

TABLE OF CONTENT:

INTRODUCTION.....	3
Ascom solution	3
Enterasys solution	3
SITE INFORMATION	4
SUMMARY	5
Known issues	6
Compatibility information.....	6
General conclusion	6
TEST RESULTS.....	7
Ascom WLAN Infrastructure Verification – VoWiFi.....	7
APPENDIX A: TEST CONFIGURATIONS.....	9
Siemens Enterasys C20 Controller v. 07.31.02.0010.....	9
Security settings (PSK)	9
PEAP-MSCHAPv2 using an external authentication server.....	10
General settings (SSID, QoS, Radio)	12
Innovaphone IP6000 (IP PBX & DHCP server).....	20
APPENDIX B: DETAILED TEST RECORDS.....	21

INTRODUCTION

This document describes necessary steps and guidelines to optimally configure the Enterasys Wireless platform with Ascom i62 VoWiFi handsets.

The guide should be used in conjunction with both Enterasys and Ascom's configuration guide(s).

Ascom solution

Ascom Wireless Solutions (www.ascom.com/ws) is a leading provider of on-site wireless communications for key segments such as hospitals, manufacturing industries, retail and hotels. More than 75,000 systems are installed at major companies all over the world. The company offers a broad range of voice and professional messaging solutions, creating value for customers by supporting and optimizing their Mission-Critical processes. The solutions are based on VoWiFi, IP-DECT, DECT, Nurse Call and paging technologies, smartly integrated into existing enterprise systems. The company has subsidiaries in 10 countries and 1,200 employees worldwide. Founded in the 1950s and based in Göteborg, Sweden, Ascom Wireless Solutions is part of the Ascom Group, listed on the Swiss Stock Exchange.

Enterasys solution

Enterasys has a rich history as a pioneer in the switching and routing market, dating back to 1983 when the company was originally formed as Cabletron Systems. Today's full portfolio of wired/wireless network infrastructure and security solutions leverages that experience and a robust technology patent portfolio to provide built-in automation, visibility and control capabilities to solve critical customer networking and mobility challenges.

Siemens Enterprise Communications is a premier provider of end-to-end enterprise communications, including voice, network infrastructure and security solutions that use open, standards-based unified communications and business applications for a seamless collaboration experience. This award-winning "Open Communications" approach enables organizations to improve productivity and reduce costs through easy-to-deploy solutions that work within existing IT environments, delivering operational efficiencies. It is the foundation for the company's OpenPath® commitment that enables customers to mitigate risk and cost-effectively adopt unified communications. Jointly owned by The Gores Group and Siemens AG, Siemens Enterprise Communications includes Cycos and Enterasys Networks. For more information about Siemens Enterprise Communications or Enterasys please visit www.siemens-enterprise.com or www.enterasys.com.

