

[ ]

# INTEROPERABILITY REPORT

Ascom i62

Cisco Autonomus mode AP 1140/1250/1260

Version 12.4(25d)JA1

i62 version 2.5.7

Ascom, Gothenburg

December 2011



## TABLE OF CONTENT:

INTRODUCTION.....	3
About Ascom .....	3
About Cisco .....	3
SITE INFORMATION .....	4
Test Topology.....	4
SUMMARY .....	5
Known Issues .....	6
APPENDIX A: TEST CONFIGURATION .....	7
Cisco AP1140/1250/1260 .....	7
Security settings (PSK) .....	7
PEAP-MSCHAPv2 using an external authentication server .....	8
General settings (QoS, Radio).....	10
Ascom i62.....	14

## INTRODUCTION

---

This document describes necessary steps and guidelines to optimally configure Cisco autonomous access points with Ascom i62 VoWiFi handsets.

The guide should be used in conjunction with both Cisco and Ascoms configuration guide(s).

### About Ascom

Ascom Wireless Solutions ([www.ascom.com/ws](http://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.

### About Cisco

Cisco, (NASDAQ: CSCO), the worldwide leader in networking that transforms how people connect, communicate and collaborate, this year celebrates 25 years of technology innovation, operational excellence and corporate social responsibility. Information on Cisco can be found at <http://www.cisco.com>. For ongoing news, please go to <http://newsroom.cisco.com>.

## SITE INFORMATION

---

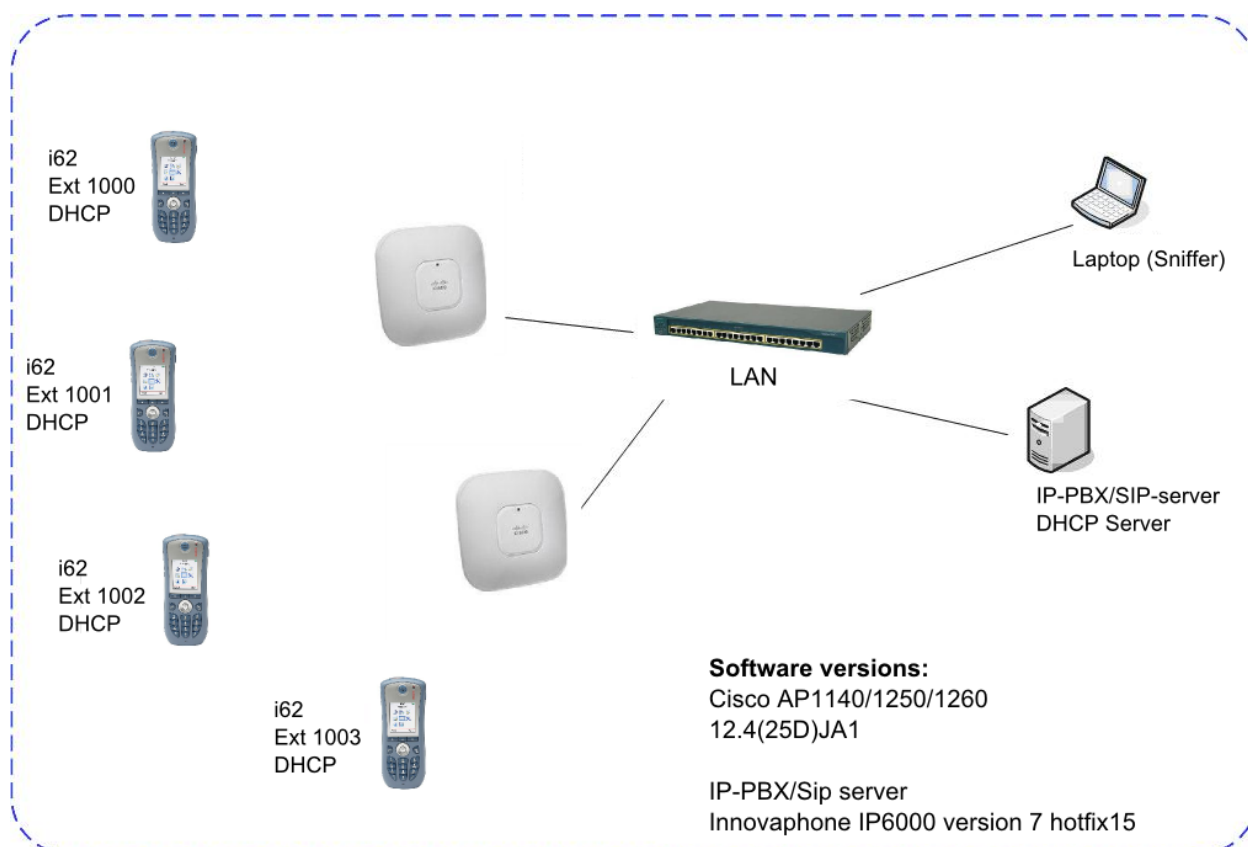
### Test Site:

