Cisco AssureWave Wireless LAN Controller

Release 7.4.110.0 Test Results

Version History

Version number	Date	Notes
0.1	Aug 8th 2013	Draft
0.2	Aug 21st 2013	Integrated vertical updates
0.3	Aug 26th 2013	CDETS fixed after release date

Executive Summary

AssureWave is a Cisco initiative that provides Wireless LAN service providers with their Cisco software version of choice.

The AssureWave program collects topology, application, and client information from various sources such as Sales Engineers, TAC and directly from customers to build test networks that simulate particular vertical environments. These test networks run additional scenarios based on this vertical information to better cover various interoperability matrices. The vertical test beds are built upon existing horizontal technologies such as Mobility, Voice, and Routing/Switching. In addition, existing Best Practices and Deployment Guides from the different technologies are referenced and deployed in the networks. This release tested the HealthCare, Retail, Enterprise and Higher Education vertical market scenarios.

The AssureWave program also proactively enlists additional testing from 3rd party partners in addition to any existing Cisco partnerships. This comprehensive testing of client and application interoperability results in a smoother introduction of a complete end-to-end wireless ecosystem.

This document summarizes what was tested for each market segment; in which specific combinations of devices and features were tested; a test summary and recommendation; and relevant open caveats.

Contents

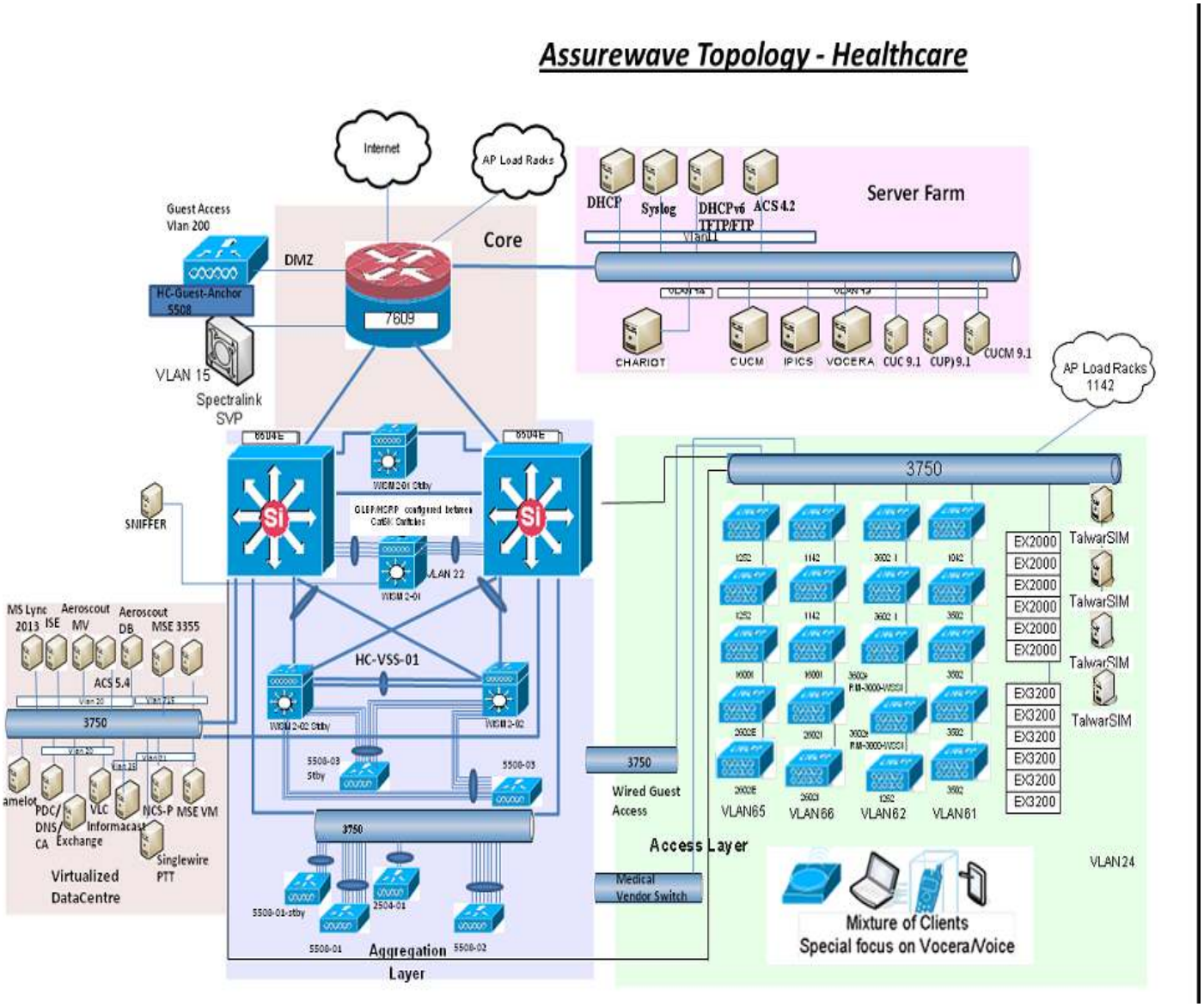
HealthCare Vertical Market

What Was Tested

- Cisco Wireless LAN Controller (5508, WISM2 and 2504) N-1 and N-2 upgrades (N-2, N-1 being previous major releases and N being current version).
- Cisco NCS N-1 Upgrade (N-1 being the previous major release and N being current version).
- Cisco Mobility Services Engine (MSE) Appliance N-1 Upgrade (N-1 being the previous major release and N being current version).
- Simultaneous client encryption methods—Open, WEP, WPA and WPA2.
- Simultaneous client EAP authentication modes—LEAP, PEAP, EAP-FAST, EAP-TLS.
- Layer 2 (inter/intra controller) and Layer 3 roaming scenarios (with voice and data clients).
- High Availability—Controller/AP, access layer failover testing.
- Voice clients including the Cisco 7921/25/26/9971, Spectralink 8030/8450, Ascom i62 and Vocera B2000/3000 badges with one-to-one, one-to-many (as applicable), wireless-to-landline, and PTT with Cisco IPICS.
- Guest Access (wired and wireless) with Open authentication methods.
- Location tracking with data/voice clients and active RFID tags.
- Interoperability between various data, voice, and RFID devices on both the 2.4 and 5Ghz bands as applicable.
- Radio Resource Management (RRM) functionality
- IPv4 Media Streaming and Multicast with Roaming
- Vlan Pooling.
- Wireless Medical Patient Monitoring Systems , IV Pumps , etc. with WEP , WPA2-PSK , WPA-PSK , 802.1x (WPA2 Enterprise) security with a/b/g radios.
- SNMP stress
- Controller HA Funnctionality with AP SSO .
- Collaboration Application Testing with Apple and Windows Devices for Cisco Jabber and Jabber IM .
- MS Lync 2013 Application Testing with Microsoft Windows Clients including Chat , Share , Video Call , Audio Call , Conferencing, Persistant Chat .

Healthcare Test Topology

Figure 1 shows the test topology for the Healthcare vertical market.



Devices and Software Tested

The following devices and software were tested as part of the AssureWave healthcare vertical market.

Table 1 Infrastructure Devices Tested for Healthcare

Infrastructure Device Information	
Device	**Version**
WS-C6504-E w/ VS-S2T-10G w/ WS-X6848-GE-TX w/ WS-X6908-10G WS-C6504-E w/ VS-S2T-10G w/ WS-X6848-GE-TX w/ WS-X6908-10G WS-C6509-E w/ VS-S2T-10G w/ WS-X6848-GE-TX w/ WS-X6908-10G w/ WS-SVC-WISM2-K9 VSS ========= WS-C6506-E w/ VS-S2T-10G w/ WS-X6848-GE-TX w/ WS-X6908-10G w/ WS-SVC-WISM2-K9 WS-C6506-E w/ VS-S2T-10G w/ WS-X6848-GE-TX w/ WS-X6908-10G w/ WS-SVC-WISM2-K9	15.1(1)SY1
WS-C3750G-24PS-S WS-C3750G-48PS-S WS-C3750X-48PS-S	12.2(44)SE 15.0(1)SE
CISCO7609 w/WS-SUP720-3B w/WS-X6548-GE-45AF w/WS-SVC-FWM-1-K9	12.2(33)SXJ2

Table 2 Controller and Access Point Devices Tested for Healthcare

Controller / Access Point Information	
Device	**Version**
AIR-CT5508-500-K9	7.4.110.0

Controller / Access Point Information	
Device	**Version**
WS-SVC-WISM2-K9	7.4.110.0
AIR-CT2504-50-K9	7.4.110.0
AIR-LAP1131AG-A-K9	7.4.110.0
AIR-LAP1142N-A-K9	7.4.110.0
AIR-LAP1242AG-A-K9	7.4.110.0
AIR-LAP1252AG-A-K9	7.4.110.0
AIR-LAP1262N-A-K9	7.4.110.0
AIR-CAP3502E-A-K9	7.4.110.0
AIR-CAP3502I-A-K9	7.4.110.0
AIR-CAP2600I-A-K9	7.4.110.0
AIR-CAP1602E/I-A-K9	7.4.110.0
AIR-CAP3602E-A-K9	7.4.110.0
AIR-CAP3602I-A-K9	7.4.110.0
AIR-LAP1042N-A-K9	7.4.110.0
AIR-AP1232AG-A-K9	12.3(8)JEE (as WGB)
AIR-AP1242AG-A-K9	12.4(25d)JA2 (as WGB)
AIR-AP1131AG-A-K9	12.4(25d)JA2(as WGB)
AIR-SAP1602I-A-K9	15.2(2)JB (as WGB)

Table 3 Network Server Devices Tested for Healthcare

Network Server Information	
Server Type	**Version**
Microsoft AD, DHCP, DNS, TFTP and FTP Services	Windows 2008 R2 Server
Microsoft CA Services	Windows 2008 R2 Server
Microsoft IAS (NPS - Radius) Server	Windows 2008 R2 Server
Microsoft Lync 2013	Windows 2008 R2 Server
Cisco ACS Radius Server	4.2(0) Build 124
Microsoft DHCPv6 Server	Windows 2008 Server (Standard)
Cisco ACS Radius Server	5.4.0.46.0a
Microsoft Exchange Server 2010	Windows 2008 R2 Server
Cisco Identity Services Engine (ISE)	1.1.3.124
Cisco Unified Call Manager (CUCM)	8.6(2a)

Network Server Information	
Server Type	**Version**
Cisco Unified Call Manager (CUCM) (Jabber)	9.1.1.20000-5
Cisco Unified Presence (CUP) (Jabber)	9.1.1.20000-5
Cisco Unity Connection (CUC) (Jabber)	9.1.1.20000-5
Vocera Server	4.3/SP1
Vocera Client Gateway	4.3/SP1
VLC Media Player	2.0.5
NCS	1.3.1
Cisco MSE 3355 Appliance	7.4.110.0
Cisco MSE VM	7.4.110.0
Linux RH SYSLOG/NTP Server	Linux RH Enterprise AS4

Table 4 Application Products Tested for Healthcare

Application Information	
Application	**Version**
IPICS	4.6(1)
AeroScout Tag Engine	4.4.2.11
AeroScout MobileView Server	4.4.3.9
Singlewire Informacast	8.1.0
Singlewire Push To Talk	2.4.0
Citrix Presentation Server	4.5
Ekahau RTLS Engine	RTLS version 5.6.11
Ekahau Vision	1.7.14

Table 5 Voice Client Devices Tested for Healthcare

Voice Client Information	
Device	**Version**
Ascom i62 Phone	4.3.12
Cisco 7921 Phone	1.4.4.3
Cisco 7925 Phone	1.4.4.3
Cisco 7926 Phone	1.4.4.3
Cisco 9971 Phone	9.3.1.33

Voice Client Information	
Device	**Version**
Spectralink 8030	119.081/131.030/132.030 (SIP)
Spectralink 8450	4.0.0.15769 (SIP)
Vocera Badge B2000/B3000	4.3/SP1 (Build 1942)