SITE INFORMATION

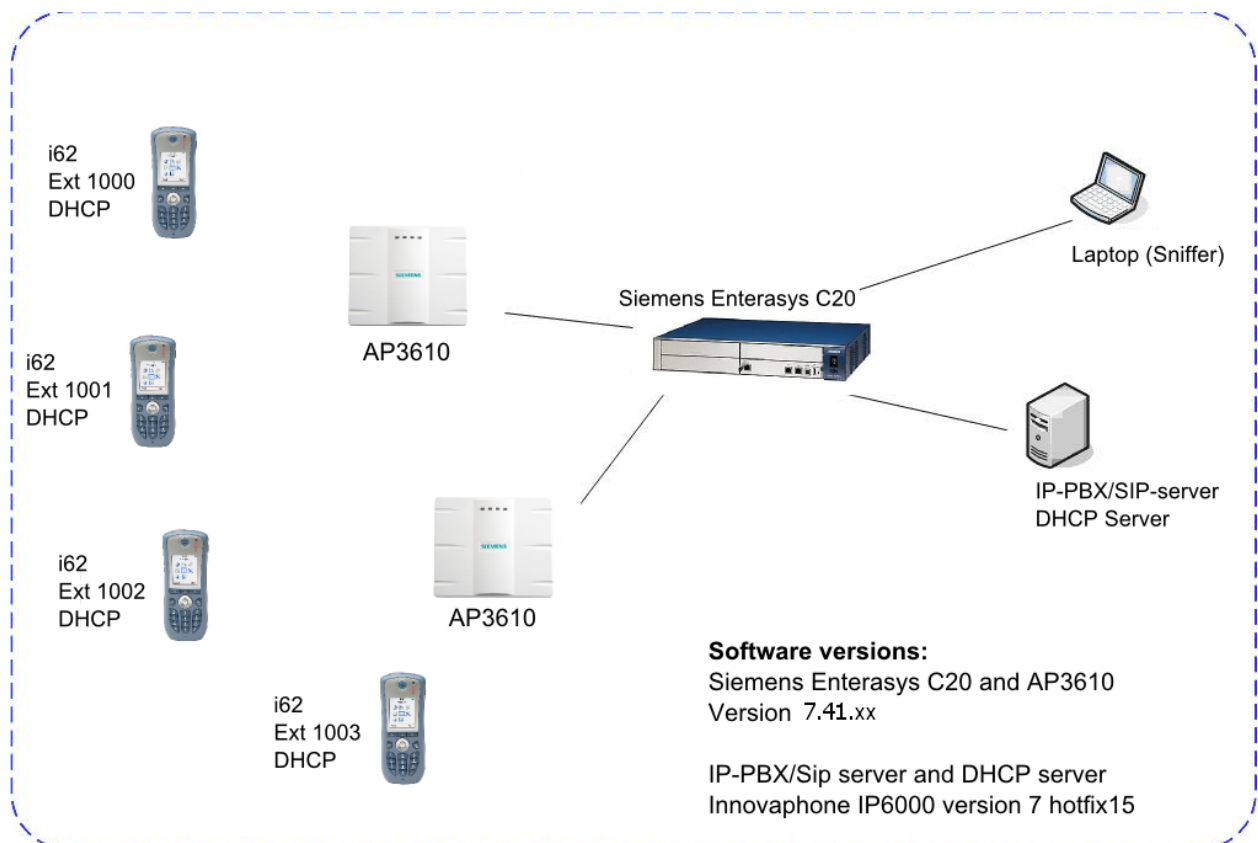
Test Site:

Ascom US
 598 Airport Blvd, Suite 300
 Morrisville, NC, US-27560
 USA

Participants:

Karl-Magnus Olsson, Ascom HQ

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	Not supported by controller
Association, WPA2-PSK / AES Encryption	OK
Association, LEAP Authentication	Not supported by controller
Association, PEAP-MSCHAPv2 Auth, TKIP Encryption	OK
Association, PEAP-MSCHAPv2 Auth, AES Encryption	OK
Association with EAP-FAST authentication	OK *
Association, Multiple ESSIDs	OK
Beacon Interval and DTIM Period	OK
Preauthentication	Not recommended
PMKSA Caching	OK
WPA2-opportunistic/proactive Key Caching	OK
WMM Prioritization	OK
Active Mode (load test)	OK
802.11 Power-save mode	OK
802.11e U-APSD	OK **
802.11e U-APSD (load test)	OK

*) EAP-FAST ok with WPA and WPA2, NOK with WEP

**) Problem with "U-APSD handshake". Make sure the system and the handset have the same configuration when it comes to U-APSD.

Roaming

High Level Functionality	Result
Roaming, Open with No Encryption	OK (Avg roaming time 12ms) *
Roaming, Open with Static WEP64	OK (Avg roaming time 15ms) *
Roaming, WPA-PSK, TKIP Encryption	OK (Avg roaming time 29ms) *
Roaming, WPA2-PSK, AES Encryption	OK (Avg roaming time 21ms) *
Roaming, LEAP, WEP/TKIP Encryption (CCKM)	Not supported by controller
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption	OK (Avg roaming time 19ms)* /**

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

**) Measured times is with opportunistic key caching enabled (default enabled)

Known issues

- U-APSD handshake. Handset tries to use U-APSD even if it is not announced by system.
Solution: Make sure to enable U-APSD in the system if enabled in the handset.
- Pre authentication not working.
Solution: Use opportunistic key caching.
- EAP-FAST with WEP not working.
Solution: Avoid WEP and use WPA or WPA2 instead.

Compatibility information

All tests were done on AP3610 (Internal antennas) and a C20 controller. Due to the fact that AP3605, AP3610, AP3620, AP3630 and AP3640 share the same WLAN chipset, their behavior can be considered to be identical. We therefore ensure compatibility/interoperability according to the list below.

