

[]

APPLICATION NOTE

VoWiFi & WLAN Infrastructure (IEEE 802.11)

Ascom i62

Cisco WLC 2106 WLAN Controller, AP1140/1230/1240/1250

Version 6.0.196.0

Ascom, Gothenburg

June 2010



TABLE OF CONTENT:

SITE INFORMATION	3
SUMMARY	4
TEST RESULTS.....	6
Ascom WLAN Infrastructure Verification – VoWiFi.....	6
APPENDIX A: TEST CONFIGURATIONS	8
Cisco WLC 2106 Version 6.0.196.....	8
Security settings.....	8
General settings (QoS, Radio).....	11
Innovaphone IP6000 (IP PBX & DHCP server)	18
APPENDIX B: DETAILED TEST RECORDS	19

SITE INFORMATION

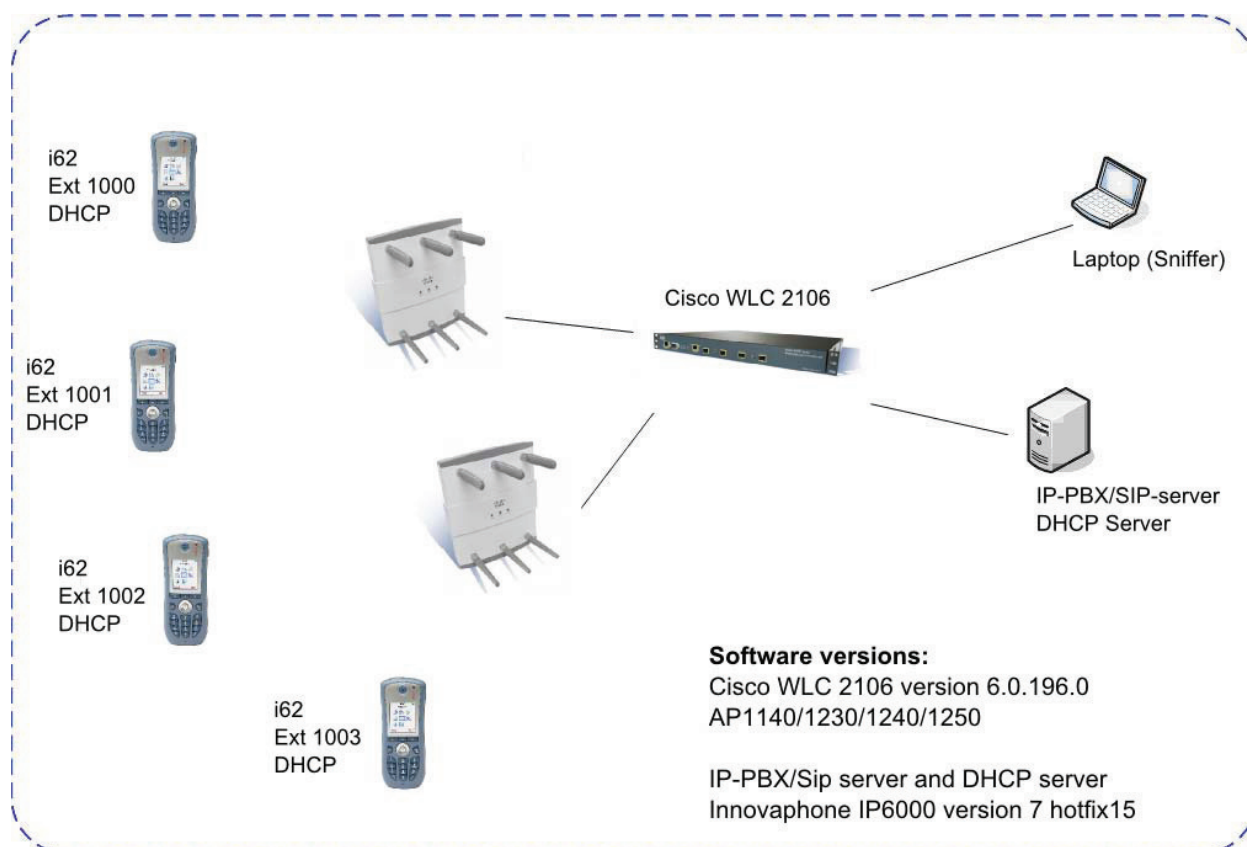
Test Site:

Ascom
Grimbodalen 2
P.O Box 87836
40276 Gothenburg
Sweden

Participants:

Karl-Magnus Olsson, Ascom HQ, Gothenburg

TEST TOPOLOGY



SUMMARY

Please refer to Appendix B for detailed results.

