Wireless Tech Update Maj 2013

Ib Hansen: ibhansen@cisco.com

Systems Engineer

21 - 23 Maj 2013

© 2010 Cisco and/or its affiliates. All rights reserved.

Agenda

- AP Update
- Software Update
- Roadmap

© 2010 Cisco and/or its affiliates. All rights reserved.

AP Update

© 2010 Cisco and/or its affiliates. All rights reserved.

Aironet 802.11abg and 802.11n G1 Series End of Sales Plans CY2012-13

Aironet AP Series	End Of Sale Announcement	End of Sale Date	HW End of Support	Software Release Support	Recommended Aironet 802.11n G2 Series
Indoor					
1130, 1240❖	Jan 2013	Jul 2013	Jul 2018	Last MD release – 8.0.x	1600
1250❖	Aug 2011	Jan 2012	Jan 2017	Last MD release – 8.0.x	2600
1040, 1140 1260❖	Apr 2013 Apr 2013	Oct 2013 Oct 2013	Sep 2018 Oct 2018	Last MD release – 8.0.x Last feature release – TBD	1600 2600
1040, 1140 for EU/ETSI❖♯	Aug 2012	Dec 2012	Sep 2018	Last MD release – 8.0.x Last feature release – TBD	1600 2600
3500	No plans currently	No plans currently	No plans currently	Beyond 8.0	3600
Outdoor					
1310	Jul 2012	Jan 2013	Q1 CY18	Last feature release – 7.0.x	1550
1520❖	Oct 2011	Mar 2012	Q1 CY17	Last MD release – 8.0.x Last feature release – 8.0	1550
1524SB❖♯	Mar 2013	Jun 2013	Q2 CY18	Last MD release – 8.0.x Last feature release – 8.0	1550

❖ Only hardware support in 8.0 for 1130,1240, 1250 and 1520. New features introduced in 8.0 will not be supported.

♯ Earlier EOS timeline for EU/ETSI due to new DFS rules starting 2013

CISCO AIRONET ACCESS POINTS

802.11n G2 Series

* Available as a Software Update in Q4CY13
** FCS Q2CY13
*** FCS Q4CY13

Second Generation 802.11n

Teleworker

600

- Up to 300 Mbps
- Seamless Connectivity with Corporate SSID for Remote Office
- Split Tunneling and Local Resource Sharing*

Enterprise Class

1600

- Up to 300 Mbps
- CleanAir Express*
- ClientLink 2.0
- VideoStream

Mission Critical

2600

- Up to 450 Mbps
- High Client Scalability
- CleanAir
- ClientLink 2.0
- VideoStream

Best in Class

3600

- Up to 1.3 Gbps
- High Client Density
- Investment Protection, Future Proof Modularity (Security, 802.11ac** or 3G Small Cell***)
- 802.11ac Support
- HD Video/VDI, VideoStream
- Best In Class Security
- ClientLink 2.0, CleanAir

Teleworker → Enterprise → Mission Critical → Best In Class

Cisco Aironet 802.11n G2 Series Comparison Matrix

**Available as a Software Upgrade in H2 CY13

Indoor AP Series	600 Teleworker	1600	2600	3600
Max Data Rate	300 Mbps	300 Mbps	450 Mbps	450 Mbps and 1.3 GbpS with 11ac Module
RF Design MIMO:Spatial Stream	2x3:2	3x3:2	3x4:3	11n: 4x4:3 11ac: 3x3:3
Performance/Coverage/ Investment Protection	◆◆	◆◆◆	◆◆◆◆	◆◆◆◆◆
Max No. of Clients	15	256	400	400 50 - 11ac Module
RRM		✔	✔	✔
CleanAir		CleanAir Express**	✔	✔
ClientLink		ClientLink 2.0	ClientLink 2.0	ClientLink 2.0 for 802.11agn EBF for 802.11ac
Max No. of ClientLink 2.0 Clients		64	256	256 – ClientLink 2.0 32 – ECBF on 11ac Module
BandSelect		✔	✔	✔
VideoStream		✔	✔	✔
Rogue AP Detection		✔	✔	✔
Adaptive wIPS		✔	✔	✔
External Antenna Opt		✔	✔	✔
Module Options	Multiple Local Ethernet Ports			WSSI (Security) –Shipping 802.11ac - Q2CY13 Cisco 3G SCM – Q4CY13
Starting List Price	$419	$695	$1095	$1495 - AP $500 – WSSI & .11ac Module

AP 700

© 2010 Cisco and/or its affiliates. All rights reserved.

FCS May 2013

Cisco Aironet 700 Series Access Point

New

FOR VALUE CONSCIOUS MID MARKET, SP WIFI, AND EMERGING MARKET CUSTOMERS
Proven RF design for basic WiFi connectivity and business applications

2x2 ANTENNA DESIGN, 2 SPATIAL STREAMS
Provides consistent reliable 802.11n RF performance

GOOD PERFORMANCE
Delivers advanced features for its class - with good performance, functionality, and reliability at a great price

WITH PROVEN RF EXCELLENCE
Integrated antennas with simultaneous dual band radios, with RRM, BandSelect, VideoStream, Rogue Detection, and WIPS

Designed For:

- **Businesses Looking for Good Performance w/ Value**

AP700 only introduced in ultra-price sensitive deals as needed

Cisco Aironet 700 Series Access Point

FCS Q2CY13

New

Designed for Value-Minded Customers Looking for Proven Good RF Performance

Indoor AP Series	700	1600
Radios	Dual Band	Dual Band
RF Design (MIMO:SS)	2x2:2	3x3:2
Client Count	200	256
Autonomous	Future	✔
Beamforming	ECBF Ready	ClientLink 2.0
Spectrum Intelligence		CleanAir Express
RRM	✔	✔
VideoStream	✔	✔
BandSelect	✔	✔
Rogue Detection	✔	✔
Adaptive wIPS	✔	✔
Limited Lifetime Warranty	✔	✔
List Price (Integrated Ant.)	$495	$695

© 2010 Cisco and/or its affiliates. All rights reserved.

AP-700 Hardware specifications…

For more see www.cisco.com/go/ap700

Integrated Antenna	• 2.4 GHz, gain 3.0 dBi, horizontal beamwidth 360° • 5 GHz, gain 5.0 dBi, horizontal beamwidth 360°
Dimensions (W x L x H)	• Access point (without mounting bracket): 7 x 7 x 2 inches (177.6 x 177.6 x 50.4 mm)
Environmental	**Cisco Aironet 702i** • Operating temperature: 32 to 104°F (0 to 40°C) • Operating humidity: 10 to 90% percent (noncondensing) • Operating Altitude Test: 40°C, 9843 ft.
System Memory	• 128 MB DRAM • 128 MB flash
Powering Options	• 802.3af Ethernet Switch • Cisco Power Injectors (AIR-PWRINJ5=, AIR-PWRINJ4=) • Cisco Local Power Supply (AIR-PWR-B=)
Power Draw	• 9.5W (maximum)

Additional:

RF OUTPUT 100 mW

Both bands US

Software - 7.5 release

Autonomous (future)

2x2 MIMO (2-SS)

20 & 40 MHz

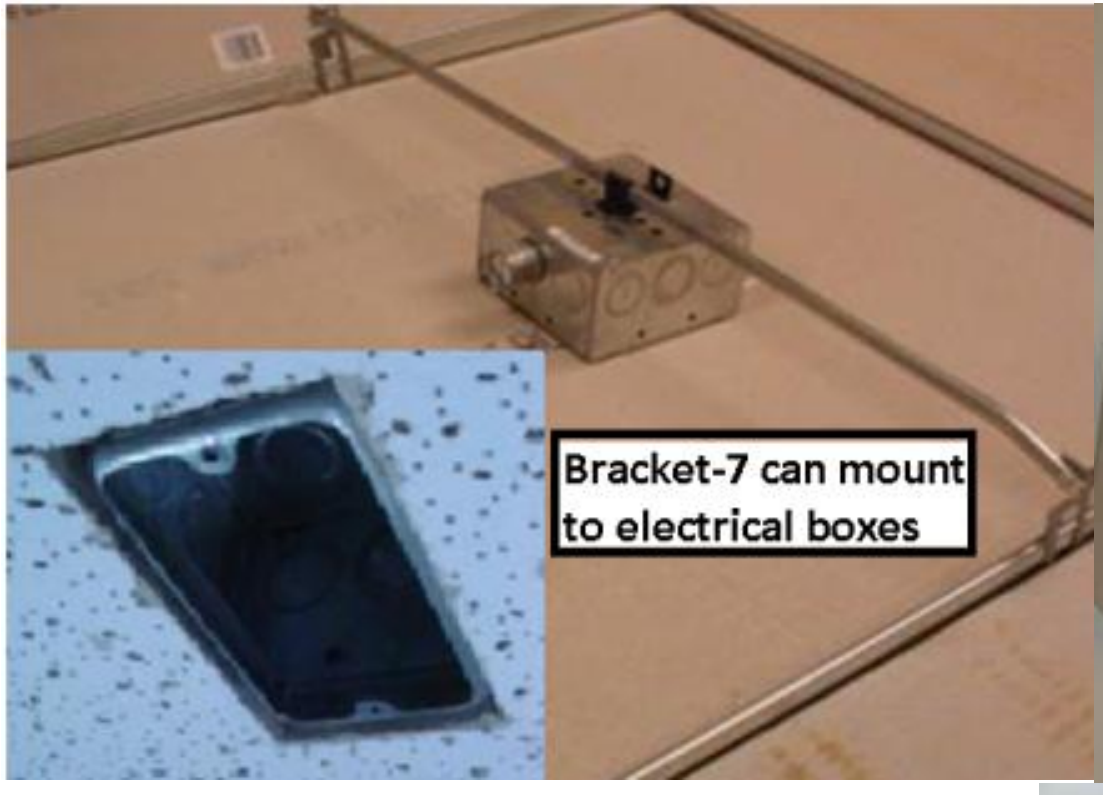
Up to 300 Mbps

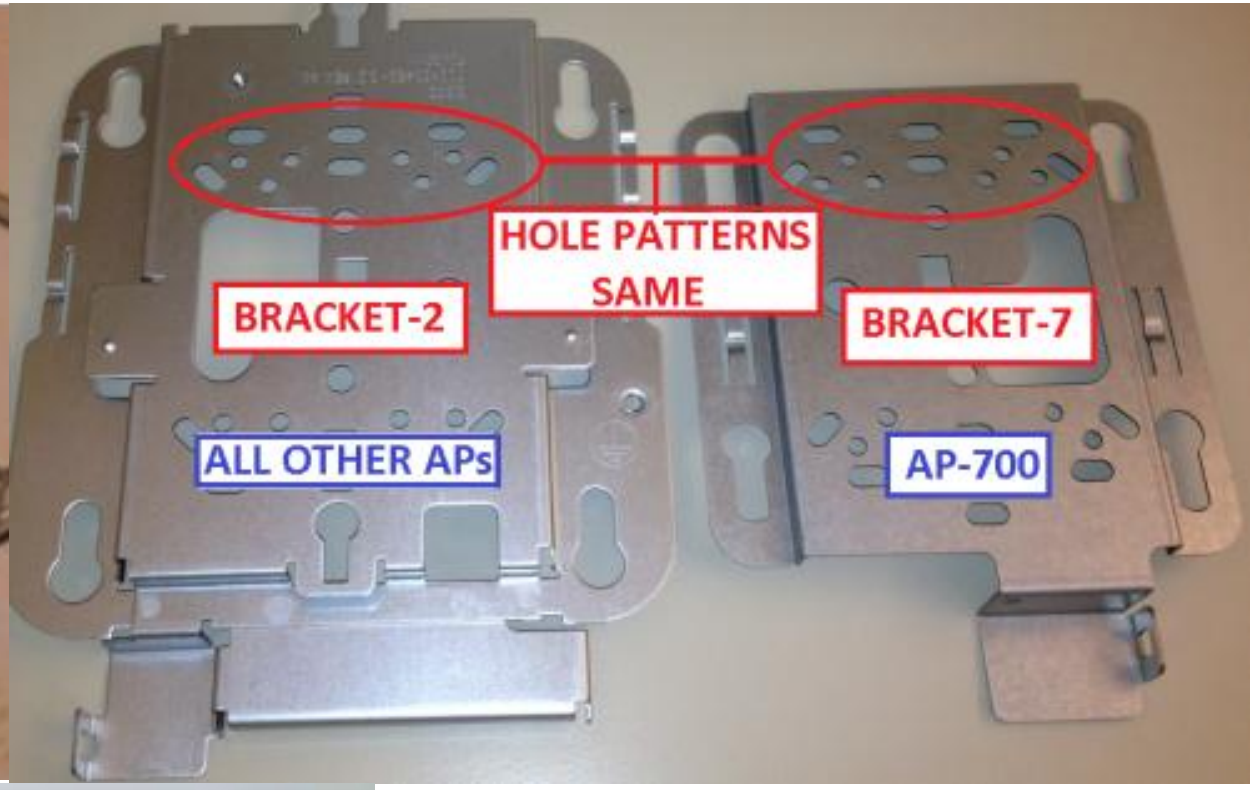
No DTLS support

100 Clients per Radio

Client Link - not supported

Understanding mounting installation options





While Bracket-3 does not work with the AP-700 you can still mount the AP-700 in the center of the tile if needed using an electrical box approach. See 3600 deployment guide for more details ☺

Although Bracket-7 is smaller the T-Rails (grid clips) are compatible with both brackets as the hole patterns are the same

AP-700 Mounting Information

- **Each AP-700 ordered includes:**
  - **New AIR-AP-BRACKET-7 (only compatible with AP-700)**
  - **Existing AIR-AP-T-RAIL-R or AIR-AP-T-RAIL-F**
  - **Optional AIR-CHNL-ADAPTER at additional cost ($5 USD).**
- **The table below details what mounting options are supported with AP-700 series.**

Mounting Option	Description	Usable with AP700 Series?
AIR-AP-BRACKET-7	*NEW* AP-702 Series Mounting Bracket	Yes
AIR-AP-T-RAIL-R	Ceiling Grid Clip for Aironet APs - Recessed Mount	Yes
AIR-AP-T-RAIL-F	Ceiling Grid Clip for Aironet APs - Flush Mount	Yes
AIR-CHNL-ADAPTER	T-Rail Channel Adapter for Cisco Aironet Access Points	Yes
AIR-AP-BRACKET-1	802.11n AP Low Profile Mounting Bracket	No
AIR-AP-BRACKET-2	802.11n AP Universal Mounting Bracket	No
AIR-AP-BRACKET-3	802.11n AP In-Ceiling Mounting Bracket	No
AP1130/1240/1250 brackets	Brackets used on legacy products	No

AP and 802.11a/b/g/n/ac review

Let’s take a quick look at the past and where we are going…

© 2010 Cisco and/or its affiliates. All rights reserved.

Review of 802.11a and 802.11b/g

For Your Reference

- 1 Transmitter & 1 Receiver (per band) – **up to 54 Mbps**
- Early diversity Access Points use two antennas with **one radio per band** sampling each antenna - choosing the one with the least multi-path distortion and then transmitting back on the same antenna
- Cisco 802.11a/b/g/ Access Points start off favoring the right (primary antenna port) then if multi-path or packet retries occur it will sample the left port and switch to that port if the signal is better.
- Since speeds were only 54 Mbps 10/100 ports were fine
- Since PoE was 15.4W the radios had plenty of power the higher gain antennas **above 6 dBi** were permitted
- Both Indoor/Outdoor was permitted without frequency restrictions 802.11n introduced restrictions for outdoors creating the 3502P

Review of 802.11n MIMO terminology

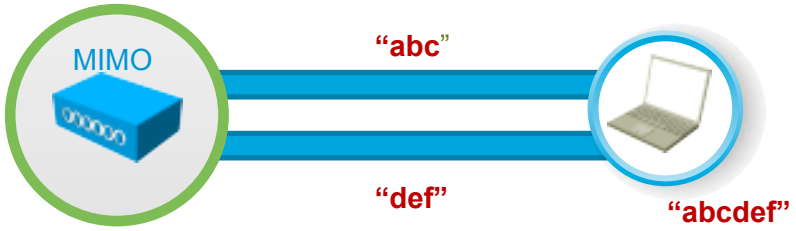
Understanding **MIMO** **M**ultiple **I**nput **M**ultiple **O**utput terminology

For Your Reference

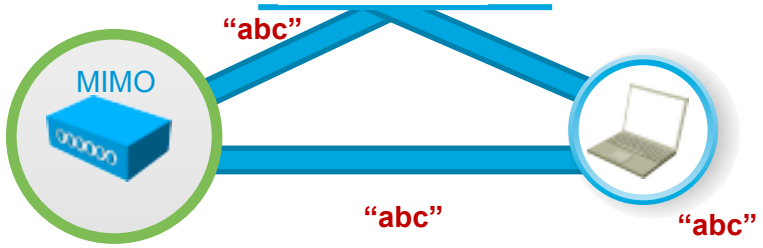
Spatial Multiplexing – A method for boosting wireless bandwidth by taking advantage of multiplexing which is the ability within the radio to send out information over two or more transmitters concurrently (in parallel) known as "spatial streams".

TxBF – Transmit beam forming – Signals that are sent on separate antennas that can be coordinated (think time shifted) to combine constructively at the receive antenna.

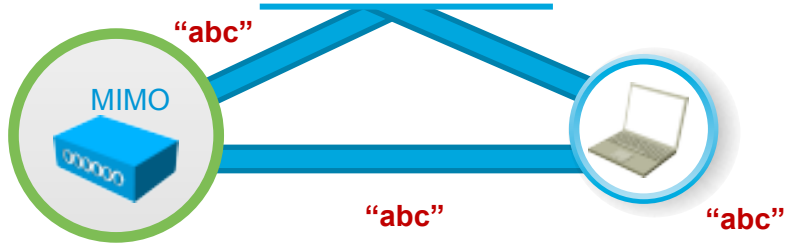
MRC – Maximal Ratio Combining a method that combines signals from multiple antennas taking into account factors such as signal to noise ratio to decode the signal with the best possible Bit Error Rate.



Sending side: send more symbols, in parallel (spatial multiplexing)



Sending side: synchronize signals for better resulting signal at receiving end (Transmit Beamforming, TxBF, ClientLink)



Receiving side: synchronize signals for better signal (Maximal Ratio Combining, MRC)

Review of 802.11n MIMO Terminology

For Your Reference

How do we get faster data rates with MIMO (Multiple-Input-Multiple-Output)

Channel Bonding – Use of more than one frequency or channel for more bandwidth.

Packet aggregation – Permits more efficient use of the RF spectrum

Guard Interval – Period of time that is used to minimize inter-symbol interference.
Short GI (400ns) Long GI (800ns) <default>

Take-away
When all things come together…

40 MHz bonded channel, short GI **450 Mbps**

Review of 802.11n Data Rates

MCS	Coding	Modulation	Streams	Signal BW =20 MHz		40 MHz	
				GI = 800 nS	GI =400 nS	GI = 800 nS	GI =400 nS
MCS0	1/2	BPSK	1	6.5	7.2	13.5	15
MCS1	1/2	QPSK	1	13	14.4	27	30
MCS2	3/4	QPSK	1	19.5	21.7	40.5	45
MCS3	1/2	16-QAM	1	26	28.9	54	60
MCS4	3/4	16-QAM	1	39	43.3	81	90
MCS5	2/3	64-QAM	1	52	57.8	108	120
MCS6	3/4	64-QAM	1	58.5	65	131.5	135
MCS7	5/6	64-QAM	1	65	72.2	135	150
MCS8	1/2	BPSK	2	13	14.4	27	30
MCS9	1/2	QPSK	2	26	28.9	54	60
MCS10	3/4	QPSK	2	39	43.3	81	90
MCS11	1/2	16-QAM	2	52	57.8	108	120
MCS12	3/4	16-QAM	2	78	86.7	162	180
MCS13	2/3	64-QAM	2	104	115.6	216	240
MCS14	3/4	64-QAM	2	117	130	243	270
MCS15	5/6	64-QAM	2	130	144.4	270	300
MCS16	1/2	BPSK	3	19.5	21.7	40.5	45
MCS17	1/2	QPSK	3	39	43.3	81	90
MCS18	3/4	QPSK	3	58.5	65	121.5	135
MCS19	1/2	16-QAM	3	78	86.7	162	180
MCS20	3/4	16-QAM	3	117	130	243	270
MCS21	2/3	64-QAM	3	156	173.3	324	360
MCS22	3/4	64-QAM	3	175.5	195	364.5	405
MCS23	5/6	64-QAM	3	195	216.7	405	450

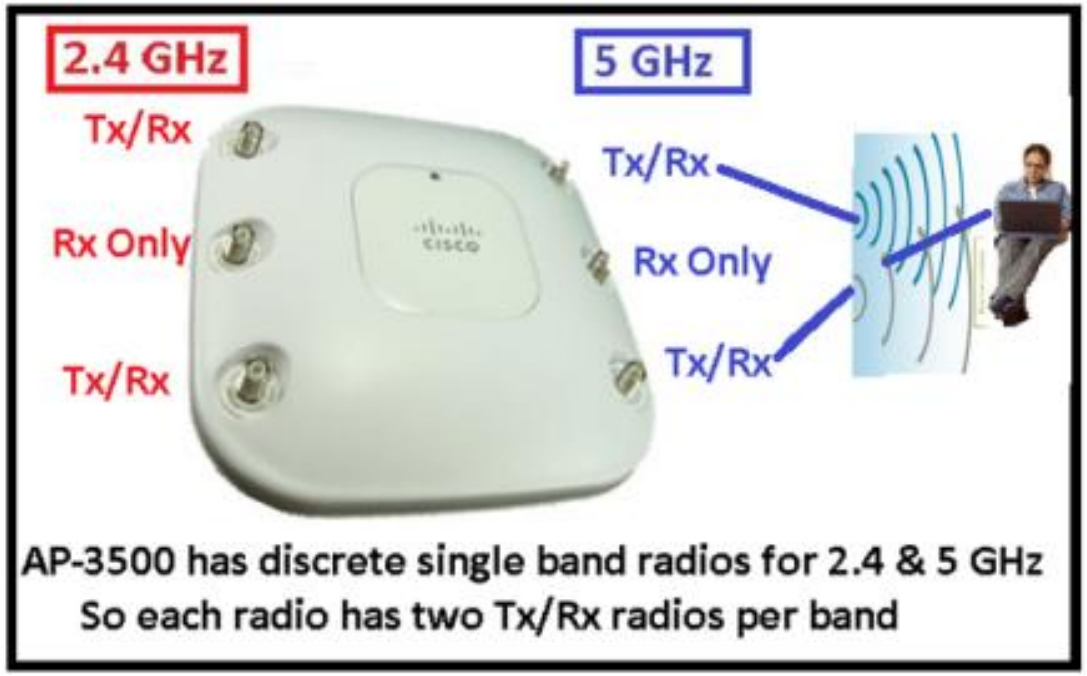
AP-1040,1140, 1250,1260,3500
New AP-700 & 1600
can support
Up to 2-Streams
300 Mbps (MCS15)

For Your Reference

AP-2600, AP3600
can support
Up to 3-Streams
450 Mbps (MCS23)
w/o .11ac module

Review – 802.11n "G1" first generation APs

- **Up to 3 radios per band – speeds up to 300 Mbps**
- **2.4 GHz (802.11b/g/n) and 5 GHz (802.11a/n) – Support for 2-spatial streams**
- **Lots of antennas (typically 6) three for each band**
- **Antennas are single band single radiating elements identified by black and blue (5-GHz) colors**
- **Introduction of ClientLink (beam-forming)**



Remember me?
I'm a 1250 ➔
Built like a tank
October 2007

Modularity is a
GOOD THING
➔

Review – 802.11n "G2" second generation APs

- **Up to 4 radios per band – speeds up to 450 Mbps**
- **Support for 3 Spatial Streams**
  2.4 GHz (802.11b/g/n) and 5 GHz (802.11a/n)
- **Antennas are dual band - dual radiating elements identified by an orange stripe resulting in the need for less physical antennas**
- **Introduction of ClientLink 2.0 better Beam-forming**
- **Introduction of upgrade option modules**

  Security Module & 802.11ac Module

Note: New .11ac module brings increased performance to the AP-3600 Access Point up to 1.3 Gbps

So let's talk about 802.11ac – Wave1

The Wi-Fi Alliance (WFA) is looking at Wave 1 today with the main features implemented being:

- Channel Bonding 80 MHz (mandatory)
- Faster modulation 256-QAM (optional)
- Ability to receive 1,2 & 3 Spatial Streams tested
  - 2SS is mandatory for non-battery-powered APs
  - Only 1SS is mandatory for battery powered AP's and clients
- **WFA's focus is on 80 MHz, 1-3SS and 256-QAM with WFA compliant products likely sporting a new Wi-Fi Certified logo**

802.11ac is happening in stages
Referred to as "Wave-1 and Wave-2

Wi-Fi CERTIFIED™ ac

Wi-Fi Alliance logo should look something like this

802.11ac Wave-1 and Wave-2

* The 802.11ac specification will be brought to market in 2 phases or “Waves”
* Each Wave of 802.11ac will require new chip sets

Feature	Wave 1 – 2013	Wave 2 – 2014/2015 Features still in Discussions			
PHY Rate	1.3 Gbps	1.3 Gbps	1.73 Gbps	2.6 Gbps	3.5 Gbps
# of Spatial Streams	3	3	4	3	4
Modulation	256 QAM	256 QAM	256 QAM	256 QAM	256 QAM
Channel Width	20, 40, 80 MHz	20, 40, 80 MHz	20, 40, 80 MHz	20, 40, 80, 160 MHz	20, 40, 80, 160 MHz
MIMO	Single User	Multi User	Multi User	Multi User	Multi User
802.11 protocol support	a, n, ac	a, n, ac	a, n, ac	a, n, ac	a, n, ac
Ethernet Uplink	GbE	GbE, Multiple GbE or 10GbE			

So let's talk about 802.11ac - How is it like .11n?