Table 6 Laptop Client Devices Tested for Healthcare

Laptop Client Information			
Device	**OS**	**Chipset**	**Driver**
Acer Aspire AO722	Win 7 Pro SP1(32 bit)	Atheros AR5B125	9.2.0.412
Acer TravelMate 5744-6467	Win 7 Pro SP1 (64 bit)	Atheros AR5B125	10.0.0.221
HP Probook 4430s	Win 8 Enterprise (64 bit)	Atheros AR9285	10.0.0.221
Dell Latitude 5530	Win 7 Pro SP1 (64 bit)	DW 1540 a/g/n	5.100.82.112
Dell Latitude 5530	Win 8 Pro Enterprise (64 bit)	DW 1540 a/g/n	6.30.59.26
Dell Latitude 5430	Win7 Pro SP1 (64 bit)	Intel N 6205 AGN	15.1.1.1
HP UltraBook Folio 13-2000	Win 7 Pro SP1 (64 bit)	Intel N 1030 bgn	14.2.0.10
HP Probook 6560b	Win 7 Pro (64 bit)	Broadcom 43224 AGN	5.60.350.23
HP Elitebook 8460p	Win 7 Pro (64 bit)	Broadcom 43224 AGN	5.100.82.82
Lenovo X120e(AMD)	Win7 Pro SP1 (64 bit)	Lenovo 1x1 11b/g/n Half Mini Adapter	1003.10.1112.2010
Fujitsu Lifebook P701	Win7 Pro (32 bit)	Intel N 6205 AGN	15.1.1.1
Toshiba Tecra R850	Win7 Pro SP1 (32 bit)	Intel N 6230 AGN	14.1.1.3
Acer TravelMate 8481T	Win 7 Pro SP1 (64 bit)	Intel N 6205 AGN	15.1.1.1
HP 3115M	Win 7 Home Premium (64 bit)	Intel N 6230 AGN	14.2.0.10
Acer Aspire 3624WXMi	WinXP/SP3	Atheros AR5005G	4.0.0.14001
Acer Aspire 9500	WinXP Pro (x86)	Atheros 5005G	4.0.0.14001
Apple MacBook Air	MacOS 10.6.7	AirPort Extreme	5.10.131.36.9
Apple MacBook Air (2013)	MacOS 10.8.4	AirPort Exteme 802.11a/b/g/n/ac Broadcom BCM43xx 1.0	6.30.223.74.35
Acer Aspire V3 -772G-9829	Windows 8 Pro (64 bit)	Atheros 5BWB222	10.0.0.225

Laptop Client Information			
Device	**OS**	**Chipset**	**Driver**
Asus Eee PC 1016PT	Win7 Pro (x86)	Intel 6200 AGN	13.5.0.6
Asus Eee PC 900	WinXP Home (x86)	Atheros AR5007EG	5.3.0.45
Asus R1F K018E	Win7 Ent (x86)	Intel 3945ABG	13.3.0.24
Dell Latitude E5410	Win7 Pro (x86)	Intel 6200 AGN	13.3.0.24
Dell Latitude E5410	Win7 Pro (x86)	Intel 6300 AGN	14.2.0.10
Dell Latitude E5410	Win8 Pro (x64)	Intel 6300 AGN	15.6.0.19
Dell Latitude E5410	Win7 Pro (x86)	Dell DW1520 AGN	5.60.48.35
Sony Vaio SVE151D11L	Win7 Pro (64 bit)	Atheros AR9485WB-EG	9.2.0.489
Sony Vaio SVE151D11L	Win8 Pro (64 bit)	Atheros AR9485WB-EG	Microsoft 3.0.0.130
Fujitsu Lifebook LH530	Win7 Pro (x64)	Atheros AR9285 GN	8.0.0.258
Fujitsu Lifebook T4215	Win7 Pro (x86)	Intel 3945ABG	13.3.0.24
Fujitsu Lifebook T4410	Win7 Pro (x86)	Intel 5100 AGN	12.4.1.4
Fujitsu Lifebook T580	Win7 Pro (x86)	Atheros AR928X	10.0.0.75
HP EliteBook 6930p	Win7 Ent (x64)	Intel 5300 AGN	14.3.2.1
HP EliteBook 6930p	WinXP Pro (x86)	Intel 5300 AGN	13.4.0.9
HP ProBook 6455b	Win7 Pro (x86)	Broadcom 4313 BG	5.60.350.11
HP ProBook 6550b	Win7 Pro (x86)	Broadcom 43224 AGN	5.60.350.11
HP/Compaq Compaq 6530b	Win7 Ent (x64)	Intel 5100 AGN	14.3.2.1
HP/Compaq Compaq 6530b	WinXP Pro (x86)	Intel 5100 AGN	13.4.0.9
HP/Compaq Compaq 6730b	Win7 Ent (x86)	Intel 5100 AGN	13.3.0.24
HP/Compaq Compaq 6830s	Win7 Ent (x86)	Intel 5100 AGN	13.3.0.24
HP/Compaq Compaq 6910p	Win7 Ent (x64)	Intel 4965 AGN	12.4.1.4
Lenovo N100	WinXP Pro (x86)	Intel 3945 AG	13.4.0.139
Lenovo SL400 2743-89U	Win7 Ent (x86)	Intel 5100 AGN	13.3.0.24
Lenovo T61	WinXP/SP3 (x86)	Intel 3945 AG	13.3.0.137
Motion Computing MC-C5v	Win7 Pro (x86)	Intel 6200 AGN	14.2.0.10
Motion Computing MC-F5	WinXP/Tablet/SP3	Intel 3945 ABG	13.4.0.139
Motion Computing J3400	Win7 Pro (x86)	Intel 5300 AGN	13.3.0.137
Panasonic ToughBook CF-52	Win7 Pro (x86)	Intel 5100 AGN	13.4.0.9
Panasonic ToughBook CF-U1	Win7 Ent (x86)	Intel 5100 AGN	13.1.1.1

Laptop Client Information			
Device	**OS**	**Chipset**	**Driver**
Sony Vaio PCG-6Q1L	Win7 Ent (x86)	Intel 3945 ABG	12.4.1.4
Sony Vaio/PCG-7133L	Win7 Ent (x64)	Intel 4965 AGN	13.3.0.137
Sony Vaio/PCG-7X1L	Win7 Ent (x86)	Intel 3945 AG	13.4.0.139
Toshiba Satellite A135-S2386	WinXP Pro (x86)	Linksys WPC600N	4.150.31.0
Toshiba Satellite A135-S4467	Win7 Ent (x86)	Intel 3945 AG	12.4.1.4
Toshiba Satellite U205-S5034	WinXP Pro (x86)	Intel 3945 AG	13.3.0.137
Toshiba Tecra A9-S9018X	WinXP Pro (x86)	Intel 4965 AGN	13.4.0.139
Toshiba Tecra M10-S3452	Win7 Ent (x64)	Intel 5100 AGN	13.4.0.9

Table 7 Tablet/Smartphone Devices Tested for Healthcare

Tablet/Smartphone Client Information		
Device	**OS**	**Version**
Apple iPod Touch	iOS	6.1.3 (10B329)
Apple iPad 2	iOS	6.1.3 (10B329)
Apple iPad 3	iOS	6.1.3 (10B329)
Apple iPhone 4S	iOS	6.1.3 (10B329)
Apple iPhone 5	iOS	6.1.4 (10B350)
Archos 43 Internet Tablet	Android	2.3.26
Samsung Galaxy Tab 7	Android	2.2.1
Google Nexus 7	Android	4.2.2 / 4.1.2
Samsung Galaxy Tab 8.9	Android	4.0.4
Samsung Galaxy Tab 10	Android	4.1.1
Dell Streak 7	Android	2.2.2
Asus Transformer TF101	Android	4.0.3
Toshiba THRiVE Tablet AT105	Android	4.0.4
Sony Tablet S SGPT111US	Android	3.2
Lenovo Thinkpad Tablet	Android	4.0.3
Motorola XOOM	Android	4.0.3
Blackberry Playbook	Blackberry	1.0.5.2342
Acer A700	Android	4.0.4

Table 8 Supplicant Devices Tested for Healthcare

Supplicant Information	
Device	**Version**
Cisco AnyConnect	3.1.00495/ 3.1.04059
Microsoft Windows ZeroConfig	Windows XP Pro, Win7 , Windows 8 , Intel Proset , HP Connection Manager

Table 9 Other Client Devices Tested for Healthcare

Other Client Information	
PDA/Handhelds	**Version/Comments**
Motorola MC75A (Healthcare version)	WM 6.5 Classic/CE OS 05.02.21840
Tags/Exciters	**Version/Comments**
AeroScout Active RFID Tags	T2, T2 w/Call Button, T3, T4, T5h, T6
AeroScout EX2000B Exciters	BOOT 60702/DSP 30811
AeroScout EX3210 Exciters	BOOT 60702/DSP 30811
Ekahau Active RFID Tags (CCX Mode)	T301A, T301B, T301BD, T301Ex, T301i, T301is, T301t, T301W
Medical Devices	**Version/Comments**
CareFusion Alaris PC 8015 Series IV Pumps w/Systems Manager	PCU SW: 9.12.0.10, System Maintenance Ver : v9.8 Alaris Systems Manager – v3.3 Motorola LA-5137
Dräger Infinity Delta Monitors w/Central Station	VFW-8.3
Dräger M300 Monitors w/Central Station	VF8.10
Philips IntelliVue X2/MP2 Patient Monitors w/Central Station	App Sw - J Version J.10.33 / Radio SW version A.01.09 / Hw Revision – A.00.12
Philips IntelliVue MX40 Patient Monitors w/Central Station	Sw Version B.01.29/B.01.33 / Hw Rev A.01.00
Baxter Spectrum Smart IV Pumps (b radio battery Module)	Sw version - v6.02.06 / Sharp 0177B / PIC :066 / CPLD : 7 / SmartBatt Charger : 17.01 /Network Module : 13
Baxter Spectrum Smart IV Pumps (b/g radio battery Module)	Sw version - v6.02.06 / Sharp 0177B / PIC :066 / CPLD : 6 / SmartBatt Charger : 17.01 / Network Module : 16
Other	**Version/Comments**

Table 10 Collaboration Client Applications Tested in Healthcare

Collaboration Client Information	
Device	**Version**
Cisco Jabber for Windows	9.2(2) / 9.2(3)
Cisco Jabber for Mac	8.6.6
Cisco Jabber for Android for Samsung S3	9.1.3.4681
Cisco Jabber for iphone	9.1.3.21455
Cisco Jabber for iPad	9.3 (21386)
MS Lync Client 2013 for Windows	15.0.4420.1017

