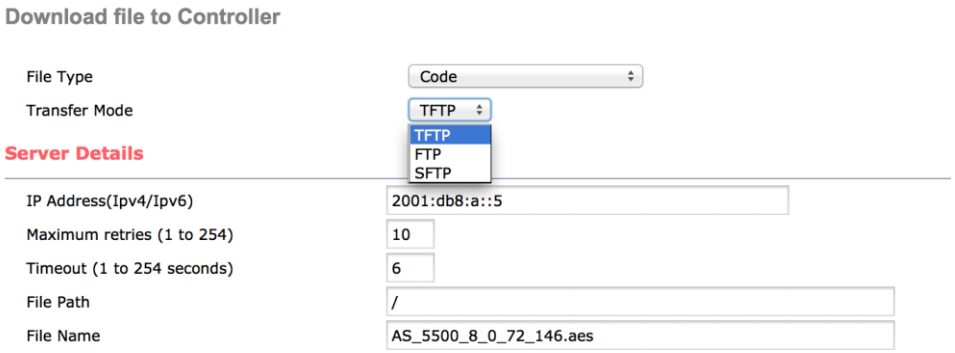


Upload/Download Using IPv6 with ftp/tftp/sftp



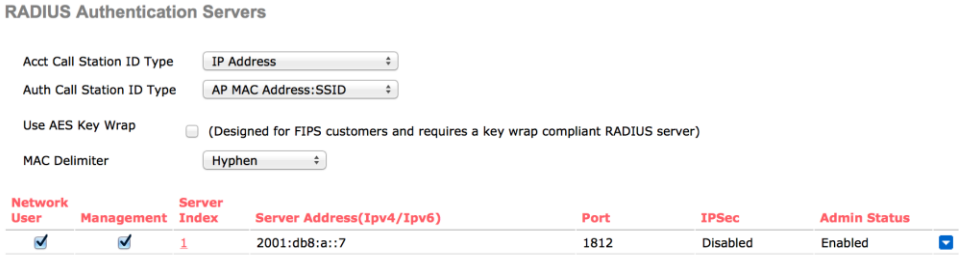
- tftp/ftp/sftp upload/download can be initiated via WLC
- Tftpd64 server is recommended
- Either IPv4 or IPv6 address can be used

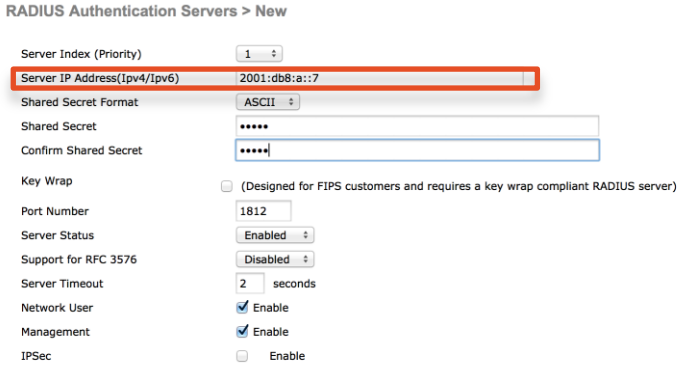
WLC GUI → Commands



RADIUSv6 Support

WLC GUI → Security → RADIUS → Authentication





- RADIUSv6 Servers can be added using their IPv6 address
  - When using IPv6, for simplicity and efficiency, bind to <u>one</u> IPv6 address (one IPv6 address bound to the WLC IPv6 management address)

TACACS+v6 Support

WLC GUI → Security → TACACS+ → Accounting

TACACS+ Accounting Servers

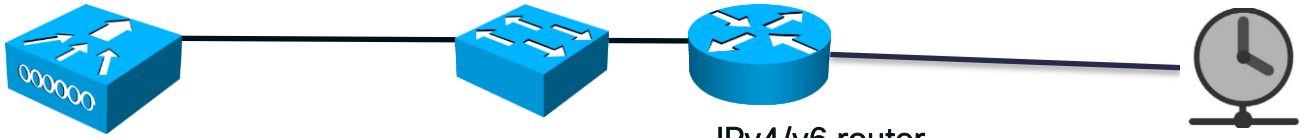
Server Index	Server Address(Ipv4/Ipv6)	Port	Admin Status
1	2001:db8:a::7	49	Enabled