802.11ac (Wave-1) introduces 256-QAM

Faster throughput happens when you can use more complex Modulation Coding Schemes (MCS) rates

MCS	Coding	Modulation	Streams
MCS0	1/2	BPSK	1
MCS1	1/2	QPSK	1
MCS2	3/4	QPSK	1
MCS3	1/2	16-QAM	1
MCS4	3/4	16-QAM	1
MCS5	2/3	64-QAM	1
MCS6	3/4	64-QAM	1
MCS7	5/6	64-QAM	1

802.11n 1-ss MCS up to 64-QAM
64-QAM uses 6 bits per symbol

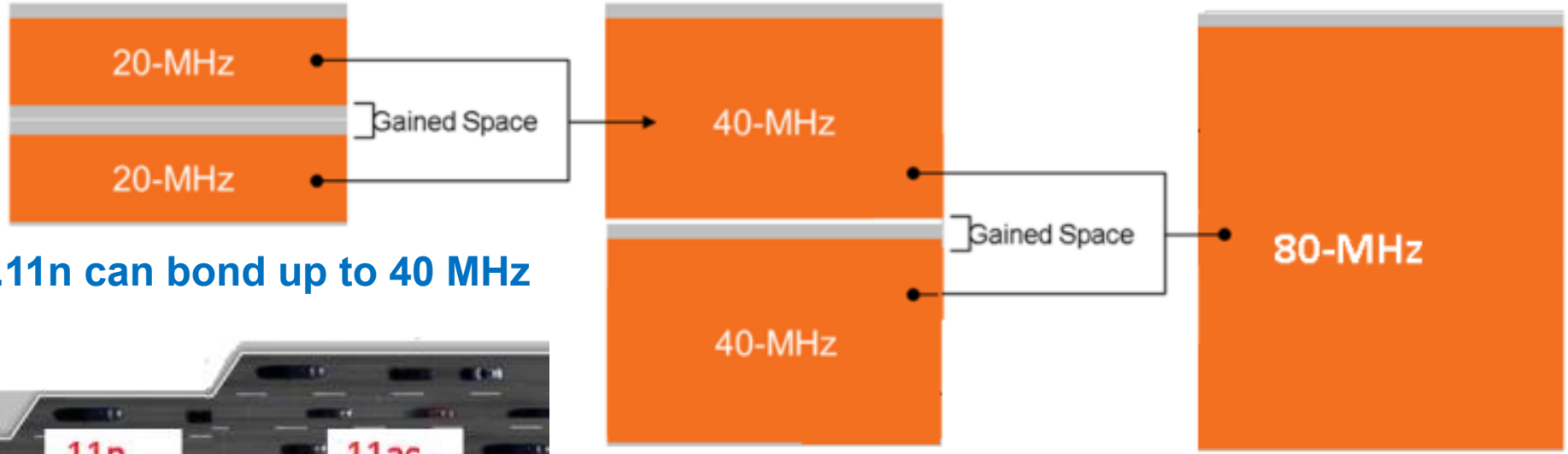
MCS	Coding	Modulation	Streams
0	1/2	BPSK	1
1	1/2	QPSK	1
2	3/4	QPSK	1
3	1/2	16-QAM	1
4	3/4	16-QAM	1
5	2/3	64-QAM	1
6	3/4	64-QAM	1
7	5/6	64-QAM	1
8	3/4	256-QAM	1
9	5/6	256-QAM	1

802.11ac 1-ss MCS supports 256-QAM
256-QAM uses 8 bits per symbol (up to 4x faster)

So let's talk about 802.11ac - How is it like .11n?

What about channel bonding?

Wave-1 allows up to 80 MHz channel bonding



802.11n can bond up to 40 MHz

802.11ac can bond up to 80 MHz (Wave-1)
***up to 160 MHz (Wave-2)**

So why is channel bonding so important?

MCS rates @ 1 Spatial Stream in Mbps

MCS	Modulation	Ratio	20 MHz channel	40 MHz channel	80 MHz channel WAVE-1
			400 ns GI	400 ns GI	400 ns GI
0	BPSK	1/2	7.2	15	32.5
1	QPSK	1/2	14.4	30	65
2	QPSK	3/4	21.7	45	97.5
3	16-QAM	1/2	28.9	60	130
4	16-QAM	3/4	43.3	90	195
5	64-QAM	2/3	57.8	120	260
6	64-QAM	3/4	65	135	292.5
7	64-QAM	5/6	72.2	150	325
8	256-QAM	3/4	86.7	180	390
9	256-QAM	5/6	N/A	200	433.3

New Phones such as the HTC One & Samsung S 4 have support for 802.11ac Wave-1

More than 1-SS requires that the client have more radios which draw more power.

The goal is to enable devices to have more throughput with less battery draw

Most mobile devices will use 1-SS

Tablets & laptops can use 2-SS or more

Expected 802.11ac Client Throughput (take-away)

1 stream (80MHz) is 433 Mbps
2 stream (80MHz) is 866 Mbps
3 stream (80MHz) is 1300 Mbps

(Now let's drop it to ~70% MAC efficiency)

BW (MHz)	#Spat Strm	MCS (QAMr5/6)	PHY rate (Mbps)	MAC thruput (Mbps)*
80	1	64	290*	210
80	1	64	330	230
80	1	256	430	300
80	2	64	650	460
80	2	256	870	610
80	3	64	980	680
80	3	256	1300	910

802.11ac Performance Table

So assuming ~70% MAC efficiency*
What's the real expected throughput?

Smartphones from 210 Mbps*

Tablets from 460 Mbps*

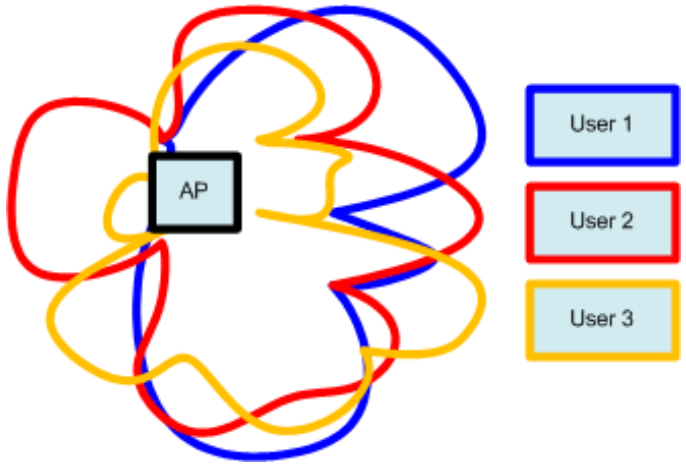
BYOD CONTINUES

High End Laptops from +680 Mbps*

How about Multi-User MIMO (MU-MIMO)
Does it work? Any caveats?

- **802.11ac MU MIMO is like 802.11n MIMO, except instead of one client, there are up to four clients**
  - AP does pre-coding for all the clients within the MU group simultaneously
  - In MU pre-coding, when AP beam-forms space-time streams to one client, it simultaneously null-steers those space-time streams to the rest.
  - All users' MPDUs are padded to the same number of OFDM symbols
- **MU-MIMO is technically risky and challenging:**
  - Needs precise channel estimation (CSI) to maintain deep nulls
  - Precise channel estimation adds overhead
  - Rate adaptation is more difficult
  - Throughput benefits are sensitive to MU grouping

WFA Wave 2 certification:
- MU-MIMO



Null-steering:To send data to user 1, the AP forms a strong beam toward user 1, shown as the top-right lobe of the blue curve. At the same time the AP minimizes the energy for user 1 in the direction of user 2 and user 3. This is called "null steering" and is shown as the blue notches. Same logic applies to red and yellow beams.

Some things to be aware of…

Quick review of positioning – then let's dive into the .11ac module

© 2010 Cisco and/or its affiliates. All rights reserved.

Three separate and discrete radios…

802.11ac Radios > Configure

General

AP Name	AP-11AC
Admin Status	Enable
Operational Status	UP
Slot #	2

11n and 11ac Parameters

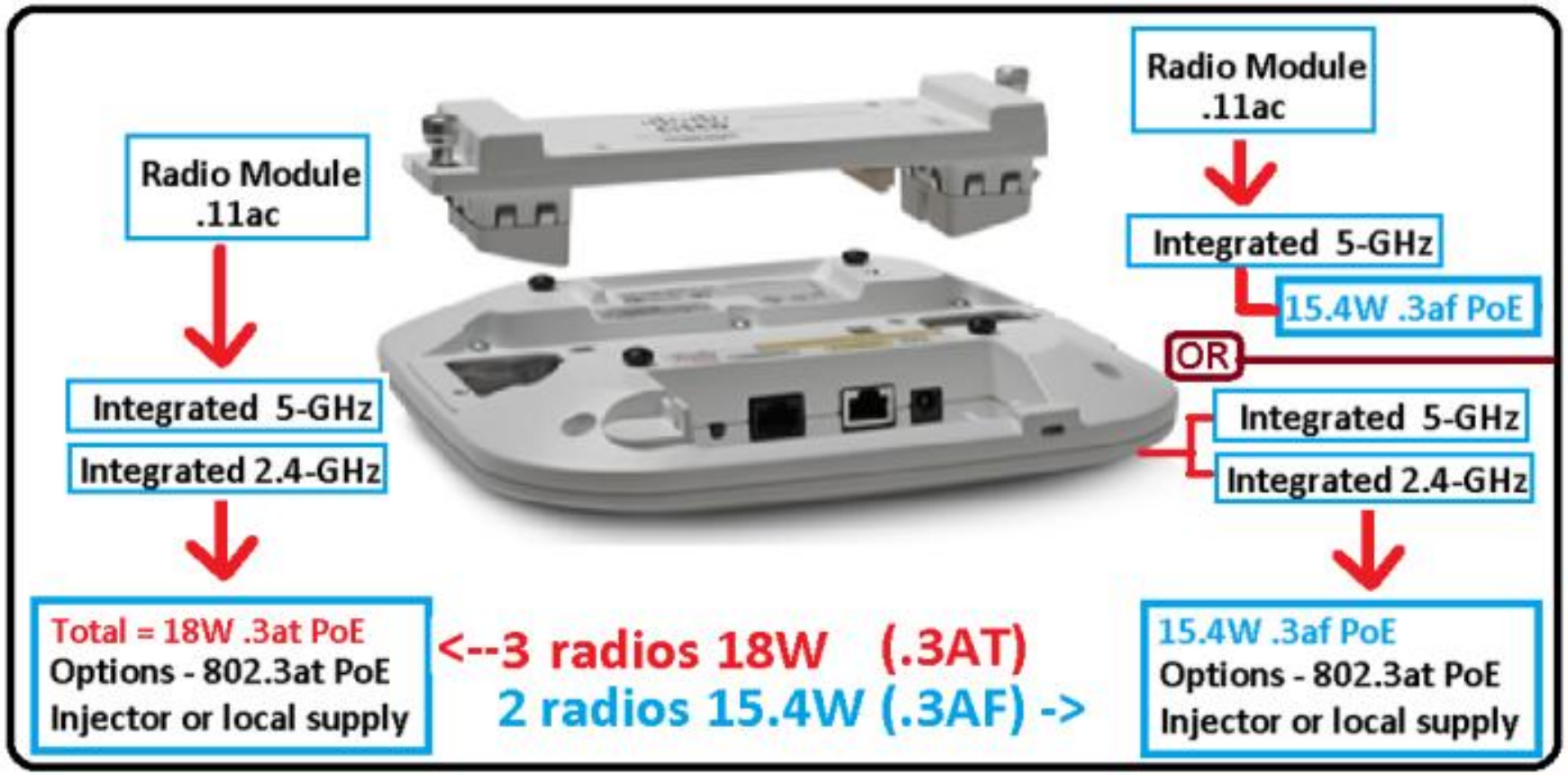
11n Supported	Yes
11ac Supported	Yes

AC clients connect to the AC module only If they require other support (legacy or CCX) They are moved to other radio

5G N clients go to the internal radio as do AC clients if no module present AC clients will be "sticky" to the AC module

The two 5-GHz radios (integrated and module) work in TANDEM and use same SSIDs so they do not compete with each other. They work in concert to support same channels (with internal radio taking lead on frequency selection) and the module performing the AC "overlay"
AP has a dual-core uP with the radio module on one core supporting up to 50 .11ac clients

Power over Ethernet – AC Radio Module



To get the module running on .3af PoE (15.4W) it is possible to disable the 2.4 GHz radio & restart.

AIR-PWR-INJ5 (PoE) Injector
Does not support three radios
Use injector - 4

All 3 radios (module + 2 internal radios) requires 18W (802.3at) source "PoE +"
If the switch doesn't support this - the module will be disabled by (default) until a proper source of power is applied such as PoE injector Cisco AIR-PWR-INJ4 or local 48VDC supply AIR-PWR-B

Modules and 3600 Series AP – Powered by Cisco Access Layer Switches

Cisco Switches 3600 Module Ready

80% of Cisco switches sold today are capable of enhanced or 802.3at PoE

Cisco Switches	802.3af - PoE	Cisco Enhanced PoE	802.3at - PoE+	UPoE
Module and 3700 – PoE ready Switches	X	✔	✔	✔
4500 E Series 47xx line card	X	X	✔	✔
4500 E Series all other copper line cards	X	X	✔	X
4500 non E Series	X	X	X	X
3850 24P/48P/48F models	X	X	✔	X
3750-X	X	X	✔	X
3750-E	X	✔	X	X
3750-G	X	X	X	X
3560-X	X	X	✔	X
3560-E	X	✔	X	X
3560-C	X	X	✔	X
2960-S	X	X	✔	X
2960-C	X	X	X	X
2960	X	X	X	X
Power Injectors		AIR-PWR-INJ4		

= Sufficient Power for the 3600 Series Access Point

© 2010 Cisco and/or its affiliates. All rights reserved.

What .11ac clients are available today?

What did we use for beta?

Beta customers provided with D-Link but new .11ac devices are being released so more will be available

Check spec sheets for # of SS

USB clients available today.

ASUS Model USB-AC53
D-Link Model DWA-182
Belkin Model F9L1106
Netgear A6200
Buffalo Model WI-U2-866D
Edimax Model EW-7822UAC
Linksys AE6000

PCI - Desktop clients

ASUS Model PCE-AC66

WGB - Like

TRENDnet Model TEW-800MB
Buffalo Model WLI-TX4-1300H
Linksys Model WUMC710
Linksys Model AC1300*

***Note: The Linksys AC1300 is the best external WGB like device so far as it supports 3-SS**

What .11ac clients are coming?

So when are these chipsets hitting the notebook computers?

Integrated Notebook devices –

Not announced but anticipated in CY13

Intel based Ultrabooks – 2x2 802.11ac Wave 1

Apple – 2x2 or 3x3 802.11ac Wave 1

Mac Rumors is saying Apple likely to use Broadcom chipset perhaps introducing a new notebook lineup at Apple WWDC in June – Note: **Mac OS X 10.8.4 beta shows AC support**

http://www.macrumors.com/2013/04/09/code-in-os-x-10-8-4-suggests-future-macs-will-offer-802-11ac-gigabit-wi-fi-support/

.11ac clients? Any issues so far?

USB clients appear a bit slow (and can have driver issues)

Some clients seem to be having trouble using DFS channels @ 80 MHz

Some client(s) that do not work well from the client steering perspective:

- **Linksys AE6000 USB (CSCuf78329)**

Linksys 11ac USB client, under certain conditions, will appear to keep trying to connect to 2.4 radio (appears to be a client driver issue) even though we drop the probe/auth/assoc due to band select/client steering features.

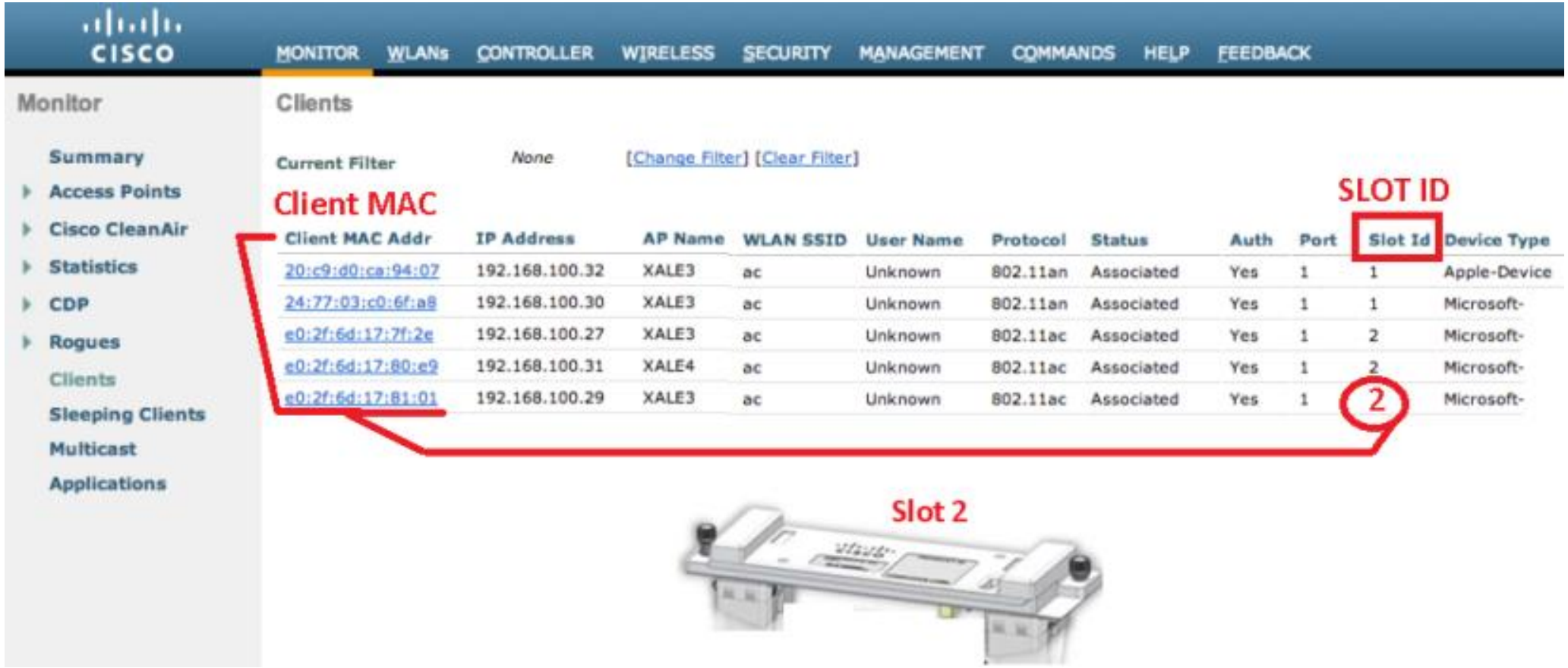
This one is a bit problematic based on MediaTek chip

Sometimes it doesn't even send probe requests on 5G band. We are still working to see if anything can be done on the AP SW side that would overcome this client problem

At this time, we cannot guarantee that this client adapter will associate to 11ac radio consistently, compared to other 11ac client adapters.

Note: Most of the clients based on Broadcom chipset appear fine

How can I tell the .11ac client is on the .11ac radio?



The client should report 11ac rates if connected to the 11ac module – If no module present the .11ac client should drop to .11n rates and connect to slot 1 (internal 5-GHz radio)

Beamforming and the .11ac Radio Module

ECBF Explicit Compressed Beam Forming - The .11ac radio module uses this method of client "channel sounding" per IEEE 802.11ac specification.

Note: The .11ac radio module does not support Cisco ClientLink 2.0, Cisco Compatible Extensions (CCX) or RRM.

This is because the .11ac radio is not a primary interface as it is controlled by the active integrated .11n radio as a virtual or "blended radio" working in tandem so same SSID, channel etc.

The primary radio still supports these features and controls when the 11ac radio module can transmit. This ensures it does not interfere with the primary integrated 11n radio providing isolation and maintaining receiver sensitivity.

ClientLink 2.0 continues to enhance legacy and .11n clients, via 11n radio and will service what the .11ac radio doesn't understand*

***(for the most part) ☺**

Troubleshooting the .11ac module

Things to look for if the module doesn't come up

Common issues arise because:

- Module isn't screwed down tightly
- Not enough PoE power (requires 802.3at) 18W
- Not configured correctly
- Not understanding the radios operate "together" so you need to configure the radio in slot 1 (5 GHz internal) first
- Not understanding SSID's for both 5 GHz need to be the same and all .11ac clients are sent to the .11ac module

Things to look for if the module is not found:

- Console will report "module radio found and ok"
- Also console CDP message for Power "Power ok – HIGH POWER inline power source"
- Perhaps remove module – verify AP ok then reinstall
- Module should show up as "slot-2"
- If you suspect PoE (try AIR-PWRB or AIR-PWR-INJ4)
- Module with not work with AIR-PWR-INJ5

Software update AireOS 7.5

© 2010 Cisco and/or its affiliates. All rights reserved.

High Availability – 7.5

© 2010 Cisco and/or its affiliates. All rights reserved.

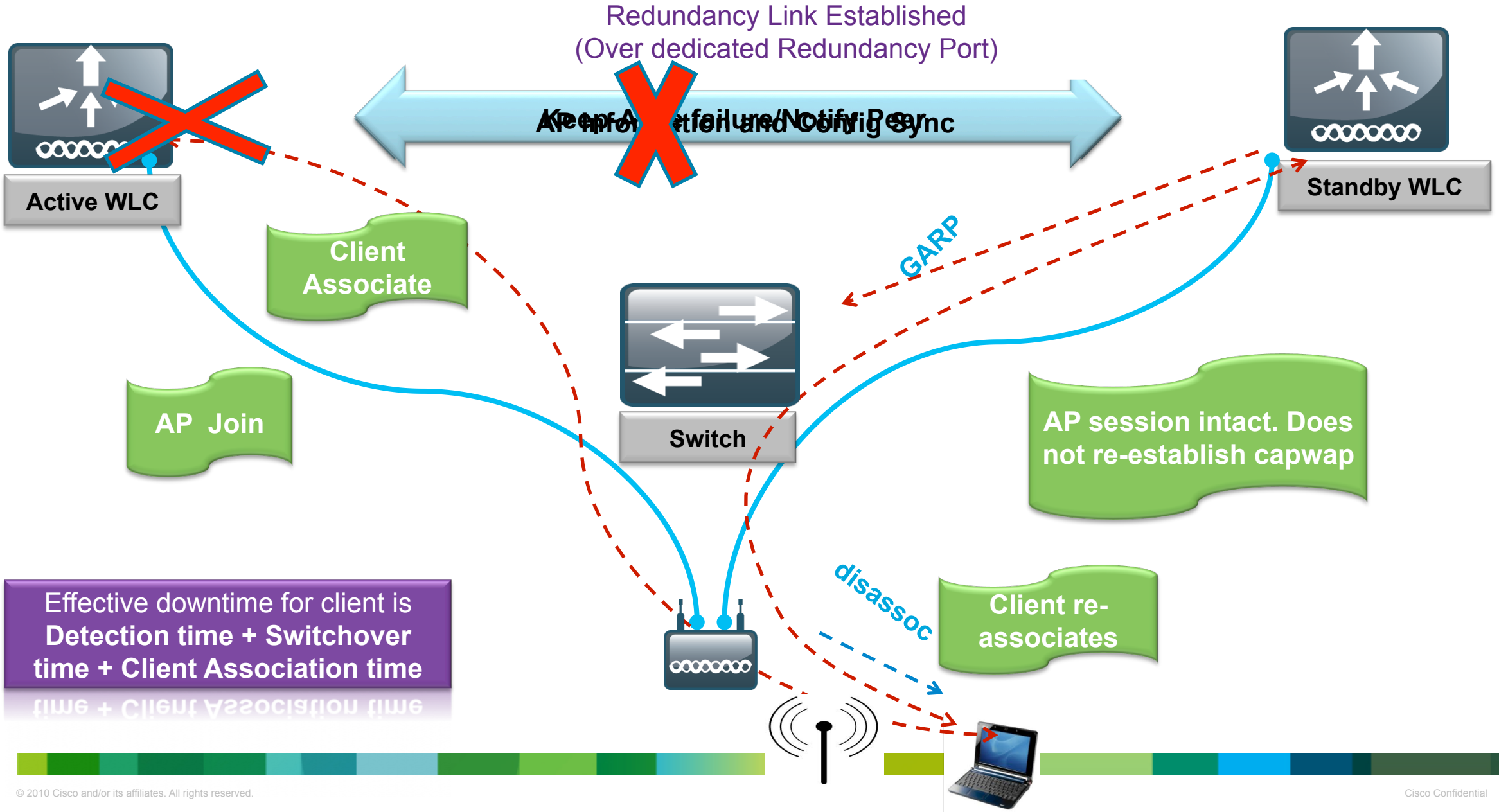
High Availability APSSO support 7.3/7.4

- Model is 1:1 (Active : Hot-Standby)
- Same management IP on Active and Standby
- Static & dynamic system configurations synced to standby.
- AP information, CAPWAP state synced to the standby. AP CAPWAP re-join is avoided on switchover.
- Supported on 5500 / 7500 / 8500 and WiSM-2
- Same hardware and software version
- Two new interfaces
  - Redundancy Port
  - Redundancy Management Interface
- Back-to-back Connectivity on the Redundancy Port between the two WLCs
- Clients are de-authenticated on failover ; forced to re-authenticate.

Effective service downtime = Detection time + Switch Over Time (Network recovery/convergence) + Client re-association time

© 2010 Cisco and/or its affiliates. All rights reserved.

Stateful HA with APSSO



© 2010 Cisco and/or its affiliates. All rights reserved.

Client SSO

© 2010 Cisco and/or its affiliates. All rights reserved.