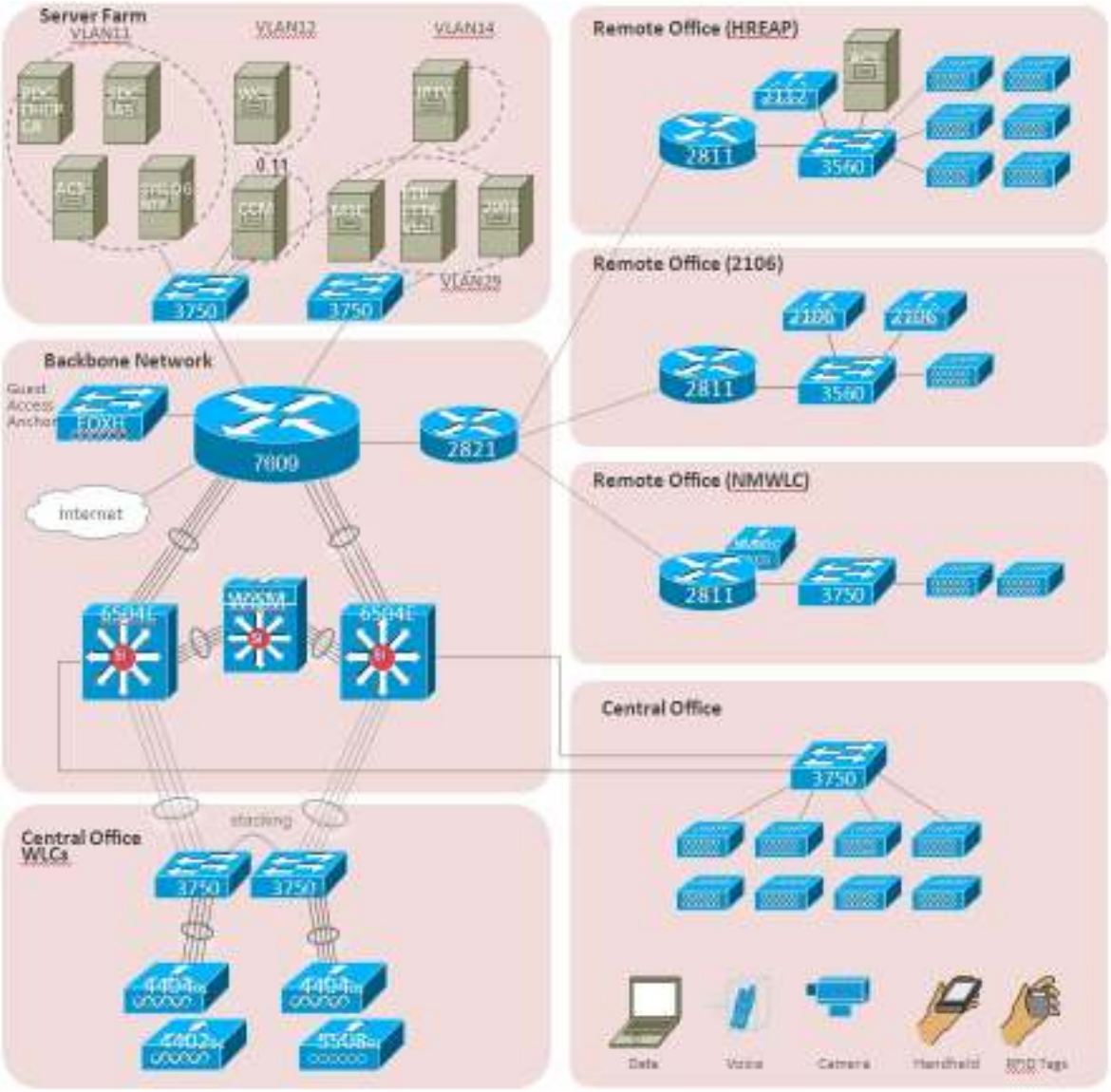
Retail Vertical Market

What Was Tested

- Cisco Wireless LAN Controller (Cisco Flex 7500, WiSM2, 5508, 2504 and 7510 Integrated) N-1 and N-2 upgrades (N-2, N-1 being previous major releases and N being current version).
- Cisco Prime NCS (NCS) N-1 Upgrade (N-1 being the previous major release and N being current version).
- Cisco Mobility Services Engine (MSE) Appliance N-1 Upgrade (N-1 being the previous major release and N being current version).
- Simultaneous client Encryption/Authentication modes (e.g. WEP, WPA, 802.1x with various methods).
- Layer 2 (inter/intra controller) and Layer 3 roaming scenarios (inter/intra controller with voice and data clients).
- High Availability (including Controller/AP, access layer failover testing).
- Voice clients including the Cisco 7920/7921 with PTT.
- Handheld clients including Symbol handhelds(MC9090, MC7090, MC3090, MC5590), Intermec handhelds(CK3, CN3, CK31), Psion 7535 G2, and PSC handhelds(Falcon 4420)
- Application-specific and Point of Sale scenarios with various Symbol, Intermec, HHP, Falcon handhelds, Zebra QL320 plus printers, Hobart wireless scales, Cisco's video surveillance solution.
- Hybrid-REAP with central and local switching, web-auth with roaming, voice, L2 roaming, CCKM, and IGMP snooping
- Guest Access (wired and wireless) with various authentication (open / local account / RADIUS account)
- Location tracking with data/voice clients and active Intermec, tags.
- Client interoperability testing with CCX and non-CCX handhelds, smart phones, laptops.
- Radio Resource Management (RRM) functionality
- IRCM(Inter Release Controller Mobility) with Layer 2 / Layer 3 roaming
- ClientLink with legacy clients

Retail Test Topology

Figure 2 shows the test topology for the Retail vertical market.



Devices and Software Tested

The following devices and software were tested as part of the AssureWave Retail vertical market.

Table 10 Infrastructure Device Devices Tested for Retail

Infrastructure Device Information	
Device	**Version**
WS-C6504-E w/WS-SUP720-3B w/WS-X6548-GE-45AF w/WS-SVC-WISM-2-K9	12.2(33)SXJ1
WS-C3750G-24PS-S WS-C3750X-48PS-S WS-C3750E-24PS	15.0(1)SE3, 12.2.(53)SE2
CISCO7609 w/WS-SUP720-3B w/WS-X6548-GE-45AF WS-SVC-FWM-1-K9	12.2(33)SXJ2
Cisco 2611XM Terminal Servers (4)	12.3(6f)
Cisco 2811/2821 ISR	12.4 (24)T

Table 11 Controller and Access Point Devices Tested for Retail

Controller/AP Information	
Device	**Version**
WS-SVC-WiSM2-1-K9	7.4.110.0
AIR-WLC5508-500	7.4.110.0
AIR-WLC5508-500	7.4.110.0
AIR-WLC7500-A-K9	7.4.110.0
AIR-WLC7500-A-K9	7.4.110.0
AIR-WLC2504-K9	7.4.110.0
WS-SVC-WiSM1-1-K9	7.0.240.0
WS-SVC-WiSM1-1-K9	7.0.240.0
AIR-LAP1242AG-A-K9	7.4.110.0
AIR-LAP1131AG-A-K9	7.4.110.0
AIR-LAP1602E/I-A-K9	7.4.110.0
AIR-LAP2602E/I-A-K9	7.4.110.0
AIR-LAP3602E/I-A-K9	7.4.110.0
AIR-LAP1252AGN-A-K9	7.4.110.0

Controller/AP Information	
Device	**Version**
AIR-AP1242AG-A-K9	7.4.110.0
AIR-AP1131AG-A-K9	7.4.110.0
AIR-AP1232AG-A-K9	12.3(8)JEB (as WGB)
AIR-AP1242AG-A-K9	12.4(21a)JA1 (as WGB)

Table 12 Network Server Devices Tested for Retail

Network Server Information	
Device	**Version**
Microsoft DHCP Server	Windows 2003 SE/SP1 Server
Microsoft DNS Server	Windows 2003 SE/SP1 Server
Microsoft TFTP/FTP Server	Windows 2003 SE/SP1 Server
Cisco ACS Radius Server	5.2.0.26
Microsoft CA	Windows 2000 Server/SP4
Cisco Unified Call Manager (CCM)	v7.1.5.33900-10
Cisco Prime Infrastructure	1.3.1
Cisco MSE 3350	7.4.110.0
Cisco IPTV Server	3.5.7.1 (on Windows 2000/SP4 Server)
Linux RH SYSLOG Server	Linux RH Enterprise AS4
Linux RH NTP Server	Linux RH Enterprise AS4
Cisco ISE	1.0.4.573
Point Of Sale Server	Windows 2003 SE/SP1 Server
Cisco Video Surveillance Operations Manager	SUSE Linux / Cisco VSOM v6.3.1

Table 13 Voice Client Devices Tested for Retail

Voice Client Information	
Device	**Version**
Cisco 7921 Phone	1.4.2

Table 14 Laptop Clients Devices Tested for Retail

Laptop Client Information			
Device	**OS**	**Chipset**	**Driver**
HP Compaq 6910p	WinXP pro/SP3	Intel 4965ABGN	14.3.2.1
IBM T61	WinVistaBus/SP2	Intel 4965AGN	14.3.2.1
IBM T61	Win XP pro/SP3	Intel 4965AGN	14.3.2.1
MacBookAir	MacOS 10.5.8	AirPort Exteme ABGN (Broadcom BCM43xx 1.0)	5.10.91.21
Asus Eee Box B202	WinXP home/SP3	Ralink 802.11n wireless	1.1.0
Dell E5410	Win7 pro	Intel 6300AGN	15.1.1.1
Dell inspiron 1525	Win XP pro/SP3	Dell 1505 draft 11n	4.170.25.12
Toshiba	Win Vista home	Intel 3945AG	13.4.0.139
Cisco	CB Adaptor	CB21ag	4.2
Fujitsu	Win 7	Intel Advanced 6205	15.1.1.1
Fujitsu	Win 7	Intel Advanced 6205	14.0.0.113
Sony Vaio	Win 7	Intel 6200 AGN	13.3.0.24
HP 6450B	Win 7	Broadcom 43224 A/G/N	5.60.48.36
HP mini and a Realtek	Win 7	RT3090 B/G/N version	3.1.16.1
Compaq mini with version	Win 7	Broadcom 4313 B/G/N	5.60.350.11 driver

Table 15 Supplicant Devices Tested for Retail

Supplicant Information	
Device	**Version**
Cisco Secure Services Client	5.1.1.18
Intel ProSet	14.1.1.0, 14.2
Cisco Aironet Desktop Utility	4.5.0.84
Microsoft Windows ZeroConfig	Windows XP Pro, Vista
OAC (Odyssey)	4.52, 4.60
Fusion (windows CE)	2.57.0.0.022B-CE-PHOTON
Fusion (Windows Mobile)	2.55.1.0.010R-WM-PHOTON

Table 16 Other Client Devices Tested for Retail

Other Client Information	
PDA/Handhelds	**Version/Comments**

Other Client Information	
PDA/Handhelds	**Version/Comments**
Intermec CK31 (2), 761 (2)	WinCE 4.20.0/FW 3.00.19.0748
Intermec CK3	WinMobile 6.1
Intermec CN3	WinCE 5.0
Intermec CK30	WinCE.NET
Psion 7535 G2	WinCE 5.0
Psion Workabout Pro Gen II	WinCE 5.0
PSC Falcon 4420 (27)	WinCE 4.20.0/FW 1.80
Symbol MC9060G (4)	WinCE 4.20.0/Version 3.17
Symbol MC9090CR	Windows Mobile 5.0
Symbol MC9060G	WinCE 4.20.0/Version 3.17
Symbol MC7090	Windows Mobile 5.0
Symbol MC3090	WinCE 5.0
Symbol MC5590	Windows Mobile 6.5
Symbol WT4090	WinCE 5.0
Symbol PPT8846	WinCE 4.20
Symbol MK2250	WinCE 4.20/ AirBEAM CE client 2.16
Tags/Exciters	**Version/Comments**
Datalogic FalconX3	Windows Mobile 6.3 Pro , Summit Client Utility version 3.03.11

Other	Version/Comments
Cisco VTAdvantage w/Camera	2.0.1
Intermec CV60	Mobile Vehicle Computer/WinXP
Intermec CV30	Mobile Vehicle Computer/WinCE 5.0
Motorola VC5090	Mobile Vehicle Computer/WinCE 5.0
Zebra QL320 , QL420	11.71
Cisco CIVS-IPC-2500W	Wireless IP camera v1.1 (802.11bg)
TRENDnet TV-IP410W/A IP Camera	Wireless IP camera (802.11bg)
Hobart QUANTUM	Wireless scale With Symbol Spectrum NIC (802.11b)
Hobart QUANTUM	Wireless scale with Cisco CB21AG NIC