WLAN Controller Features

High Level Functionality	Result
Association, Open with No Encryption	OK
Association, Open with Static WEP64/128	OK
Association, WPA-PSK, TKIP	OK
Association, WPA2-PSK, TKIP / AES Encryption	OK
Association, LEAP Authentication	Not supported
Association, PEAP-MSCHAPv2 Auth., TKIP Encryption	OK
Association, PEAP-MSCHAPv2 Auth., AES Encryption	OK
Association, EAP-MD5 Authentication	OK
Association, Multiple ESSIDs	OK
Beacon Interval and DTIM Period	OK
Preauthentication	Not supported by controller
PMKSA Caching	OK
WPA2-opportunistic/proactive Key Caching	OK
WMM Prioritization	OK
Active Mode (load test)	Not tested *
802.11 Power-save mode	OK
802.11e U-APSD	OK
802.11e U-APSD (load test)	Not tested *

*) "Maximum number of calls" not tested.

Roaming

High Level Functionality	Result
Roaming, Open with No Encryption	OK (Avg roaming time 10ms) *
Roaming, Open with Static WEP64	OK (Avg roaming time 11ms)*
Roaming, WPA-PSK, TKIP Encryption	OK (Avg roaming time 28ms)*
Roaming, WPA2-PSK, AES Encryption	OK (Avg roaming time 32ms)*
Roaming, LEAP, WEP/TKIP Encryption (CCKM)	Not supported by controller
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption	OK (Avg roaming time 33ms)* *

*) Average roaming times are measured using 802.11a/n. In general the 802.11a roaming times were slightly better than using b/g speeds. Refer to the test protocol in Appendix B for details.

* *) Result with opportunistic key caching enabled. Without opportunistic key caching the result is in average 342ms

General Conclusions

Overall the outcome of interoperability verification, including association, authentication and roaming produced good results. Roaming times are in general fully acceptable with expected roaming time of 32ms when using WPA2-AES. When using PEAP-MSCHAPv2 the average roaming time was over 300ms.

In order to use 802.11n speeds and features WPA2 and AES-CCMP encryption must be used, either with PSK or using Radius server. Open encryption is also supported but is not recommended.

If U-APSD shall be used in the handset it is very important that the WMM parameters in the Cisco WLC are set correctly since U-APSD handles a bi-directional data stream where the up and downlink must be transmitted within the same EDCA Access Category.

To use U-APSD, make sure to set QoS to Platinum for the current WLAN profile and set WMM to Allowed. Also set EDCA profile for 802.11b/g to "Voice Optimized" and disable low latency MAC.

The tested Cisco WLAN Controllers are of model 2100 series which basically covers the complete Cisco range of WLAN controllers from an interoperability point of view.

- WLC 5500 is an up scaled WLC4400 which it eventually will replace.
- WISM is essentially two-4400 build in a cat6k card slot.
- 3750G is similar to WLC 4400 just a different form factor.