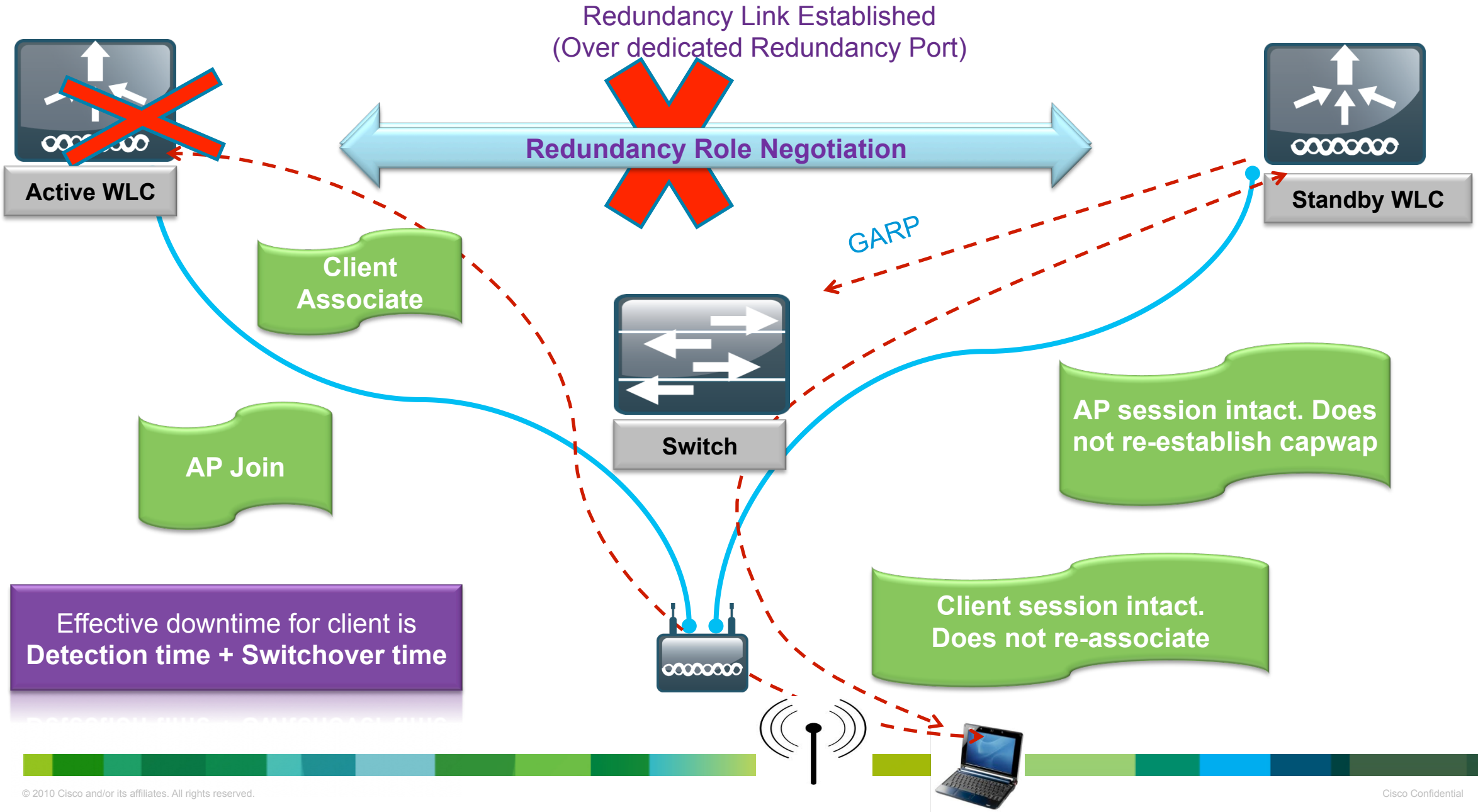
Stateful HA with Client SSO

- Client's information is synced to the Standby
  - ✓ Client information is synced when client moves to RUN state.
  - ✓ Client re-association is avoided on switch over
- Fully authenticated clients(RUN state) are synced to the peer.
- The intermediate client state events are not synced
- Transient clients are de-authenticated after switch over.

Effective service downtime = Detection time + Switch Over Time (Network recovery/convergence)

© 2010 Cisco and/or its affiliates. All rights reserved.

Stateful HA with Client SSO



© 2010 Cisco and/or its affiliates. All rights reserved.

HA Topologies

© 2010 Cisco and/or its affiliates. All rights reserved.

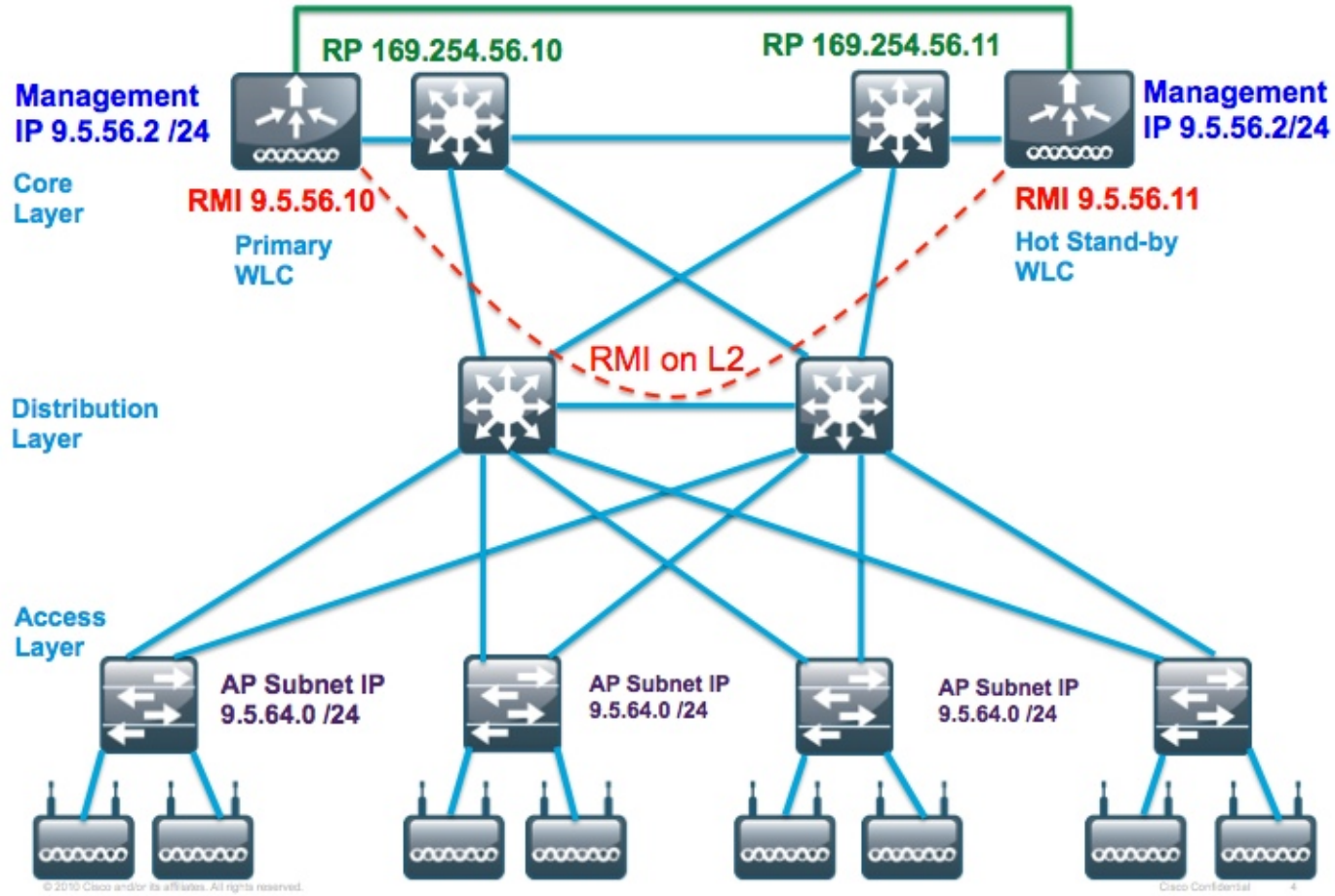
Supported HA Topologies – 7.5

1. Two 5508 , 7500 or 8500 connected via back-to-back RP port in the same data center
2. Two 5508 , 7500 or 8500 connected via RP port over L2 VLAN/fiber in the same or different data center
3. Two 5508, 7500 or 8500 connected to a VSS pair.

4. Two WiSM-2 on the same chassis
5. Two WiSM-2 on different chassis with redundancy VLAN extended over L2 network
6. Two WiSM-2 on different chassis in VSS mode

© 2010 Cisco and/or its affiliates. All rights reserved.

WLC 5508/7500/8500 Back-to-back RP Connectivity



Configuration on Primary WLC:

- configure interface address management 9.5.56.2 255.255.255.0 9.5.56.1
- configure interface address redundancy-management 9.5.56.10 peer-redundancy-management 9.5.56.11
- configure redundancy unit primary
- configure redundancy mode sso

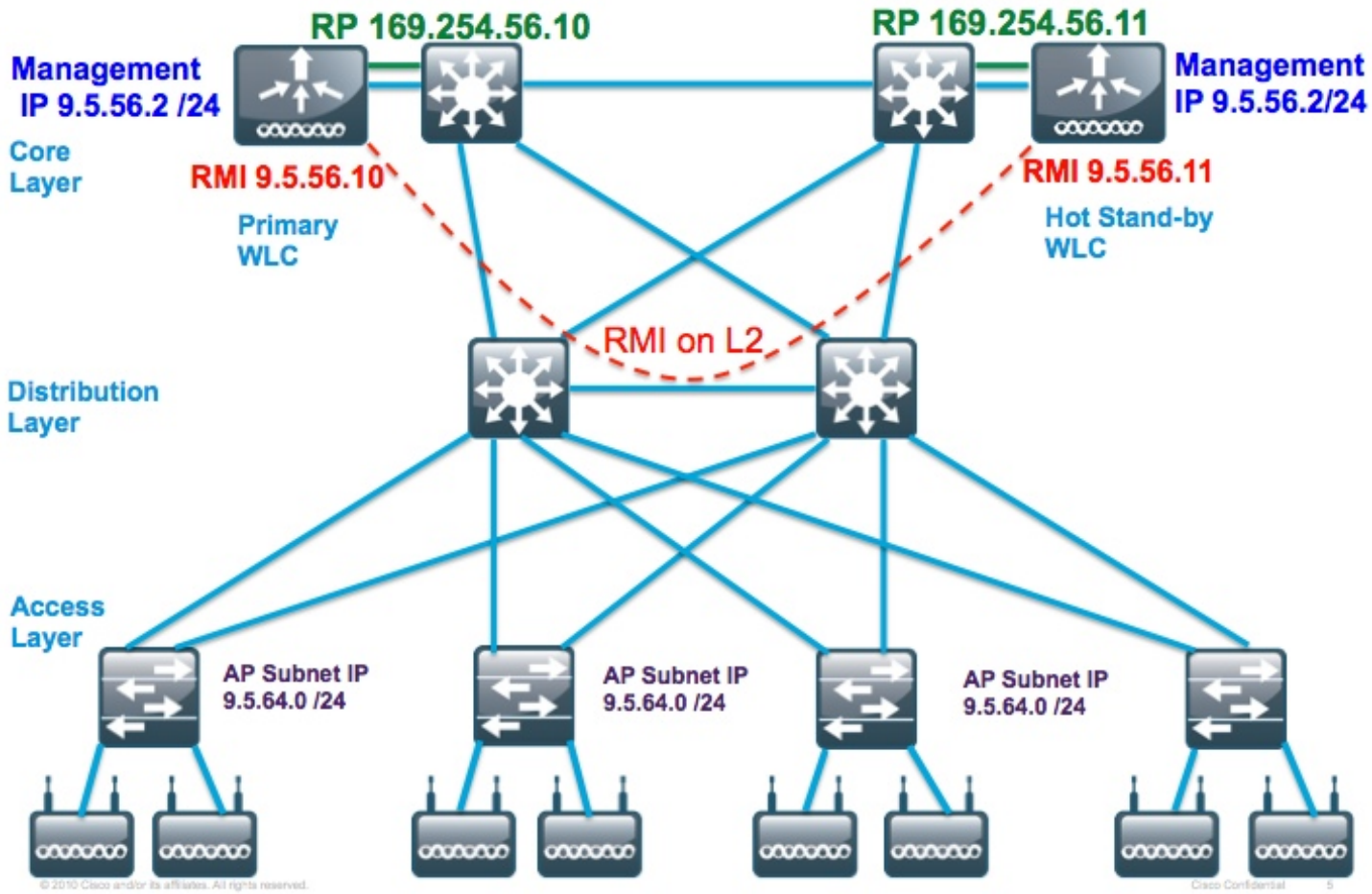
Configuration on Hot Standby WLC:

- configure interface address management 9.5.56.3 255.255.255.0 9.5.56.1
- configure interface address redundancy-management 9.5.56.11 peer-redundancy-management 9.5.56.10
- configure redundancy unit secondary
- configure redundancy mode sso

Management GW is monitored with 12 pings

© 2010 Cisco and/or its affiliates. All rights reserved.

WLC 5508/7500/8500 RP Connectivity via Switches



Configuration on Primary WLC:

- configure interface address management 9.5.56.2 255.255.255.0 9.5.56.1
- configure interface address
  redundancy-management 9.5.56.10
  peer-redundancy-management 9.5.56.11
- configure redundancy unit primary
- configure redundancy mode sso

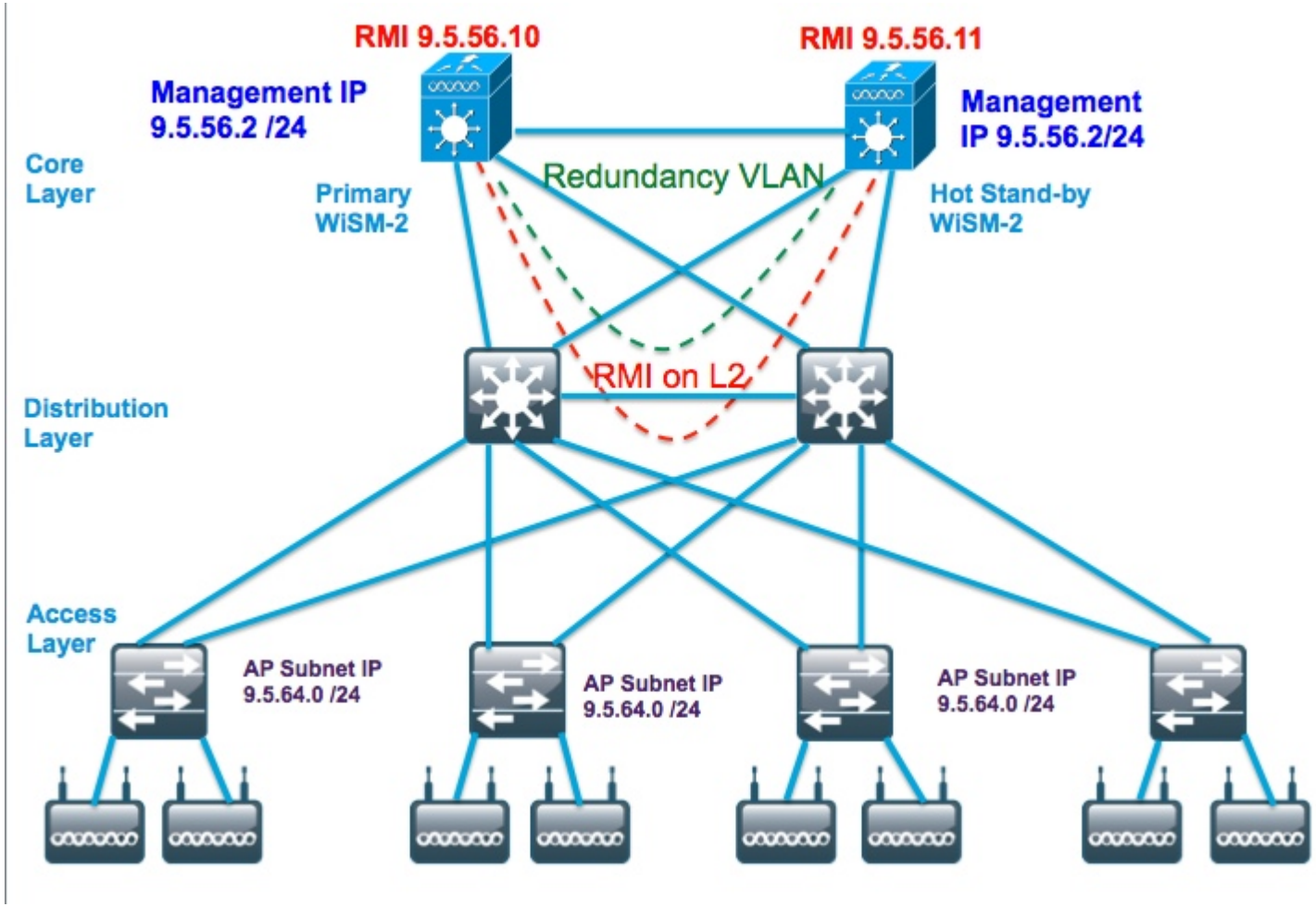
Configuration on Hot Standby WLC:

- configure interface address management 9.5.56.3 255.255.255.0 9.5.56.1
- configure interface address
  redundancy-management 9.5.56.11
  peer-redundancy-management 9.5.56.10
- configure redundancy unit secondary
- configure redundancy mode sso

RTT Latency : 80 ms or less default ; Bandwidth: 60 Mbps or more ; MTU: 1500

© 2010 Cisco and/or its affiliates. All rights reserved.

WiSM-2 connectivity over L2 Redundancy VLAN

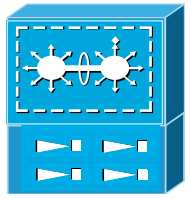


Configuration on Cat6k

wism service-vlan 192 (service port VLAN)
wism redundancy-vlan 169 (redundancy port VLAN)
wism module 6 controller 1 allowed-vlan 24-38 (data VLAN)

© 2010 Cisco and/or its affiliates. All rights reserved.

WiSM-2 in a VSS Pair

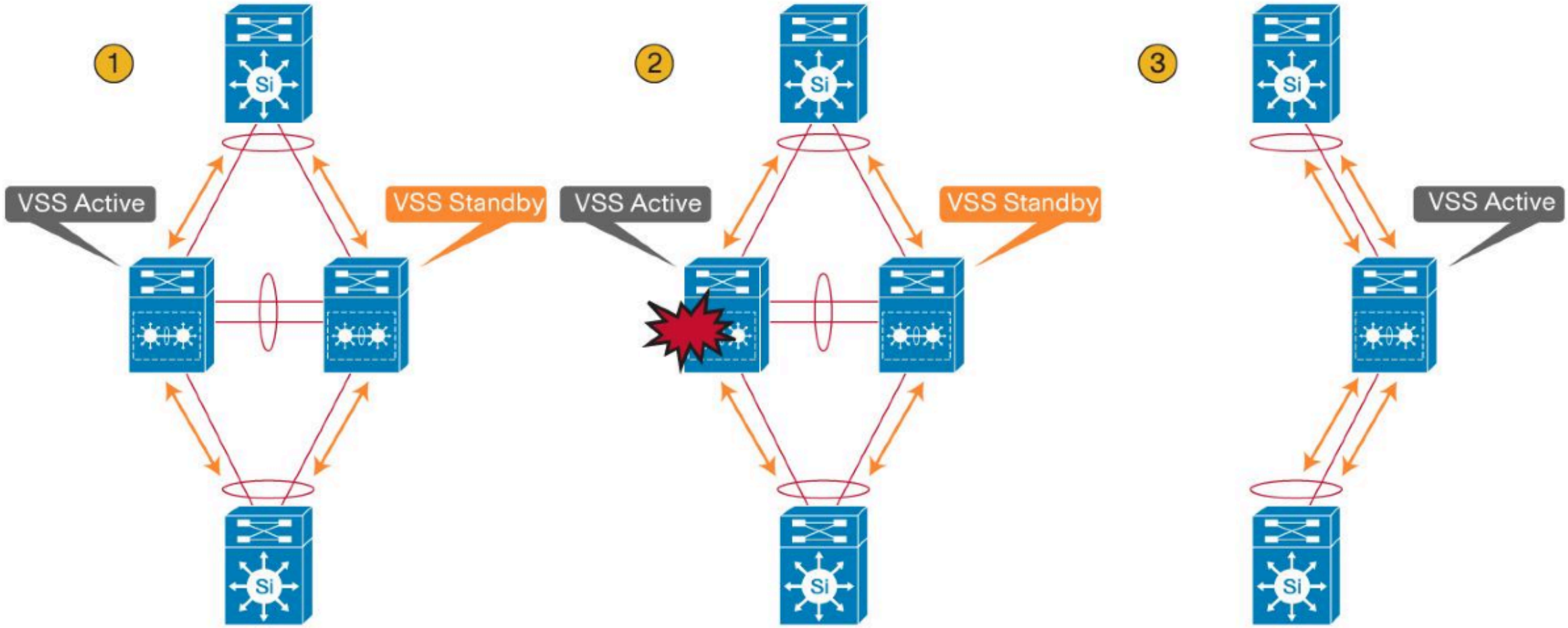


Virtual Switch System (VSS)

Switch-1 (VSS Active)		Switch-2 (VSS Standby)
Control Plane Active	VSL	Control Plane Standby
Data Plane Active	Failover/State Sync VLAN	Data Plane Active
FWSM Active		FWSM Standby
WiSM-2 Active		WiSM-2 Backup

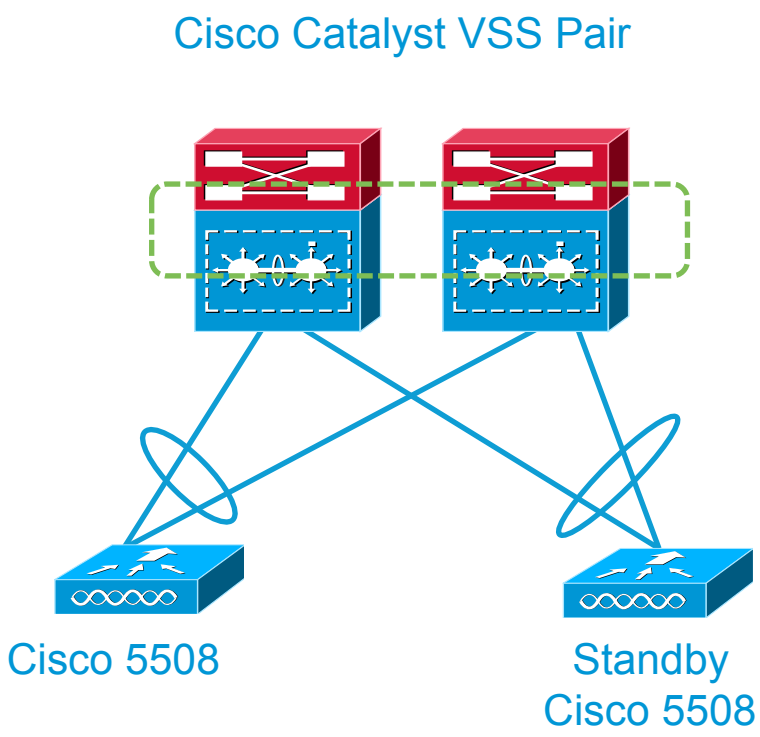
© 2010 Cisco and/or its affiliates. All rights reserved.

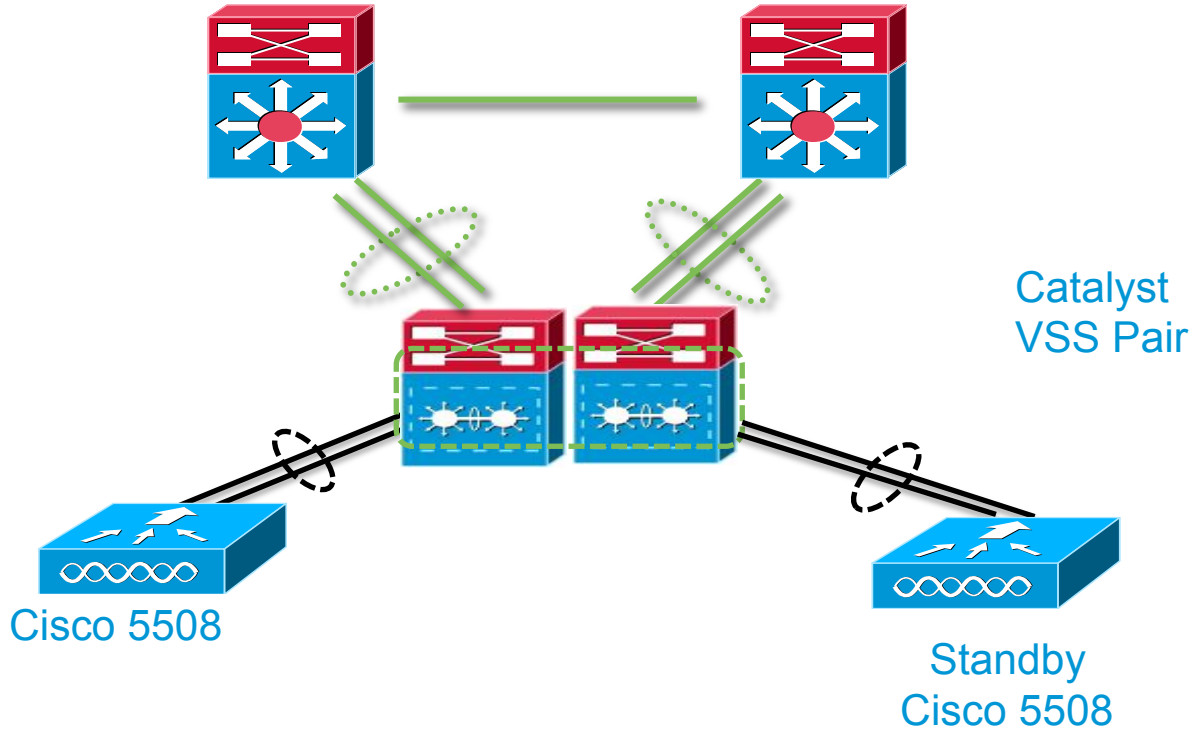
WiSM-2 in a VSS Pair



© 2010 Cisco and/or its affiliates. All rights reserved.

WLC 5508/7500/8500 Connected to VSS Pair





© 2010 Cisco and/or its affiliates. All rights reserved.