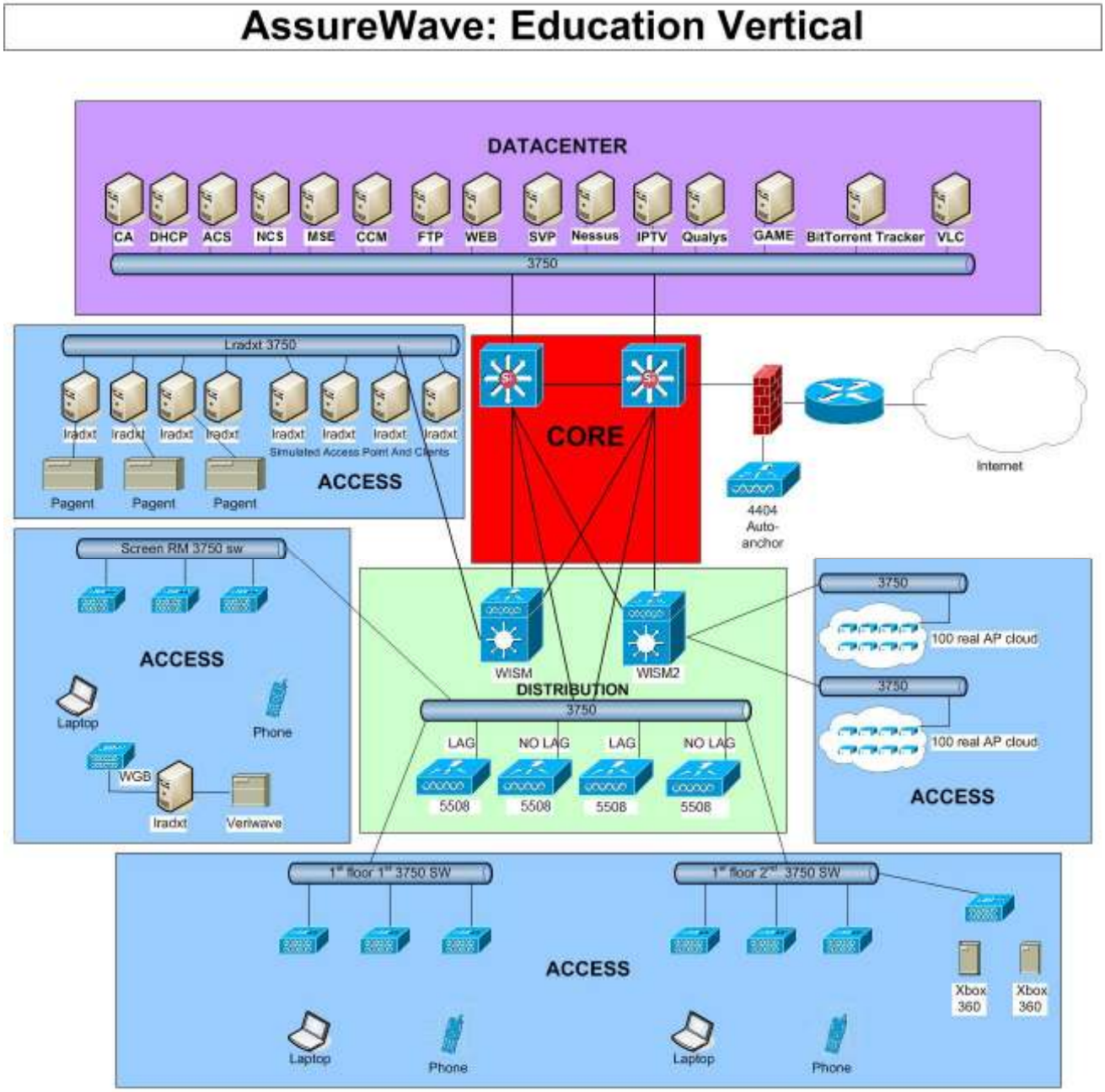
Higher Education Vertical Market

What Was Tested

- Cisco Wireless LAN Controller (WiSM and 5508) N-1 and N-2 upgrades (N-2, N-1 being previous major releases and N being current version).
- Cisco Prime NCS (NCS) N-1 Upgrade (N-1 being the previous major release and N being current version).
- Cisco Mobility Services Engine (MSE) N-1 Upgrade (N-1 being the previous major release and N being current version).
- Cisco Mobility Services Engine (MSE) Appliance N-1 Upgrade (N-1 being the previous major release and N being current version).
- Simultaneous client Encryption/Authentication modes (e.g. WEP, WPA, WPA2, WebAuth, and 802.1x with various methods).
- Layer 2 (inter/intra controller) and Layer 3 roaming scenarios, with and symmetric tunneling.
- High Availability (including Controller/AP, access layer failover testing) with HSRP and redundant supervisors for WiSM modules.
- Guest Access (wired and wireless) with various authentication methods.
- Multicast Traffic to Wireless Clients.
- Device profiling
- BitTorrent file sharing traffic to Wireless Clients.
- Networked Gaming Applications between Wireless Clients.
- Rogue Access Point and Rogue Client detection and containment.
- Security applications and appliances scanning/attacking network infrastructure including but not limited to Codenomicon, QualysGuard, NMAP, and Nessus.
- Radio Resource Management (RRM) functionality

Education Test Topology

Figure 3 shows the test topology for the Higher Education vertical market.



Devices and Software Tested

The following devices and software were tested as part of the AssureWave Higher Education vertical market.

Table 17 Infrastructure Devices Tested for Education

Infrastructure Device Information	
Device	**Version**
WS-C6504-E w/WS-SUP720-3B w/WS-X6548-GE-45AF w/WS-SVC-WISM-1-K9 w/WS-SVC-WISM-2-K9	12.2(18)SXF7 12.2(33)SXJ
WS-C3750G-24PS-S WS-C3750G-48PS-S WS-C3750E-24PD	12.2(25)SEE3, 12.2(44)SE, 12.2(37)SE1, 12.2(25)SEB4,
CISCO7609 w/WS-SUP720-3B w/WS-X6548-GE-45AF	12.2(18)SXF
Cisco 2611XM Terminal Servers (3)	12.4(12)
Catalyst 4506	12.2(40)SG(2.41)

Table 18 Controller and Access Point Devices Tested for Education

Controller/AP Information	
Device	**Version**
AIR-WLC5508-500	7.4.110.0
AIR-WLC7500-A-K9	7.4.110.0
WS-SVC-WISM-1-K9	7.0.240.0
WS-SVC-WISM-2-K9	7.4.110.0
AIR-LAP1142N-A-K9	7.4.110.0
AIR-AP1131AG-N-K9	7.4.110.0
AIR-LAP1242AG-A-K9	7.4.110.0
AIR-AP1252AG-A-K9	7.4.110.0
AIR-LAP1252AG-A-K9	7.4.110.0
AIR-LAP3602E-A-K9	7.4.110.0
AIR-LAP1602E/I-A-K9	7.4.110.0
AIR-LAP2602E-A-K9	7.4.110.0
AIR-LAP3502E-A-K9	7.4.110.0
AIR-AP1242AG-A-K9	12.4(10b)JA (as WGB)

Table 19 Network Server Devices Tested for Education

Network Server Information	
Device	**Version**
Microsoft DHCP Server	Windows 2008 SR1 Server
Microsoft DNS Server	Windows 2003 SE/SP1 Server
Microsoft TFTP/FTP Server	Windows 2003 SE/SP1 Server
Cisco ACS Radius Server	4.1 (on Windows 2000/SP4 Server)
Game Server	Valve Steam Half-Life 2 Dedicated Server
Microsoft CA	Windows 2003 Server/SP2
Cisco Unified Call Manager (CCM)	5.1.3.7000-5
BitTorrent Tracker	BNBT EasyTracker 7.7r3.2004.10.27
VLC Media Player	0.9.9a
Cisco Prime Infrastructure	1.3.1
Cisco Identity Services Engine (ISE)	1.1.3.124
Cisco MSE Appliance	7.4.110.0
Cisco IPTV Server	3.5.7.1 (on Windows 2000/SP4 Server)
Linux RH SYSLOG Server	Linux RH Enterprise AS4
Linux RH NTP Server	Linux RH Enterprise AS4
Qualys	QualysGuard Enterprise
BitTorrent Server/Client	Azureus 3.0.4.2

Table 20 Laptop Client Devices Tested for Education

Laptop Client Information			
Device	**OS**	**Chipset**	**Driver**
Apple PowerBook	10.6.7	Airport A/G/N	1.0 5.10.131.36.9
Apple MacBook	10.6.7 10.6.8	Airport A/G/N	1.0 5.10.131.36.9 1.0 5.10.131.42.4
Apple MacBook Air	10.6.7	Airport A/G/N	1.0 5.10.131.36.9
Apple MacBook	10.7 10.7.4	Airport A/G/N	1.0 5.100.98.75.6 1.0 5.106.198.4.2
Apple MacBook	10.6.7	Airport A/G/N	1.0 5.10.131.36.9
Sony VGN-N350E	Microsoft Vista	Intel 3945ABG	13.4.0.139
Sony VGN-N250N	Microsoft Vista	Intel 3945ABG	13.4.0.139
Sony VGN-N1306	Microsoft XP	Intel 3945ABG	13.4.0.139
Compaq Presario C500	Microsoft Vista	Broadcom 802.11BG	4.102.15.56

Laptop Client Information			
Device	**OS**	**Chipset**	**Driver**
Compaq Presario V6000	Microsoft Vista	Broadcom 802.11BG	4.102.15.56
Compaq 5201US	Microsoft Vista	Broadcom 802.11BG	4.10.40.1
HP Compaq nx9420	Microsoft Vista	Intel 3945ABG	13.4.0.139
HP Mini 1035NR	Microsoft XP	Broadcom 802.11B/G	4.170.77.3
Lenovo T60 ThinkPad	Microsoft Vista	Intel 3945ABG	13.4.0.139
Lenovo X60s ThinkPad	Microsoft XP	Intel 4965AGN	14.3.0.6
Lenovo 3000 N100	Microsoft Vista	Broadcom 802.11BG	4.102.15.56
Toshiba A135-S4427	Microsoft Vista	Intel 3945ABG	13.4.0.139
Toshiba A135-S4447	Microsoft Vista	Intel 3945ABG	13.4.0.139
Toshiba A135-S4467	Microsoft Vista	Intel 3945ABG	13.4.0.139
Toshiba A135-S2386	Microsoft Vista	Atheros AR5006EG	7.1.0.90
Toshiba Satellite A205-S4639	Microsoft Vista	Intel 4965AGN	13.4.0.139
Toshiba Satellite P205-S6267	Microsoft Vista	Intel 4965AGN	12.4.0.21
Toshiba Satellite A205-S4577	Microsoft Vista	Intel 3945ABG	12.4.0.21
Toshiba Tecra A6-EZ6411	Microsoft Vista	Intel 3945ABG	12.4.0.21
Lenovo W510	Windows 7	Intel 6300 AGN	15.1.1.1
Toshiba Satellite A205-S4577	Microsoft Vista	Intel 5100 N	14.3.0.6

Table 21 Supplicant Devices Tested for Education

Supplicant Information	
Device	**Version**
Cisco Secure Services Client	5.1.0.56
Intel ProSet	12.4.0.21, 14.2, 15.1.1.1
ADU	4.4.0.88
ZeroConfig	(with Windows)

Table 22 Other Devices Tested for Education

Other Device Information	
PDA/Handhelds	**Version/Comments**
Microsoft Xbox 360	Microsoft Xbox 360 Wireless Adapters
Apple IPod Touch Gen2	Version 6.0 (10A403)
Brother MFC-845CW	Wireless Printer
Apple iPhone 4, 4S	Version 6.0(10A403), 6.1.2(10B146), 6.1.3 (10B329)

Apple iPad	Version 4.3 (8F190) , 5.1.1 (9B206)
Apple IPad2	Version 6.1.3 (10B329)
Apple IPad3	6.1.3 (10B329)
Lexmark Wireless Printer	Pinnacle Pro 901
Samsung Galaxy Tab 7	2.2.1
Kindle Fire	6.0

Enterprise Vertical Market

What Was Tested

- Cisco Wireless LAN Controller (5508, 4402, 4404, WiSM, WiSM-2, Cisco Flex 7500 and 3750 Integrated) N-1 and N-2 upgrades (N-2, N-1 being previous major releases and N being current version).
- Cisco Prime NCS (NCS) N-1 Upgrade (N-1 being the previous major release and N being current version).
- Cisco Mobility Services Engine (MSE) Appliance N-1 Upgrade (N-1 being the previous major release and N being current version).
- Controller operation with LAG.
- Controller operation with multiple AP managers to cover different customer flavors (WISM-only support LAG).
- Multicast operation with unicast mode.
- Multicast operation with multicast mode.
- 16 WLANs configured with different types of security and class of service—802.1*x*, WPA/WPA2 (LEAP/PEAP/TLS), web-auth, etc.
- Multicast operation with PIM sparse-dense mode in wired network routing.
- Controller, AP, authentication servers operating across MPLS VPN network.
- Six controllers configured in one roaming domain.
- For layer3 roaming, both symmetric tunnel and un-symmetric tunnel cases are covered. The controllers are configured in the same mode, either symmetric tunnel or un-symmetric tunnel).
- Flex mode controller and AP support
- Layer2 roaming (CCKM and non-CCKM).
- Auto-anchor and auto-anchor N+1.
- WGB (including layer 2 and layer 3 roaming).
- TACACS+ for controller administration and accounting.
- Wired guest access.
- IDS and IPS.
- Radio Resource Management (RRM) functionality
- Voice Calls with Cisco 7920/7921 IP phones and Spectralink.
- Network redundancy with HSRP and controller redundancy with configuring primary/secondary/tertiary controllers.
- Controllers trunked to Catalyst 3750 switches with the management interfaces of the controllers and access points deployed in different subnets.
- Hybrid-REAP support, including central switching and local switching.
- Controller access controller and traffic control via access-list.