Ascom  
Grimbodalen 2  
P.O Box 87836  
40276 Gothenburg  
Sweden

### Participants:

Janne Hofgren Patala, Ascom HQ, Gothenburg  
Karl-Magnus Olsson, Ascom HQ

## Test Topology



## SUMMARY

---

### WLAN Features

High Level Functionality	Result
Association, Open with No Encryption	OK
Association, WPA-PSK, TKIP	OK
Association, WPA2-PSK, TKIP / AES Encryption	OK
Association, LEAP Authentication	OK*
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 tested
PMKSA Caching	OK
WPA2-opportunistic/proactive Key Caching	Not supported by AP
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

### Roaming

High Level Functionality	Result
Roaming, Open with No Encryption	OK
Roaming, WPA-PSK, TKIP Encryption	OK
Roaming, WPA2-PSK, AES Encryption	OK
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption	OK*

\* ) Note that Cisco APs in autonomous mode does not utilize opportunistic/proactive key caching. It means that the first visit to a new AP will generate a higher roaming time. Typically ~400ms.

## Known Issues

- Sometimes the Cisco autonomous access points ends up in a state where buffered and indicated packets are never released to requesting handset. Reported to Cisco TAC.
- Due to the regulations of the DFS channels, a client that does not support radar detection is not allowed to actively scan for APs in these channels. The client will then have to perform passive scanning which means that it only listens for beacons. For a voice client, this will affect an ongoing call to some degree by introducing a slight increase in jitter in the voice stream. The VoWiFi Handset can use the DFS channels, but the voice quality may be distorted and roaming delayed. The DFS channel scan algorithm is optimized and uses both passive scanning and active scanning when it is regulatory ensured that transmitting is allowed.

## APPENDIX A: TEST CONFIGURATION

### Cisco AP1140/1250/1260

In the following chapter you will find screenshots and explanations of basic settings in order to get a Cisco AP1140/1250/1260 to operate with an Ascom i62.

The configuration file is found at the bottom of this chapter.

### Security settings (PSK)

The screenshot shows the configuration interface for a Cisco AP. The left sidebar contains a menu with options like HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, and SERVICES. The main content area is titled 'Security: Encryption Manager - Radio0-802.11N2.4GHz'. Under 'Encryption Modes', the 'Cipher' option is selected, and 'AES CCMP' is chosen from the dropdown menu. Below this, the 'Encryption Keys' section shows four keys, each with a 'Transmit Key' radio button, an 'Encryption Key (Hexadecimal)' input field, and a 'Key Size' dropdown menu set to '128 bit'.

Configuration of security profile WPA2-PSK AES/CCMP encryption (1). Set Cipher under SECURITY/Encryption Manager.

