[ ]

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

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) 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

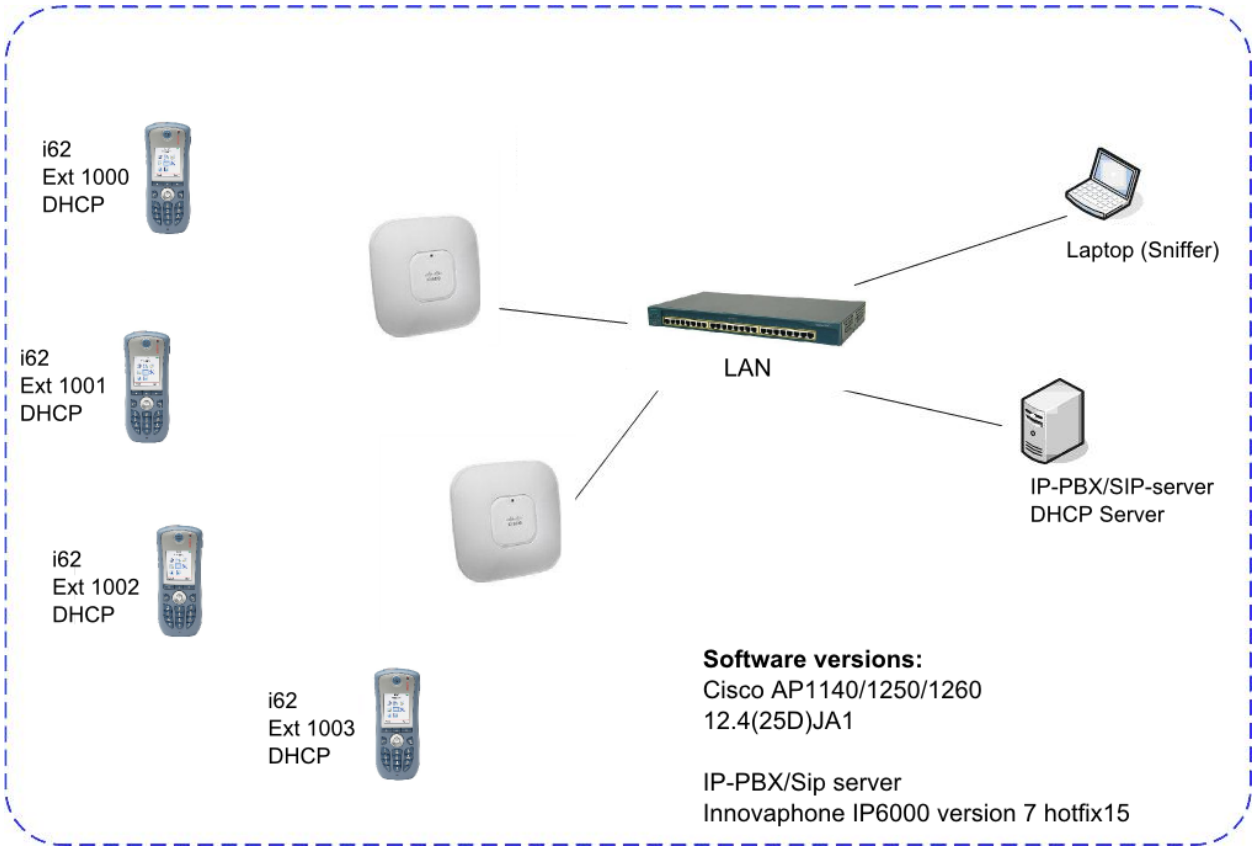
Cisco, (NASDAQ: CSCO), the worldwide leader in networking that transforms how people connect, communicate and collaborate, this year celebrates 25 years of technology innovation, operational excellence and corporate social responsibility. Information on Cisco can be found at http://www.cisco.com. For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