TEST RESULTS

Ascom WLAN Infrastructure Verification – VoWiFi

Software Versions:

- Cisco WLC 2106 V6.0.196.0
- AP1140/1230/1240/1250
- Ascom i62, v2.1.17

Signaling Protocol:

- SIP, Innovaphone IP6000 used as SIP server. Version 7 hotfix 15

Configuration of WLAN System:

- Beacon Interval: 100ms
- DTIM Period: 5
- 802.11b/g/(n)
- 802.11a
- WMM/ U-APSD Enabled
- 802.11d Regulatory Domain: World mode

Ascom i62 Configuration:

- World Mode Regulatory Domain set to World mode.
- IP DSCP for Voice: 0x2E (46) – Expedited Forwarding
- IP DSCP for Signaling: 0x1A (26) – Assured Forwarding 31
- Transmit Gratuitous ARP: Enable

Known Issue(s):

- AP 1140 and 1250 must be configured to 102ms beacon period if used in a mixed Cisco environment. Refer to configuration details in Appendix A.
- Cisco bug report CSCta29484. The AP will be seen to cease transmission of beacons for 10 second intervals. This will result in worst case end up in a lost WLAN connection

Keep in mind that security options and power save modes were adjusted according to requirements in individual test cases. Please refer to appendix A for information regarding device configuration.

Test Areas

Association and Authentication: 100% pass (13/13)