**Client Authentication Settings**

**Methods Accepted:**

☒ Open Authentication: < NO ADDITION >

☐ Shared Authentication: < NO ADDITION >

☐ Network EAP: < NO ADDITION >

**Server Priorities:**

**EAP Authentication Servers**

☒ Use Defaults [Define Defaults](#)

☐ Customize

Priority 1: < NONE >

Priority 2: < NONE >

Priority 3: < NONE >

**MAC Authentication Servers**

☒ Use Defaults [Define Defaults](#)

☐ Customize

Priority 1: < NONE >

Priority 2: < NONE >

Priority 3: < NONE >

---

**Client Authenticated Key Management**

**Key Management:** Mandatory ☐ CCKM ☒ Enable WPA WPAv2

**WPA Pre-shared Key:** ..... ☒ ASCII ☐ Hexadecimal

Configuration of security profile WPA2-PSK AES/CCMP encryption (2). Set Key Management to Mandatory and choose to enable WPA (WPAv2)

**Note.** By Choosing “WPA”, both WPA and WPA2 are enabled. (Mixed mode)

## PEAP-MSCHAPv2 using an external authentication server

**SERVER MANAGER** GLOBAL PROPERTIES

Hostname: AP1202 AP1202 uptime is 3 weeks, 3 days, 9 hours, 3 minutes

**Security: Server Manager**

**Backup RADIUS Server**

Backup RADIUS Server: (Hostname or IP Address)

Shared Secret:

[Apply](#) [Delete](#) [Cancel](#)

**Corporate Servers**

**Current Server List**

< NEW >

192.168.10.162

[Delete](#)

Server: 192.168.10.162 (Hostname or IP Address)

Shared Secret: .....

Authentication Port (optional): 1812 (0-65536)

Accounting Port (optional): 1812 (0-65536)

[Apply](#) [Cancel](#)

**Default Server Priorities**

**EAP Authentication**

Priority 1: < NONE >

Priority 2: < NONE >

**MAC Authentication**

Priority 1: < NONE >

Priority 2: < NONE >

**Accounting**

Priority 1: < NONE >

Priority 2: < NONE >

Configuration of authentication using Radius sever (Step1). The IP address and the secret must correspond to the IP and the credential used by the Radius server. Tests were performed with FreeRadius.



Client Authentication Settings

Methods Accepted:

☐ Open Authentication: < NO ADDITION >

☐ Shared Authentication: < NO ADDITION >

☒ Network EAP: < NO ADDITION >

Server Priorities:

EAP Authentication Servers

☐ Use Defaults [Define Defaults](#)

☒ Customize

Priority 1: 192.168.10.162

Priority 2: < NONE >

Priority 3: < NONE >

MAC Authentication Servers

☒ Use Defaults [Define Defaults](#)

☐ Customize

Priority 1: < NONE >

Priority 2: < NONE >

Priority 3: < NONE >

Client Authenticated Key Management

Key Management:

Mandatory

☐ CCKM

☒ Enable WPA

WPAv2

WPA Pre-shared Key:

.....

☒ ASCII
 ☐ Hexadecimal

IDS Client MFP

☒ Enable Client MFP on this SSID:
 

Optional

Configuration of authentication using Radius sever (Step 2). Under the tab SECURITY/SSID Manager, select Network EAP as Methods Accepted (Select <NO ADDITION>) and then choose the server created in the previous step.

**Note. By Choosing “WPA”, both WPA and WPA2 are enabled. (Mixed mode)**

## General settings (QoS, Radio)

The screenshot shows the configuration page for a Cisco Aironet 1140 Series Access Point. The left sidebar contains a navigation menu with options: HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, IP Address, GigabitEthernet, Radio0-802.11N<sup>2.4GHz</sup>, Radio1-802.11N<sup>5GHz</sup>, SECURITY, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG. The main content area is titled 'Cisco Aironet 1140 Series Access Point' and shows the 'Hostname Cisco1142'. Under the 'Network Interfaces: IP Address' section, the 'Configuration Server Protocol' is set to 'Static IP'. The 'IP Address' is 192.168.0.199, the 'IP Subnet Mask' is 255.255.255.0, and the 'Default Gateway IP Address' is 192.168.0.1. There are also checkboxes for 'Disable DHCP Address Binding' and 'Override DHCP Default Gateway'.