SSO Behavior and Recommendations

- RTT latency on Redundancy Link : 80 milliseconds or less. 80% of keepalive timer.
- Preferred MTU on Redundancy Link : 1500 or above.
- Bandwidth on Redundancy Link : 60 Mbps or more.

- 5500 / 7500 / 8500 : RP Connectivity between Active and Standby
  - ✓ Via Switches (7.5)
  - ✓ Back-to-back (7.3, 7.4, 7.5)
- WiSM-2 : single 6500 chassis OR different chassis using VSS setup/extending redundancy VLAN.

- Recommended to have Redundancy Link and RMI Connectivity between WLCs on different switches or on different L2 networks
- Keepalive/Peer Discovery timers should be left with default timer values for better performance
- Default box failover detection time is 3 *100 = 300+60 = 360 +jitter (12 msec)= ~400 msec

© 2010 Cisco and/or its affiliates. All rights reserved.

Client SSO Limitations

- Standby maintains 2 client lists:
  - List for client in RUN state
  - Transient list for clients in all other states
- ONLY Clients in RUN state are maintained during failover
  - Transient list is deleted
  - Clients in transitions like roaming, dot1x key regeneration, webauth logout, etc. are disassociated
  - Posture and NAC OOB are not supported, since client is not in RUN state
- Some clients, and some information about clients are not sync between Active and Standby
  - CCX Based apps - need to be re-started post Switch-over
  - Client Statistics are not synced
  - PMIPv6, NBAR, SIP static CAC tree are not synced, need to be re-learned after SSO
  - WGB and clients associated to it are not synced
  - OEAP(600) clients are not synced
  - Passive clients are not synced
- New mobility is not supported

© 2010 Cisco and/or its affiliates. All rights reserved.

Application Visibility & Control

Phase 2

© 2010 Cisco and/or its affiliates. All rights reserved.

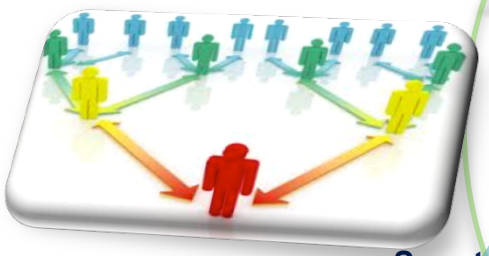
Tomorrow's Solution to manage the network…

DPI of packet contents up to L7. Inspect ~1000 protocols and sub-protocols using advanced classification mechanisms

Natively Integrated into Cisco WLC

Simple to Enable

Web Based Eco-System to manage the solution



Discover

Control

Report

Smarter decisions on how to handle network traffic- Per application and per user prioritization and control

Get visibility into network users and traffic pattern & capacity & trends

Application Visibility & Control
AVC

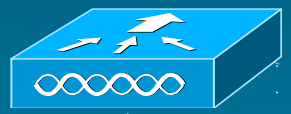
© 2010 Cisco and/or its affiliates. All rights reserved.

How AVC solution works

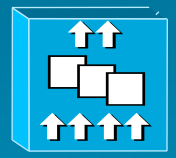
Deep Packet Inspection

DPI engine (NBAR2) identifies applications using L7 signatures

WLC rel 7.5



NFv9



Reporting Tools

Perf. Collection & Exporting

WLC collects application bandwidth, response time metrics, and export to management tool

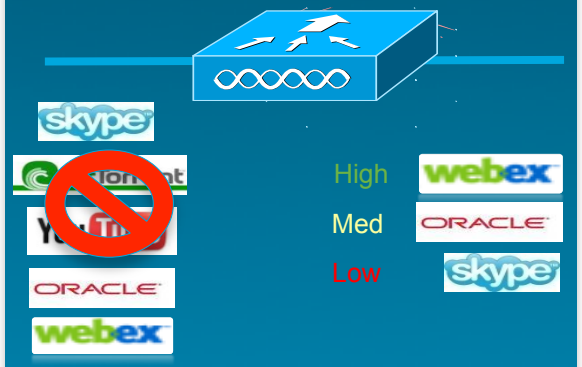
App Visibility & User Experience Report

App	BW	Transaction Time	…
WebEx	3 Mb	150 ms	…
Citrix	10 Mb	500 ms	…

Reporting Tool

Advanced reporting tool aggregates and reports application performance

WLC rel 7.5



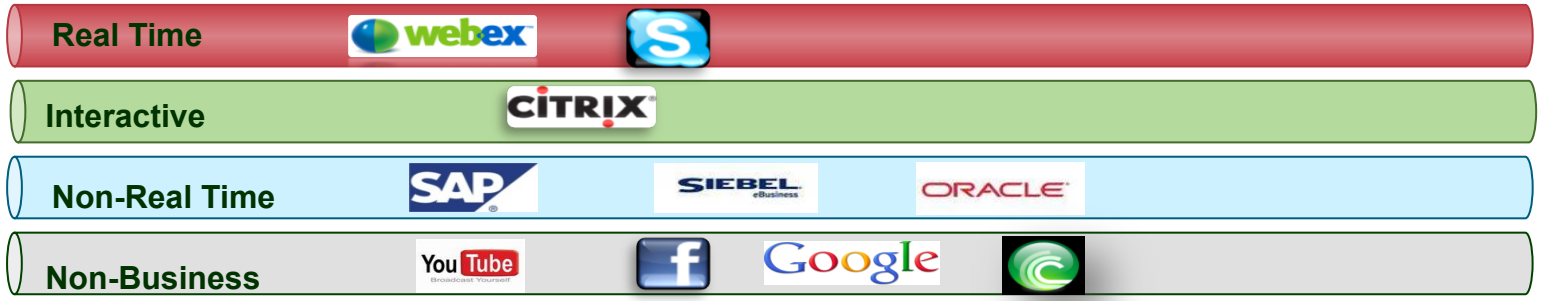
Control

Use QoS to control application bandwidth usage to improve application performance

© 2010 Cisco and/or its affiliates. All rights reserved.

AVC Use Cases

- More applications mixed on WLAN
- Bottleneck in the wireless spectrum
- Are dedicated Voice and Data WLAN still feasible ?

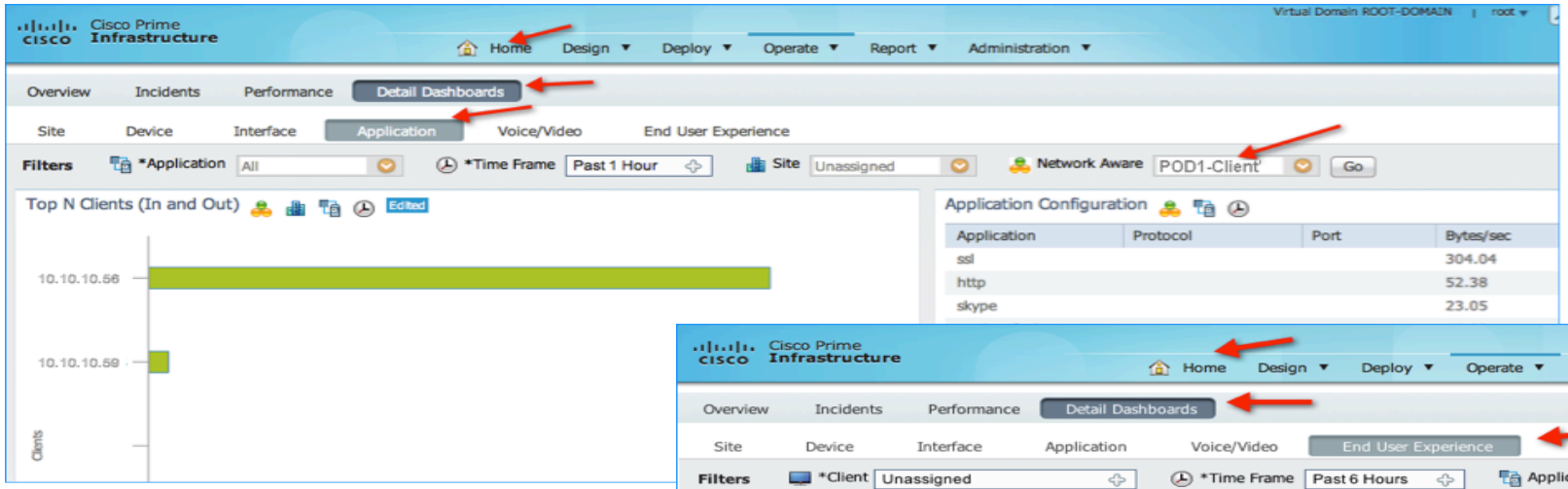


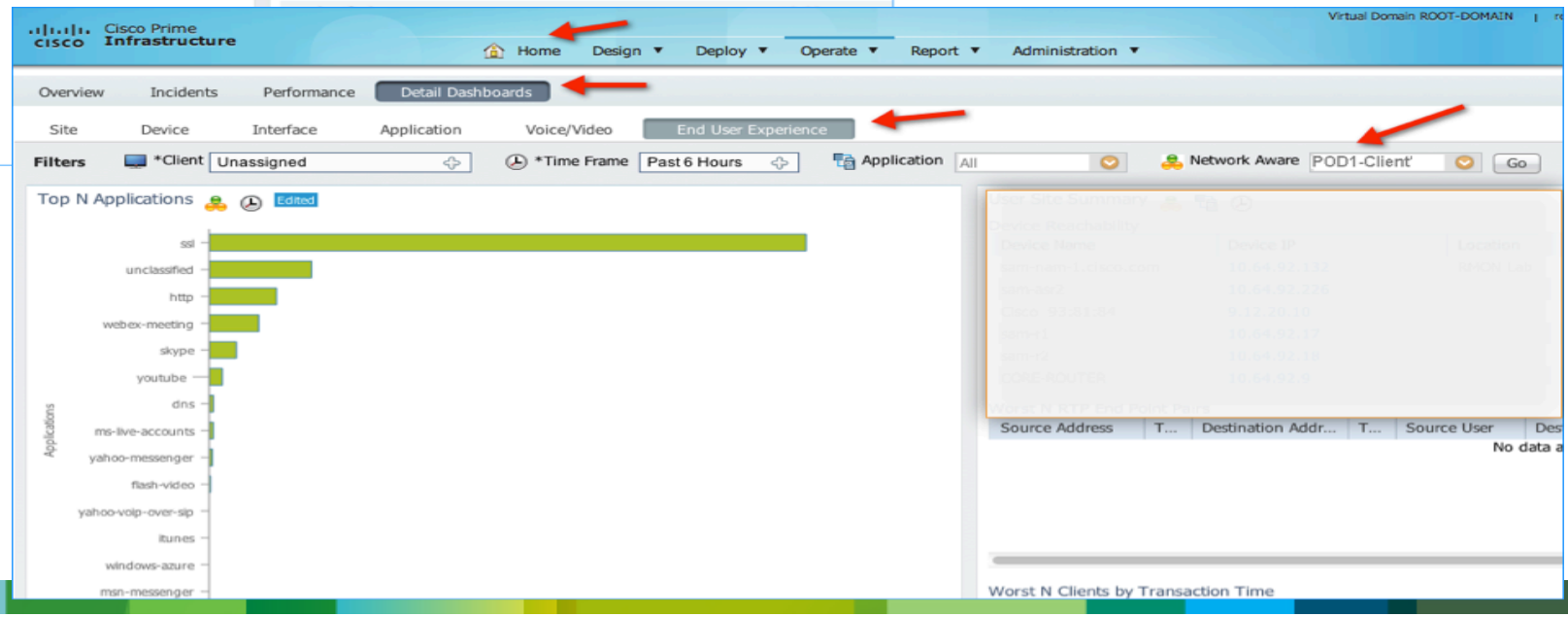
© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco PI 1.4 - AVC Monitoring

- AVC monitoring of Client and Application statistics

Note: PAM Assurance license is required on PI 2.0 for NetFlow Monitoring - available in bundle sizes of 15, 50, 100, 500, 1,000, and 5,000 NetFlow-enabled devices.





© 2010 Cisco and/or its affiliates. All rights reserved.

NBAR /AVC Summary

- NBAR on WLC can classify and take action on 1039 different applications.
- Two actions either DROP or MARK are possible on any classified application.
- Maximum 16 AVC profiles can be created on WLC.
- Each AVC profile can be configured with maximum 32 rules.
- Same AVC profile can be mapped to multiple WLANs. But one WLAN can have only one AVC profile.
- Only 1 NetFlow exporter and monitor can be configured on WLC.
- NBAR stats are displayed only for top 10 applications on GUI. CLI can be used to see all applications.
- If AVC profile mapped to WLAN has a rule for MARK action, that application will get precedence as per QOS profile configured in AVC rule overriding the QOS profile configured on WLAN.
- Any application, which is not supported/recognized by NBAR engine on WLC, is captured under bucket of UNCLASSFIED traffic.

© 2010 Cisco and/or its affiliates. All rights reserved.

AVC Protocol Pack

© 2010 Cisco and/or its affiliates. All rights reserved.

AVC Phase 2 – Protocol Pack support

- In Phase 2 of the AVC supports for a Protocol Pack has been added
- Major Protocol packs include support for new Protocols, updates and bug fixes
- Minor protocol packs typically do not include support for new protocols
- Protocol packs are targeted to a specific platform type and Version and released separately

Note 1: For AVC phase 2 the NBAR Protocol Packs are supported on 5500, 7500, 8500 and WiSM2 controllers on Local and Flex Mode APs (For WLANs configured for central switching only). 2500 series controllers do not support Protocol Packs, updates will be integrated.

Note 2: Protocol packs are software packages that allow updating the signature support without replacing the image on the Controller.

© 2010 Cisco and/or its affiliates. All rights reserved.

NBAR2 1000+ Application Recognition

Examples of apps recognized by NBAR2 as of XE 3.6S and 15.2(3)T

- List of protocols and applications supported by NBAR2 http://www.cisco.com/en/US/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html
- Protocol pack update starts 15.2(4)S and XE 3.7.0 S on CCO:

http://software.cisco.com/download/release.html?mdfid=282993672&flowid=20841&softwareid=284509011&release=4.0.0&relind=AVAILABLE&rellifecycle=&reltype=latest

© 2010 Cisco and/or its affiliates. All rights reserved.

Protocol Pack - Compatibility

- Protocol packs are released for specific NBAR engine versions
  - For example, rel 7.5 WLC has NBAR engine 13, so protocol packs for it are written for engine 13 (pp-adv-asr1k-152-4.S-**13**-3.0.0.pack)
- Loading a protocol pack can be done if the engine version on the platform is same or higher than the version required by the protocol pack (13 in the example above).
- Therefore:
  - PP 3.0 for version 13 can be loaded on top of version 13 or version 14
  - BUT PP 3.0 for version 14 could not be loaded in engine version 13
  - Loading the wrong version will generate an error
- It is strongly recommended to use the protocol pack that is the exact match for the engine

© 2010 Cisco and/or its affiliates. All rights reserved.

Loading Protocol Pack

- Loading a protocol pack is CLI command only (no GUI or PI/SNMP support)

```
(Cisco Controller) >transfer download datatype avc-protocol-pack
(Cisco Controller) >transfer download start
Mode.............................. FTP
Data Type......................... AVC Protocol Pack
FTP Server IP..................... A.B.C.D
FTP Server Port................... 21
FTP Path.......................... /
FTP Filename...................... pp-adv-asr1k-152-4.S-13-2.1.0.pack
FTP Username...................... cisco
FTP Password...................... *********
Starting tranfer of AVC Protocol Pack
This may take some time.
Are you sure you want to start? (y/N)
```

```
Transfer Canceled

(5508-60-Active) >transfer download datatype avc-protocol-pack

(5508-60-Active) >transfer download start

Mode.............................................. TFTP
Data Type......................................... AVC Protocol Pack
TFTP Server IP.................................... 10.70.0.59
TFTP Packet Timeout............................... 6
TFTP Max Retries.................................. 10
TFTP Path.....................................
TFTP Filename..................................... pp-adv-asr1k-152-4.S-13-4.0.0.
pack

Starting tranfer of AVC Protocol Pack

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

- Not supported on 2500 controllers due to memory limitations
- On 2500, the protocol pack is included in new code release, not between codes

© 2010 Cisco and/or its affiliates. All rights reserved.

Loading Protocol Pack

Use show command to view Protocol Pack before installation
(Cisco Controller) >**show avc engine version**

```
(5508-60-Active) >show avc engine version

 AVC Engine Version: 13

(5508-60-Active) >show avc protocol-pack version

 AVC Protocol Pack Name: Advanced Protocol Pack
 AVC Protocol Pack Version: 1.0

(5508-60-Active) >
```

Use show command to view Protocol Pack version after installation
(Cisco Controller) >**show avc protocol-pack version**

```
(5508-60-Active) >show avc protocol-pack version

 AVC Protocol Pack Name: Advanced Protocol Pack
 AVC Protocol Pack Version: 4.0

(5508-60-Active) >show avc engine version

 AVC Engine Version: 13

(5508-60-Active) >
```

© 2010 Cisco and/or its affiliates. All rights reserved.

Bonjour Phase-2

© 2010 Cisco and/or its affiliates. All rights reserved.

The Protocol Problem

- Why Bonjour services need modifications?

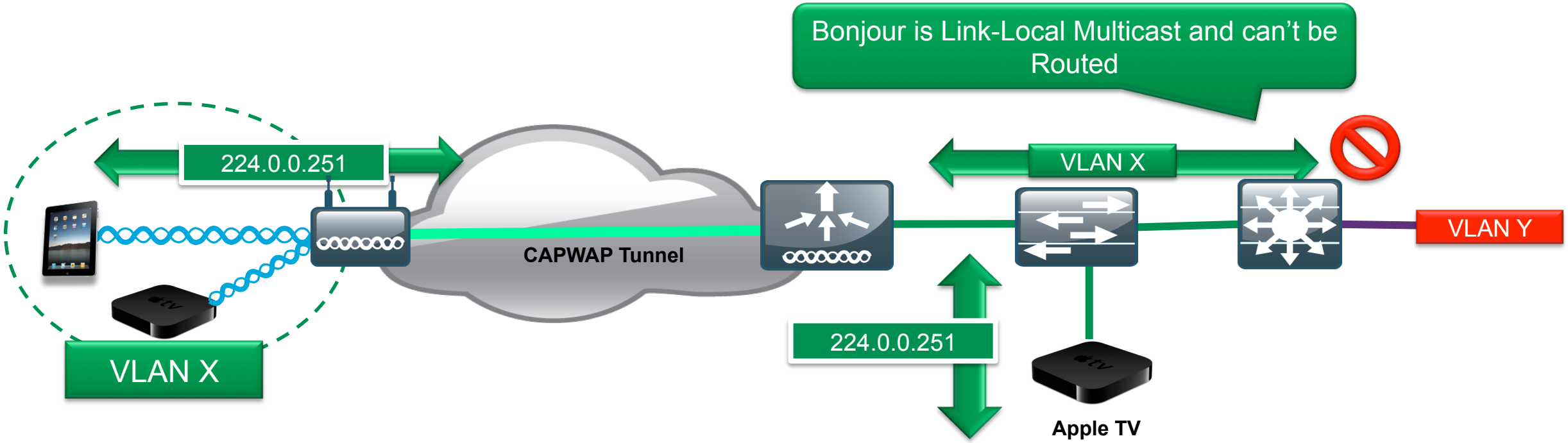
Bonjour

- Apple service discovery protocol
- mDNS packets advertise and discover services clients
- Does not cross subnets or VLANs.

Result: Clients can't see services on other subnets

© 2010 Cisco and/or its affiliates. All rights reserved.

Deployment Challenges



- Bonjour is link local multicast and thus forwarded on Local L2 domain
- AirPlay (Apple TV) and AirPrint supported only on a single VLAN
- mDNS operates at UDP port 5353 and sent to the reserved group addresses:
  - IPv4 Group Address – 224.0.0.251
  - IPv6 Group Address – FF02::FB

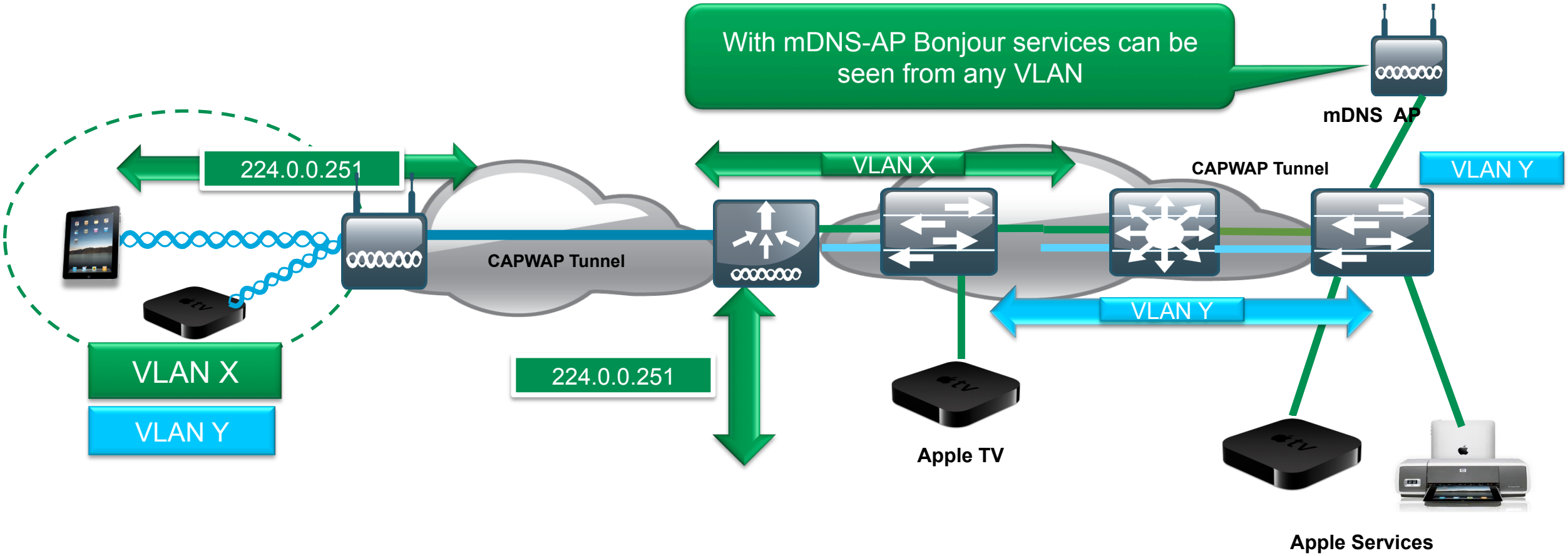
© 2010 Cisco and/or its affiliates. All rights reserved.

Bonjour Services Enhancements Phase 2

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

© 2010 Cisco and/or its affiliates. All rights reserved.

Deployment Changes with Bonjour Services Phase 2



- Bonjour is link local multicast and thus forwarded on Local L2 domain
- mDNS AP snoop Bonjour services behind the Router or not L2 adjacent VLANs and forwards them to WLC in CAPWAP tunnel.

© 2010 Cisco and/or its affiliates. All rights reserved.

Bonjour Phase 2 – mDNS AP

- Given that mDNS Bonjour is a L2 multicast protocol and cannot be routed makes it enterprise unfriendly
- In rel 7.5 any of the AP's associated with the WLC as "mDNS-AP" forwards the mDNS packets received at the AP from the switch
- This enhancement allows the controller to have the visibility of wired service providers, which are on VLANs that are not visible to the controller.
- VLAN visibility at the WLC is achieved by APs forwarding the mDNS advertisements to the controller.
- The mDNS packet between AP and controller will be forwarded in CAPWAP data tunnel similar to mDNS packets from wireless client. Both capwap v4 and v6 tunnels will be supported.
- APs can be either in access mode or trunk mode to learn the mDNS packets from wired side and forward to the controller.
- The maximum number of VLANs that AP can snoop is **10**.

© 2010 Cisco and/or its affiliates. All rights reserved.

Bonjour Phase 2 – mDNS AP

- This feature is supported on local and monitor mode AP, and not on FlexConnect Mode APs
- If a mDNS AP joins/resets (or) joins the same/another controller, the behavior is as follows :
  - If the global snooping is disabled on the controller , then a payload will be sent to AP to disable mDNS snooping.
  - If the global snooping is enabled on the controller, then the configuration of the AP previous to reset/ join procedure will be retained.

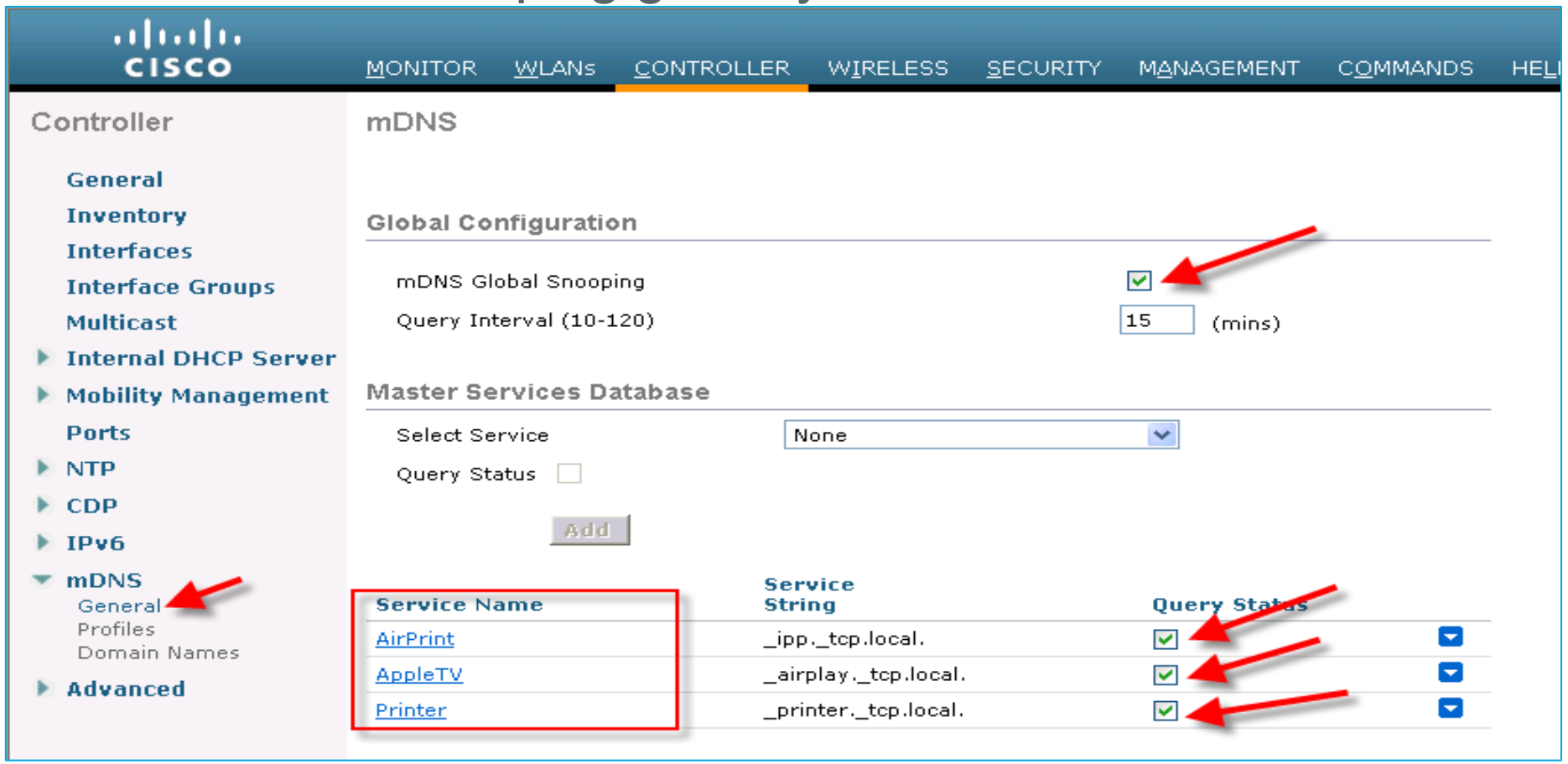
NOTE:

- **Disabling global snooping on WLC will disable the mDNS AP snooping as well; mDNS AP will retain configuration**
- **mDNS AP will not forward advertisements if it joins another controller with Global snooping disabled**
- **Configuring same VLANs on multiple mDNS APs can cause flapping, no two mDNS-AP's can duplicate advertisements of the same VLAN.**

© 2010 Cisco and/or its affiliates. All rights reserved.

Configuring mDNS Snooping

Enable mDNS snooping globally and add services

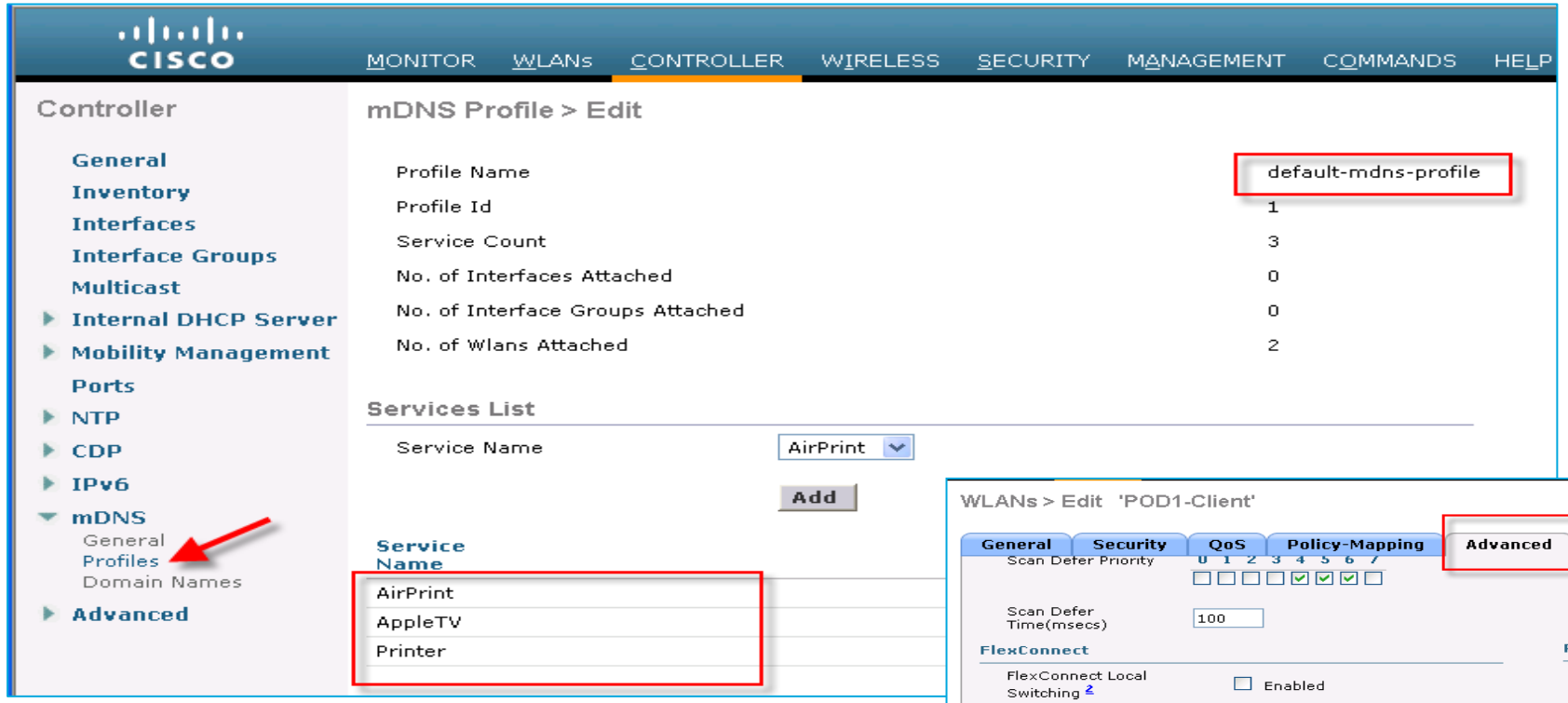


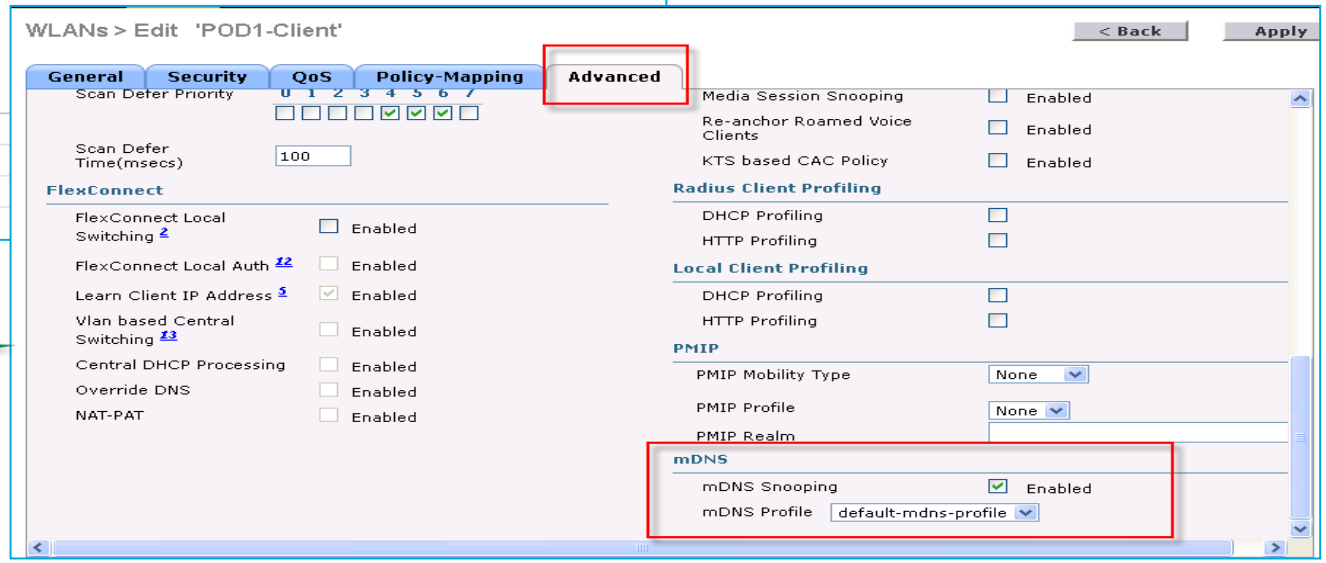
Maximum of 6400 on 5508 or WiSM-2 and 16000 on 7500/8500 services can be configured *

© 2010 Cisco and/or its affiliates. All rights reserved.

Configure mDNS profile per WLAN

Create custom profile per WLAN





Enable mDNS snooping profile on the desired VLAN or WLAN

© 2010 Cisco and/or its affiliates. All rights reserved.

Configure mDNS- AP from CLI ONLY

1. Configure switch port for mDNS-AP in trunk mode or Access Mode