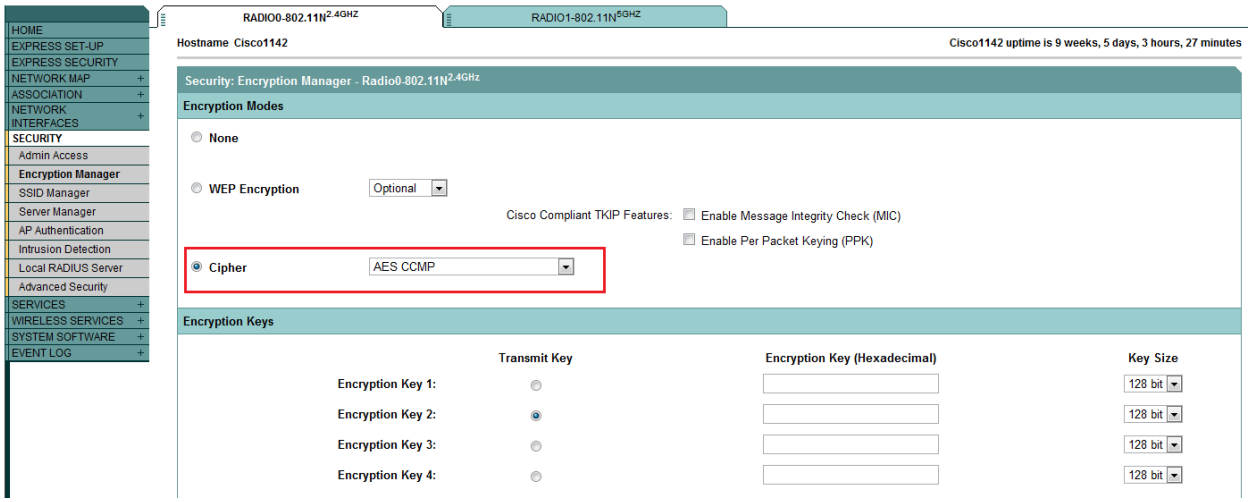
APPENDIX A: TEST CONFIGURATION

Cisco AP1140/1250/1260

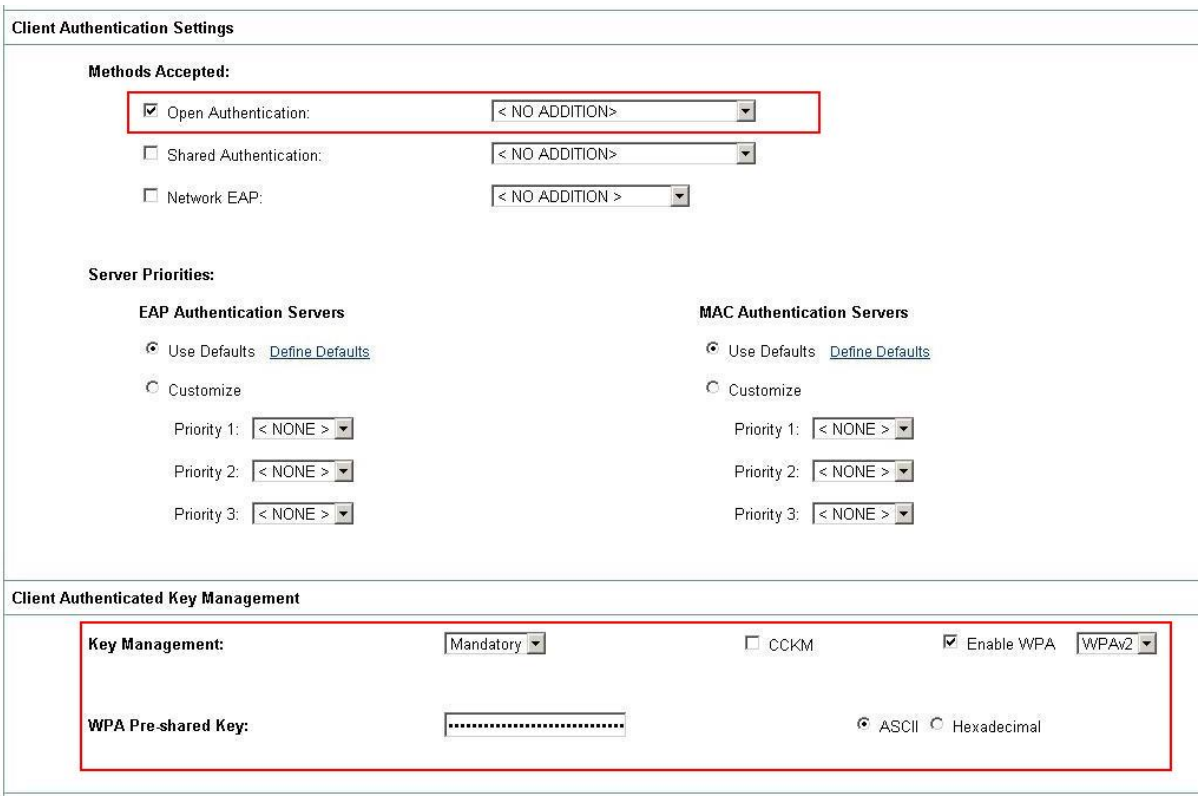
In the following chapter you will find screenshots and explanations of basic settings in order to get a Cisco AP1140/1250/1260 to operate with an Ascom i62.