- Only security settings available through the web GUI were tested.
- LEAP authentication not yet supported by i62.
- FreeRadius was used in the test cases where an authentication server was needed.

Power Save: 100 % pass (3/3)

- Power save and U-APSD passed both when using 802.11a and 802.11b/g

QOS: 100% pass (1/1)

- WMM has to be enabled on controller.
- Loadtest done with iPerf. No noticeable degeneration of voice quality.

“Maximum Number of Calls”: 0% pass (0/0) Not tested

- Not tested

Roaming and Handover Times: 100% pass (6/6)

- LEAP authentication not supported.

Battery Lifetime: 100% Pass (3/3)

- > 100 hrs battery lifetime in idle mode (DTIM period = 5) *
- ~ 5 hrs battery lifetime with ongoing call in active mode *
- ~ 18 hrs battery lifetime with ongoing call in U-APSD mode *

*) Note that figures are “Up to” values which have been measured in a lab environment. There are a number of different variables that affects both standby time and talk time.

Stability: 100% Pass (1/1)

- Stable call for the duration of >24 hours in U-APSD mode.
- Call stability not tested in active mode.

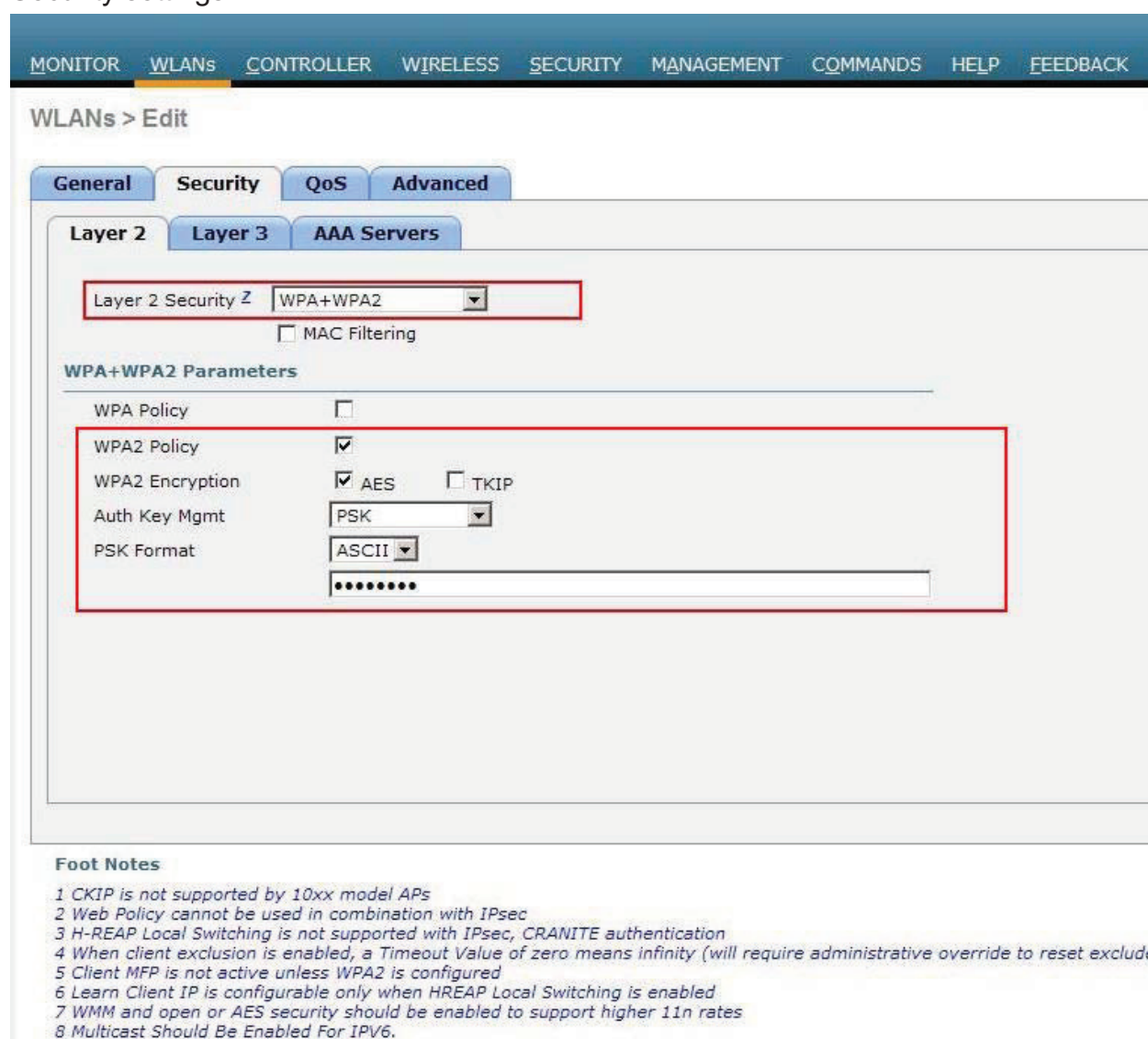
Please keep in mind that metrics do NOT account for untested cases.