```
interface GigabitEthernet1/0/17
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 70
 switchport trunk allowed vlan 70,71
 switchport mode trunk
```

2. Configure mDNS-AP **Trunk Mode** or **Access Mode**:

(WLC)> config mdns ap enable/disable <APName/all> vlan <vlan-id>

(WLC) >show mdns ap summary

(WLC) >config mdns ap vlan add/delete <vlanid> <AP Name>

(WLC)> config mdns ap enable/disable <APName/all> - no VLAN Config in Access Mode

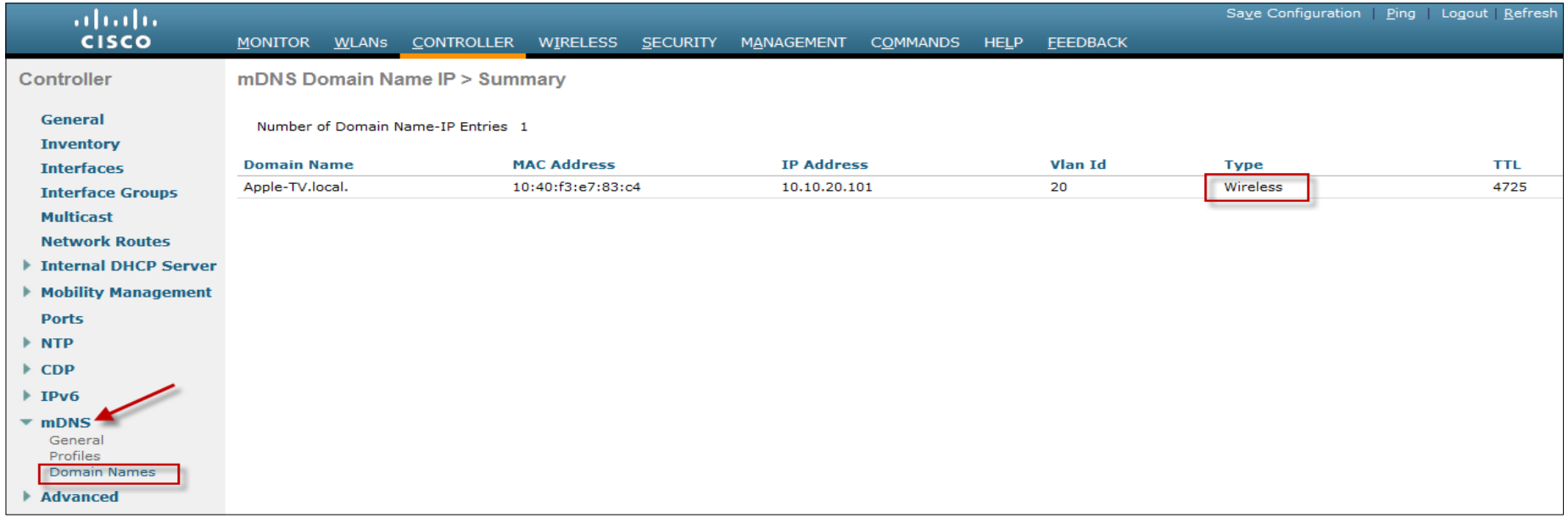
```
(Cisco Controller) >config mdns ap enable AP6073.5caa.030b vlan 71

 Requested state is already set on the AP.

(Cisco Controller) >show mdns ap summary

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

   AP Name              Ethernet MAC       Number of Vlans     VlanIdentifiers
------------------   --------------------  -----------------  ---------------------
AP6073.5caa.030b      60:73:5c:aa:03:0b          1                70
```

```
(Cisco Controller) >config mdns ap vlan add 71 AP6073.5caa.030b

(Cisco Controller) >show mdns ap summary

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

   AP Name              Ethernet MAC       Number of Vlans     VlanIdentifiers
------------------   --------------------  -----------------  ------------------
-----------
AP6073.5caa.030b      60:73:5c:aa:03:0b          2                70,71
```

© 2010 Cisco and/or its affiliates. All rights reserved.

Summary of Bonjour enabled devices

Bonjour enabled devices advertising service is shown as Domain Name



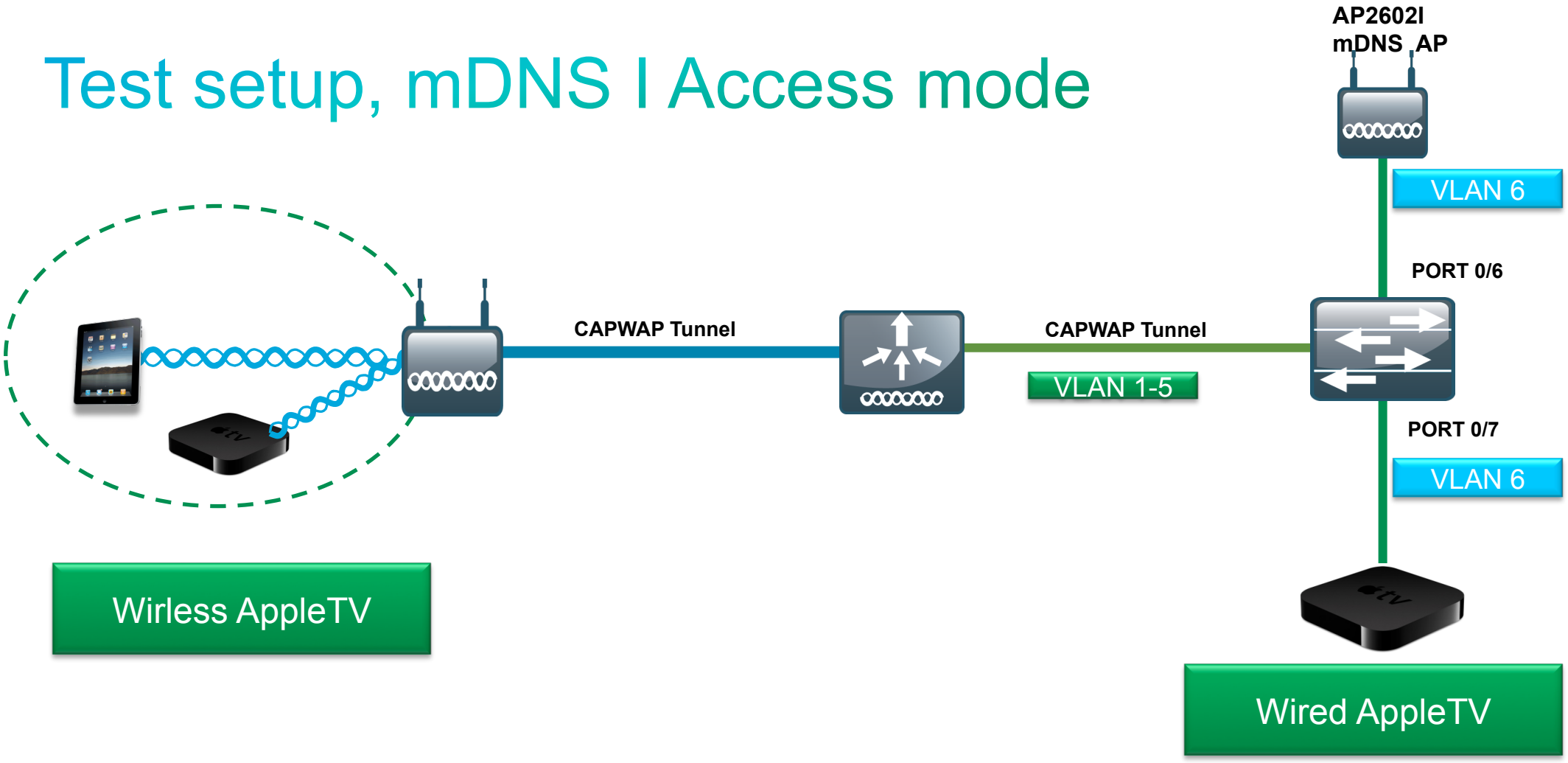
mDNS enabled AP

© 2010 Cisco and/or its affiliates. All rights reserved.

mDNS AP Demo

© 2010 Cisco and/or its affiliates. All rights reserved.

Test setup, mDNS I Access mode



© 2010 Cisco and/or its affiliates. All rights reserved.

Test setup, mDNS I Access mode

- Switch config

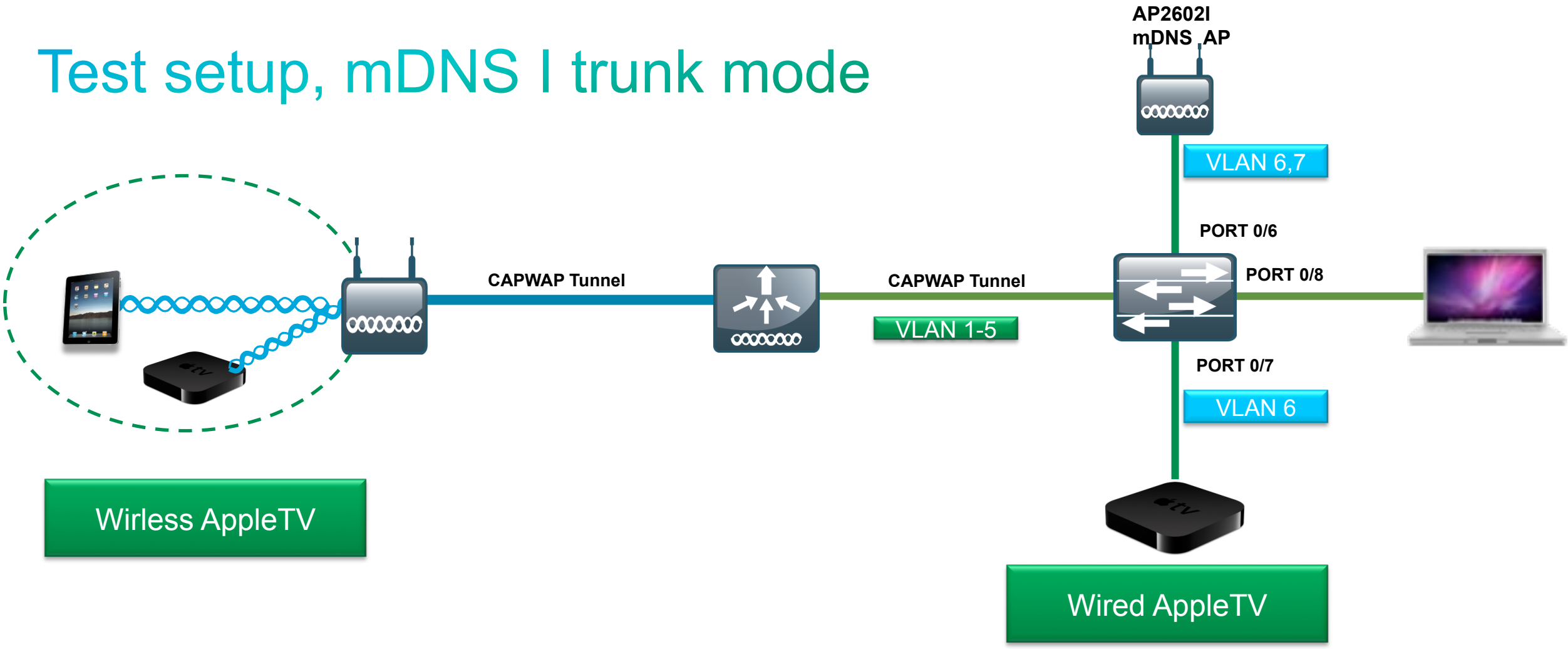
- Int GI0/6
- Switchport mode access
- Switchport access vlan 6

- AP Config

- Config mdns ap enable AP2602I vlan 6

© 2010 Cisco and/or its affiliates. All rights reserved.

Test setup, mDNS I trunk mode



© 2010 Cisco and/or its affiliates. All rights reserved.

Test setup, mDNS I trunk mode

- Switch config

- Int GI0/6
- Switchport trunk encapsulation dot1q
- Switchport trunk native vlan 6
- Switchport trunk allowed vlan 6,7
- Switchpoty mode trunk

- AP Config

- Config mdns ap enable AP2602I vlan 6
- Config mdns ap vlan add 7 AP2602I

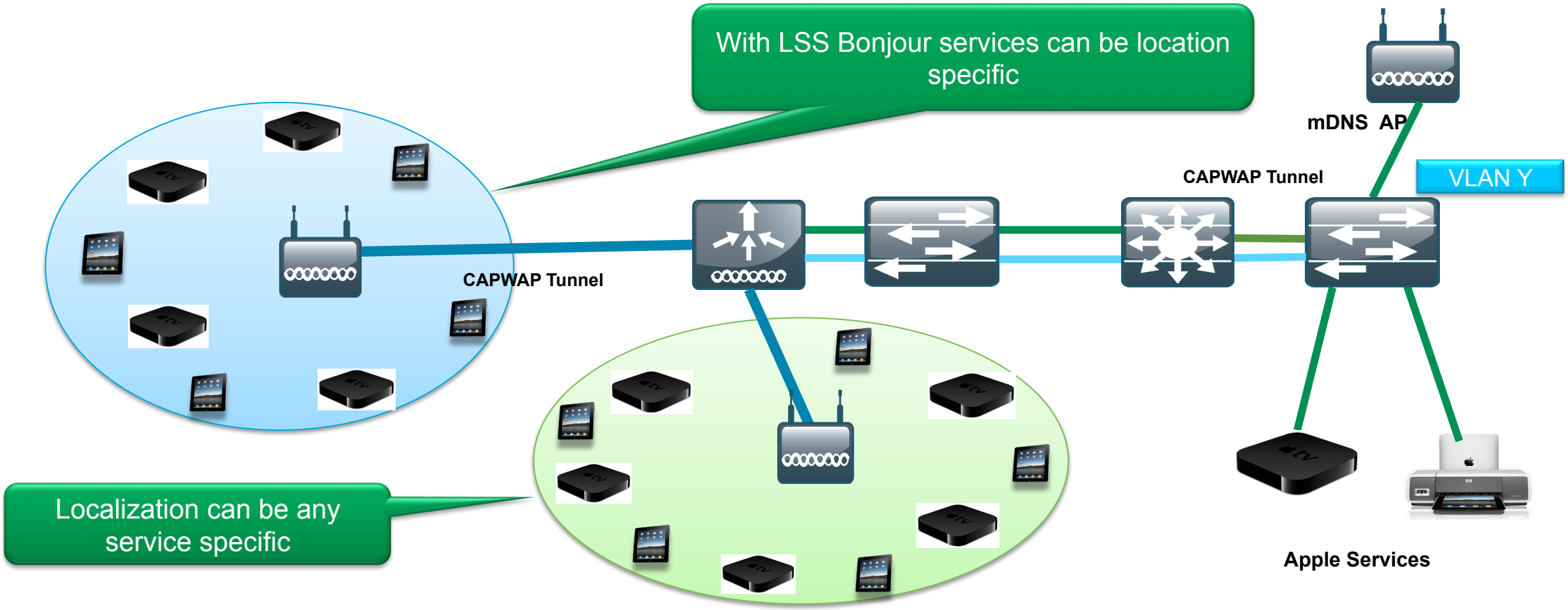
© 2010 Cisco and/or its affiliates. All rights reserved.

Bonjour Services Enhancements Phase 2

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

© 2010 Cisco and/or its affiliates. All rights reserved.

Deployment Changes with LSS



- WLC responds with the sub-set of SP-DB for the service being queried subject to the client profile
- Wireless SP-DB entries are filtered based on the AP-NEIGHBOR-LIST if LSS is enabled for the service

© 2010 Cisco and/or its affiliates. All rights reserved.

Bonjour Phase 2 – Location Specific Service

- Prior to rel 7.5 WLC responds with the complete SP-DB for the service being queried subject to the client profile – which could be overwhelming
- With LSS all valid wireless only mDNS service advertisements received at the WLC will be tagged with the MAC address of the AP associated with the service
- In 7.5 rel wireless entries are filtered in the SP list based on the querying client location using the RRM database and respond sent with a subset of the SP-DB
- Querying-client's AP base radio MAC address is used to query the RRM-DB to get the AP-NEIGHBOR-LIST.
- Wireless SP-DB entries are filtered based on the AP-NEIGHBOR-LIST if LSS is enabled for the service.
- If LSS is disabled for any service then the wireless SP-DB entries will not be filtered while responding to any query from a wireless client for the said service.
- Wired SP-DB entries are never filtered.
- LSS status cannot be enabled for services with ORIGIN set to WIRED and vice-versa.

© 2010 Cisco and/or its affiliates. All rights reserved.

Configure LSS services from CLI

1. Once the basic bonjour gateway setup is configured the LSS can be enabled by accessing the WLC CLI, LSS is disabled by default on the WLC

```
(Cisco Controller) >show mdns service summary
Number of Services.............................. 7

Service-Name                     LSS    Origin      No SP    Service-string
-------------------------------- ----   ----------  -----    ---------------
AirPrint                         No     All           1      _ipp._tcp.local.
AirTunes                         No     All           2      _raop._tcp.local.
AppleTV                          No     All           2      _airplay._tcp.local.
HP_Photosmart_Printer_1          No     All           0      _universal._sub._ipp._tcp.local.
HP_Photosmart_Printer_2          No     All           1      _cups._sub._ipp._tcp.local.
Printer                          No     All           0      _printer._tcp.local.
Scanner                          No     All           0      _scanner._tcp.local.
```

2. Configure LSS services from CLI:

(WLC) >config mdns service lss <enable / disable> <service_name/all>

```
(Cisco Controller) >config mdns service lss enable all

(Cisco Controller) >show mdns service summary
Number of Services.............................. 7

Service-Name                     LSS    Origin      No SP    Service-string
-------------------------------- ----   ----------  -----    ---------------
AirPrint                         Yes    All           1      _ipp._tcp.local.
AirTunes                         Yes    All           2      _raop._tcp.local.
AppleTV                          Yes    All           2      _airplay._tcp.local.
HP_Photosmart_Printer_1          Yes    All           0      _universal._sub._ipp._tcp.local.
HP_Photosmart_Printer_2          Yes    All           1      _cups._sub._ipp._tcp.local.
Printer                          Yes    All           0      _printer._tcp.local.
Scanner                          Yes    All           0      _scanner._tcp.local.
```

© 2010 Cisco and/or its affiliates. All rights reserved.

Bonjour Services Enhancements Phase 2

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

© 2010 Cisco and/or its affiliates. All rights reserved.

Bonjour Phase 2 – Priority MAC

- Prior to rel 7.5 we had a limitation of 100 service providers per 64 service types and this was insufficient for some services
- In rel 7.5 implementation this restriction is removed and there is only a global service-provider limit per platform i.e.**6400** on WLC 2500/5500/WiSM-2 and **16000** on WLC7500/8500.
- In addition there is provision to configure up to **50 MAC** addresses per service and these mac addresses are the SP MACs that need priority
- Priority MAC guarantees that any service advertisements originating from these MACs for the configured services will be learnt even if the SP-DB is full
- Priority MAC configured with an optional parameter “ap-group” which only applies to wired Service Providers to associate a sense of location to the wired SP devices
  - Priority MAC configured with “ap-group” places that wired SP higher in the order than the other wired devices
  - Wired SP with “ap-group” matching the client’s “ap-group” are higher up in order. Meaning the client will see wired devices nearby first.
  - Please note only the order is changing and not the contents for the wired SP.

© 2010 Cisco and/or its affiliates. All rights reserved.

Configure Priority MAC services from CLI

Once the basic bonjour gateway setup is configured Priority MAC can be enabled by accessing the WLC CLI

1. Command **"show mdns service detailed <service_name>"** will show the priority MAC addresses configured for the service.