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

Security settings (PSK)



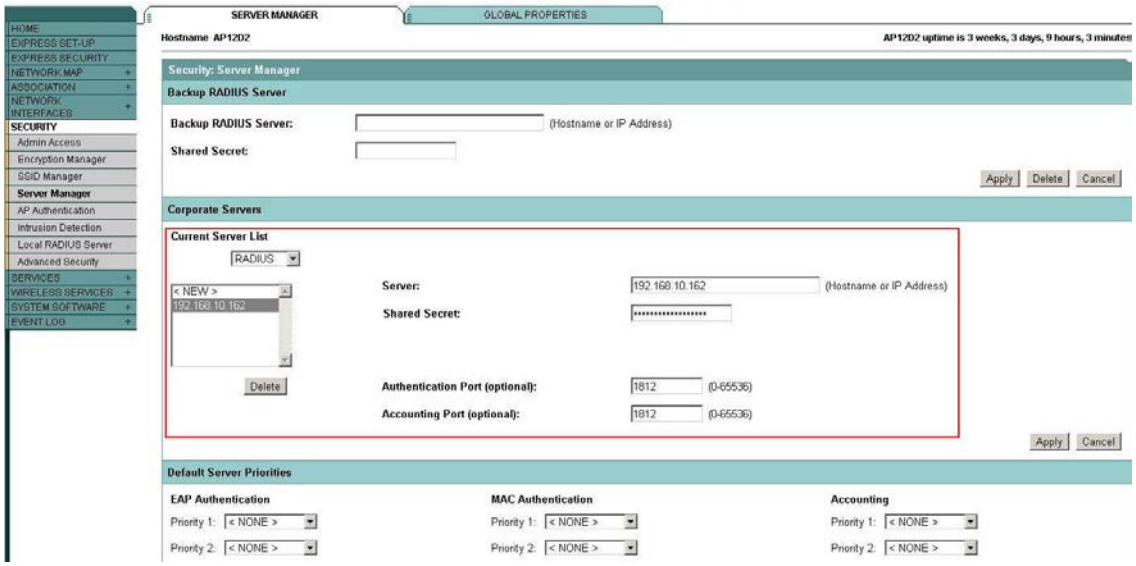
Configuration of security profile WPA2-PSK AES/CCMP encryption (1). Set Cipher under SECURITY/Encryption Manager.