TACACS+ Accounting Servers > New

Server Index (Priority)	1
Server IP Address(Ipv4/Ipv6)	2001:db8:a::7
Shared Secret Format	ASCII
Shared Secret	•••••
Confirm Shared Secret	•••••
Port Number	49
Server Status	Enabled
Server Timeout	5 seconds

- TACACS+v6 Servers can be added using their IPv6 address

NTPv3



Mgmt: 2001:db8:a::2/64
10.10.10.2

IPv4/v6 router
2001:db8:a::1/64
10.10.10.1

IP: 2001:db8:a:6/64
NTP Server

IOS CLI Configuration

```
ntp master
ntp authentication-key 1 md5 1511021F0725 7
ntp authenticate
ntp trusted-key 1
ntp server 2001:db8:a::6 version 3
```

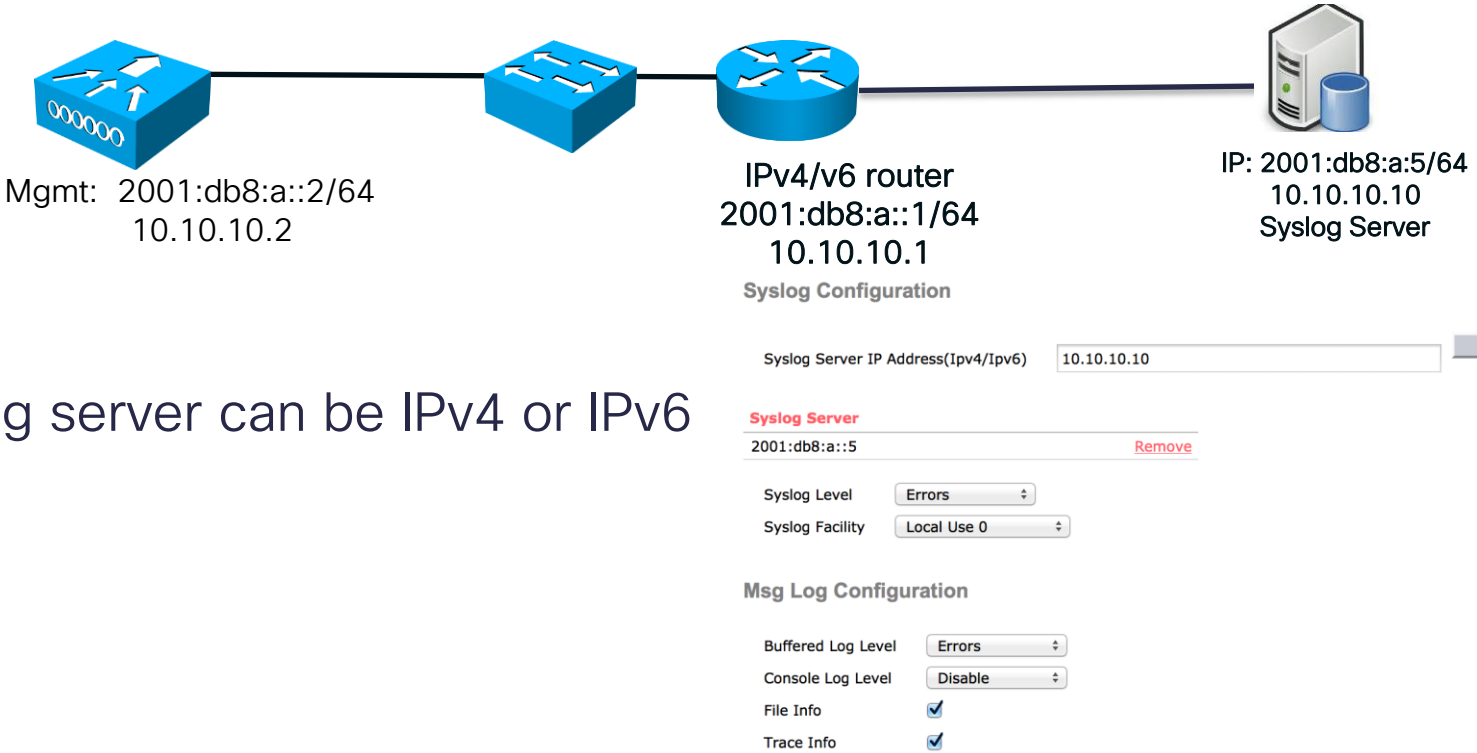
- NTP server can be configured with IPv4 or IPv6 address
- Recommended NTP server is Cisco IOS router/switch