APPENDIX A: TEST CONFIGURATIONS

Cisco WLC 2106 Version 6.0.196

In the following chapter you will find screenshots and explanations of basic settings in order to get a Cisco WLC WLAN system to operate with an Ascom i62. Please note that security settings were modified according to requirements in individual test cases.

Security settings



WLANs > Edit

General **Security** **QoS** **Advanced**

Layer 2 **Layer 3** **AAA Servers**

Layer 2 Security Z **WPA+WPA2**

☐ MAC Filtering

WPA+WPA2 Parameters

WPA Policy ☐

WPA2 Policy ☒

WPA2 Encryption ☒ AES ☐ TKIP

Auth Key Mgmt **PSK**

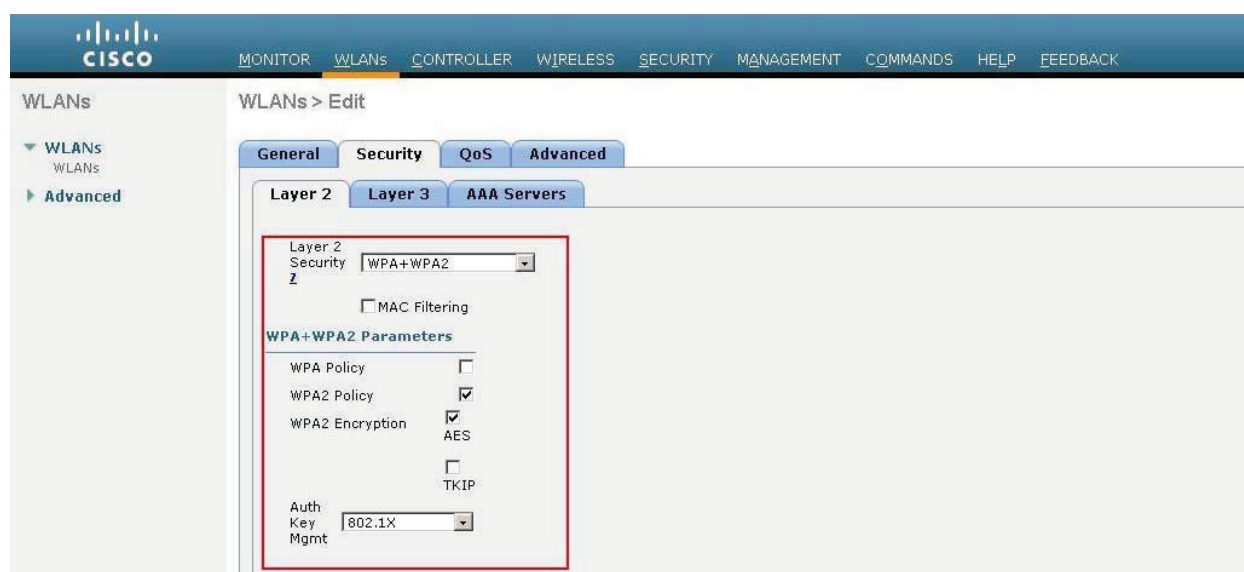
PSK Format **ASCII**

.....

Foot Notes

1 CKIP is not supported by 10xx model APs
 2 Web Policy cannot be used in combination with IPsec
 3 H-REAP Local Switching is not supported with IPsec, CRANITE authentication
 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset exclude
 5 Client MFP is not active unless WPA2 is configured
 6 Learn Client IP is configurable only when HREAP Local Switching is enabled
 7 WMM and open or AES security should be enabled to support higher 11n rates
 8 Multicast Should Be Enabled For IPV6.

Security profile WPA2-PSK, AES encryption



Configuration of authentication using Radius sever, 802.1X (Step 1). In this example is WPA2-AES/CCMP used.



Configuration of authentication using Radius sever (Step 2). Select the server to use. The server is configured under tab Security/Radius. See configuration of server below.

Security

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

RADIUS Authentication Servers > New

Server Index (Priority)	1
Server IP Address	192.168.1.44
Shared Secret Format	ASCII
Shared Secret	*****
Confirm Shared Secret	*****

Key Wrap ☐ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Port Number: 1812

Server Status: Enabled

Support for RFC 3576: Enabled

Server Timeout: 2 seconds

Network User: ☒ Enable

Management: ☒ Enable

IPSec: ☐ Enable

Configuration of authentication using Radius sever (Step 3). The IP address and the secret must correspond to the IP and the credential used by the Radius server. Tests were performed with FreeRadius.

General settings (QoS, Radio)

The screenshot shows the 'WLANs > Edit' configuration page. The 'QoS' tab is selected. Under 'Quality of Service (QoS)', the 'Platinum (voice)' profile is selected. Under 'WMM', the 'WMM Policy' is set to 'Allowed'. The '7920 AP CAC' and '7920 Client CAC' checkboxes are both unchecked.

Make sure that WMM is enabled and Quality of Service (QoS) platinum profile is selected.

The screenshot shows the 'WLANs > Edit' configuration page with the 'Advanced' tab selected. Under 'Coverage Hole Detection', the 'Coverage Hole Detection' and 'Enable Session Timeout' checkboxes are unchecked. Under 'DTIM Period (in beacon intervals)', the values for '802.11a/n (1 - 255)' and '802.11b/g/n (1 - 255)' are both set to 5. The 'Scan Defer Priority' is set to 0, and the 'Scan Defer Time (msecs)' is set to 100.

Disable “coverage Hole Detection” and “Session timeout”. Set DTIM period to Ascom recommended value 5. DTIM value 5 values are recommended in order to allow maximum battery conservation without impacting the quality.

Channel configuration. See picture below for additional information.

Ascom recommended settings for 802.11b/g/n are to only use channel 1, 6 and 11. For 802.11a/n use channels according to the infrastructure manufacturer and country regulations.

Note. For 802.11a/n, if using channels where DFS is mandatory roaming performance will be degraded due passive scan. Ascoms recommendation is therefore to avoid usage of DFS channels if possible.

Note. For 802.11a/n, if enabling more than 8 channels the roaming performance will be degraded.