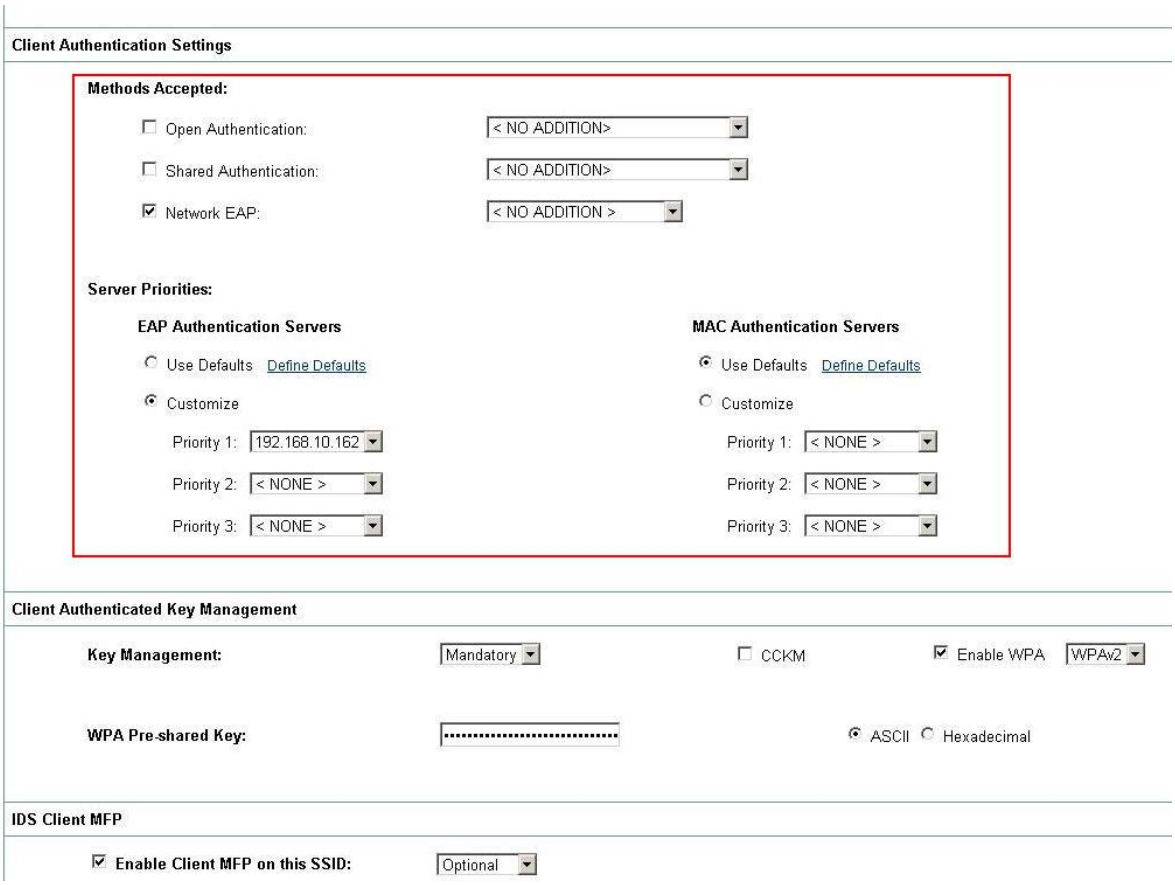
Configuration of security profile WPA2-PSK AES/CCMP encryption (2). Set Key Management to Mandatory and choose to enable WPA (WPAv2)

Note. By Choosing "WPA", both WPA and WPA2 are enabled. (Mixed mode)

PEAP-MSCHAPv2 using an external authentication server



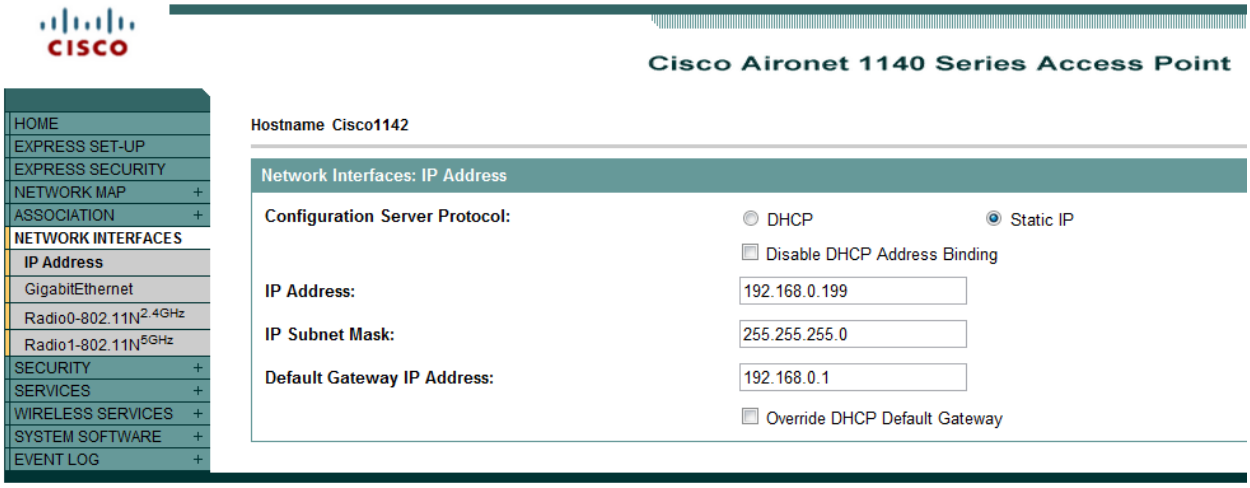
Configuration of authentication using Radius sever (Step1). The IP address and the secret must correspond to the IP and the credential used by the Radius server.
Tests were performed with FreeRadius.