- Longevity test with multiple SNMP walk to cause CPU as high as 90%
- Lradxt to simulate 150 APs and 3000 clients.
- Roaming during heavy traffic.
- 120 simulated clients with Veriwave.
- Reliable multicast for video

Enterprise Test Topology

Figure 4 shows the MPLS/VPN based core test topology for the Enterprise vertical market.

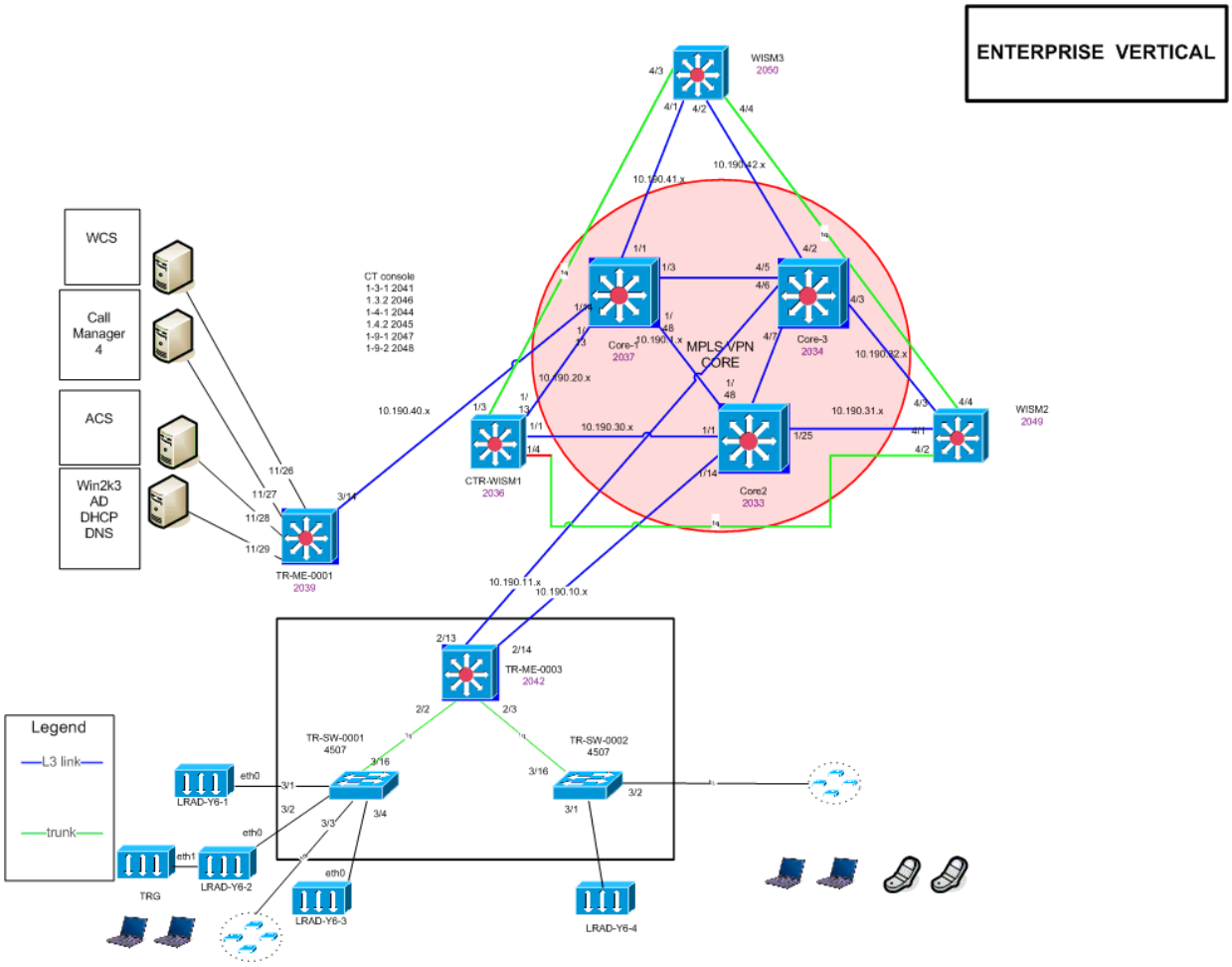
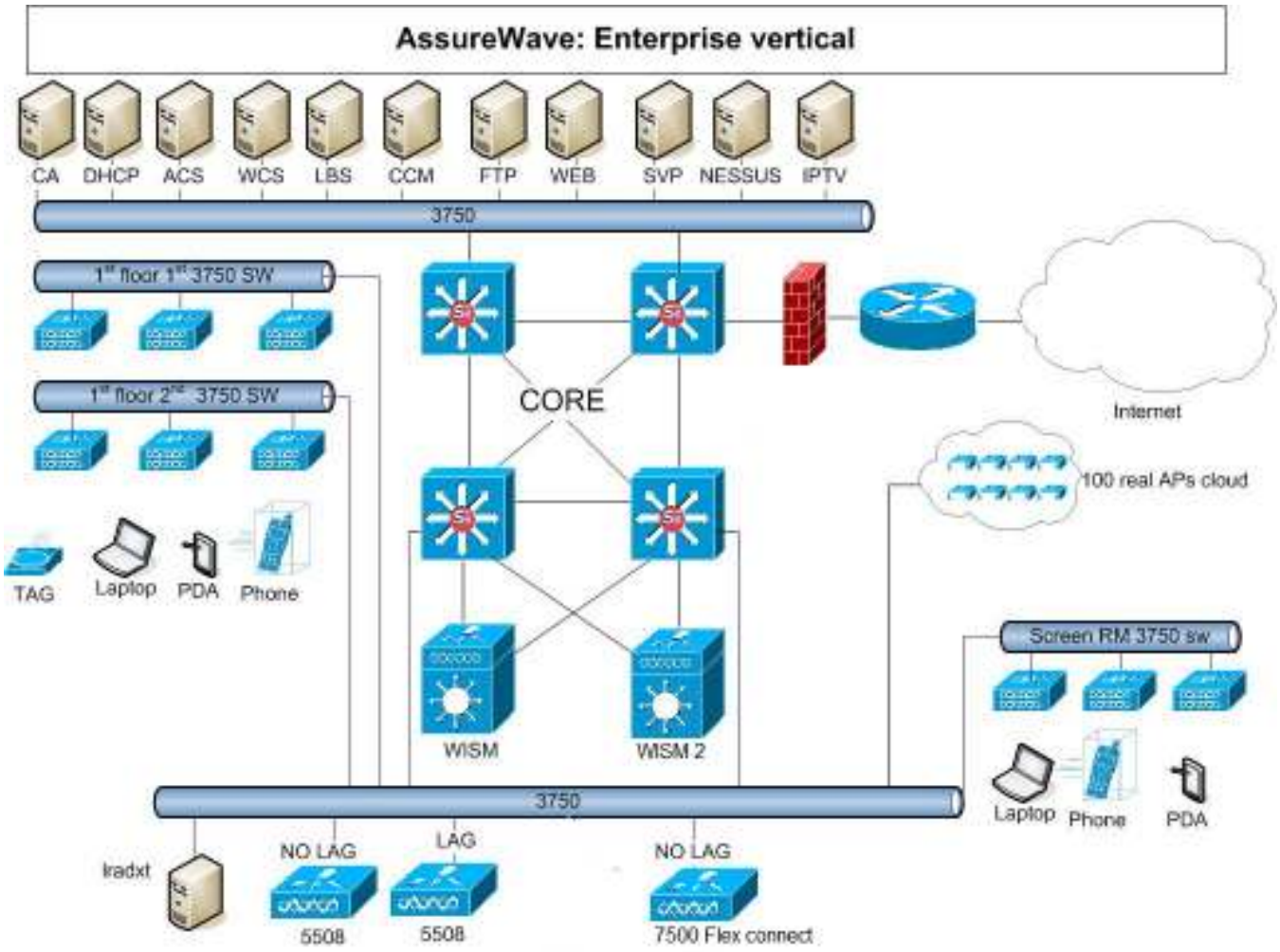


Figure 5 shows the standard IP core network.



Devices and Software Tested

The following devices and software were tested as part of the AssureWave Enterprise vertical market.

Table 23 Infrastructure Devices Tested for Enterprise

Infrastructure Device Information	
Device	**Version**
WS-C6504-E w/WS-SUP720-3B w/WS-X6548-GE-45AF w/WS-SVC-WISM-1-K9 WS-C6509-E w/WS-SVC-WISM-1-K9 w/WS-SVC-WISM-1-K9 w/WS-SVC-WISM2-K9	12.2(18)SXF12 122(33).SXJ
WS-C3750G-24PS-S WS-C3750G-48PS-S WS-C3750E-24PS-S	12.2(40)SE
CISCO7609 w/WS-SUP720-3B w/WS-X6548-GE-45AF w/WS-SVC-FWM-1-K9	12.2(18)SXF7
Cisco 2611XM Terminal Servers	12.3(6f)

Table 24 Controller and Access Point Devices Tested for Enterprise

Controller/AP Information	
Device	**Version**
AIR-WLC5508-500	7.4.110.0
AIR-WLC7500-A-K9	7.4.110.0
WS-C3750G-24WS-S25	7.4.110.0
WS-SVC-WISM-1-K9	7.0.240.0
WS-SVC-WISM-2-K9	7.4.110.0
AIR-LAP1242AG-A-K9	7.4.110.0
AIR-LAP1131AG-A-K9	7.4.110.0
AIR-LAP1240AGN-A-K9	7.4.110.0
AIR-LAP1142N-A-K9	7.4.110.0
AIR-LAP1262N-A-K9	7.4.110.0
AIR-LAP3502E-A-K9	7.4.110.0
AIR-LAP1042N-A-K9	7.4.110.0
AIR-LAP3602E/I-A-K9	7.4.110.0

Controller/AP Information	
Device	**Version**
AIR-LAP1602E/I-A-K9	7.4.110.0
AIR-LAP2600E-A-K9	7.4.110.0
AIR-AP1242AG-A-K9	7.4.110.0
AIR-AP1131AG-A-K9	7.4.110.0
AIR-AP1232AG-A-K9	12.3(11)JX1 (as WGB)
AIR-AP1242AG-A-K9	12.4(10b)JA (as WGB)
AIR-AP1131AG-A-K9	12.4(10b)JA (as WGB)