Supported access points with Enterasys Wireless version 07.41.01.xxxx or above:

AP3605
AP3610
AP3620
AP3630 (Converted to Fit Mode)
AP3640 (Converted to Fit Mode)

Supported controller platforms with Enterasys Wireless version 07.41.01.xxxx or above:

C20/C20N
C25
C4110
C5110

General conclusion

The verification, including association, authentication and roaming test produced excellent results.

Roaming times were in general good with roaming times of 21ms and 19ms when using WPA2-PSK/AES and PEAP-MSCHAPv2 (WPA2/AES).

Load tests showed that it was possible to maintain 18 simultaneous calls on one access point when using 802.11bg with the minimum basic rate set to 11Mbps.

Load tests showed that it was possible to maintain 16 simultaneous calls on one access point when using 802.11an with the minimum basic rate set to 6Mbps.

TEST RESULTS

Ascom WLAN Infrastructure Verification – VoWiFi

Software Versions:

- Enterasys C20 Version 07.41.01.xxxx
- AP3610
- Ascom i62, v2.2.14

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/n
- WMM/ U-APSD Enabled
- 802.11d Regulatory Domain: World mode
- Minimum basic rate set to 11Mbps

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

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 (14/14)

- Only security settings available through the web GUI were tested.
- FreeRadius was used in the test cases where an authentication server was needed.

Power Save: 100 % pass (2/3)

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

QOS: 100% pass (1/1)

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

“Maximum Number of Calls”: 100% pass (5/5)

- 802.11bgn. It was not possible to maintain more than 10 phones in in call on one single access point.
- 802.11an. All tests, including both test in Active mode and in U-APSD, passed and it was possible to make 8 calls including 16 phones on one single access point.

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

- FreeRadius was used in the test cases where an authentication server was needed.

Battery Lifetime: 100% Pass (3/3)

- > 80 hrs battery lifetime in idle mode (DTIM period = 5) *
- 4h+ battery lifetime with ongoing call in active mode *
- 15h + 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.
- Stable call for the duration of >24 hours in active mode.
- Stability tested both on 802.11a/n and 802.11b/g/n in U-APSD mode.

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

APPENDIX A: TEST CONFIGURATIONS

Enterasys Wireless C20 Controller v. 07.41.01.xxxx

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

Security settings (PSK)

The screenshot displays the 'Virtual Network Configuration' interface for a WLAN service named 'CompTest80211SI'. The 'Privacy' tab is selected, showing the following configuration:

- WLAN Services:** WPA - PSK (selected)
- WPA v.1:** WPA v.1, Encryption: Auto
- WPA v.2:** WPA v.2, Encryption: AES only
- Broadcast re-key interval:** 3600 seconds (30 - 86400 seconds)
- Group Key Power Save Retry:**
- Input Method:** Input String, Input Hex
- Pre-shared key String:** [Redacted] [Unmask] (min 8 characters; max 63)

A note at the bottom of the configuration area states: "Note: using WEP or WPAv1 privacy will limit 11n performance to legacy AP rates".

The interface also shows a status bar at the bottom with the following information:

- WLAN Service saved successfully
- [C20_1 | C20 Office | 06 days, 05:32] User: admin Port status: [Icons]
- Software: 07.41.01.0190 | Tracing: Inactive | Admin Users: 1
- © 2006-2011 Enterasys Networks. All Rights Reserved.

Security profile WPA2-PSK, AES encryption

PEAP-MSCHAPv2 using an external authentication server.

Configuration of authentication using external Radius sever, 802.1X (Step 1). In this example is WPA2-AES/CCMP used. "Opportunistic Keying" is strongly recommended as Key Management Option.

The screenshot shows the 'Virtual Network Configuration' interface for 'WLAN: CompTest80211SI'. The 'Auth & Acct' tab is selected. The 'Authentication' section shows 'Mode: 802.1x' and 'With HTTP Redirection' checkbox. The 'RADIUS Servers' section shows a table with one server 'intop radius' selected for authentication.

Server	Auth	Acct
intop radius	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Configuration of authentication using external Radius sever (Step 2). Select the server to use. The server is created/configured in next step.

Add RADIUS Server

RADIUS Server

Server Alias:

Hostname/IP:

Shared Secret:

Default Protocol:

Allow per WLAN Service Customization

Authentication

Priority:

Total Number of Tries:

RADIUS Request Timeout: (seconds)

Port:

Accounting

Priority:

Total Number of Tries:

RADIUS Request Timeout: (seconds)

Interim Accounting Interval: (minutes)

Port:

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

Note that depending on which Authentication method used it might be necessary to add a certificate into the i62. PEAP-MSCHAPv2 requires a Root certificate and EAP-TLS requires both a Root certificate and a client certificate.