WLC GUI → Controller → NTP Server → New

NTP Servers > New

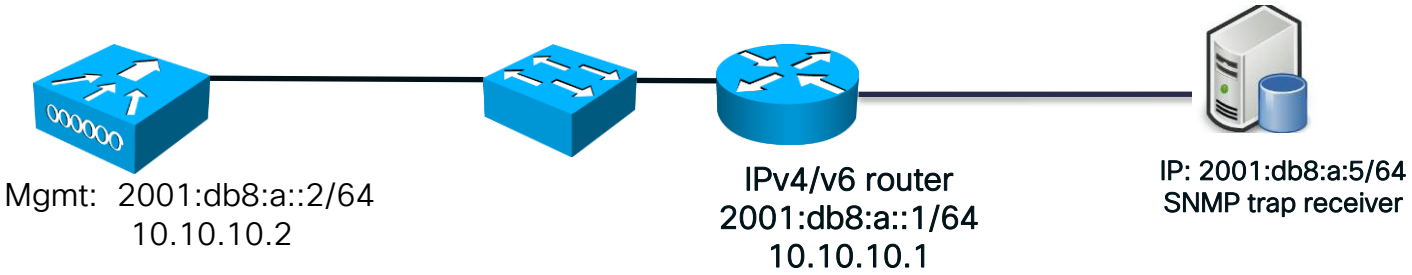
Server Index (Priority)	1
Server IP Address(Ipv4/Ipv6)	2001:db8:a::6
Enable NTP Authentication	☑
Key Index	1