Table 25 Network Server Devices Tested for Enterprise

Network Server Information	
Server Type	**Version**
Microsoft AD, DHCP, DNS, TFTP and FTP Services	Windows 2003 SE/SP1 Server
Microsoft CA Services	Windows 2000/SP4 Server
Cisco ACS Radius Server	4.2 (on Windows 2003 SE/SP1 Server)
Cisco ACS Appliance Server	5.0 appliance 5.2.0.26
Cisco Unified Call Manager (CUCM)	8.0.3
Cisco Prime Infrastructure	1.3.1
Cisco IPTV Server	3.5.7.1 (on Windows 2000/SP4 Server)
Linux RH SYSLOG Server	Linux RH Enterprise AS4
Linux RH NTP Server	Linux RH Enterprise AS4
Spectralink SVP-100 Server	173.028/174.028/175.028 (SCCP)

Table 26 Application Software Products Tested for Enterprise

Application Software Information	
Application	**Version**
IPTV scheduled and on demand	v3.4
V-brick media appliance	V2.0.0b

Table 27 Voice Client Devices Tested for Enterprise

Voice Client Information	
Device	**Version**
Cisco 7920 Phone	3.0.2
Cisco 7921 Phone	1.4.2

Voice Client Information	
Device	**Version**
Cisco IP Communicator	2.1.1

Table 27 Laptop Client Devices Tested for Enterprise

Laptop Client Information			
Device	**OS**	**Chipset**	**Driver**
Acer Aspire 3623WXCi	WinXP/SP2	Atheros AR5005G	4.0.0.14001
Acer Aspire 3624WXMi	WinXP/SP2	Atheros AR5005G	5.3.0.35
Acer Aspire 5610-4537	Vista/HP	Intel 3945ABG	13.4.0139
HP Probook 4710s	WinXP/SP2	Intel 5100 AGN	14.3.2.1
Toshiba Satellite A105	WinXP/SP2	Intel 3945ABG	13.4.0.139
Toshiba Satellite A135	Vista/HP	Intel 3945ABG	13.4.0.139
Toshiba Tecra 8000	WinXP/SP2	Cisco CB21ABG	4.5.0.310
HP 6530b	WinXP/SP2	Intel 5100 AGN	14.3.0.6
Toshiba U205	Vista/HP	Intel 3956ABG	13.4.0.139
Compaq 5201US	Microsoft Vista	Broadcom802.11BG	4.10.40.1
HP Compaq nx9420	Microsoft Vista	Intel 3945ABG	13.4.0.139
Lenovo T60 ThinkPad	Microsoft Vista	Intel 3945ABG	13.4.0.139
Lenovo T61 ThinkPad	Microsoft XP	Intel 4965ABG	15.1.1.1
Lenovo X60s ThinkPad	Microsoft XP	Intel 3945ABG	13.4.0.139
Lenovo 3000 N100	Microsoft Vista	Broadcom802.11B	4.102.15.56
Fujitsu Lifebook A-Series	Microsoft Vista	Broadcom802.11BG	7.1.0.90
Lenovo W510 ThinkPad	Windows 7	Intel 6300 N	15.1.1.1

Table 28 Supplicant Devices Tested for Enterprise

Supplicant Information	
Device	**Version**
Cisco Secure Services Client	4.2, 5.0.1
Intel ProSet	13.5.0, 14.2, 15.1.1
Cisco Aironet Desktop Utility	4.5.0.88
Microsoft Windows ZeroConfig	Windows XP Pro, Vista

AssureWave Test Summary and Recommendation

Test Summary

The AssureWave certification for this release is **Pass**.

Please refer to the 7.4.110.0 Release Notes for additional information pertaining to this release. Carefully review the Open Caveats list below to make a determination if any of these issues may affect your installation

We summarize our testing results into three categories:

- Pass—The underlying assumption for certifying and publishing a Cisco AssureWave release is that testing passed because all individual tests passed. Failure of any test has to be properly resolved or closed, or the Cisco AssureWave engineering team must determine that the defect that caused failure will not affect network performance.
- Fail—If a given test fails and the effect on Cisco's customer base is deemed broad enough, the entire release fails. Failed releases are neither certified nor documented. If a test fails and the effect on the customer base is determined to be minor, the release may still be certified, with Distributed Defect Tracking System entries noted so that customers can review the testing to see if they are affected.

Open Caveats

This release contains the following significant open caveats

For the entire list please review the release notes

http://www.cisco.com/en/US/docs/wireless/controller/release/notes/crn74mr01.pdf

- **CSCud47264 Symptom: Controller web GUI displays duplicate domain IP names, but the controller CLI displays them correctly. Use CLI**
  - **Condition**: When the service provider domain name is more than 32 characters, the controller web GUI displays duplicate entries. This issue occurs in only the controller web GUI.
  - **Workaround**: Use controller CLI.
- **CSCud48620 Symptom: On a channel with high utilization and interference numbers, the RRM DCA algorithm might not change the channel when it should.**
  - As a result, the channel assignment for a few access points may be suboptimal, which can negatively impact performance.
  - **Condition**: If a channel change that is required to avoid the high utilization or interference has an adverse effect on the RF neighborhood, it might prevent the channel change. Release 6.0.182.0.
  - **Workaround**: Configure DCA back to aggressive mode.
- **CSCue50917 Symptom: When a RAP loses its wired connection, the RAP fails to restore connectivity as a MAP through the radio backhaul.**
  - The mesh adjacency is correctly built to a nearby MAP, and the RAP gets an IP address and can even join its controller, but shortly afterwards a radio reset is observed which causes the RAP to disconnect. The

RAP goes into a loop till the wired connectivity is restored. Error messages similar to the following are displayed on the RAP console:

- Feb 8 19:37:54.919: %CAPWAP-3-ERRORLOG: Selected MWAR '5500-5'(index 0).
- *Feb 8 19:37:54.919: %CAPWAP-3-ERRORLOG: Go join a capwap controller ~
- *Feb 8 19:37:45.139: %CAPWAP-5-JOINEDCONTROLLER: AP has joined controller
- 5500-5 ~ *Feb 8 19:37:45.183: %MESH-6-ADJ_VIDB_LINK: Mesh neighbor
- 0021.a1f9.fa0f VIDB Virtual-Dot11Radio0 forwarding ~ *Feb 8 19:37:46.075:
- %LINK-6-UPDOWN: Interface Dot11Radio1, changed state to down *Feb 8
- 19:37:46.083: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
- reset ~ *Feb 8 19:37:47.075: %LINEPROTO-5-UPDOWN: Line protocol on
- Interface Dot11Radio1, changed state to down *Feb 8 19:37:47.099:
- %DOT11-6-DFS_SCAN_START: DFS: Scanning frequency 5700 MHz for 60 seconds.
- ~ *Feb 8 19:38:21.751: %MESH-4-NO_POTENTIAL_PARENT: There are no potential
- parents *Feb 8 19:38:24.751: %MESH-4-NO_POTENTIAL_PARENT: There are no
- potential parents *Feb 8 19:38:24.751: %MESH-6-LINK_UPDOWN: Mesh station
- 0021.a1f9.fa0f link Down *Feb 8 19:38:24.951: %MESH-6-ADJ_VIDB_LINK: Mesh
- neighbor 0021.a1f9.fa0f VIDB Virtual-Dot11Radio0 going down *Feb 8
- 19:38:24.955: %LINK-6-UPDOWN: Interface Virtual-Dot11Radio0, changed state
- to down10 *Feb 8 19:38:25.955: %LINEPROTO-5-UPDOWN: Line protocol on
- Interface Virtual-Dot11Radio0, changed state to down
- **Condition**: Mesh deployment on the following controller software releases: 7.0.230.0, 7.2.x, 7.3.112.0
- **Workaround**: None.

- **CSCud64396 Symptom: The controller might stop working if a Syslog server entry is being removed from the GUI when the server is unreachable.**
  - **Condition**: Syslog server configured on the controller with TLS enabled. The Syslog server entry is removed using the controller GUI while it is unreachable, but the controller still considers it to be “connected”, as per “TLS auth status” that can be seen by entering the show logging command on the controller CLI.
  - **Workaround**: None.

- **CSCud80390 Symptom: MAC flap on Layer 2 switch connected to the remote LAN port of Cisco 600 Series OEAP.**
  - **Condition**: Wired computers plugged into the Layer 2 switch connected to the remote LAN port communicate with each other with only pings.
  - **Workaround**: Configure static ARP entries to prevent the MAC flap.

- **CSCud86140 Symptom: AP intermittently does not send probe response when there are other APs in the neighborhood on the same channel.**
  - **Condition**: There need to be other APs or traffic on the same channel for this issue to occur.
  - **Workaround**: If the client hears probes from other surrounding APs, the client should be able to join another AP. Some NICs might prefer to hear probes from a specific AP. Even with the AP having the issue, eventually, the probe response might be transmitted after a few attempts.

- **CSCud89654 Symptom: On a local-switching-enabled 802.1X WLAN, if the clients associate with a local AP (not FlexConnect AP), after successful authentication, only url-redirect attributed is accepted by the controller, not url-redirect-acl attribute, which causes failures on redirection thereafter.**
  - **Condition**: 802.1X WLAN with local switching enabled; Release 7.2 and later.
  - **Workaround**: Disable local switching on the WLAN. You will have to segregate the local AP from FlexConnect APs on different controllers, making it an impossible solution to mix them together on a single controller.

- **CSCud97325 Symptom: Cisco AP3600 and Cisco AP2600 send invalid frames sourced with address 0000.0104.xxxx.**
  - This might result in security warnings on the switch, such as the following: %AUTHMGR-5-SECURITY_VIOLATION: Security violation on the interface GigabitEthernet3/46, new MAC address (0000.0104.d634) is seen.
  - **Condition**: This issue occurs when the primary or secondary controller is changed in the AP High Availability tab. This issue is observed with only Cisco Aironet 2600 and 3600 Series access points.
  - **Workaround**: None.

- **CSCue02826 Symptom: The 5-GHz radio on AIR-CAP1552E-N-K9 in the non-Bridge mode fails to enable if the controller is configured for Brazil (-T) Regulatory Domain.**
  - **Condition**: Release 7.3.101.0.
  - **Workaround**: Use the Bridge mode in the AP.

- **CSCue18790 Symptom: Cisco AP1600, Cisco AP2600, and Cisco AP3600 might transmit management and control frames at maximum power, regardless of the configured power settings.**
  - **Condition**: Cisco AP1600, Cisco AP2600, and Cisco AP3600.
  - **Workaround**: None.

- **CSCue32755 Symptom: Wireless clients are unable to associate with the mesh APs.**
  - **Condition**: When the wired clients are not operational; clients are connected to the mesh AP with Ethernet bridging enabled.
  - **Workaround**: Reboot the mesh AP for the wired and wireless clients to associate.

- **CSCue42242 Symptom: When the controller detects more than 21 ad hoc rogues, the controller GUI shows only the first 20 entries (first page).**
  - **Condition**: More than 21 ad hoc rogues detected.
  - On the controller GUI, choose Monitor > Rogue > Adhoc Rogues and click on Unclassified Adhoc or Custom Adhoc.
  - The first page shows correctly, but it is not possible to browse to the subsequent pages.
  - **Workaround**: On the controller CLI, enter the show rogue adhoc summary command.

- **CSCue55153 Symptom: Controller stops communicating with CAM with SNMPv3.**
  - **Condition**:
  - Enable HA.
  - Add controller to CAM with SNMPv3 (should have an authorization and authentication passwords)
  - Failover from primary to secondary controller.
  - **Workaround**: Delete and add the controller in CAM again.

- **CSCuf35269 Symptom: The 802.11u domain is lost after a controller reboot.**
  - **Condition**: Same domain name is used on two different WLANs. This is allowed on CLI, but configuration validation fails on boot.
  - **Workaround**: Reconfigure the domain, or use different domain names.

- **CSCuf74326 Symptom: Cisco Virtual Wireless Controller is given a valid license with an AP count.**
  - Installation of the controller is successful, and the show license summary command shows the license in use with the correct count. However, the homepage of the controller GUI shows “0 access points supported” and APs are denied association with the controller.
  - **Condition**: This issue occurs only when you provide a license file that contains only adder licenses and not the base feature.
  - **Workaround**: Request for a correct base feature AP count license file.

- **CSCug27084 Symptom: The standby controller in an HA pair could reboot in a loop if the HA role negotiation succeeds, but the configuration synchronization fails.**
  - **Condition**: Low memory **Condition** on the controller.
  - **Workaround**: Reboot the primary controller.