IP address settings. Example shows configuration with static IP.

The screenshot shows the 'Data Rates' and 'MCS Rates' configuration page. The 'Data Rates' section has a red border and contains a table with columns for data rates (1.0Mb/sec to 54.0Mb/sec) and radio types (802.11b, 802.11g, 802.11n). The 'MCS Rates' section has a table with columns for MCS rates (0 to 15) and radio types (802.11b, 802.11g, 802.11n). The 'Data Rates' table shows that 11.0Mb/sec is selected for 802.11g and 12.0Mb/sec for 802.11n. The 'MCS Rates' table shows that 6 is selected for 802.11g and 12 for 802.11n.

Network Interfaces/Radio. The default data rate set will work just fine, however 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.

DefaultRadio Channel:	Channel 11 - 2462 MHz	▼ Channel 11 2462 MHz
Least Congested Channel Search: (Use Only Selected Channels)	Channel 1 - 2412 MHz Channel 2 - 2417 MHz Channel 3 - 2422 MHz Channel 4 - 2427 MHz Channel 5 - 2432 MHz Channel 6 - 2437 MHz Channel 7 - 2442 MHz Channel 8 - 2447 MHz Channel 9 - 2452 MHz Channel 10 - 2457 MHz Channel 11 - 2462 MHz Channel 12 - 2467 MHz Channel 13 - 2472 MHz	
Channel Width:	20 MHz	▼ 20 MHz
World Mode	<input type="radio"/> Disable <input type="radio"/> Legacy <input checked="" type="radio"/> Dot11d	
Multi-Domain Operation:		
Country Code:	US (United States)	<input checked="" type="checkbox"/> Indoor <input type="checkbox"/> Outdoor
Receive Antenna:	<input checked="" type="checkbox"/> Diversity <input type="checkbox"/> Left (B) <input type="checkbox"/> Center(C) <input type="checkbox"/> Right (A)	
Transmit Antenna:	<input checked="" type="radio"/> Diversity <input type="radio"/> Left (B) <input type="radio"/> Right (A)	
Internal Antenna Configuration:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
	Antenna Gain(dBi): 0 (-128 - 128)	
Traffic Stream Metrics:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Aironet Extensions:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	

For 802.11b/g/n Ascom support only 3 channel deployments using channel 1,6 and 11. For 802.11a/n use channels according to the infrastructure manufacturer and country regulations. Enable Dot11d and chose your country.

**Note.** Due to the regulations of the DFS channels, a client that does not support radar detection is not allowed to actively scan for APs in these channels. The client will then have to perform passive scanning which means that it only listens for beacons. For a voice client, this will affect an ongoing call to some degree by introducing a slight increase in jitter in the voice stream. The VoWiFi Handset can use the DFS channels, but the voice quality may be distorted and roaming delayed. The DFS channel scan algorithm is optimized and uses both passive scanning and active scanning when it is regulatory ensured that transmitting is allowed.

Since the passive part of the scan phase is limited to 70 ms, a beacon interval of less than 70 ms (e.g. 60 ms) will give the best roaming performance.

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

For 802.11an: Using 40 MHz channels will reduce the number of non DFS channels to only 2 in ETSI regions.

Traffic Stream Metrics:	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
Aironet Extensions:	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
Ethernet Encapsulation Transform:	<input checked="" type="radio"/> RFC1042	<input type="radio"/> 802.1H
Reliable Multicast to WGB:	<input checked="" type="radio"/> Disable	<input type="radio"/> Enable
Public Secure Packet Forwarding:	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
Beacon Privacy Guest-Mode:	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable

Beacon Period:	<input type="text" value="100"/> (20-4000 Kusec)	Data Beacon Rate (DTIM):	<input type="text" value="5"/> (1-100)
Max. Data Retries:	<input type="text" value="64"/> (1-128)	RTS Max. Retries:	<input type="text" value="64"/> (1-128)
Fragmentation Threshold:	<input type="text" value="2346"/> (256-2346)	RTS Threshold:	<input type="text" value="2347"/> (0-2347)