Syslog over IPv6



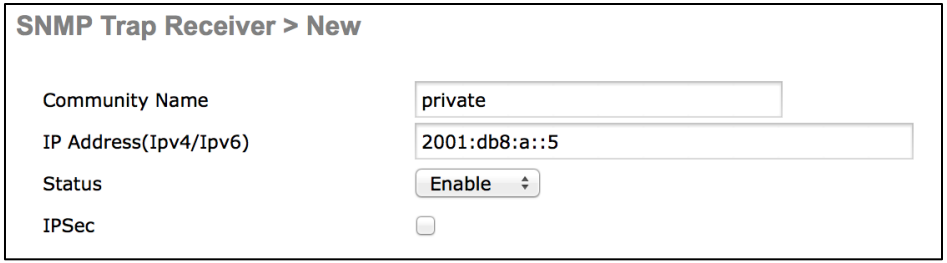
- Syslog server can be IPv4 or IPv6

SNMP Trap Receiver

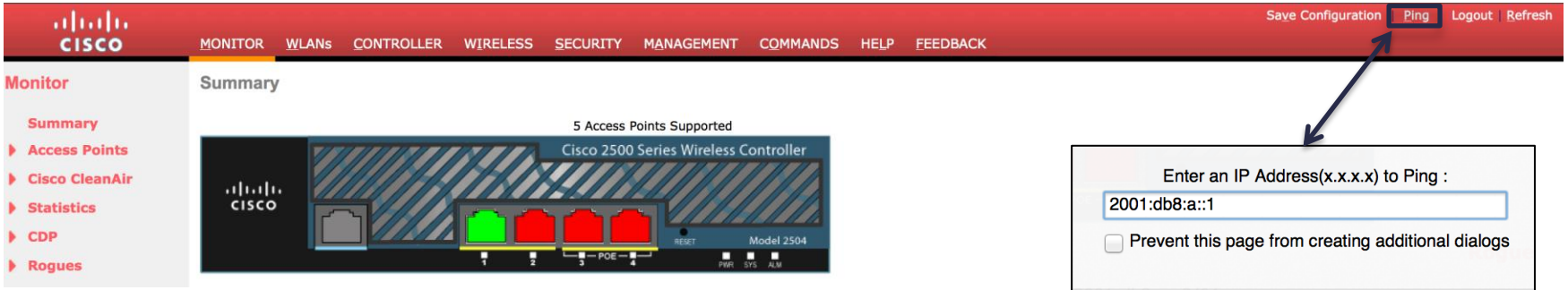


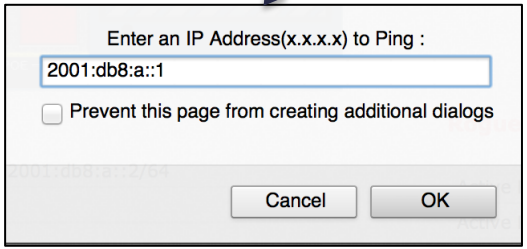
- SNMP MIBs are send to the IPv6 destination
- Prime Infrastructure will not support IPv6 until 2.2 release
- iREASONING MIB Browser was used to test with IPv6

WLC GUI → Management → Trap Receivers



PINGv6





- Ping supports IPv4 and IPv6
- Link-local and Globally unique addresses can be pinged
- Both WLC GUI and CLI supported

```
(Cisco Controller) >ping 2001:db8:a::1

Send count=3, Receive count=3 from 2001:db8:a::1
```

UDP Lite

WLC CLI: config ipv6 capwap udplite en/disable

```
(Cisco Controller) >config ipv6 capwap udplite ?

enable          Enables IPv6 Capwap UDP Lite
disable         Disables IPv6 Capwap UDP Lite
```

```
(Cisco Controller) >show ipv6 summary

Global Config.............................. Enabled
Reachable-lifetime value.................... 300
Stale-lifetime value........................ 86400
Down-lifetime value......................... 30
RA Throttling............................... Enabled
RA Throttling allow at-least................ 1
RA Throttling allow at-most................. 1
RA Throttling max-through................... 10
RA Throttling throttle-period............... 600
RA Throttling interval-option............... passthrough
NS Mulitcast CacheMiss Forwarding........... Disabled
NA Mulitcast Forwarding..................... Enabled
IPv6 Capwap UDP Lite....................... Enabled
Operating System IPv6 state ................ Enabled
```

- UDP Lite computes checksum on the pseudo header of datagram
- Enabling UDP Lite speeds up packet processing time
- The IP protocol id is 136, uses same CAPWAP ports as UDP
- Enabling UDP Lite would require that the network firewall allows protocol 136
- Switching between UDP and UDP Lite causes all APs to re-join WLC
- Enabled by default