General settings (SSID, QoS, Radio)

The screenshot shows the 'Virtual Network Configuration' page for 'WLAN: CompTest80211SI'. The interface includes a navigation menu on the left with options like 'Global', 'Virtual Networks', and 'WLAN Services'. The main content area is divided into tabs: 'WLAN Services', 'Privacy', 'Auth & Acct', and 'QoS'. Under 'WLAN Services', there are two sections: 'Core' and 'Status'. The 'Core' section contains fields for 'Name' (CompTest80211SI), 'Service Type' (Standard), 'SSID' (CompTest80211SI), and 'Default Topology' (-). The 'Status' section has an 'Enable' checkbox which is checked. To the right, the 'Wireless APs' section shows a 'Select APs' dropdown and a table with columns 'Radio 1', 'Radio 2', and 'AP Name'. The table contains one row with checked boxes for 'Radio 1' and 'Radio 2', and the value '1018022623430000' for 'AP Name'. At the bottom, there are buttons for 'New', 'Delete', 'Save', and 'Advanced...'.

General SSID settings.

The screenshot shows the 'Virtual Network Configuration' interface for 'WLAN: CompTest80211SI'. The interface includes a navigation menu on the left with 'WLAN Services' selected. The main content area has tabs for 'WLAN Services', 'Privacy', 'Auth & Acct', and 'QoS'. Under the 'QoS' tab, there is a 'Wireless QoS' section with a red border containing the following options:

- Legacy
- WMM
- 802.11e
- Turbo Voice
- U-APSD

Other options include 'Flexible Client Access' (disabled) and an 'Advanced' button. At the bottom, there are 'New', 'Delete', and 'Save' buttons.

Make sure that WMM is enabled. In this example U-APSD is enabled which is strongly recommended in order to increase battery performance.

- All APs
- AP Default Settings
- AP Multi-edit
- AP 802.1x Multi-edit
- Client Management
- Access Approval
- AP Maintenance
- Load Groups
- AP Registration
- Sensor Management
- CompTest80211SI
- HipathNAC

1018022623430000

AP Properties	WLAN Assignment	Radio 1	Radio 2	Static Configuration	802.1x																										
Base Settings		BSS Info		00:1F:45:80:D4:D8 HipathNAC																											
Basic Radio Settings		<table border="1"> <tr> <td>Admin Mode</td> <td>On</td> </tr> <tr> <td>Radio Mode</td> <td>b/g/n</td> </tr> <tr> <td>Channel Width</td> <td>20MHz</td> </tr> <tr> <td>RF Domain</td> <td>MyDomain</td> </tr> <tr> <td>Current Channel ¹</td> <td>6: 2437MHz</td> </tr> <tr> <td>Last Requested Channel</td> <td>Auto</td> </tr> <tr> <td>Request New Channel</td> <td>-</td> </tr> <tr> <td>Auto Tx Power Ctrl (ATPC)</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Current Tx Power Level</td> <td>18 dBm</td> </tr> <tr> <td>Max Tx Power</td> <td>20 dBm</td> </tr> <tr> <td>Min Tx Power ²</td> <td>8 dBm</td> </tr> <tr> <td>Auto Tx Power Ctrl Adjust</td> <td>0 dB</td> </tr> <tr> <td>Channel Plan</td> <td>Auto</td> </tr> </table>				Admin Mode	On	Radio Mode	b/g/n	Channel Width	20MHz	RF Domain	MyDomain	Current Channel ¹	6: 2437MHz	Last Requested Channel	Auto	Request New Channel	-	Auto Tx Power Ctrl (ATPC)	<input checked="" type="checkbox"/>	Current Tx Power Level	18 dBm	Max Tx Power	20 dBm	Min Tx Power ²	8 dBm	Auto Tx Power Ctrl Adjust	0 dB	Channel Plan	Auto
Admin Mode	On																														
Radio Mode	b/g/n																														
Channel Width	20MHz																														
RF Domain	MyDomain																														
Current Channel ¹	6: 2437MHz																														
Last Requested Channel	Auto																														
Request New Channel	-																														
Auto Tx Power Ctrl (ATPC)	<input checked="" type="checkbox"/>																														
Current Tx Power Level	18 dBm																														
Max Tx Power	20 dBm																														
Min Tx Power ²	8 dBm																														
Auto Tx Power Ctrl Adjust	0 dB																														
Channel Plan	Auto																														
<input type="button" value="Copy to Defaults"/> <input type="button" value="Reset to Defaults"/> <input type="button" value="Add Wireless AP"/> <input type="button" value="Save"/>																															

Ascom recommended settings for 802.11b/g/n are to use only channel 1, 6 and 11. Due to the limited number of non-overlapping channels using 802.11b/g/n it is recommended to use 20MHz channel width.