- **CSCug46616 Symptom: RRM group leader is not operational and does not do channel or power update.**
  - **Condition**: This issue might occur if you have APs hearing each other when associated through a large set of controllers where RF group name is identical.
  - **Workaround**: Options are as follows:
    - Limit the RF group size to 1000 APs. Place the APs accordingly and avoid salt and pepper deployment.
    - If you already are in this state, you can restart the group leader election by entering these commands:
  - config advanced 802.11a group-mode restart (If RRM is in the 802.11a band)
  - config advanced 802.11b group-mode restart (If RRM is in the 802.11b band)

- **CSCug49505 Symptom: Cisco AP3500 stops working.**

  - **Condition**: LWAPP Rogue Monitoring process is on.
  - **Workaround**: None.

- **CSCug53945 Symptom: After a Cisco AP reboot, the radio which was disabled before Cisco AP reboot is somehow reenabled automatically. This occurs when the Cisco AP belongs to an RF profile.**
  - **Condition**: Cisco AP joins nondefault AP group and the AP group has the RF profile.
  - **Workaround**: Disable radio on AP again after the reboot.

- **CSCug59937 Symptom: Controller reboot with traceback tpcv2ConstructApProfile.**
  - **Condition**: TPCv2 in an enabled state.
  - **Workaround**: None.

- **CSCug82976 Symptom: Cisco APs that are configured with submode PPPoE are losing the submode configuration (Submode = Unconfigured) after moving from one controller to another or after rebooting the Cisco AP when associating with the second controller.**
  - **Condition**: Reboot the PPPoE submode Cisco AP associated with the primary controller.
  - **Workaround**: None.

- **CSCuh05276 Symptom: Controller might trigger a reaper reset crash at "apfFindRogueApEntry" while adding rogue rules on the controller, due to a deadlock**
  - **Condition**: Adding rogue rules on the controller.
  - **Workaround**: None.

- **CSCuh14797 Symptom: In Export Anchor-Foreign scenario, in both Foreign to Foreign as well as fresh association to a Foreign, if packets are not reaching to Export Anchor due to network issues, then after three retries, there will not be any further exchange. The request will go to Export Anchor and the client will stay in that state until it moves out.**
  - **Condition**: Network issues between mobility peers.
  - **Workaround**: None. Instead, fix the underlying connectivity issues.

- **CSCuh26964 Symptom: During dynamic rf-group, an HA switchover controller stopped working.**
  - **Condition**: While running dynamic rf-group between an HA Cisco WiSM2 controller and Cisco 5500 Series standalone controller, enter the show advanced 802.11a group command in the standalone controller CLI. On a forced switchover, the standby controller stopped working.
  - **Workaround**: None.

- **CSCuh89626 Symptom: Client displays the following message: "Ignoring 802.11 assoc request from mobile radio is NOT enabled"**
  - **Condition**: Cisco AP is operational, but the controller shows the Cisco AP as nonoperational.
  - **Workaround**: Disable the Cisco AP and then reenable it.
  - More Information: This issue is only observed after three or more days of continuously disabling and then enabling the radio state every minute on internal testing.

- **CSCui25877 Symptom: Radio PCI resets are observed on Cisco AP1600.**
  - **Condition**: PCI resets on Cisco AP1600 with high load.
  - **Workaround**: None.

- **CSCui32908 Symptom: A Cisco AP stopped working and then rebooted.**
  - **Condition**: Unknown.
  - **Workaround**: Unknown. Check any CDP events on the connected switch.

- **CSCug90218 Symptom: In the controller GUI, access points appear in an unknown state.**
  - **Condition**: Unknown.
  - **Workaround**: Reboot the controller.

- **CSCug92421 Symptom: Controller reports many stale client entries.**
  - **Condition**: Cisco Flex 7500 Series Wireless Controllers with Release 7.3.103.14 having many clients.
  - **Workaround**: None.

- **CSCug98625 Symptom: WebAuth redirect fails when local switching is enabled on a WLAN. Manual redirect and redirect with central switching works.**
  - **Condition**: Local switching is enabled on a WLAN.
  - **Workaround**: Add a dummy interface on the controller with the IP address of the VLAN that is locally switched for the client. The VLAN IDs need not be the same, however, the IP addresses must be same. The VLAN must be trunked to the controller.

- **CSCuh10735 Symptom: RADIUS failover occurs when the controller sends RADIUS request packets with the same ID to the RADIUS server six times and receives no response from the RADIUS server.**
  - **Condition**: Release 7.3.112.0.
  - **Workaround**: None.

- **CSCuh16539 Symptom: When you disable the radio of a Cisco AP2600, the radio gets enabled after the access point reloads.**
  - **Condition**: Release 7.4.x
  - **Workaround**: None.
- **CSCuh16842 Symptom: Client gets IPv6 address from a different VLAN.**
- A sample message is given below:
- Overriding interface of client from 'vlan20' to 'vlan30' within interface group 'vlan20-30'
  - **Condition**:
  - VLAN is in an interface group.
  - Client sends traffic from either a static IP address or a previously allocated IP address.
  - Client traffic does not match the assigned VLAN.
  - **Workaround**: Use DHCP required.

- **CSCuh20357 Symptom: Cisco Services-Ready Engine (SRE) controller configured as a DHCP server shows reversed octet for the default gateway and DNS server values. For example, 4.3.2.1 instead of 1.2.3.4.**
  - **Condition**: Cisco Wireless Controller on Cisco SRE using Release 7.4.x.
  - **Workaround**: Use an external DHCP server or downgrade the controller to a release that is earlier than Release 7.4.x.

- CSCuh20715 **Symptom**: Cisco 5508 controller with Release 7.3.101.0 stopped working on Reaper Reset: Task "LDAP DB Task 2" missed software watchdog .
  - **Condition**: Unknown.
  - **Workaround**: None.

- CSCuh25790 **Symptom**: In an HA-enabled 5508 controller with 430 access points, when you perform predownload on all the access points, the controller does not reset.
  - **Condition**: High AP count and failed predownlaod.
  - **Workaround**: Reboot the controller using the reset system forced command.

- CSCuh28190 **Symptom**: AP stopped working once and the log was found on the controller and TFTP server.
  - **Condition**: Unknown.
  - **Workaround**: None. Access point resets on its own.

- **CSCuh31410 Symptom: Access point radio resets during the FlexConnect state change.**
  - **Condition**: Restore access point connectivity to controller.
  - **Workaround**: None.

- **CSCuh39893 Symptom: Controller on Release 7.3 or 7.4 fails to authenticate the One Time Password (OTP) users authenticating with TACACS+. The following debug output is displayed when you use the debug aaa tacacs enable command:**
  - TPLUS_AUTHEN_STATUS_GETPASS
  - auth_cont get_pass reply: pkt_length=25
  - processTplusAuthResponse: Continue auth transaction
  - No auth response from: <SERVER IP>, retrying with next server
  - Preparing message for retransmit. Decrypting first

- Forwarding request to <SERVER IP> port=4900
- AUTH Socket closed underneath
- No auth response from: <SERVER IP>, retrying with next server
- Preparing message for retransmit. Decrypting first
- Forwarding request to <SERVER IP> port=4900
- AUTH Socket closed underneath Exhausted all available servers for Auth/Author packet
- **Condition**: This issue occurs in the following **Condition**:
- Controller uses Release 7.3 or 7.4.
- TACACS+ is used for management user authentication.
- OTP is used for TACACS+. Static passwords are not affected.
- **Workaround**:
- Extend the TACACS+ management server timeout value by using the following commands:
- config tacacs auth disable server-index
- config tacacs auth mgmt-server-timeout server-index 10
- config tacacs auth enable server-index

- **CSCuh44119 Symptom: Cisco 8510 controller does not update the config line after disabling DHCP proxy using the config dhcp proxy disable bootp-broadcast disable command.**
  - **Condition**: Release 7.4.100.60.
  - **Workaround**: Manually enter the line in the config file or modify the configuration directly on the controller using the CLI or the GUI.

- **CSCuh46996 Symptom: Wired clients behind a third party WGB device fail to get an IP address.**
- **Condition**:
  - Third party bridge associates to an access point in H-REAP (FlexConnect) local switching mode.
  - Controller is using release higher than Release 7.0.116.0.
  - **Workaround**: None.

- **CSCuh49135 Symptom: Beacon loss in Cisco AP1130.**
  - **Condition**: Cisco AP1130 in FlexConnect mode.
  - **Workaround**: None.

- **CSCue51838 Symptom: Flash is not accessible for Cisco AP1520 or Cisco AP1550.**
  - **Condition :** The APs will continuously write the following flash error to the console: Write of the Private File nvram:/lwapp_ap.cfg Failed *Feb 8 15:10:34.947:
  - %LWAPP-3-CLIENTERRORLOG: Save LWAPP Config: error saving config file *Feb 8 15:10:35.115: Write of the Private File nvram:/lwapp_ap.cfg Failed *Feb 8 15:10:35.119: %LWAPP-3-CLIENTERRORLOG: Save LWAPP Config: error saving config file *Feb 8 15:10:40.211: and can generate one of these two error messages, when a "dir" command is done: opening flash:/ (Invalid argument) opening flash:/ (Device or resource busy)
  - **Workaround**: Reboot the Cisco AP.

- **CSCuf03454 Symptom: Controller fails intermittently.**
  - **Condition**: Web pass through clients anchored from foreign controller to anchor controller.
  - **Workaround**: Reboot the controller.

- **CSCuf08099 Symptom: New AP801 on C1941, cannot enable the radios. T**
- he radios gets reset continuously, and IOS shows 802.11 driver process using 99 percent CPU. Reloading the AP or router does not change.
  - **Condition**: This occurs when AP801 joins controller using Release 7.4.x.
  - **Workaround**: None.

- **CSCuf60628 Symptom: When AP which is in FlexConnect local switching mode, fails over from primary controller to secondary controller, the client protocol displays 802.11b, instead of 802.11g.**
  - **Condition**: This occurs in controller 7.3.112.0.
  - **Workaround**: None.

- **CSCuf61599 Symptom: Clients are unable to join.**
  - **Condition**: This occurs in controller 7.3 5500 with FlexConnect and NAT/PAT AP IP.

- **Workaround**: Enable data encryption.

- **CSCug19563 Symptom: WiSM2 secondary controller DP stops responding due to deadlock in HA configuration while it gets booted and synchronizes with the primary controller.**
  - **Condition**: This occurs rarely when there are multiple reboot of controller in HA configuration. The controller recovers after reboot.
  - **Workaround**: None.

- **CSCug27515 Symptom: Clients on 802.11n rates gets disconnected or experiences data transfer issues when certain segment number orders are used.**
  - **Condition**: When client leading segment number is lower than the window (lower order).
  - **Workaround**: For Apple devices, disable AQM in the Apple wireless driver. Disable A-MPDU. Also refer CSCug65693 for Workaround.

- **CSCug32970 Symptom: Memory leak in EAP.**
  - **Condition**: This issue occurs during excessive mesh AP Authentication.
  - **Workaround**: None.

- **CSCug38794 Symptom: WiSM2 stops responding and reboots (bcastReceiveTask 1332).**
  - **Condition**: Unknown.
  - **Workaround**: None.

- **CSCug53680 Symptom: AP stops responding due to unexpected exception to CPUvector.**
  - **Condition**: There is no outstanding trigger.
  - **Workaround**: None.

- **CSCug57216 Symptom: Ascom phone stops receiving voice packets.**
  - **Condition:** 11n in use Voice traffic QoS markings are lost on downstream direction.
  - **Workaround:** Either fix QoS markings or disable 11n.

- **CSCug89084 Symptom: Clean Air sensor goes down and requires a reboot.**
  - **Condition**: First found on monitor mode APs.
  - **Workaround**: Reboot the AP.

- **CSCuc02814 Symptom: When broadcast SSD is disabled, the client is unable to associate with the controller.**
  - **Condition**: Disable the broadcast SSID in controller. A client is unable to associate.
  - **Workaround**: A non-Cisco client is able to associate.