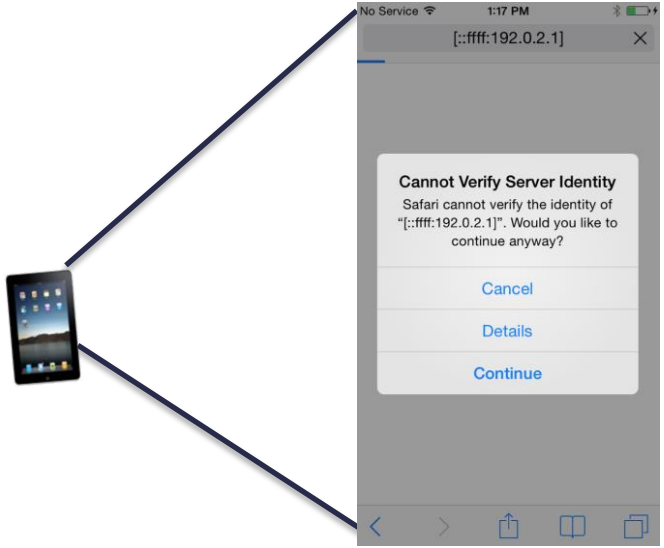
CDPv6

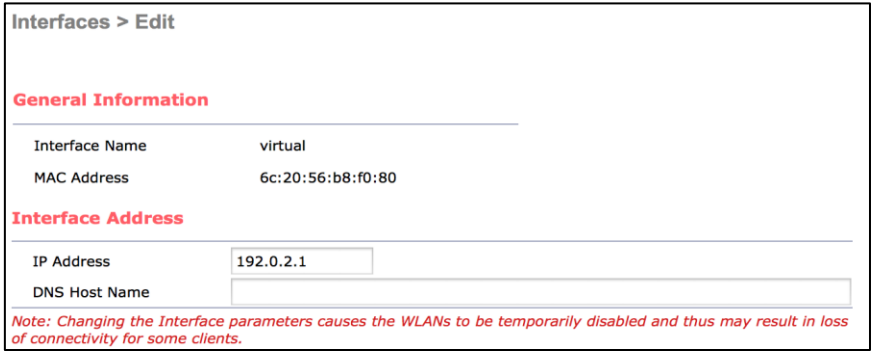
- CDP detects both IPv4 / IPv6 Neighbors

```
(cisco_controller) >show ap cdp neighbors all
AP Name          AP IP          Neighbor Name      Neighbor Port
----------------  ---------------  ------------------  --------------
Ap1              10.10.10.104      LAB1  GigabitEthernet2/0/17
  IP address: 10.10.10.104
Ap2              2001:db8:a:0:1827:91bf:c41b:9683  LAB1  GigabitEthernet2/0/5
  IP address: 2001:db8:a::1
  IPv6 address: 2001:db8:a::1  (global unicast)
  IPv6 address: fd09:db8:a::1  (global unicast)
  IPv6 address: fe80::6abd:abff:fe8c:7643  (link-local)
```

IPv6 Guest Access

- Virtual IP address is IPv4 only
- Uses IPv4-Mapped address for IPv6 web-authentication clients
- Virtual IP should be the same for all WLCs in the same mobility group
- For example the IPv6 address will display as [::ffff:192.0.2.1]