Root Parent Timeout:	<input type="text" value="0"/> (0-65535 sec)
Root Parent MAC 1 (optional):	<input type="text"/> (HHHH.HHHH.HHHH)
Root Parent MAC 2 (optional):	<input type="text"/> (HHHH.HHHH.HHHH)
Root Parent MAC 3 (optional):	<input type="text"/> (HHHH.HHHH.HHHH)
Root Parent MAC 4 (optional):	<input type="text"/> (HHHH.HHHH.HHHH)

Under tab SECURITY/SSID Manager Set Beacon Period to 100ms and Set DTIM period to Ascoms recommended value 5. DTIM value 5 values are recommended in order to allow maximum battery conservation without impacting the quality. Using a lower DTIM value is possible but will reduce the standby time slightly.

It is necessary to create a QoS role that maps a DSCP value to a Class Selector value. In this case we have mapped Expedited Forwarding (DSCP 0x2e/46) to Class selector 6 (Voice < 10ms latency). Different mappings may have to be done depending on which DSCP values that are used for voice.

VLAN  
ARP Caching  
WIRELESS SERVICES +  
SYSTEM SOFTWARE +  
EVENT LOG +

Delete Classification

Match Classifications:

IP Precedence: Routine (0)  
IP DSCP: ☒ Expedited Forwarding  
☐ (0-63)  
IP Protocol 119  
Filter: No Filters defined [Define Filters](#)  
Rate Limiting:  
Bits per Sec.: (8000-2000000000)  
Conform Action: Transmit

Apply Class of Service

Best Effort (0)  
Voice <10ms Latency (6)  
Best Effort (0)

Burst Rate (Bytes): (1000-512000000)  
Exceed Action: Drop

Apply

Delete

Cancel

Apply Policies to Interface/ VLANs

	Radio0-802.11N <sup>2.4GHz</sup>	Radio1-802.11N <sup>5GHz</sup>	GigabitEthernet0
Incoming	Voice	Voice	< NONE >
Outgoing	Voice	Voice	< NONE >

Apply

Cancel

Apply the “Rule” for both incoming and outgoing traffic on the radio interfaces used.

HOME  
EXPRESS SET-UP  
EXPRESS SECURITY  
NETWORK MAP +  
ASSOCIATION +  
NETWORK INTERFACES +  
SECURITY +  
SERVICES  
Telnet/SSH  
Hot Standby  
CDP  
DNS  
Filters  
HTTP  
QoS  
STREAM  
SNMP  
SNTP  
VLAN  
ARP Caching  
WIRELESS SERVICES +  
SYSTEM SOFTWARE +  
EVENT LOG +