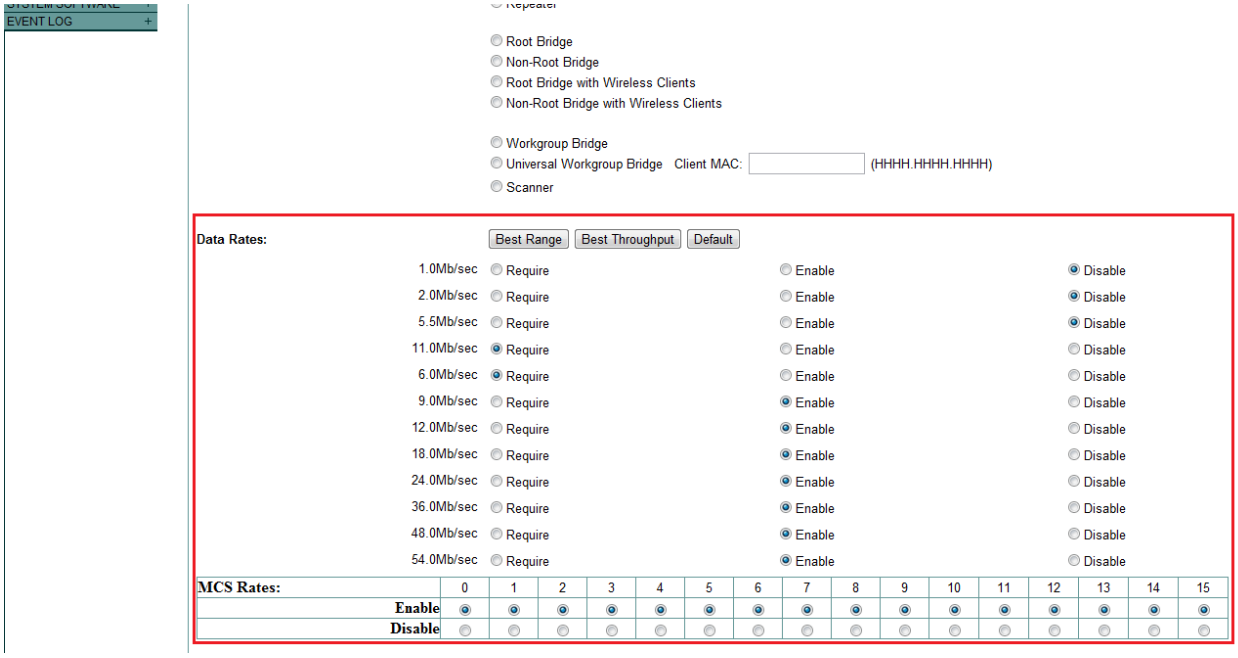
Configuration of authentication using Radius sever (Step 2). Under the tab SECURITY/SSID Manager, select Network EAP as Methods Accepted (Select <NO ADDITION>) and then choose the server created in the previous step.

Note. By Choosing "WPA", both WPA and WPA2 are enabled. (Mixed mode)