802.11b/g Global Parameters

General

802.11b/g Network Status	<input checked="" type="checkbox"/> Enabled
802.11g Support	<input checked="" type="checkbox"/> Enabled
Beacon Period (millisecs)	100
Short Preamble	<input type="checkbox"/> Enabled
Fragmentation Threshold (bytes)	2346
DTPC Support	<input checked="" type="checkbox"/> Enabled

11n Parameters

ClientLink	<input type="checkbox"/> Enabled
------------	----------------------------------

CCX Location Measurement

Mode	<input type="checkbox"/> Enabled
------	----------------------------------

Data Rates**

1 Mbps	Disabled
2 Mbps	Disabled
5.5 Mbps	Disabled
6 Mbps	Supported
9 Mbps	Supported
11 Mbps	Supported
12 Mbps	Mandatory
18 Mbps	Supported
24 Mbps	Supported
36 Mbps	Supported
48 Mbps	Supported
54 Mbps	Supported

**** Data Rate 'Mandatory' implies that clients who do not support that specific rate will not be able to associate. Data Rate 'Supported' implies that any associated client that also supports that same rate may communicate with the AP using that rate. But it is not required that a client be able to use the rates marked supported in order to associate. The actual data rates that are supported depend on the channel selected as different channels may have different bandwidths. The reason is that we show data rates and allow the user to select the data rates. But in reality, the AP will pick the next lower data rate allowed for that channel if the chosen data rate is not supported.**

Set Beacon Period to 100ms for AP1230 and 1240. For AP1140 and 1250 the Beacon Period should be set to 102ms. Very important in installations with mixed AP population!

Ascom recommends disabling the lowest speeds and have 6mbits as lowest supported speed. To further optimize performance it is recommended to disallow 802.11b clients to associate by setting the 6 Mbps or 12Mbps rate to mandatory in the 802.11g configuration.

The screenshot shows the Cisco Wireless configuration interface for Dynamic Channel Assignment (DCA). The left sidebar shows the navigation tree with 'DCA' highlighted under '802.11b/g/n' > 'RRM'. The main content area is titled '802.11b > RRM > Dynamic Channel Assignment (DCA)'. Under the 'Dynamic Channel Assignment Algorithm' section, the 'Channel Assignment Method' is set to 'OFF' (highlighted with a red box). Other settings include 'Interval: 10 minutes', 'AnchorTime: 0', and 'Invoke Channel Update Once'. Below this, there are checkboxes for 'Avoid Foreign AP interference', 'Avoid Cisco AP load', and 'Avoid non-802.11a noise', all of which are checked. The 'Channel Assignment Leader' is '00:23:33:b2:a6:a0' and 'Last Auto Channel Assignment' is '108 secs ago'. The 'DCA Channel List' shows a list of channels with '1, 6, 11' selected. A table below lists channels 1 through 5, with channel 1 checked.

Ascom do not support Dynamic Channel Assignment.

The screenshot shows the Cisco Wireless configuration interface for Tx Power Control (TPC). The left sidebar shows the navigation tree with 'TPC' highlighted under '802.11b/g/n' > 'RRM'. The main content area is titled '802.11b > RRM > Tx Power Control (TPC)'. Under the 'Tx Power Level Assignment Algorithm' section, the 'Power Level Assignment Method' is set to 'Fixed' (highlighted with a red box). Other settings include 'Automatic' (Every 600 sec), 'On Demand', and 'Invoke Power'. The 'Maximum Power Level Assignment' is '100', 'Minimum Power Level Assignment' is '-100', and 'Power Threshold' is '-70'. The 'Power Neighbor Count' is '3' and 'Power Assignment Leader' is '00:23:33:b2:a6:a0'. The 'Last Power Level Assignment' is '79 secs ago'.

Ascom do not support Dynamic Power Assignment.

Wireless

802.11b/g > EDCA Parameters

General

EDCA Profile: Voice Optimized

Enable Low Latency MAC: ☐

Turn this ON only if DSCP marking is correct for media (RTP) and signaling packets

Wireless

- Access Points
 - All APs
 - Radios
 - 802.11a/n
 - 802.11b/g/n
 - Global Configuration
- Advanced
 - Mesh
 - HREAP Groups
 - 802.11a/n
 - 802.11b/g/n
 - Network
 - RRM
 - RF Grouping
 - TPC
 - DCA
 - Coverage
 - General
 - Client Roaming
 - Voice
 - Video
 - EDCA Parameters
 - High Throughput (802.11n)
 - Country

Use “EDCA Profile” Voice Optimized and disable low latency MAC.