QoS POLICIES

RADIO0-802.11N<sup>2.4GHz</sup> ACCESS CATEGORIES

RADIO1-802.11N<sup>5GHz</sup> ACCESS CATEGORIES

ADVANCED

Hostname Cisco1142  
Cisco1142 uptime is 9 weeks

Services: QoS Policies - Advanced

IP Phone

QoS Element for Wireless Phones :  
☐ Enable ☐ Dot11e  
☒ Disable

IGMP Snooping

Snooping Helper: ☒ Enable ☐ Disable

AVVID Priority Mapping

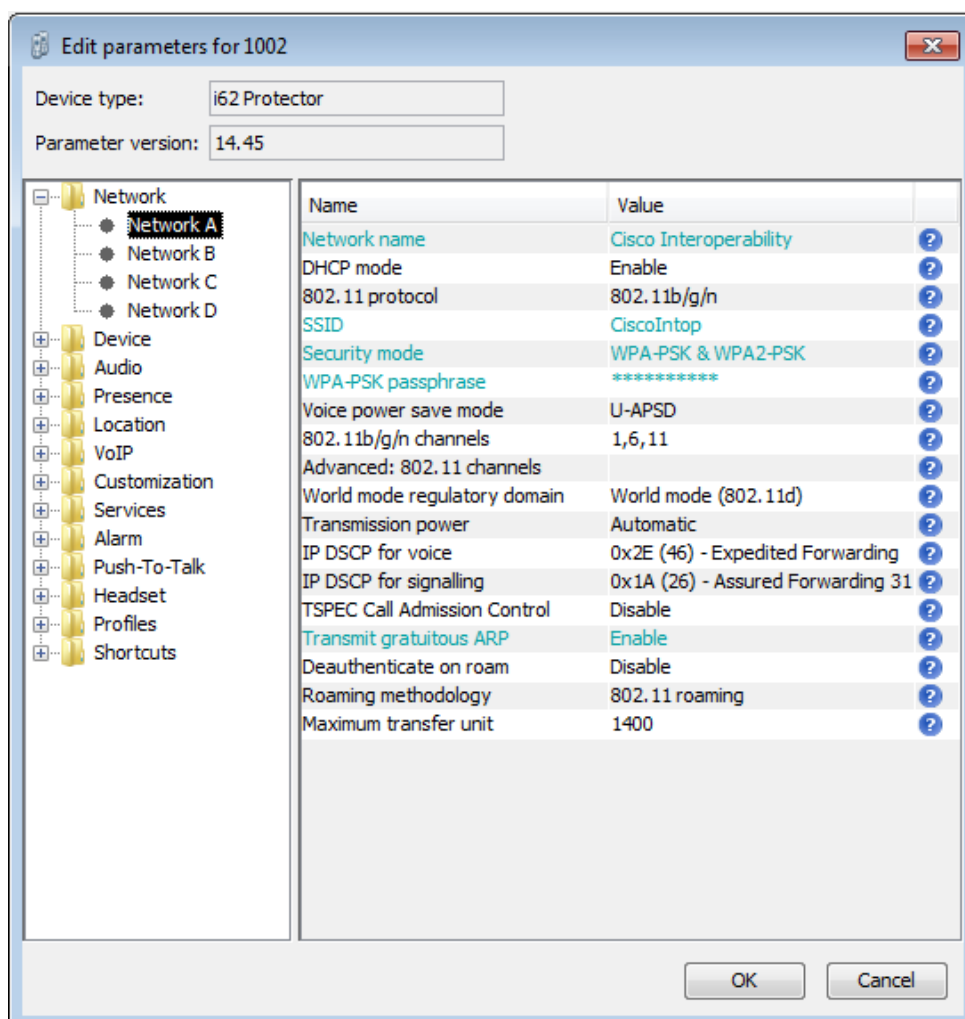
Map Ethernet Packets with CoS 5 to CoS 6: ☒ Yes ☐ No

WiFi MultiMedia (WMM)

Enable on Radio Interfaces:  
☒ Radio0-802.11N<sup>2.4GHz</sup>  
☒ Radio1-802.11N<sup>5GHz</sup>

Select yes to secure correct AVVID priority mapping and enable WMM for all used interfaces.