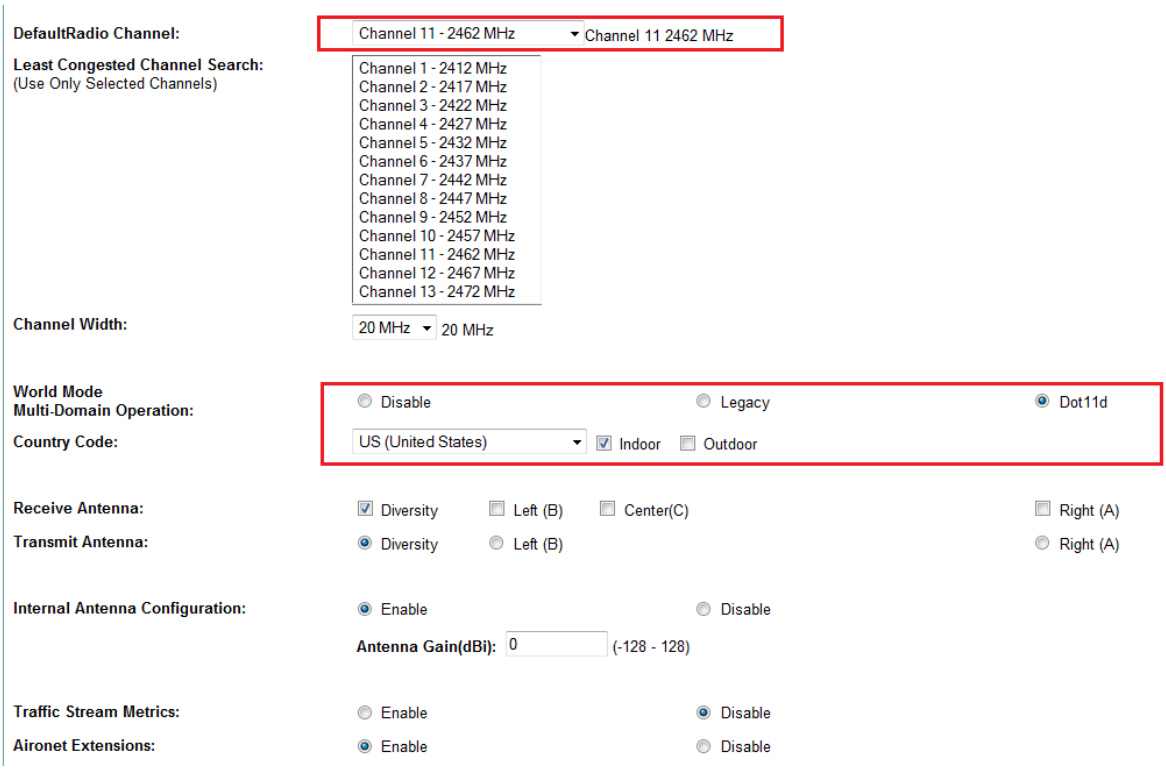
General settings (QoS, Radio)



IP address settings. Example shows configuration with static IP.



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.



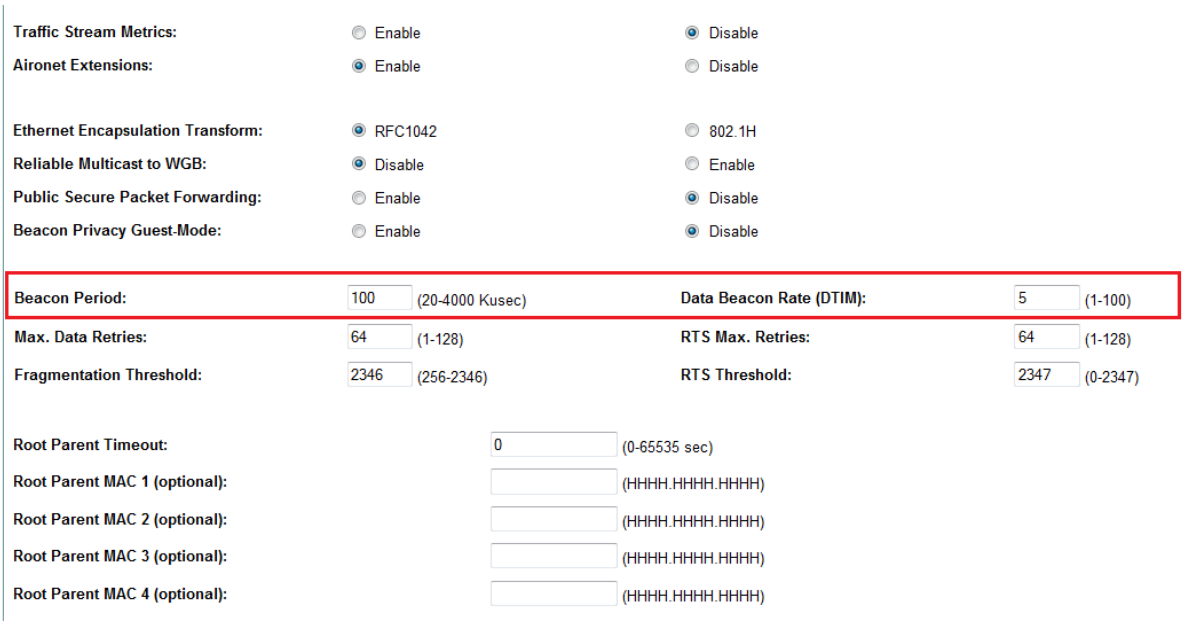
For 802.11b/g/n Ascom support only 3 channel deployments using channel 1,6 and11. For 802.11a/n use channels according to the infrastructure manufacturer and country regulations. Enable Dot11d and chose your country.