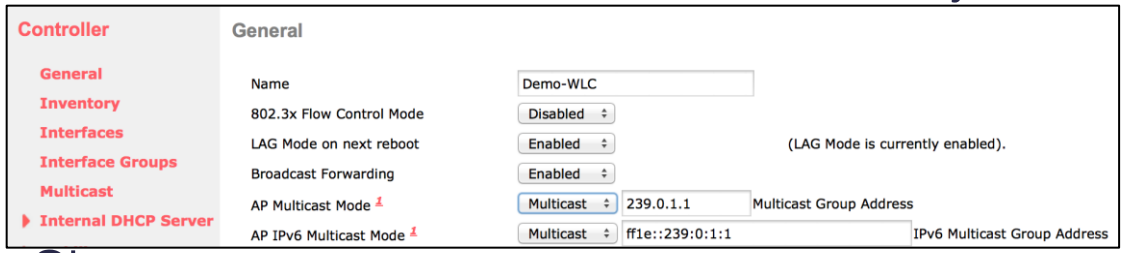


AP Multicast Mode – Unicast/multicast

- Enable ipv6 multicast-routing on IOS router/switch

Router(config)#ipv6 multicast-routing

- IPv6 AP multicast works the same way as IPv4



- Show capwap mcast

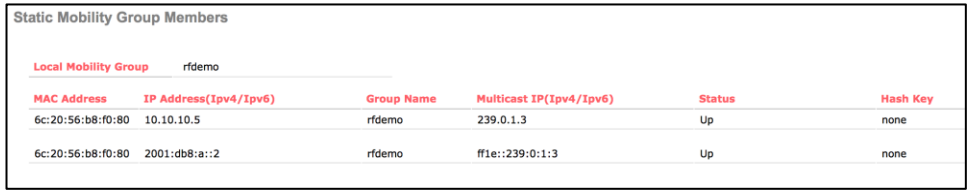
```
Cisco_ap#sh capwap mcast
CAPWAP MULTICAST
    Multicast Group: FF1E::239:0:1:1, Source: FD09:9:5:94::11
V1 Rpt Sent:                0; V2 Rpt Sent:                0
V3 Rpt Sent:                0; Leave Sent:                 0
V1 Query Rcvd:              0; V2 Query Rcvd:              0
V3 Query Rcvd:              0; V1 Rpt Rcvd:                0
V2 Rpt Rcvd:                0; V3 Rpt Rcvd:                0
MLD Qry Rcvd:            7990; MLD Rpt Rcvd:               0
MLD Qry Sent:               0; MLD Rpt Sent:            7987
```

AP joins via CAPWAPv6 tunnel

IPv6 Multicast / Mobility Multicast

- IPv6 multicast messaging for mobility/roaming for IPv6 is NOT there in 8.0 (removed, deferred to later release).
- No IPv6 field for mobility multicast messaging :

- The Mobility Group Members can still have an IPv6 address, and are displayed in Controller->Mobility Management



Mobility Groups / Auto Anchor

Mobility Group Member > New

Member IP Address(Ipv4/Ipv6)	10.10.10.5
Member MAC Address	4c:00:82:71:51:c0
Group Name	rfdemo
Hash	none

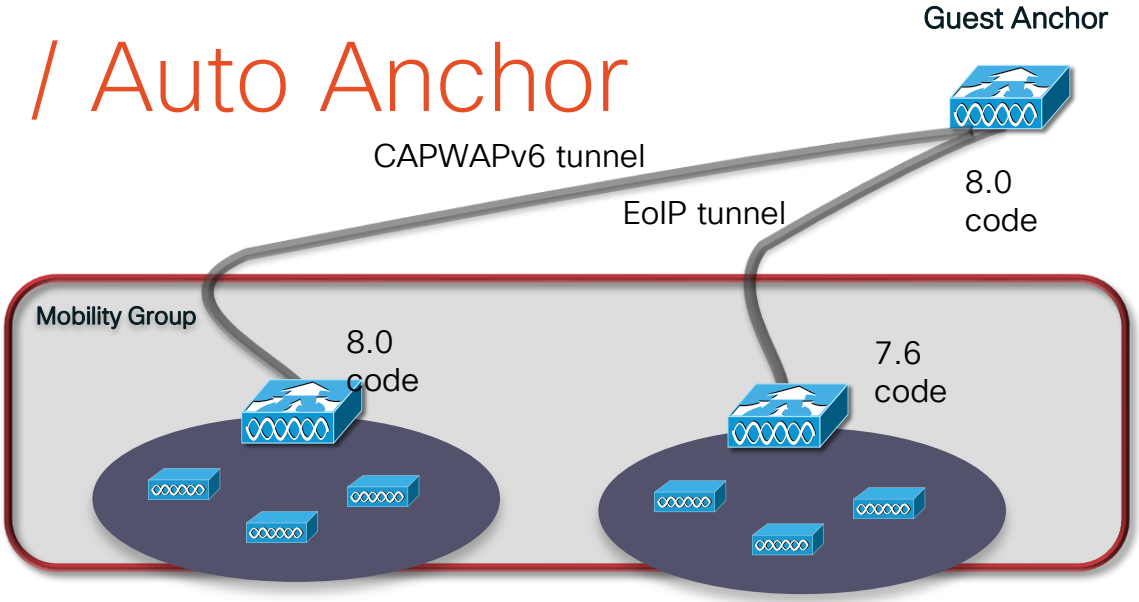
1. Hash is not supported for IPv6 members

Mobility Group Member > New

Member IP Address(Ipv4/Ipv6)	10.10.10.8
Member MAC Address	6c:20:56:b8:f0:8f
Group Name	rfdemo
Hash	none