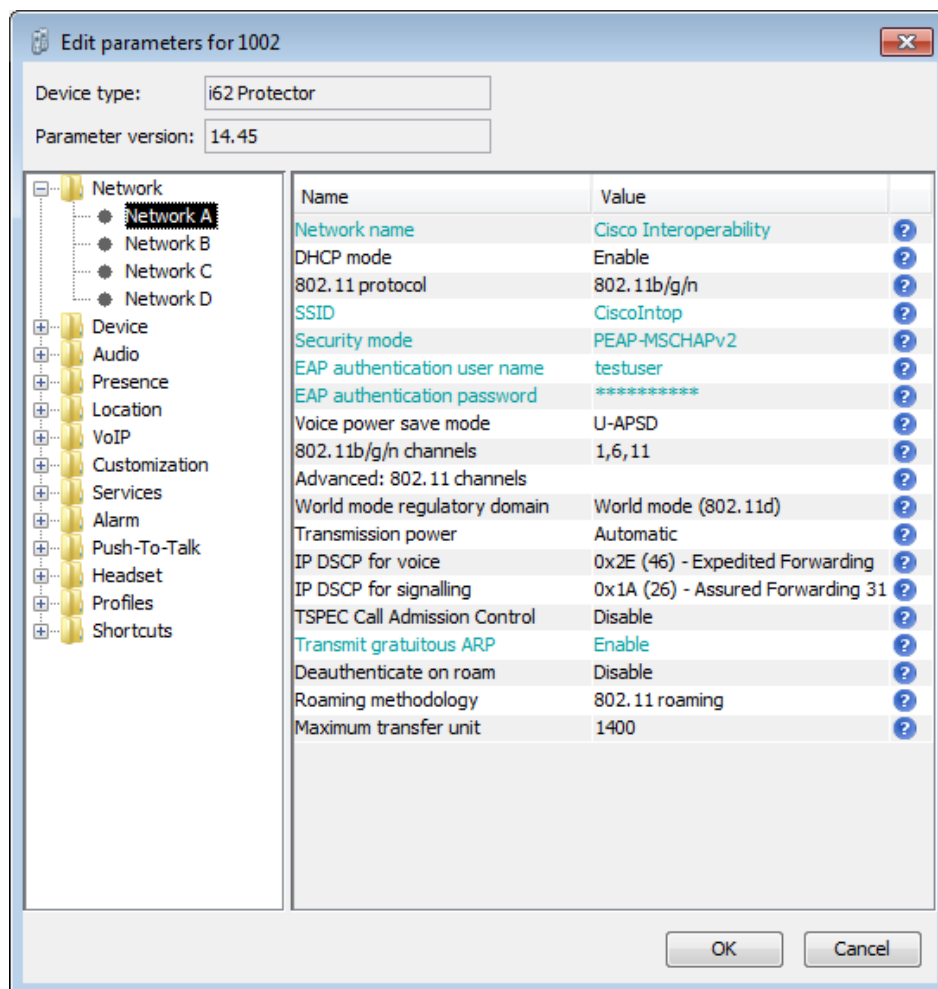
## Ascom i62



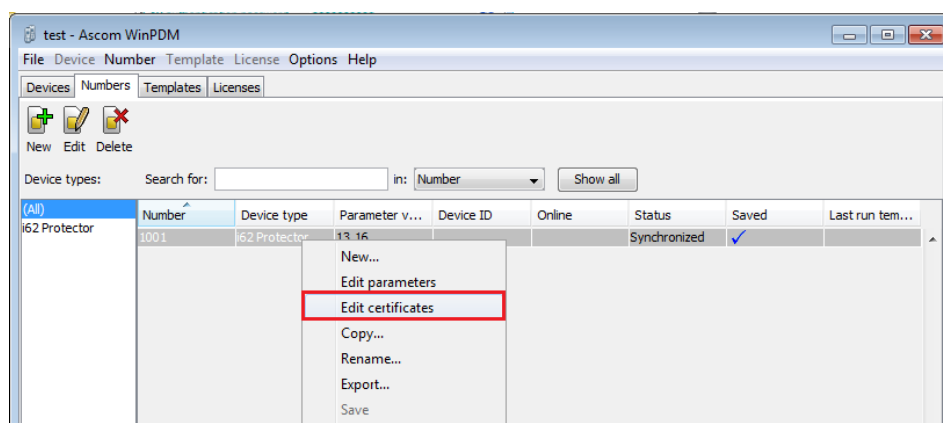
i62 network settings for WPA2-PSK

### Configuration:

See attached file (config\_ap\_1142n.txt) for configuration.



i62 network settings for 802.1X authentication (PEAP-MSCHAPv2)



If 802.1X Authentication is used a root certificate has to be uploaded to the phone by "right clicking" -> Edit certificates

## i62 configuration:

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

## 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	2011-12-06	SEKMO	Draft
R1	2011-12-15	SEKMO	Minor changes after review. R1 state.