Wireless

Edit QoS Profile

QoS Profile Name: platinum

Description: For Voice Applications

Per-User Bandwidth Contracts (k) *

Average Data Rate	0
Burst Data Rate	0
Average Real-Time Rate	0
Burst Real-Time Rate	0

Over the Air QoS

Maximum RF usage per AP (%)	100
Queue Depth	100

Wired QoS Protocol

Protocol Type: None

** The value zero (0) indicates the feature is disabled*

Wireless

- Access Points
 - All APs
 - Radios
 - 802.11a/n
 - 802.11b/g/n
 - Global Configuration
- Advanced
 - Mesh
 - HREAP Groups
 - 802.11a/n
 - 802.11b/g/n
 - Network
 - RRM
 - RF Grouping
 - TPC
 - DCA
 - Coverage
 - General
 - Client Roaming
 - Voice
 - Video
 - EDCA Parameters
 - High Throughput (802.11n)
 - Country
 - Timers
 - QoS
 - Profiles
 - Roles

Depending on the infrastructure (switches) "Protocol Type" may have to be disabled.

Ascom i62

Name	Value
Network name	Cisco Interoperability
DHCP mode	Enable
802.11 protocol	802.11b/g/n
SSID	Cisco Interoperability
Security mode	WPA-PSK & WPA2-PSK
WPA-PSK passphrase	*****
Voice power save mode	U-APSD
802.11b/g/n channels	1,6,11
Advanced: 802.11 channels	
World mode regulatory domain	World mode (802.11d)
Transmission power	Automatic
IP DSCP for voice	0x2E (46) - Expedited Forwarding
IP DSCP for signalling	0x1A (26) - Assured Forwarding 31
TSPEC Call Admission Control	Disable
Transmit gratuitous ARP	Enable

Recommended i62 setting.

System => <A|B|C|D>

- DHCP mode: Enable
- ESSID: Cisco Interoperability
- Authentication: <n/a>*
- Encryption: <n/a>*
- Voice Power Save Mode: <n/a>*
- 802.11 b/g/n Channels: 1,6,11
- IP DSCP for VOICE: 0x2E (46) – Expedited forwarding
- IP DSCP for SIGNALING: 0x68 (26) - Assured Forwarding 31
- Transmit Gratuitous ARP: Enable

VoIP => General

- VoIP Protocol: SIP
- Endpoint Number <Extension no>
- Endpoint ID < Extension no >

VoIP => SIP

- SIP Proxy IP address: <ip>

**) Security options and voice power save mode will change depending on individual test case.*

Other settings were left at their defaults.

i62 configuration:

See attached file (i62 templates.tpl) for i62 configuration.

Innovaphone IP6000 (IP PBX & DHCP server)

The Innovaphone IP6000 was configured with a static IP address of 192.168.10.1. Signaling is less relevant here since testing homes in on interoperability in relation to the WLAN infrastructure and not features of the IP PBX. During the tests the IP6000 also was used as DHCP server.

IP6000 configuration:

See attached file (complete-IP6000-08-03-a6.txt) for IP6000 configuration.

APPENDIX B: DETAILED TEST RECORDS

VoWIFI

Pass	28
Fail	0
Comments	7
Untested	9
Total	44

See attached file (WLANinteroperabilityTestReport_Cisco WLC.xls) for detailed test results.

MISCELLANEOUS

Please refer to the test specification for WLAN systems on Ascom's interoperability web page for explicit information regarding each test case.

See URL (requires login):

<https://www.ascom-ws.com/AscomPartnerWeb/en/startpage/Sales-tools/Interoperability>

Document History

Rev	Date	Author	Description
PA	2010-09-13	SEKMO	Draft
A	2010-09-30	SEKMO	Rev A