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.

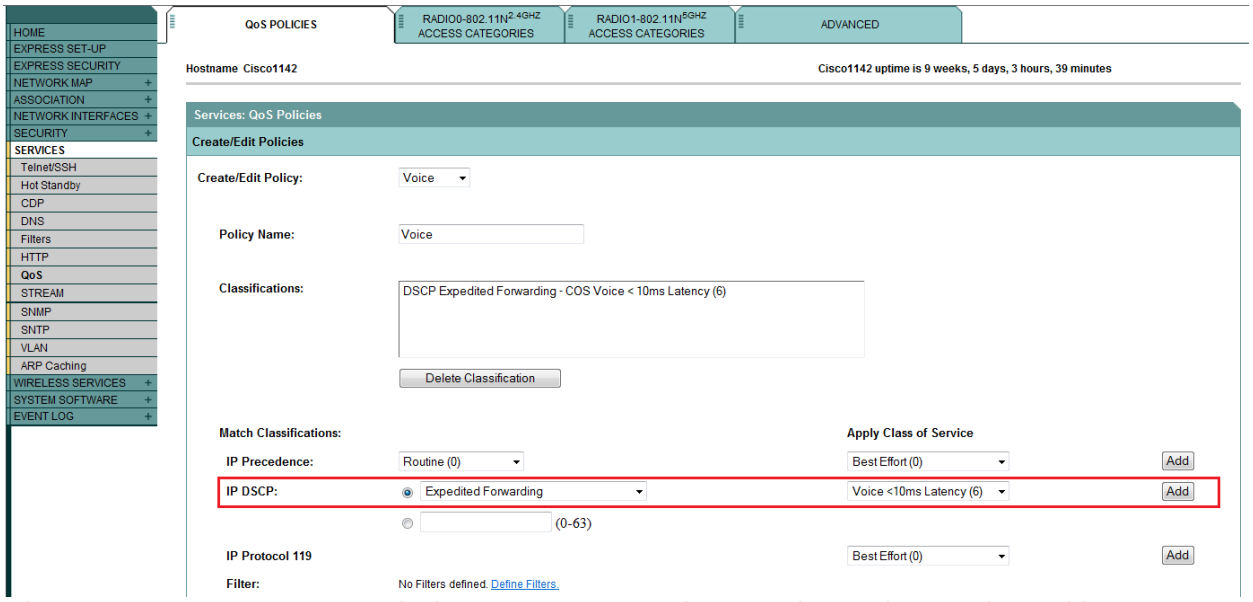
Since the passive part of the scan phase is limited to 70 ms, a beacon interval of less than 70 ms (e.g. 60 ms) will give the best roaming performance.

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

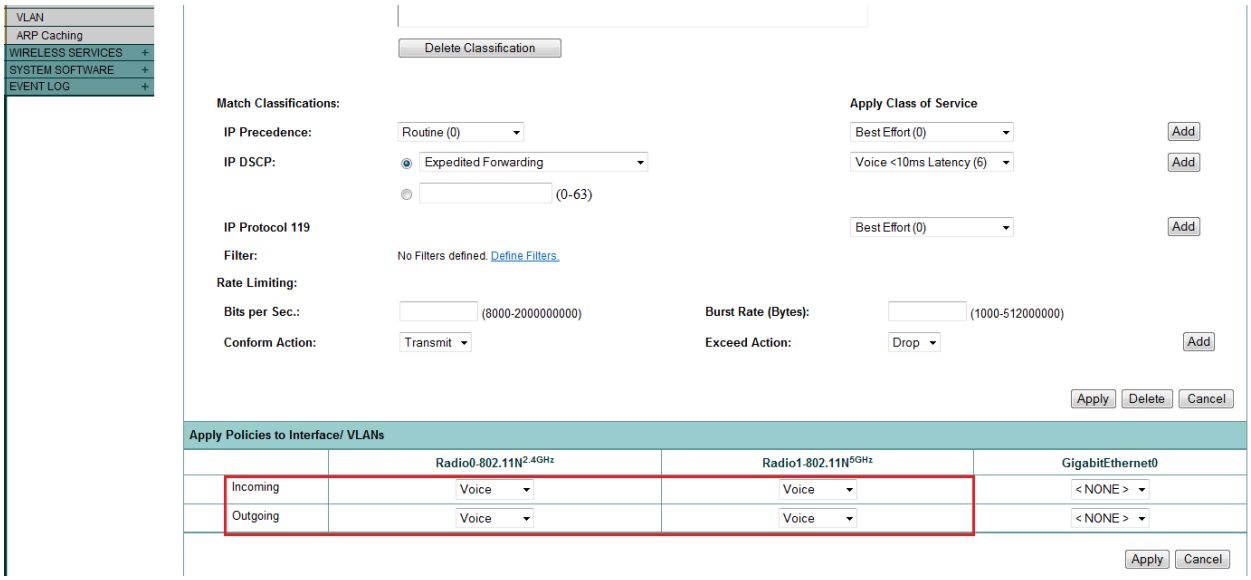
For 802.11an: Using 40 MHz channels will reduce the number of non DFS channels to only 2 in ETSI regions.