1. Hash is not supported for IPv6 members

Both Ends must be IPv4



- Guest Anchor should be 8.0 code
- This allows 8.0 WLCs sharing the mobility group to connect using CAPWAPv6
- WLCs running pre-8.0 will join using EoIP
- No need for New Mobility with this configuration

Wireless – IPv6

Features not supported in WLAN 8.0 release

- Deployment Modes
  - Flexconnect – Local switched
  - Mesh/Outdoor
  - Teleworker/OEAP
  - Converged Access
- Services
  - Bonjour
  - AVC
  - Trustsec
- Unsupported APs:
  - Bridge mode APs/AP with 64Mb RAM
    - OEAP 600
    - ISR 800/802
    - 1130/1240/1250
    - 1310/1410
    - 1520
- Misc. configuration Options
  - Internal DHCPv6 Server
  - DHCPv6 Proxy
  - Auto configuration
  - Dynamic interfaces
  - RA Interfaces
  - OSCP and CA Server URL
  - VLAN pooling
- Protocols
  - NTP v4
  - MLD v2
  - IPsec v3 and IKE v2
  - RLDP and CIDS
  - PMIP v6
  - New Mobility

Monitoring and Troubleshooting Commands

Monitoring IPv6

- Show commands have been modified to accommodate IPv6 info:

```
(Cisco Controller) >show interface detailed management

Interface Name..................................... management
MAC Address........................................ 40:55:39:a5:ef:20
IP Address......................................... 172.31.255.40
IP Netmask......................................... 255.255.255.0
IP Gateway......................................... 172.31.255.1
External NAT IP State............................ Disabled
External NAT IP Address......................... 0.0.0.0
Link Local IPv6 Address......................... fe80::4255:39ff:fea5:ef20/64
STATE ............................................ REACHABLE
Primary IPv6 Address............................ 2001:14::2/64
STATE ............................................ REACHABLE
Primary IPv6 Gateway............................ fe80::1
```

Monitoring IPv6

- Show commands have been modified to accommodate IPv6 info:

```
(Cisco Controller) >show system route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
172.31.255.0    0.0.0.0         255.255.255.0   U     0      0        0 dtl0
127.0.0.0       0.0.0.0         255.0.0.0       U     0      0        0 lo
0.0.0.0         172.31.255.1    0.0.0.0         UG    0      0        0 dtl0

Kernel IPv6 routing table
Destination       Next Hop           Flags Metric Ref    Use Iface
::1/128              ::               U     0      1        1 lo
::ffff:192.0.2.1/128 ::               U     0      0        1 lo
::/64                ::               U     256    0        0 dtl0
2001:14::2/128       ::               U     0      0        1 lo
2001:14::/64         ::               U     256    0        0 dtl0
fe80::1/128          ::               U     128    0        0 dtl0
fe80::200:ff:fe00:103/128::           U     0      0        1 lo
```

Troubleshooting IPv6

- IPv6 had its own set of command family for clients (this is not new):

```
(Cisco Controller) >debug ipv6 ?

neighbor-binding Configures the IPV6 neighbor-binding debug options
address-learning Configures the IPV6 address-learning debug options
rules            Configures the IPV6 address-learning debug options
dhcp             Configures the IPV6 dhcp debug options
```

- For native IPv6, debug commands have been modified to include IPv6 info:

```
(Cisco Controller) >debug capwap packet enable

*spamApTask4: Jun 01 07:55:40.291: CAPWAP Control mesg Sent to 2001:14::209, Port 43147
*spamApTask4: Jun 01 07:55:40.292:                Msg Type   :   CAPWAP_WTP_EVENT_RESPONSE
*spamApTask4: Jun 01 07:55:40.292:                Msg Length : 0
*spamApTask4: Jun 01 07:55:40.292:                Msg SeqNum : 50
*spamApTask4: Jun 01 07:55:40.292: <<<<  End of CAPWAP Packet  >>>>
```

Thank you.