- **CSCuc45005 Symptom: Controller stops working while running controller release 7.3.101.0.**
  - **Condition**: Unknown.
  - **Workaround**: None

- **CSCuc51315 Symptom: Controllers stops working if you clear the AP join statistics.**
  - **Condition**: This problem occurs only when you clear the AP join statistics (Monitor > Statistics > AP join Statistics > Clear)
  - **Workaround**: None

- **CSCuc65606 Symptom: Cisco 4400 Controller stops working in spamreceive in release 7.0.235.3**
  - **Condition**: None.
  - **Workaround**: None.

- **CSCuc70159 Symptom: Autonomous AP running software version 15.2 loses clock information after reboot.**
  - **Condition**: Autonomous AP running software version 15.2. Clock information is lost even when “clock save interval” is configured. This is important for WGB situations where the AP must use certificate-based authentication (EAP-TLS, PEAP), and the certificate validation fails the time check.
  - **Workaround**: Perform the following:
  - Manually configure the clock after an AP reboot.
  - Configure SNTP for applications where AP is not operating as WGB with
  - certificate-based authentication by entering this command on the AP console:

- ap(config)#sntp server a.b.c.d {version 1|2|3}

- **CSCuc93681 Symptom: Controller intermittently stops working.**
  - **Condition**: Any controller running software versions from 7.0 through 7.4.
  - **Workaround**: None.

- **CSCuc98178 Symptom: If you remove the HSRP configuration, it leads the CAPWAP APs to keep sending data traffic to the old HSRP MAC while the control traffic is sent to the new correct gateway MAC.**
  - **Condition**: Cisco AP3500 and HSRP gateway.
  - **Workaround**: Reboot AP.

- **CSCud16495 Symptom: Cisco Flex 7510 Series Wireless LAN Controller stops working when it is part of a HA pair. After this, the controller reloads and becomes active.**
  - **Condition**: Controller is part of an HA pair.
  - **Workaround**: None.

- **CSCud37443 Symptom: Clients are able to connect in b/g band even though Radio Policy for a SSID specifically set to "a only".**
  - **Condition**: Create a WLAN with radio policy set to "a only" Configure the phones/clients in b/g mode and they successfully connect.
  - **Workaround**: None.

- **CSCud41334 Symptom: The Ethernet bridged client of Mesh AP (MAP) does not work.**
  - **Condition**: If the Ethernet bridged client (for example, a PC) has been plugged into the Ethernet port of a MAP before MAP joins the controller, then the client will not work. The issue is seen on a AP1140, AP3500 and AP3600 (all indoor mesh APs). The issue is not seen on AP1552 (outdoor mesh AP).
  - **Workaround**: Ensure that the bridged client is not plugged into the MAP Ethernet port, and then reload the MAP. Let MAP join the controller before plugging the client into the MAP Ethernet port. The client gets a valid IP address and should respond to pings.

- **CSCuh55653 Symptom: AIR-CT5508-K9 unexpected reboot happens in Cisco controller 7.4.x software version with "apfMsConnTask_5" task suspended.**
  - **Condition**: Crash happens under normal **Condition** without any changes in hardware or software configuration or network topology.
  - **Workaround**: None.

- **CSCuh56264 Symptom: Client disassociated from fast transition roam due to key failure. This issue occurs only when both PMF and FT are supported.**
  - **Condition**: Client has negotiated both PMF and FT capabilities with the access point.
  - **Workaround**: Disable PMF or FT.

- **CSCuh65005 Symptom: When the client is not authenticated by RSA/RADIUS server using webauth, Cisco controller places the client in RUN state. This issue is caused by the usage of two factor authentication.**
  - **Condition**: Unknown.
  - **Workaround**: Non-usage of two factor authentication. Cisco controller does not support two factor authentication.

- **CSCuh71233 Symptom: The 3600 AP running in FlexConnect mode stops working with the following decode:**
  - Pid 65: Process "CAPWAP 802.11 MAC Management Reception " stack 0x87AFC14
  - savedsp 0x5516CE4 Flags: analyze prefers_new wakeup_posted Status 0x00000000 Orig_ra 0x00000000 Routine 0x0287B380 Signal 0 Caller_pc 0x00000000 Callee_pc 0x00000000 Dbg_events 0x00000000 State 0 Totmalloc 6733804 Totfree 2192816 Totgetbuf 119844 Totretbuf 0 Edisms 0x0 Eparm 0x0 Elapsed 0x17598 Ncalls 0x5CD019 Ngiveups 0x0 Priority_q 4 Ticks_5s 3 Cpu_5sec 0 Cpu_1min 6 Cpu_5min 0 Stacksize 0xEA60 Lowstack 0xEA60 Ttyptr 0x54ED758 Mem_holding 0x61E3C Thrash_count 0 Wakeup_reasons 0x0FFFFFFF Default_wakeup_reasons 0x0FFFFFFF Direct_wakeup_major 0x00000000 Direct_wakeup_minor 0x00000000 Regs R14-R31, CR, PC, MSR at last suspend; R3 from proc creation, PC unused: R3 : 00000000 R14: 05350000 R15: 05350000 R16: 05350000 R17: 04230000 R18:

04230000 R19: 04090000 R20: 04DD0000 R21: 04DD0000 R22: 04DD0000 R23: 087BE138 R24: 087BE128 R25: 087BE130 R26: 087BE0B8 R27: 00029200 R28: 00000000
  - R29: 00000000 R30: 04460000 R31: 00000005 CR: 28004042 PC : 022A04FC MSR: 00029200
  - **Condition**: Unknown.
  - **Workaround**: None.

- **CSCuh86976 Symptom: Cisco NCS SNMP polling hangs as Cisco controller hangs while performing a SNMPwalk on the bsnMeshNeighsTable table for the Cisco controller 6.0.199.4.**
  - **Condition**: SNMPwalkon bsnMeshNeighsTable.
  - **Workaround**: None.

- **CSCuh87571 Symptom: Image upgrade fails in a high availability environment even when the standby is up and running. The standby HOT does not display any image download activity.**
  - **Condition**: Occurs on AP 5508/Wism2 high availability environment.
  - **Workaround**: Reset the system and retry the image download.

- **CSCuh94366 Symptom: Clients are unable to connect to receive DHCP information post upgrade.**
  - **Condition**: Usage of mDNS gateway on interface group.
  - **Workaround**: Usage of other VLANs.

- **CSCui02779 Symptom: Cisco OEAP fails to connect when a failover occurs from LDPE to Non LDPE controller when in a high availability setup.**
  - **Condition**: Unknown.
  - **Workaround**: None.

- **CSCui05324 Symptom: Clients are unable to associate to the access point radio.**
  - The access point continues to beacon, but when the client sends an 802.11 authentication frame, the access point fails to respond with an authentication response. This issue occurs when the use of the current transmit queues is equal to the limit - the radio is unable to transmit.
  - **Condition**: Unknown.
  - **Workaround**: You must perform the following **Workaround**:
  - Write a script that goes out to each access point and monitors the usage of the
  - radio transmit queues. If a radio is found whose transmit queue utilization is
  - nearing its limit, then issue the following command:
  - clear interface <interfacename>
  - Manually reset the AP's impacted radio.

- **CSCsy66246 Symptom: An 802.11n AP does not downshift rates for retries when low latency MAC is enabled.**
  - The AP sends three retransmissions but the data rate for retransmissions is
  - the same as the data rate at which the initial packet was sent.
  - **Condition**: Using an 802.11n AP with low latency MAC enabled.
  - **Workaround**: Do not enable low latency MAC.

- **CSCty84682 Symptom: AP is not forwarding Multicast data and IGMP querier messages.**
  - **Condition**: Upon fresh reload of an AP.
  - **Workaround**: Perform shut or no shut on the WLAN.

- **CSCub87374 Symptom: APs may not be able to join controller (with release 7.2 or 7.4) and the controller indicates the limit for maximum APs supported is reached.**
  - **Condition**: Controller indicates the limit for maximum APs supported is reached when it has not been reached as indicated in the show license capacity command.
  - **Workaround**: Reboot the controller with evaluation license.

- **CSCuc80103 Symptom: WiSM2 is unreachable and unable to ping. All APs are dropped from the controller, and unable to ping the Management interface's gateway (through console) at the time of failure. Failure**
  - **Condition** will recover on it's own typically within minutes.

- **CSCud57784 Symptom: In the Cisco 5508 Series Wireless Controller, when the MAC Filtering authentication is enabled from the GUI using the following procedure, client authentication fails.**
  - Choose Security > AAA > RADIUS > Authentication to open the RADIUS

- Authentication page. Define more than one RADISU servers.
- Choose Security > AAA > MAC Filtering and set the RADIUS Compatibility
- Mode as Free RADIUS.
- In the WLAN setting, select the MAC Filtering check box, select the
- Authentication server that you have selected. The index number of the server is 1.
- Choose Security > AAA > RADIUS > Authentication. Delete the Radius server
- which has index number 1.
- In the WLAN setting, select Authentication server which has index number other
- than 1.
- **Condition**: None specified.
- **Workaround**: From the WLAN controller GUI, choose Security > AAA > RADIUS > Authentication, and define a dummy radius server which has index 1.

- **CSCui18377 Symptom: Cisco Aironet 1242 Access Point generates tracebacks and coredump after the controller upgrades to 7.4.100.60. Additionally, the radios also reset as shown in the log below:**
  - Jul 10 06:02:54.569: %SYS-2-BADSHARE: Bad refcount in datagram_done, >
  - ptr=125F318, count=0 -Traceback= <HEX Tracebacks>
  - **Condition**: The Cisco Aironet 1242 Access Point generates tracebacks and
  - coredumps when upgraded to the Cisco WLC software version 7.4.100.60
  - **Workaround**: None.

- CSCui22463 **Symptom**: Cisco WLC fails to respond when software version 7.4.103.6 is used.
  - **Condition**: The Cisco WLC fails to respond when mDNS snooping enabled on software version 7.4.103.6.
  - **Workaround**: Disable mDNS snooping.

- **CSCui23134 Symptom: Cisco WLC fails to respond with the task spamPacketDumpHandleIntraRoamCase**
  - **Condition**: The Cisco WLC fails to respond when the ap packet-dump command is used.
  - **Workaround**: Do not use ap packet-dump feature.

- **CSCue26844 Symptom: Cisco WLC controller fails to respond and resets the spectrumNMSPTask**
  - **Condition**: Cisco WLC fails to respond under normal condition : unknown.
  - **Workaround**: None.

- **CSCtw92430 Symptom: In an HA scenario, when the default management gateway is broken, the standby or active controller goes into maintenance mode and never comes out of that mode even after the connection is restored.**
  - **Condition**:
  - Configure an HA pair and configure a standby and active controller.
  - Shut down the management default gateway and ensure that one controller goes
  - into maintenance mode after a reboot.
  - After some time, restore the management gateway connection and try to make the
  - controller in maintenance mode come back to the corresponding mode after the
  - connection is restored.
  - The controller always remains in the maintenance mode until a manual reboot is
  - performed and the status is shown to be in negotiation.
  - **Workaround**: Perform a manual reboot of the controller.

- CSCuc72493 **Symptom**: The APs disjoin after the switchover if the Cisco 8500 WLC has 6000 APs and 64000 clients on the full load.
  - **Condition**: This happens when the Cisco 8500 controller is fully loaded.
  - **Workaround**: None.

Caveats resolved after release of 7.4.110.0

These are additional open caveats that were resolved via an engineering special. If you are impacted by any of these issues, please contact Cisco TAC on how to obtain the special.

- CSCug53945 disabled radio is enabled after AP reload when AP group uses RF profile
- CSCuh72474 Interface inside a group gets Dirty due to DHCP flood by client and NAK
- CSCui20773 Bcast queue is full -"RX Multicast Queue Full"
- CSCui58670 WLC sends M5 key with protected flag = 0 for a 802.11r SSID after a roam
- CSCui59553 Provide command to disable/customize dead GW detection for HA