```
(Cisco Controller) >show mdns service detailed AppleTV

Service Name.................................... AppleTV
Service Id...................................... 3
Service query status............................ Enabled
Service LSS status.............................. Enabled
Service learn origin............................ Wireless and Wired
Number of Profiles.............................. 1
Profile......................................... default-mdns-profile

Number of Service Providers ..................... 2
Number of priority MAC addresses ................ 0
ServiceProvider                                MAC Address       AP Radio MAC          Vlan Id    Type       TTL      Time left
                                                                                                             (sec)     (sec)
--------------------                           ----------------  ----------------      -------    ------     -----    ---------

ADLER-DELL4500._airplay._tcp.local.            00:26:b9:cb:ee:f2        ------             0       Wired       4500      3911

Office Apple TV._airplay._tcp.local.           70:56:81:db:cd:a0  20:3a:07:49:03:20      0       mDNS AP     4500      3911
```

2. Configure Priority MAC from CLI:

(WLC) >config mdns service priority-mac <add /delete> <mac address> <service_name> [ap-group <group-name]

```
Number of Service Providers ..................... 2
Number of priority MAC addresses ................ 1
        Sl.No        MAC Address                  AP group name
        -----    -------------------    ---------------------------------
                                                                  1          70:56:81:db:cd:a0        -----
```

© 2010 Cisco and/or its affiliates. All rights reserved.

Bonjour Services Enhancements Phase 2

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

© 2010 Cisco and/or its affiliates. All rights reserved.

Bonjour Phase 2 – Origin Based Services

- Prior to rel 7.5 once a service is configured it learnt from wired / wireless and there is no option to restrict the learning to wired only or wireless only or all
- In 7.5 rel the origin of the Bonjour service can be configured for **wired/wireless/ all**
- The origin is set to “All” by default for all the services
- All services seen at the controller and not learnt will be added to the bonjour browser

Note: 1. All services learnt from mDNS AP are treated as wired and similarly for guest also they are treated as wired
2. When the learn origin is WIRED then LSS cannot be enabled for the service, since LSS only applies to wireless services

© 2010 Cisco and/or its affiliates. All rights reserved.

Configure Origin Based services from CLI

1. Once the basic bonjour gateway setup is configured Origin Based Services are enabled by default

```
(Cisco Controller) >show mdns service summary
Number of Services.............................. 7

Service-Name                     LSS    Origin      No SP     Service-string
-------------------------------- ----   ----------  -----     ---------------
AirPrint                         No     All           1       _ipp._tcp.local.
AirTunes                         No     All           2       _raop._tcp.local.
AppleTV                          No     All           2       _airplay._tcp.local.
HP_Photosmart_Printer_1          No     All           0       _universal._sub._ipp._tcp.local.
HP_Photosmart_Printer_2          No     All           1       _cups._sub._ipp._tcp.local.
Printer                          No     All           0       _printer._tcp.local.
Scanner                          No     All           0       _scanner._tcp.local.
```

2. Configure Origin Based Service from CLI:

(WLC) >config mdns service origin <wired/wireless/all <service_name/all>

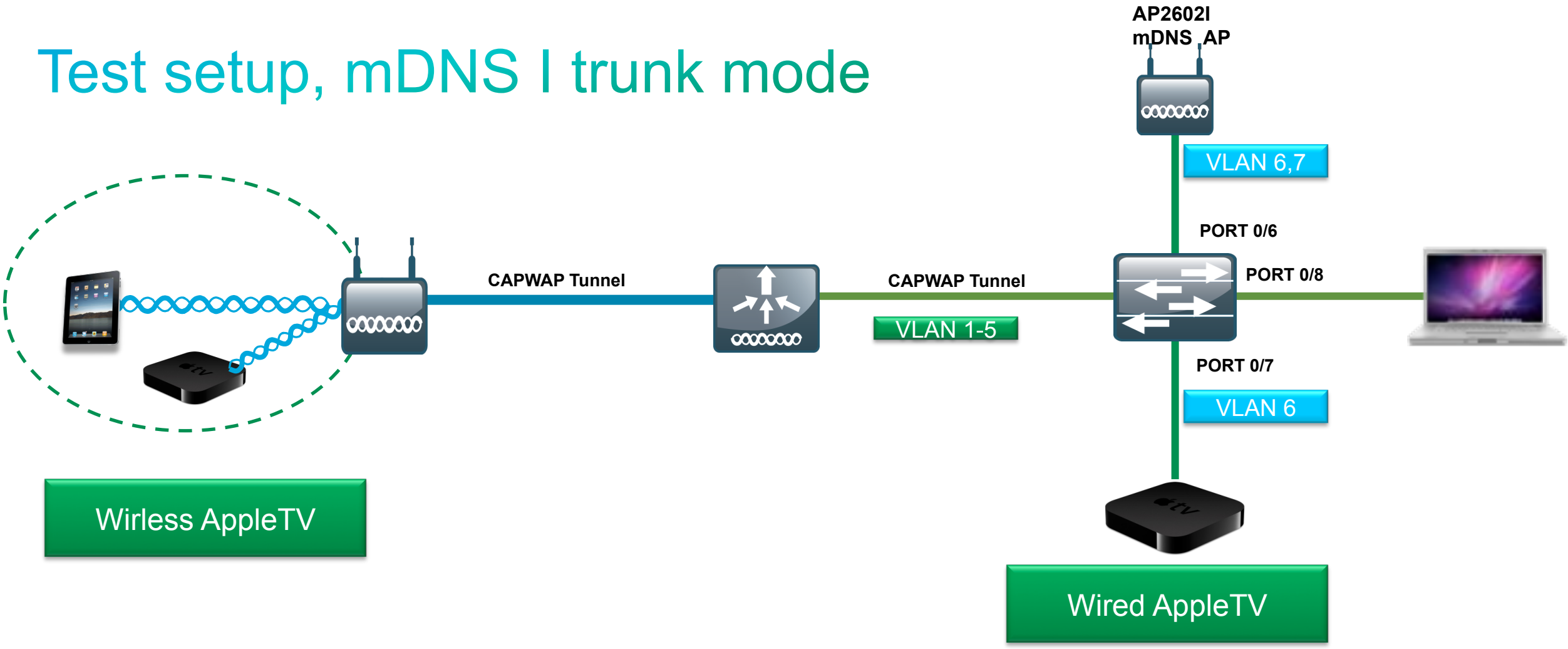
```
(Cisco Controller) >config mdns service origin wireless AppleTV

(Cisco Controller) >show mdns service summary
Number of Services.............................. 7

Service-Name                     LSS    Origin      No SP     Service-string
-------------------------------- ----   ----------  -----     ---------------
AirPrint                         Yes    All           1       _ipp._tcp.local.
AirTunes                         Yes    All           2       _raop._tcp.local.
AppleTV                          Yes    Wireless      0       _airplay._tcp.local.
HP_Photosmart_Printer_1          Yes    All           0       _universal._sub._ipp._tcp.local.
HP_Photosmart_Printer_2          Yes    All           1       _cups._sub._ipp._tcp.local.
Printer                          Yes    All           0       _printer._tcp.local.
Scanner                          Yes    All           0       _scanner._tcp.local.
```

© 2010 Cisco and/or its affiliates. All rights reserved.

mDNS AP Demo

© 2010 Cisco and/or its affiliates. All rights reserved.

Test setup, mDNS I trunk mode



© 2010 Cisco and/or its affiliates. All rights reserved.

Test setup, disable Apple Lært via wireless

- AP Config

- Config mdns service origin wired AppleTV

- Kun AppleTVs som er lært fra den kablede net læres
- Se dette under controller – mdns – general – appletv

- Se på controller at wireless AppleTV ikke læres:

  Show mdns servcies not-learnt

© 2010 Cisco and/or its affiliates. All rights reserved.

FlexConnect Group specific WLAN-VLAN mapping

© 2010 Cisco and/or its affiliates. All rights reserved.

FlexConnect Group specific WLAN-VLAN Mapping

- WLAN Specific WLAN-VLAN Mapping
- **FlexConnect Group Specific WLAN-VLAN Mapping** 7.5
- AP Specific WLAN-VLAN Mapping

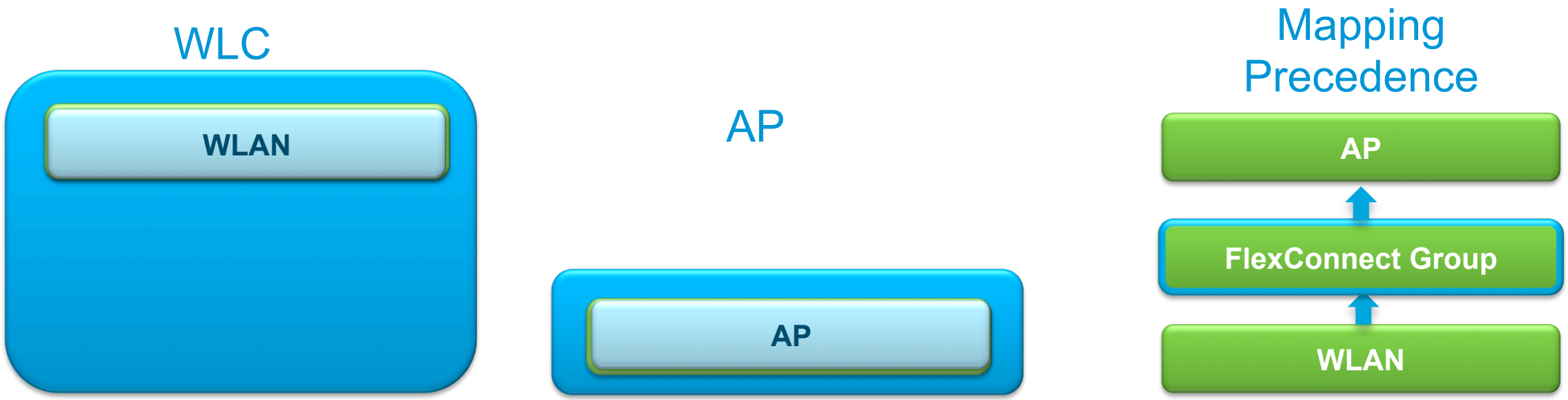
- Mapping at FlexConnect Group pushed to all APs in the Group.
  - ✓ The WLAN should be locally switched
  - ✓ WLAN should be broadcasted on the FlexConnect AP.

© 2010 Cisco and/or its affiliates. All rights reserved.

FlexConnect Group specific WLAN-VLAN Mapping

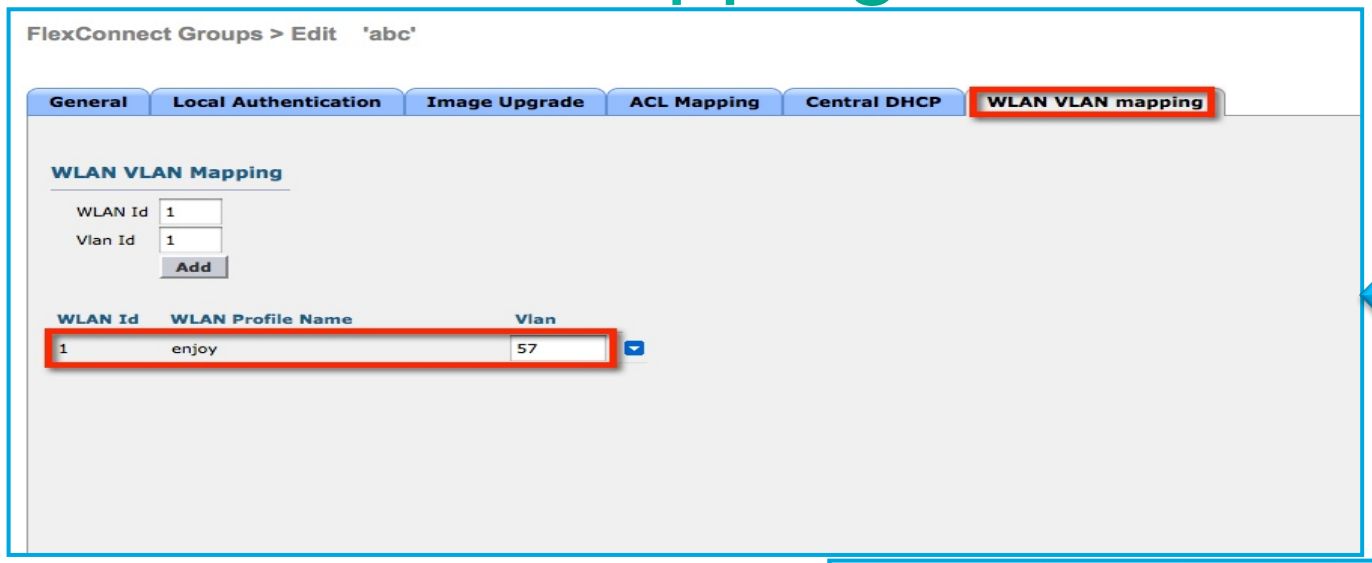
WLAN-VLAN Mapping Precedence:

- WLAN level WLAN-VLAN mapping has the lowest precedence.
- Higher precedence mapping will override the mapping of lower precedence.
- AP level WLAN-VLAN mapping has the highest precedence.
- On deletion of a mapping. the next highest precedence mapping will take effect.



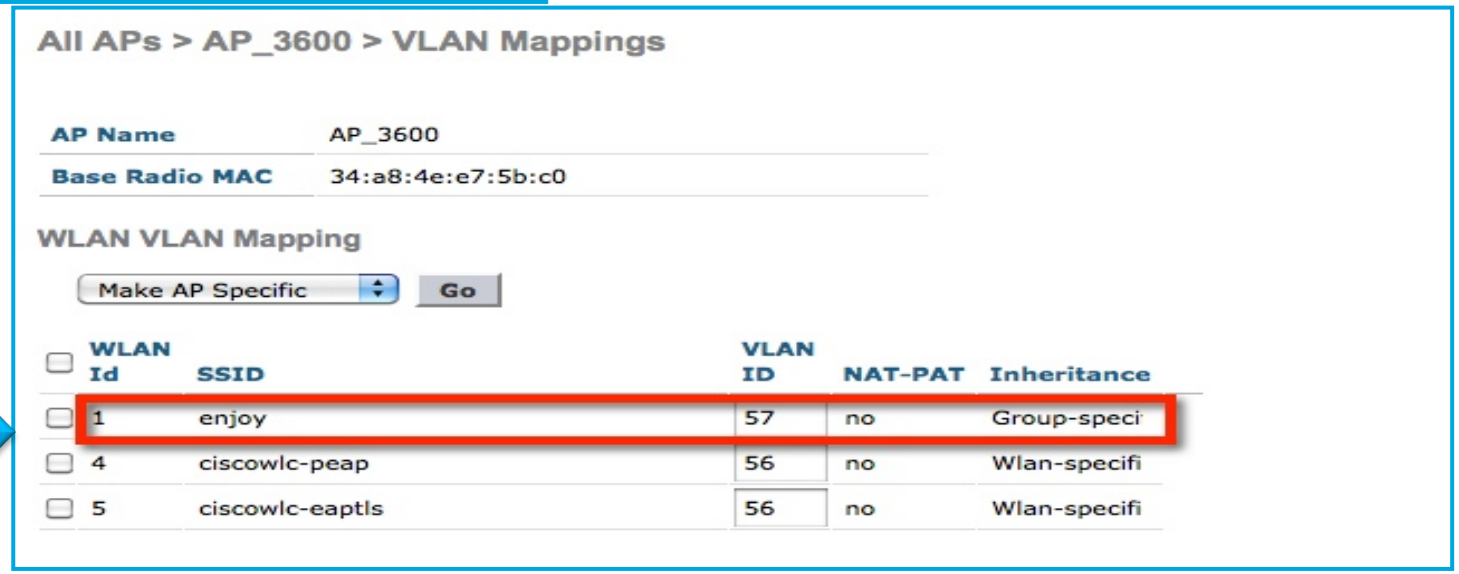
© 2010 Cisco and/or its affiliates. All rights reserved.

WLAN-VLAN Mapping Web-GUI



FlexConnect Group specific WLAN-VLAN Mapping

VLAN Mappings at AP



© 2010 Cisco and/or its affiliates. All rights reserved.

WLC Internal Policy Classification Engine

© 2010 Cisco and/or its affiliates. All rights reserved.

Client Profiling

- ISE offers a rich set of BYOD features: e.g. device identification, onboarding, posture and policy
- Customers who do not deploy ISE but still require some of ISE features directly in WLC:
  - Native profiling of identifying network end devices based on protocols like HTTP, DHCP
  - Device-based policies enforcement per user or per device policy on the network.
  - Statistics based on per user or per device end points and policies applicable per device.

© 2010 Cisco and/or its affiliates. All rights reserved.

Client Profiling

- WLC-based local policy consists of 2 separate elements.

  Profiling can be based on:

  - *Role* - defining user type or the user group the user belongs to.
  - *Device type* – e.g. Windows, OS_X, iPad, iPhone, Android, etc.
  - *EAP Type* - check what EAP method the client is getting connected to.

  Action is policy that can be enforced after profiling:

  - *VLAN* - override WLAN interface with VLAN id on WLC
  - *QoS level* – override WLAN QoS
  - *ACL* – override with named ACL
  - *Session timeout* – override WLAN session timeout value
  - *Time of day* – policy override based on time of the day, else default to WLAN.

© 2010 Cisco and/or its affiliates. All rights reserved.

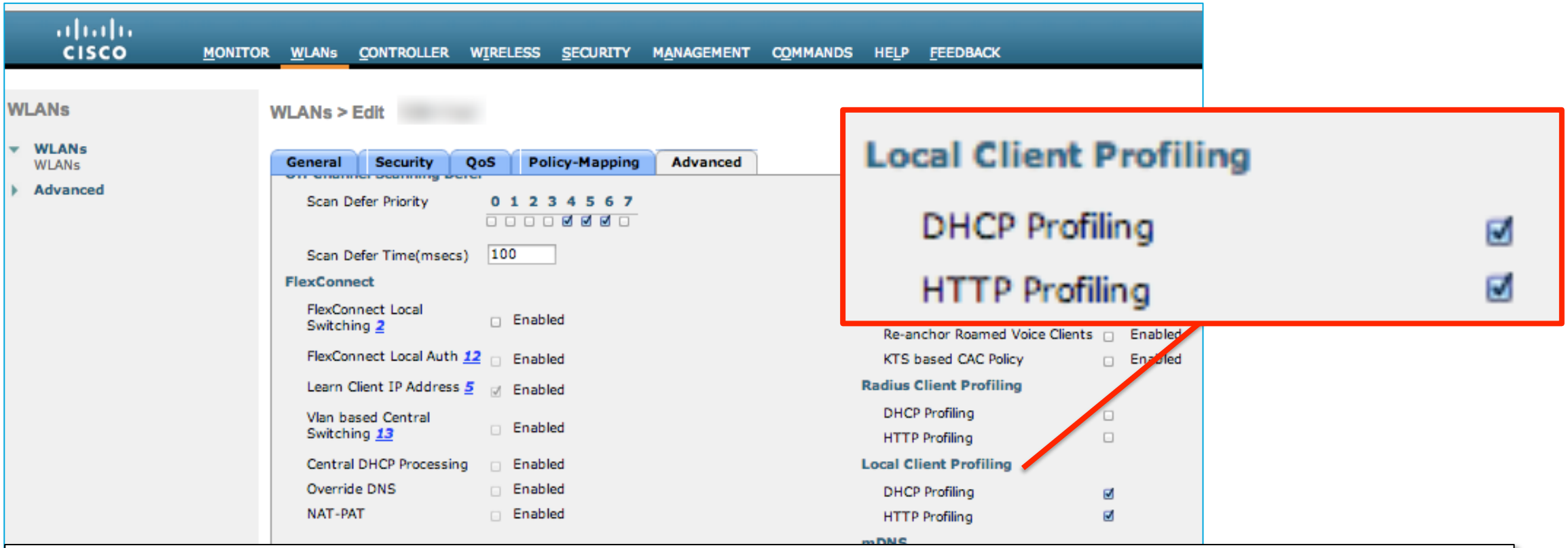
Configuring Client Profiles

- Client profiling uses pre-existing profiles in the controller
  - Custom profiles are not supported in this release
- Wireless clients are profiled based on the MAC OUI, DHCP,HTTP user agent
  - DHCP is required for DHCP profiling, Webauth for HTTP user agent
- 7.5 release contains 88 pre-existing profiles:

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

Number of Builtin Classification Profiles: 88
ID   Name                                       Parent Min CM Valid
==== ========================================== ====== ====== =====
   0 Android                                                None     30    Yes
    1 Apple-Device                                           None     10    Yes
    2 Apple-MacBook                                             1     20    Yes
    3 Apple-iPad                                                1     20    Yes
    4 Apple-iPhone                                              1     20    Yes
    …/…
```

Local Client Profiling Configuration

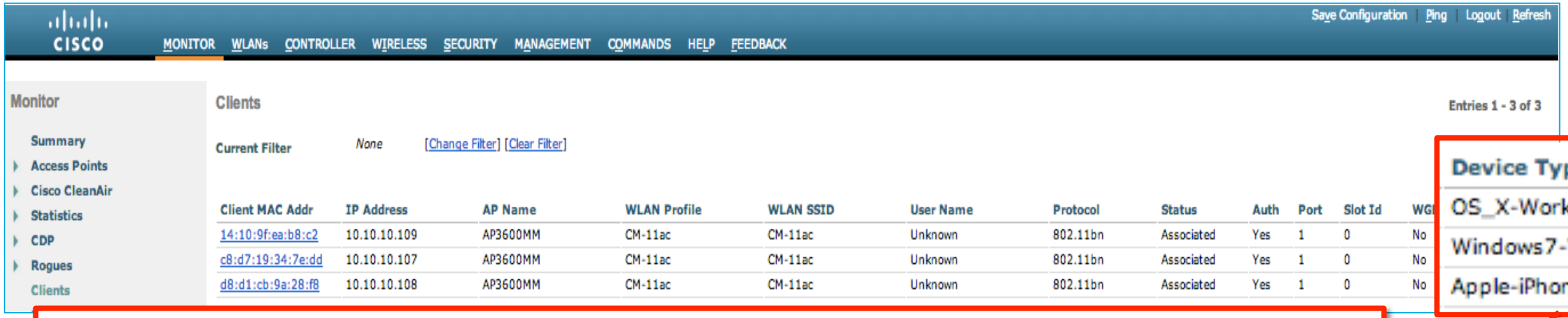
- At the WLAN level, enable Local Client Profiling (DHCP and HTTP)
  - DHCP required is checked automatically when selecting DHCP profiling




```
config wlan profiling {local | radius} {dhcp | http | all} <wlan ID>
(Cisco Controller) >config wlan profiling local all enable 1
```

Client Profiles

- When profiling is enabled, a client Device Type can be shown on WLAN.