Advanced
✕

Base Settings

DTIM Period	5	Beacon Period	100
RTS/CTS Threshold	2346	Frag. Threshold	2346
Max % of non-unicast traffic per Beacon period	100		
Maximum Distance [m]	100		

Basic Radio Settings

Dynamic Channel Selection	Off
Min Basic Rate	11 Mbps

11b Settings

Preamble	Short
----------	-------

11g Settings

Protection Mode	Auto
Protection Rate	11 Mbps
Protection Type	CTS Only

11n Settings

Protection Mode	Enabled
Aggregate MSDUs	Disabled
Aggregate MSDU Max Length	4096
Aggregate MPDUs	Disabled
Aggregate MPDU Max Length	65535
Agg. MPDU Max # of Sub-frames	64
ADDBA Support	Disabled

Under Radio 2 / Advanced; Set DTIM period to value 5 and beacon period to 100ms. These values are recommended in order to allow maximum battery conservation without impacting the quality.

- All APs
- AP Default Settings
- AP Multi-edit
- AP 802.1x Multi-edit
- Client Management
- Access Approval
- AP Maintenance
- Load Groups
- AP Registration
- Sensor Management
- CompTest80211SI
- HipathNAC

1018022623430000

AP Properties	WLAN Assignment	Radio 1	Radio 2	Static Configuration	802.1x
Basic Radio Settings					
Admin Mode		On			
Radio Mode		a/n			
Channel Width		40MHz			
RF Domain		MyDomain			
Current Channel ¹		165: 5825MHz			
Last Requested Channel		Auto			
Request New Channel		-			
Guard Interval		Short			
Auto Tx Power Ctrl (ATPC)		<input checked="" type="checkbox"/>			
Current Tx Power Level		18 dBm			
Max Tx Power		18 dBm			
Min Tx Power ²		0 dBm			
Auto Tx Power Ctrl Adjust		0 dB			
Channel Plan		All Non-DFS-Channels			
View					
Copy to Defaults		Reset to Defaults		Add Wireless AP	
Save					

Configuration of 802.11a/n: use channels according to the infrastructure manufacturer and country regulations.

Advanced

Base Settings

DTIM Period: 5 Beacon Period: 100

RTS/CTS Threshold: 2346 Frag. Threshold: 2346

Max % of non-unicast traffic per Beacon period: 100

Maximum Distance [m]: 100

Basic Radio Settings

Dynamic Channel Selection: Off

Min Basic Rate: 6 Mbps

11n Settings

Protection Mode: Enabled

40MHz Protection Mode: CTS only

40MHz Prot. Channel Offset: 20MHz

40MHz Channel Busy Threshold: 50

Aggregate MSDUs: Disabled

Aggregate MSDU Max Length: 4096

Aggregate MPDUs: Disabled

Aggregate MPDU Max Length: 65535

Agg. MPDU Max # of Sub-frames: 64

ADDBA Support: Disabled

Close

Under Radio 1 / Advanced; Set DTIM period to value 5 and beacon period to 100ms. These values are recommended in order to allow maximum battery conservation without impacting the quality.'

802.11a/n

Non-DFS	
36:	5180 MHz
40:	5200 MHz
44:	5220 MHz
48:	5240 MHz
149:	5745 MHz
153:	5765 MHz
157:	5785 MHz
161:	5805 MHz
165:	5825 MHz

DFS	
52:	5260 MHz
56:	5280 MHz
60:	5300 MHz
64:	5320 MHz

Close

Note: If using channels where DFS is mandatory roaming for 802.11a, performance will be degraded due passive scan only. Ascom recommends avoiding the use of DFS channels.