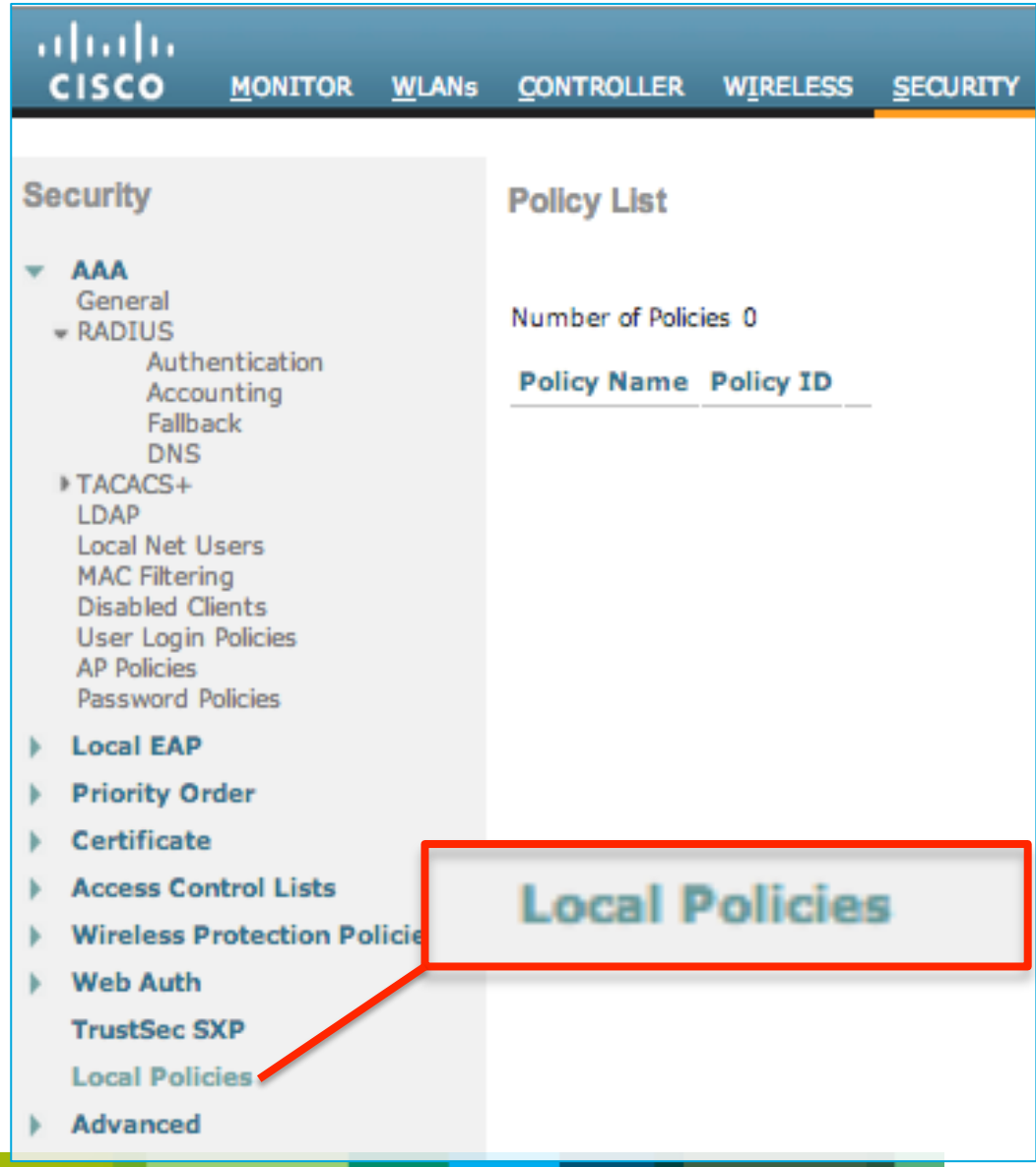



```
(Cisco Controller) >show client summary devicetype

Number of Clients.............................. 3

MAC Address       AP Name          Status        Device Type
----------------- ---------------- ------------- --------------------------------

14:10:9f:ea:b8:c2 AP3600MM           Associated    OS_X-Workstation
c8:d7:19:34:7e:dd AP3600MM           Associated    Windows7-Workstation
d8:d1:cb:9a:28:f8 AP3600MM           Associated    Apple-iPhone
```

© 2010 Cisco and/or its affiliates. All rights reserved.

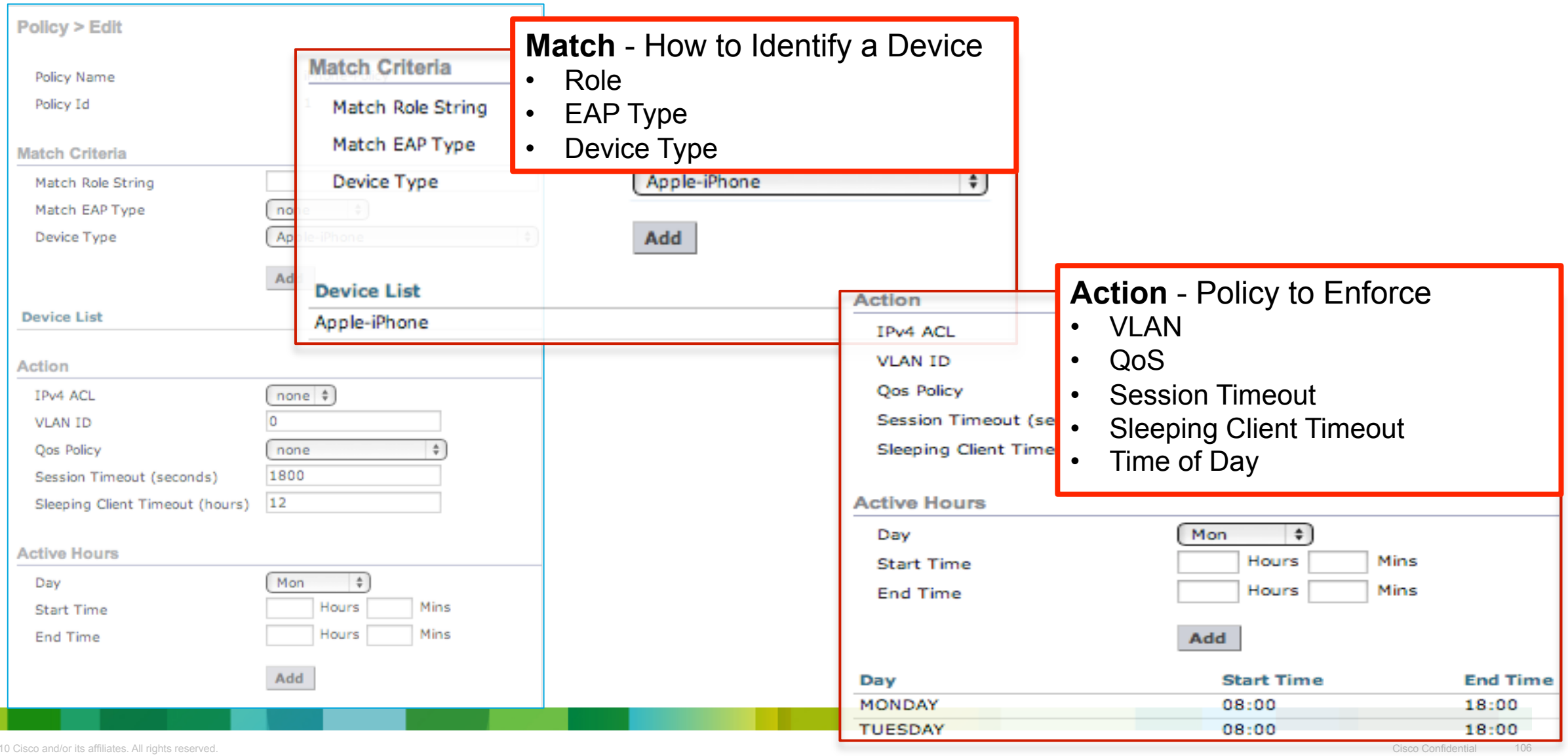
Security Local Policies

- When profiling is enabled, a client Device Type can be shown on WLAN.
- Up to 64 policies per WLC
- Can be applied to WLAN or AP Group
- Multiple matching criteria per policy; any match will trigger policy
- Policy action overrides WLAN setting; use WLAN default if action attribute is not defined



© 2010 Cisco and/or its affiliates. All rights reserved.

Security Local Policies



Match - How to Identify a Device

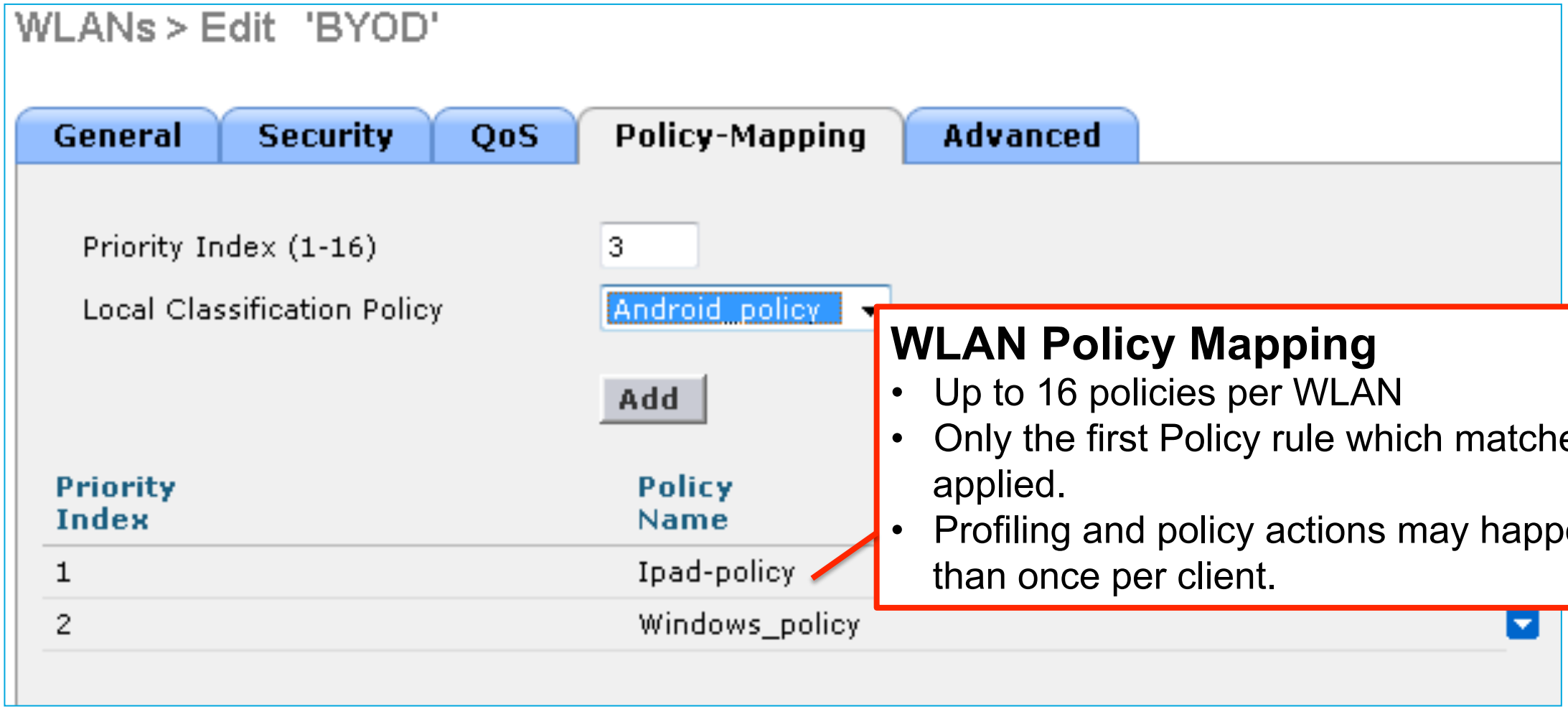
- Role
- EAP Type
- Device Type

Action - Policy to Enforce

- VLAN
- QoS
- Session Timeout
- Sleeping Client Timeout
- Time of Day

© 2010 Cisco and/or its affiliates. All rights reserved.

Configure Policies on WLAN



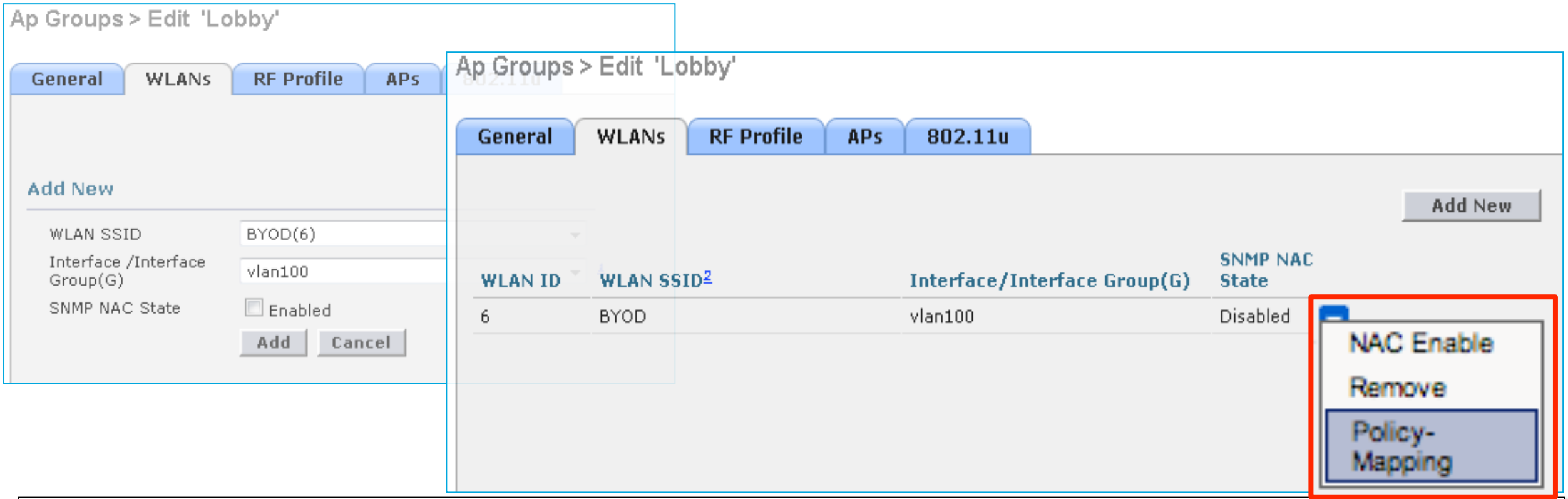
WLAN Policy Mapping

- Up to 16 policies per WLAN
- Only the first Policy rule which matches is applied.
- Profiling and policy actions may happen more than once per client.

© 2010 Cisco and/or its affiliates. All rights reserved.

Applying Policies to an AP Group

- Apply the policies based on user location using AP-groups.
  - -The AP group policy overrides the general WLAN policies

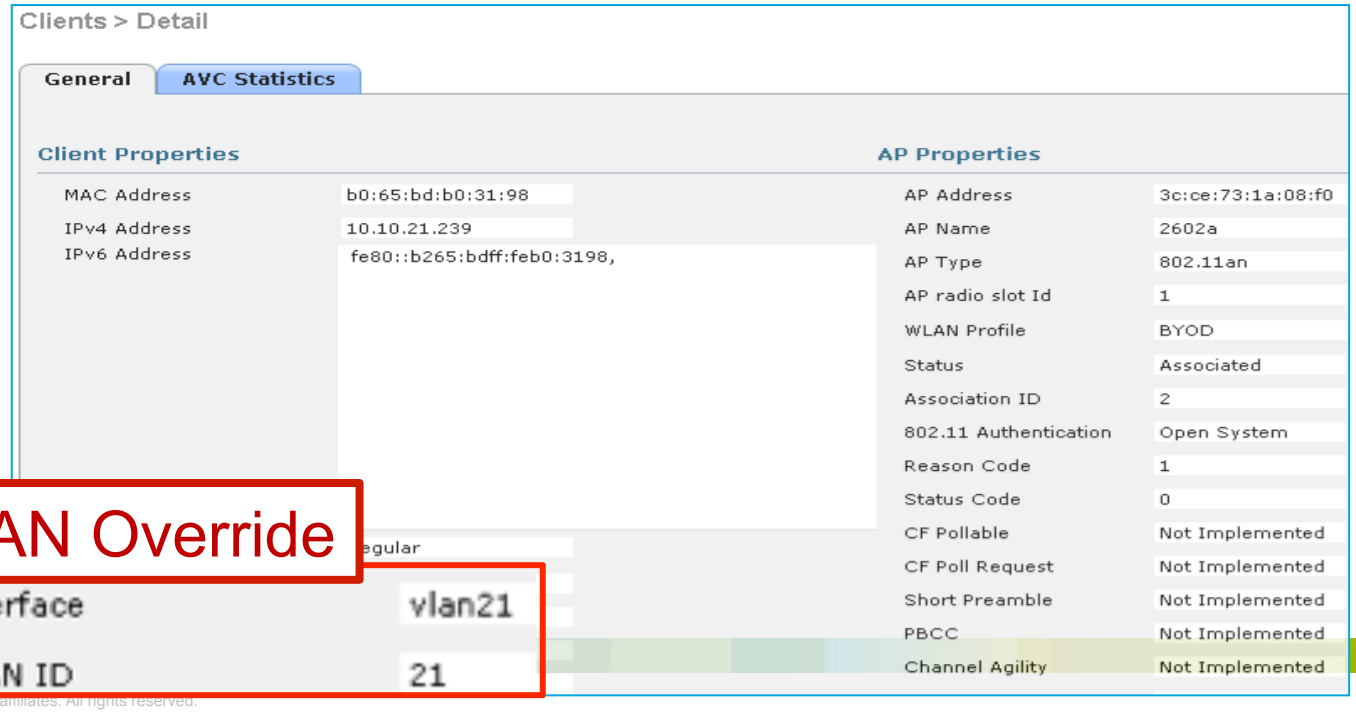


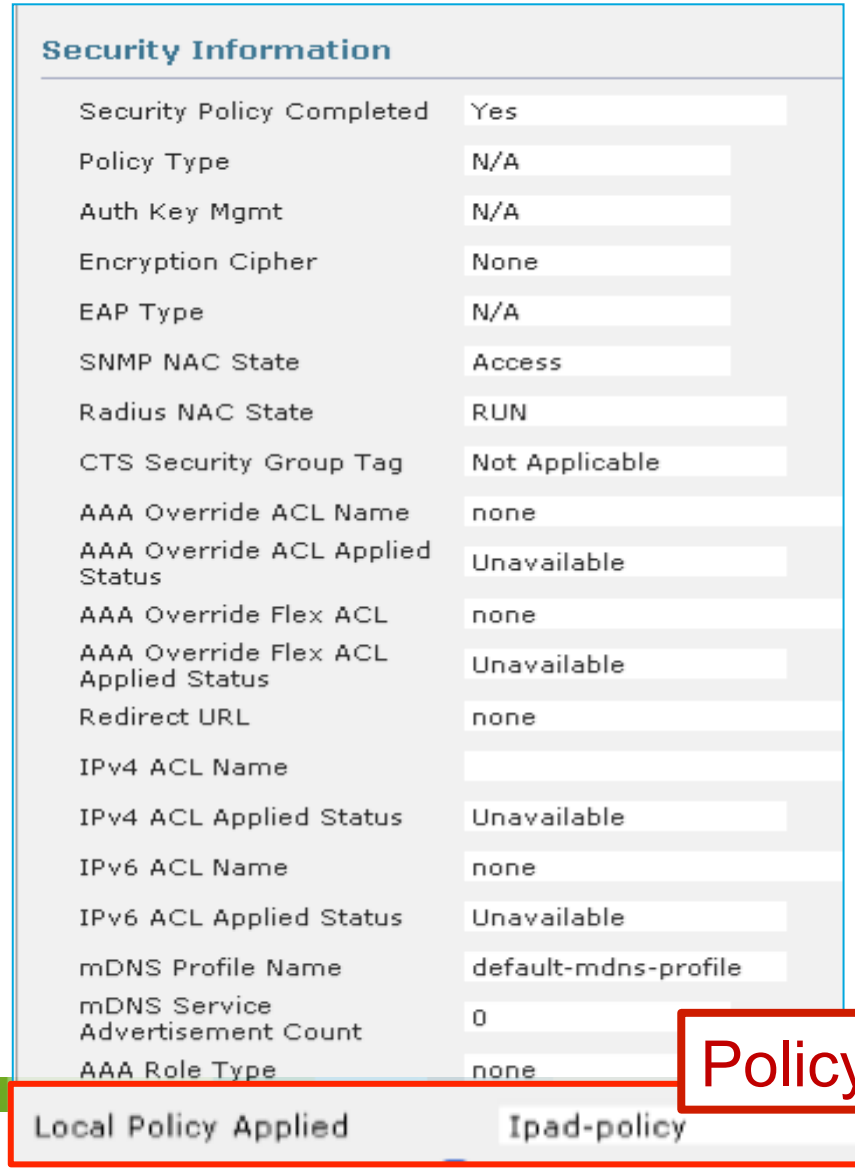

```
(Cisco Controller) >config wlan apgroup policy {add | delete} <priority index> <policy name>
<ap group name> <WLAN ID>
```

© 2010 Cisco and/or its affiliates. All rights reserved.

Verifying Local Profiling and Policy Enforcement

- Once clients associate, you can verify the policies
- Policy action will be done after:
  - L2 authentication
  - L3 authentication
  - When device sends http traffic and gets the device profiled.





© 2010 Cisco and/or its affiliates. All rights reserved.

Limitations

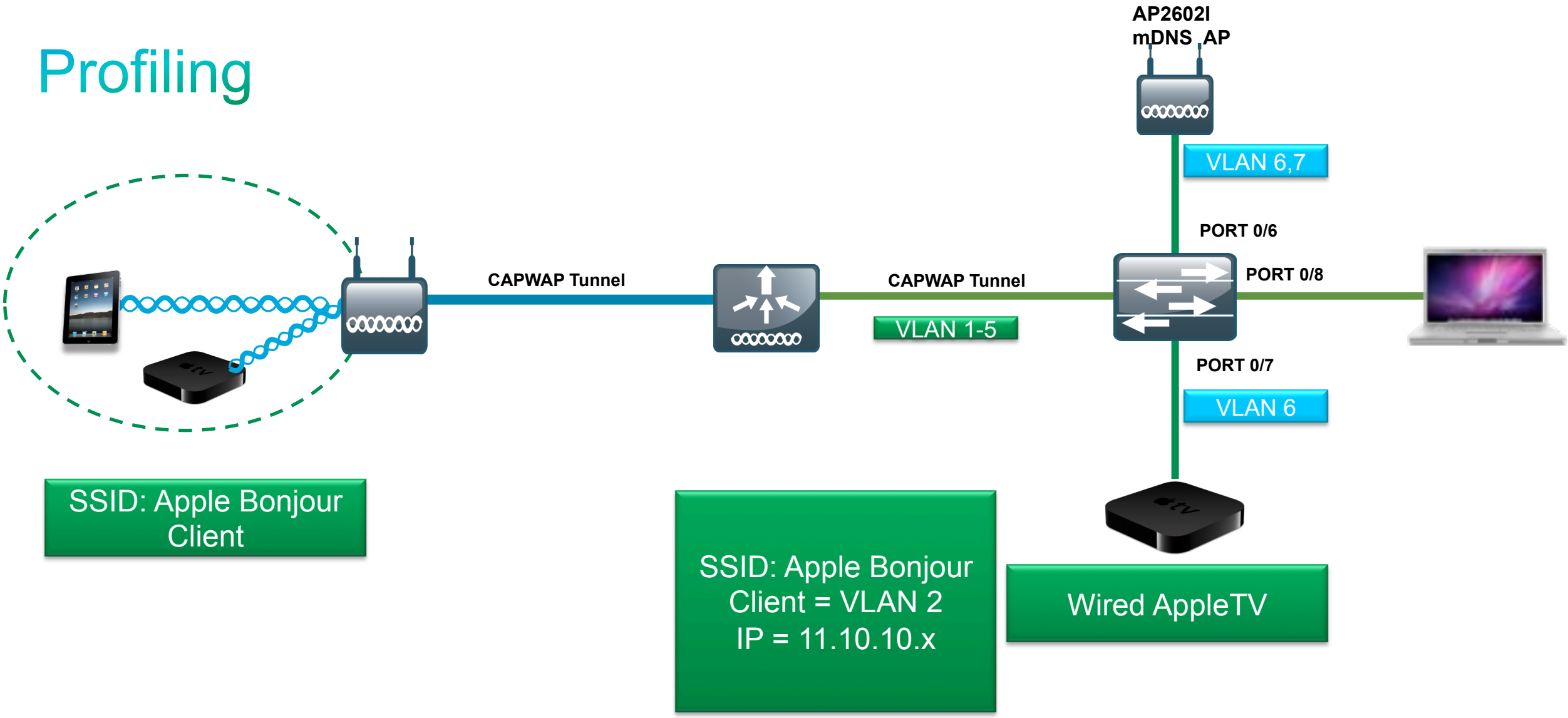
- When local profiling is enabled radius profiling is not allowed.
- If AAA override is enabled, the AAA override attributes will have higher precedence.
- Wired clients behind the WGB won't be profiled and policy action will not be done.
- Only the first Policy rule which matches is applied,
- Up to 16 policies per WLAN can be configured and globally 64 policies will be allowed.
- Policy action will be done after any of the following:
  - L2 authentication is complete
  - L3 authentication
  - When device sends http traffic and gets the device profiled: profiling and policy actions may happen more than once per client.

© 2010 Cisco and/or its affiliates. All rights reserved.

Proffiling demo

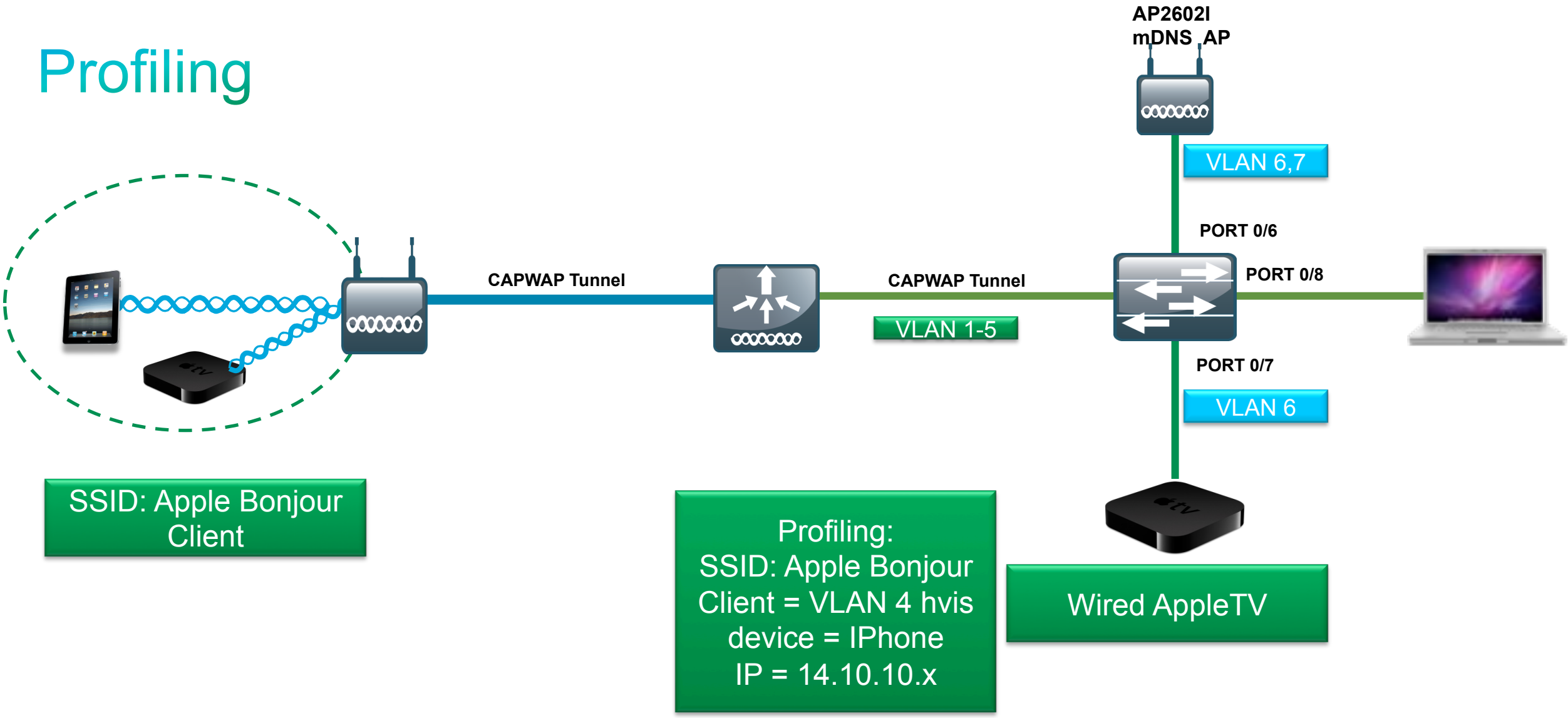
© 2010 Cisco and/or its affiliates. All rights reserved.

Profiling



© 2010 Cisco and/or its affiliates. All rights reserved.

Profiling



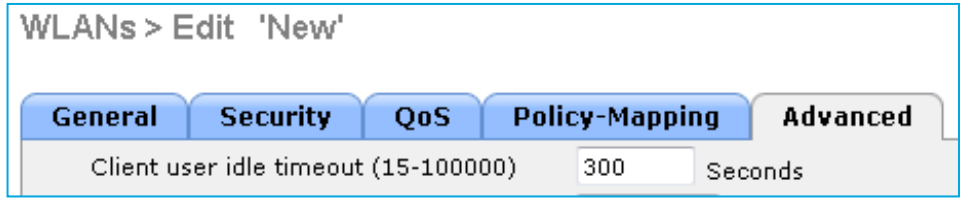
© 2010 Cisco and/or its affiliates. All rights reserved.

Guest Access Enhancements
Sleeping Client

© 2010 Cisco and/or its affiliates. All rights reserved.

Sleeping Client Enhancement

- Up to 7.4, client device connected to the WLC on web-auth enabled WLANs has to enter login credentials every time the client goes to sleep and wakes up.
- With 7.5, client entry is cached for a configurable duration (up to 30 days / 720 hours)
  - Sleeping interval is configured on a per WLAN basis
  - When exceeding the user-idle timeout, client database entry is moved to a cache section of the db, for the duration of the cache duration

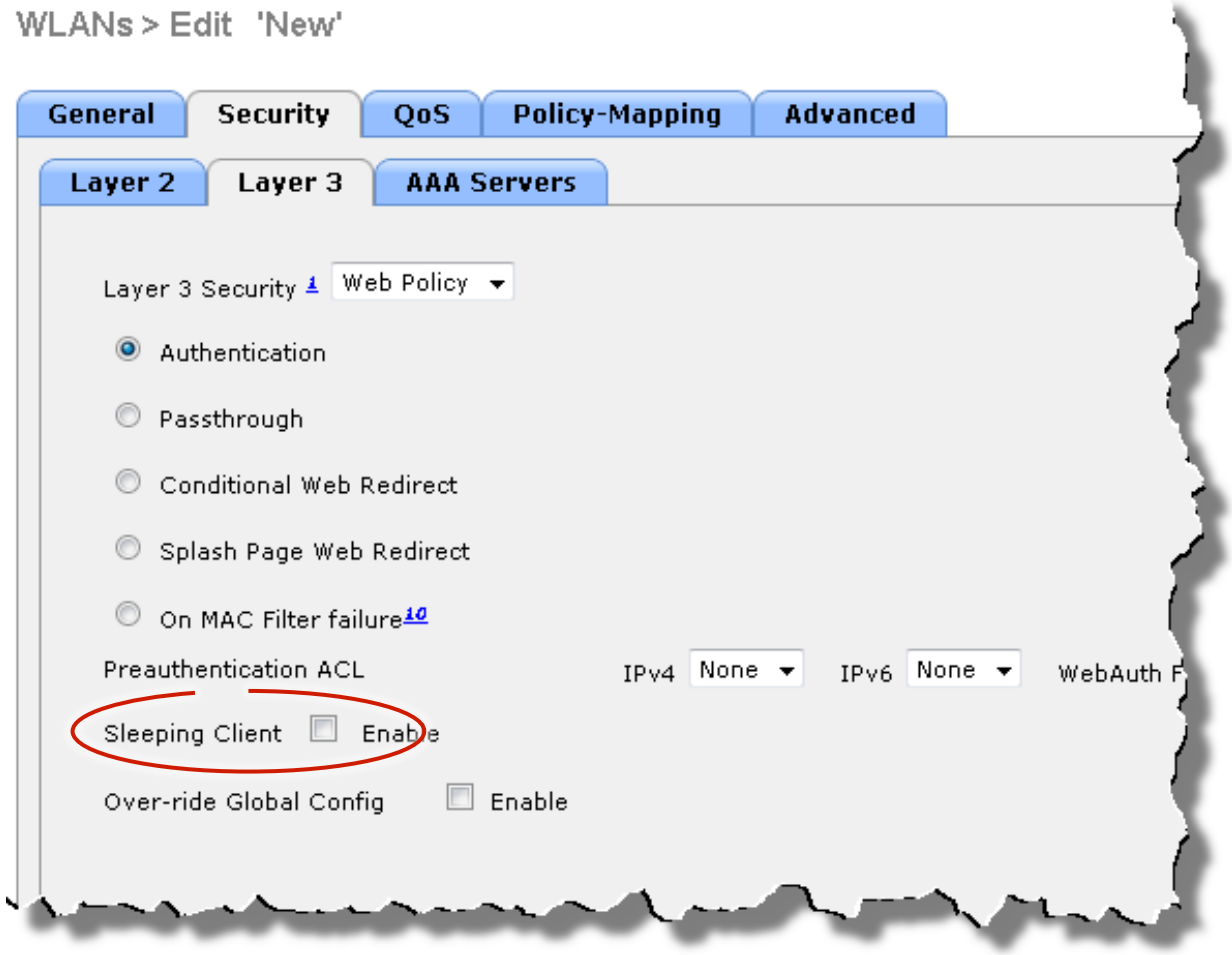


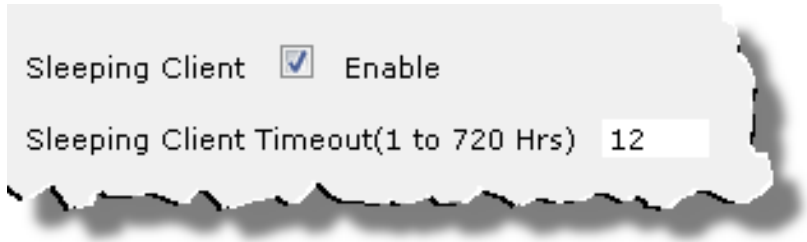
- Client waking up is remembered and does not need to re-enter credentials
- Cached information is passed as client roams: client does not need to re-enter credentials even when waking up in another AP cell (same WLAN, same mobility group)

© 2010 Cisco and/or its affiliates. All rights reserved.

Sleeping Client Configuration

- Configured from the Layer 3 Security section of the WLAN



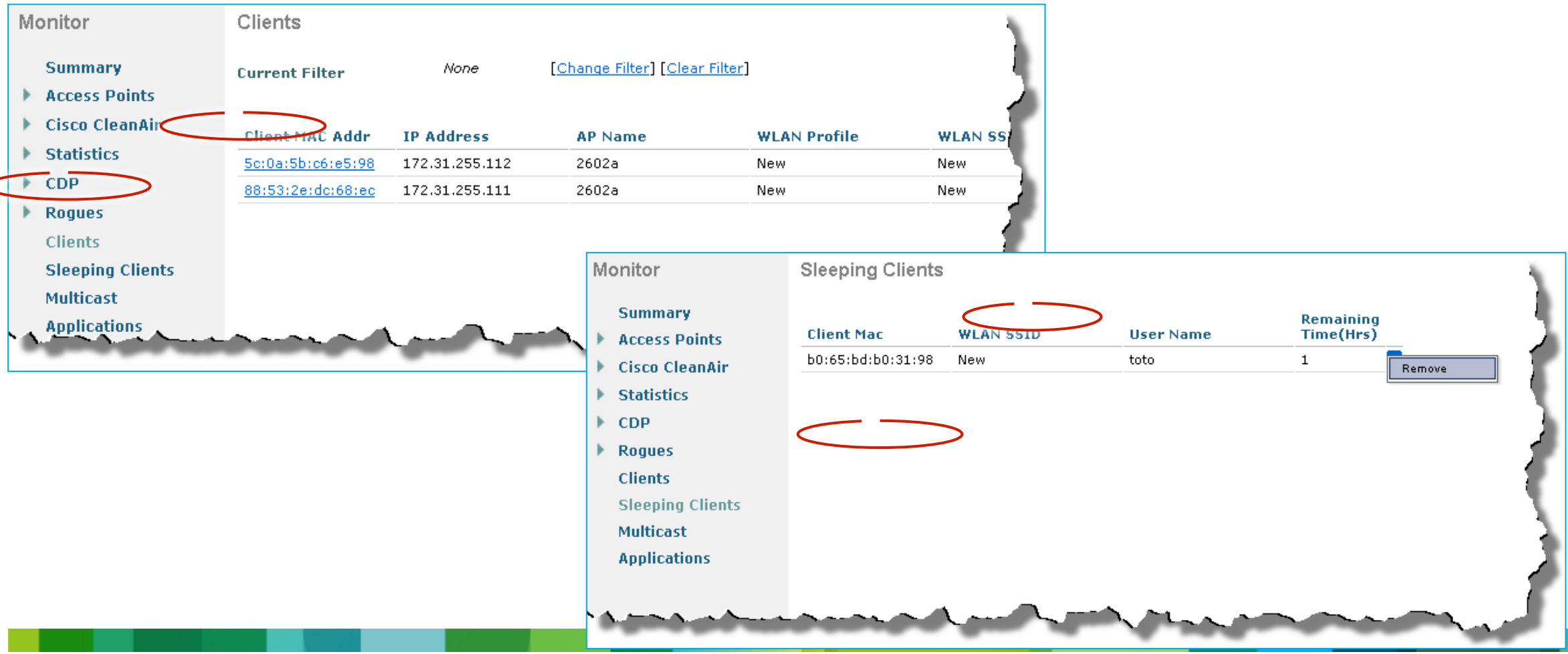


Configuring the timeout also enables the feature on the WLAN

© 2010 Cisco and/or its affiliates. All rights reserved.

Sleeping Client Verification

- Same information is visible in GUI:



© 2010 Cisco and/or its affiliates. All rights reserved.

Sleeping Client Limitations

- Supported only for L3 security enabled WLANs like **Webauth**, **Webpassthrough** and **Webauth on macfilter failure** and **Webauth on L2 security**

  Range 1hour to 30 days.

- Mobility scenarios supported for old/flat mobility
- No support for New mobility architecture
- Flex Support: supported for all FlexConnect scenarios (central switching, Local Switching internal webauth and Local Switching external webauth)
- HA Impact: client entry is synced between active and backup, but not sleeping timer: if active fails, client may have to re-enter credentials while re-joining the backup

© 2010 Cisco and/or its affiliates. All rights reserved.

7.5 Virtual Wireless LAN Controller

© 2010 Cisco and/or its affiliates. All rights reserved.

Virtual WLC 7.5 Release

- Data DTLS for Virtual controller supporting OEAP based solutions.
- Rate limiting support parity with other controllers.

© 2010 Cisco and/or its affiliates. All rights reserved.

Data DTLS

- CAPWAP Control is encrypted by default
- CAPWAP Data is encapsulated but not encrypted by default
- Option to encrypt data traffic for specific APs has been introduced since 7.0MR1
- 7.5 adds support for DTLS Data encryption between APs and vWLCs
- Performance impact: without Data DTLS, average vWLC throughput is about 200 Mbps, with all APs using Data DTLS, average vWLC throughput is about 100 Mbps

© 2010 Cisco and/or its affiliates. All rights reserved.

Configuring DTLS

```
(Virtual WL

NAME: "Chassis"     , DESCR: "Cisco Wireless Controller"
PID: AIR-CTVM-K9,  VID: V01,  SN: VMware-56

(Virtual WLC) >show sysinfo
Product Version..................................... 7.5.x
config ap link-encryption enable/disable <Cisco AP>/all
```

© 2010 Cisco and/or its affiliates. All rights reserved.

Verification

- Commands available as on other platforms for verifying data DTLS

```
(Virtual WLC) >show dtls connections

      AP Name          Local Port        Peer IP         Peer Port          Ciphersuite
 ------------------- ------------ ----------------  -------------  ------------------------------
 CMX1-1600           Capwap_Ctrl    10.10.10.109      16032          TLS_RSA_WITH_AES_128_CBC_SHA
 CMX1-1600           Capwap_Data    10.10.10.109      16032          TLS_RSA_WITH_AES_128_CBC_SHA

(Virtual WLC) >show ap link-encryption all

                Encryption  Dnstream  Upstream    Last
AP Name              State    Count     Count  Update
------------------  ---  --------  --------  ------
CMX1-1600             En        21        26    0:30
```

This AP uses DTLS
Only for CAPWAP control

This AP uses DTLS for CAPWAP control and for CAPWAP Data

Encrypted packets stats

© 2010 Cisco and/or its affiliates. All rights reserved.

Rate Limiting

- With most controllers, you can assign rate limiting to client traffic
- Upstream traffic rate-limiting introduced in 7.3 release
- 7.5 release adds rate-limiting support for vWLC
- Rate limiting can be configured from the QoS profile page or at the WLAN level
- WLAN configuration overrides the parameters configured in the QoS Profile.

© 2010 Cisco and/or its affiliates. All rights reserved.

Rate Limiting

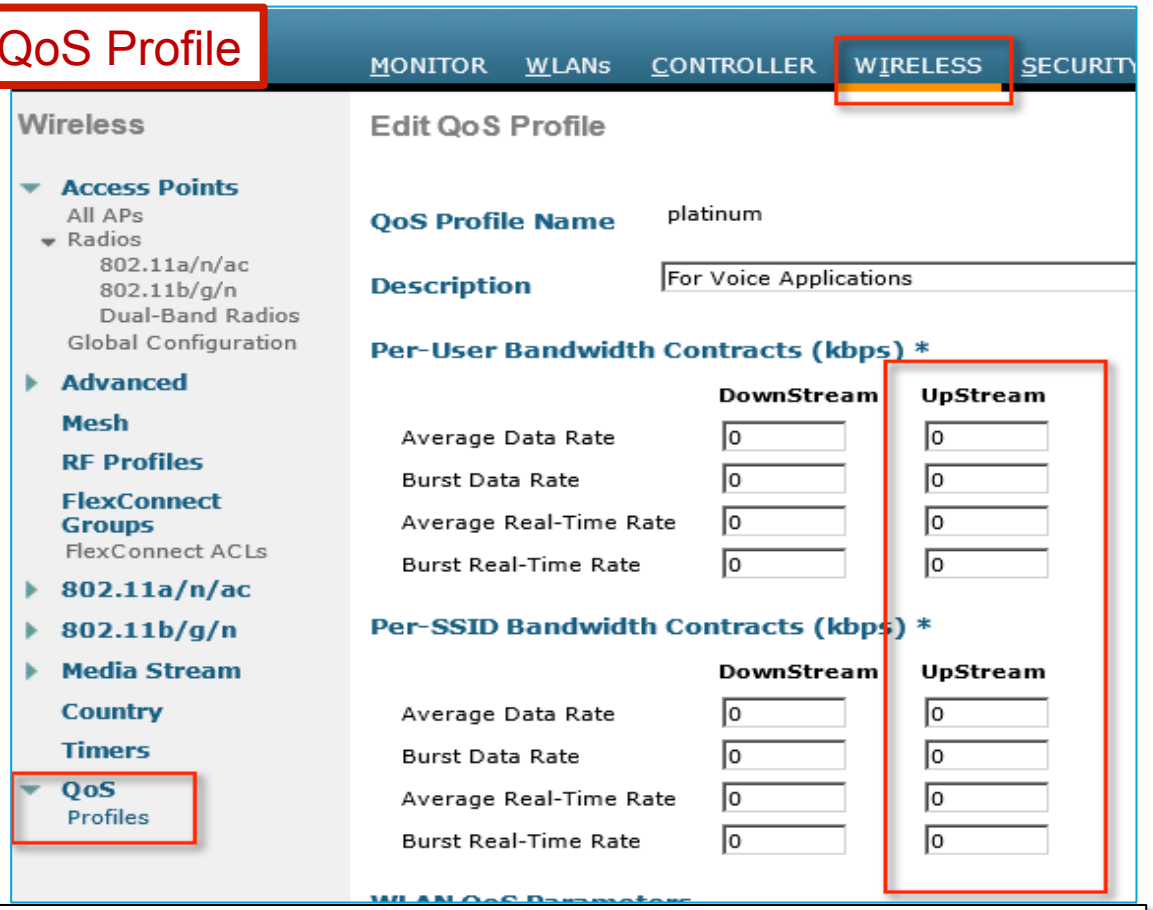
- Rate limiting is enforced at the AP level
- vWLC cannot enforce rate-limiting at the controller level
  - Per-client downstream rate limiting is not supported for central switching WLANs when traffic is terminated at the vWLC
  - Per-client downstream rate limiting is supported if the vWLC is a foreign controller tunneling traffic to another platform, e.g. 5508

	FlexConnect Central Switching	FlexConnect Local Switching	FlexConnect Standalone
Per-Client Downstream	Not Supported	Supported	Supported
Per-SSID Downstream	Supported	Supported	Supported
Per-Client Upstream	Supported	Supported	Supported
Per-SSID Upstream	Supported	Supported	Supported

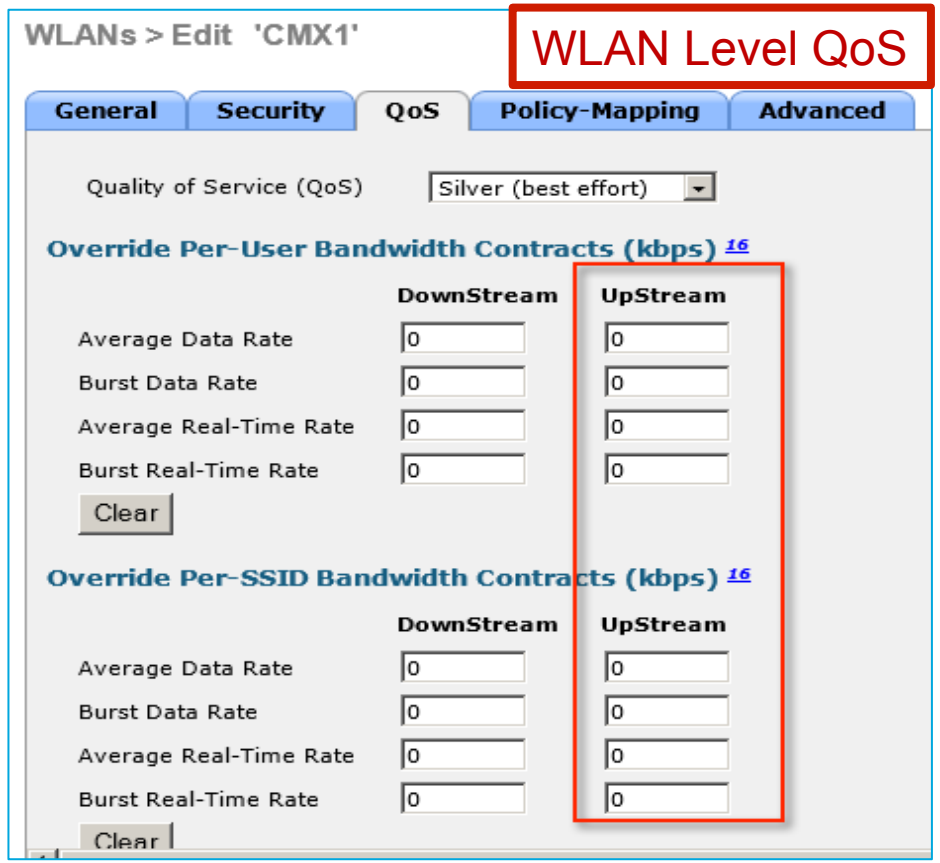
© 2010 Cisco and/or its affiliates. All rights reserved.

Configuring Rate-Limiting on vWLC

QoS Profile



WLAN Level QoS




```
config qos [average-data-rate | average-realtime-rate | burst-data-rate | burst-realtime-rate] [bronze | gold | silver | platinum] [per-ssid | per-client] [downstream | upstream] limit in kbps
```

```
config wlan override-rate-limit id [average-data-rate | average-realtime-rate | burst-data-rate | burst-realtime-rate] [per-ssid | per-client] [downstream | upstream] limit in kbps
```

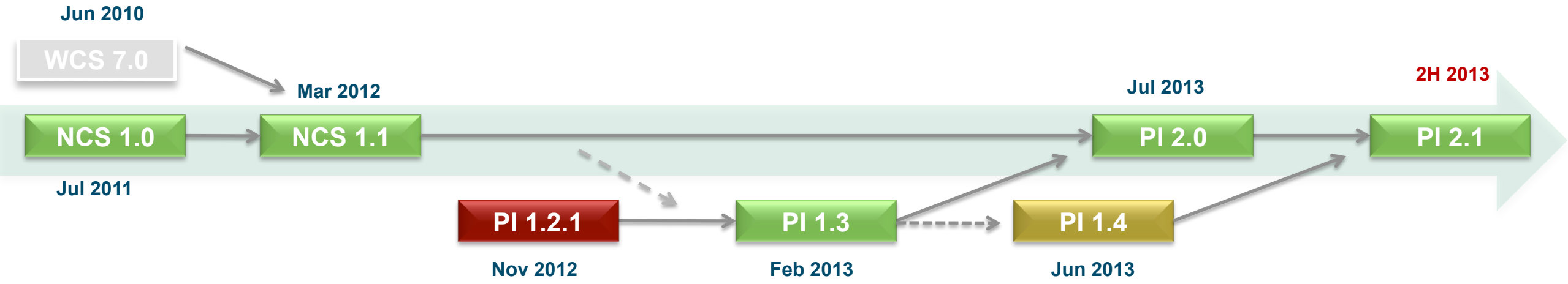
© 2010 Cisco and/or its affiliates. All rights reserved.

Software roadmap

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco Prime Infrastructure

Recommended Upgrade Paths

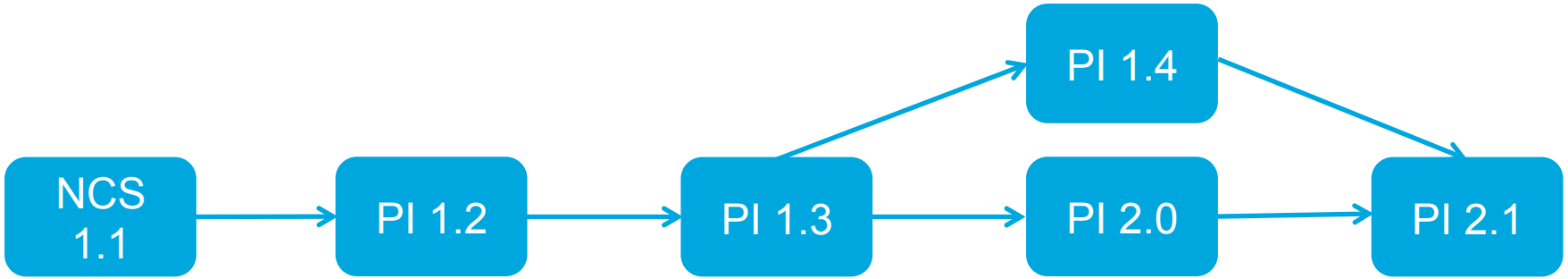


Version	WLC	Issue	Recommendation	Exception
NCS 1.1	7.2		Remain until 2.0	Require WLC 7.3+ or Bug fixes
PI 1.2	7.3	CSAT issues	Upgrade to 1.3	
PI 1.3	7.4		Remain until 2.0	Require WLC 7.5 (802.11ac module or AP-700)
PI 1.4	7.5	No path to 2.0	Remain until 2.1	
LMS 4.2	N/A		Review LMS to PI migration doc here	LMS feature parity will occur throughout the PI 2.x release train

© 2010 Cisco and/or its affiliates. All rights reserved.

Interop AireOS Controller Release with Cisco Prime Infrastructure, ISE & MSE

WLC	CPI	MSE	ISE
7.4	1.3	7.4	1.1.1
7.4 MR	1.3	7.4	1.1.1
7.5	1.4, 2.1	7.5	1.1.2, 1.1.3
8.0	2.1	8.0	1.2



© 2010 Cisco and/or its affiliates. All rights reserved.

Thank you.