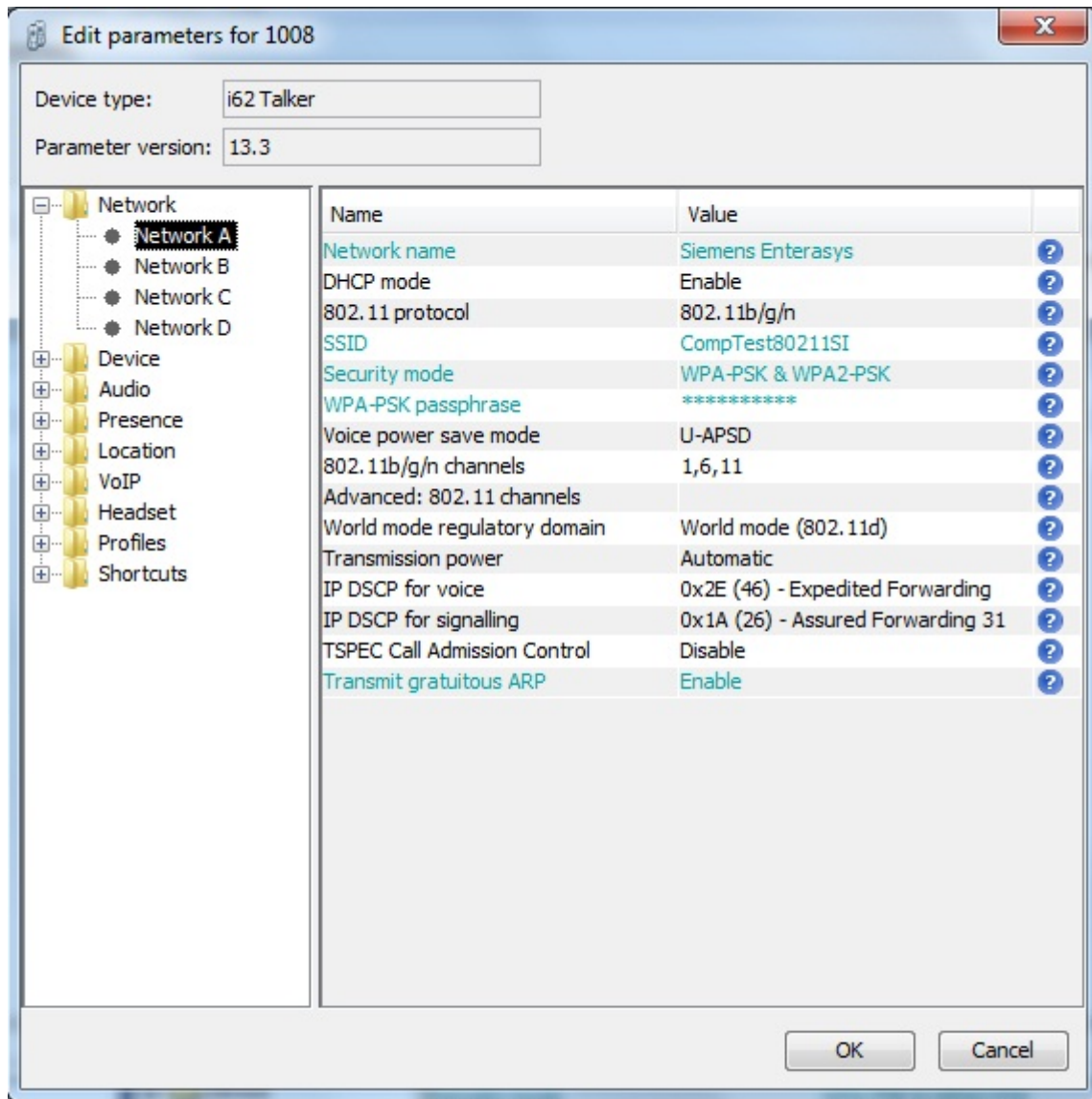
Note for 802.11an: Performance will be degraded if more than 8 channels are enabled for roaming.

Note for 802.11an: Using 40 MHz channels will reduce the number of no DFS channels to 2 in ETSI regions.

Controller configuration

See attached file (controller_config.cli) for controller configuration.

Ascom i62



Recommended i62 Network settings.

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	30
Fail	1
Comments	12
Untested	2
Total	45

See attached file (WLANinteroperabilityTestReport_Enterasyx.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	2010-11-07	SEKMO	Draft
PB	2011-02-25	SEKMO	Draft 2. Updated with test result from i62 sw 2.2.14
PC	2011-03-21	SEKMO	Draft 3. Added/changed "introduction" and "Summary" chapter