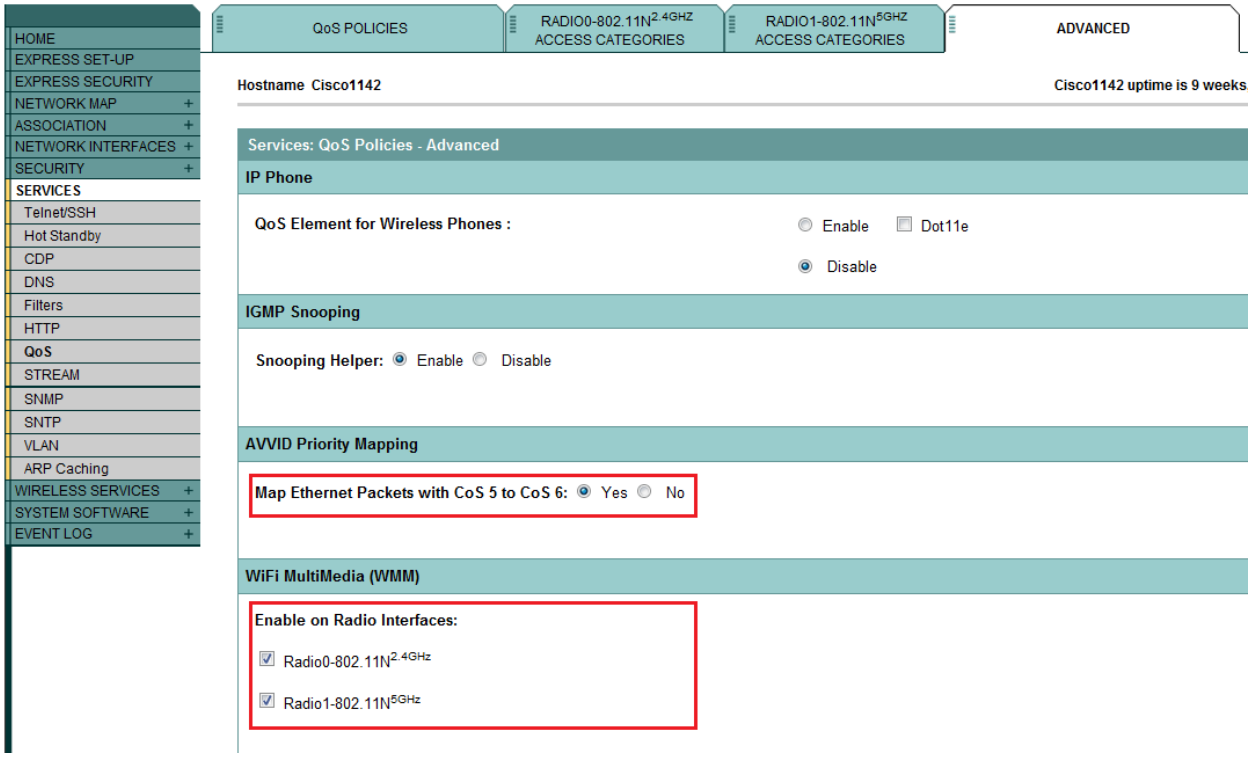
Under tab SECURITY/SSID Manager Set Beacon Period to 100ms and Set DTIM period to Ascoms recommended value 5. DTIM value 5 values are recommended in order to allow maximum battery conservation without impacting the quality. Using a lower DTIM value is possible but will reduce the standby time slightly.



It is necessary to create a QoS role that maps a DSCP value to a Class Selector value. It 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.

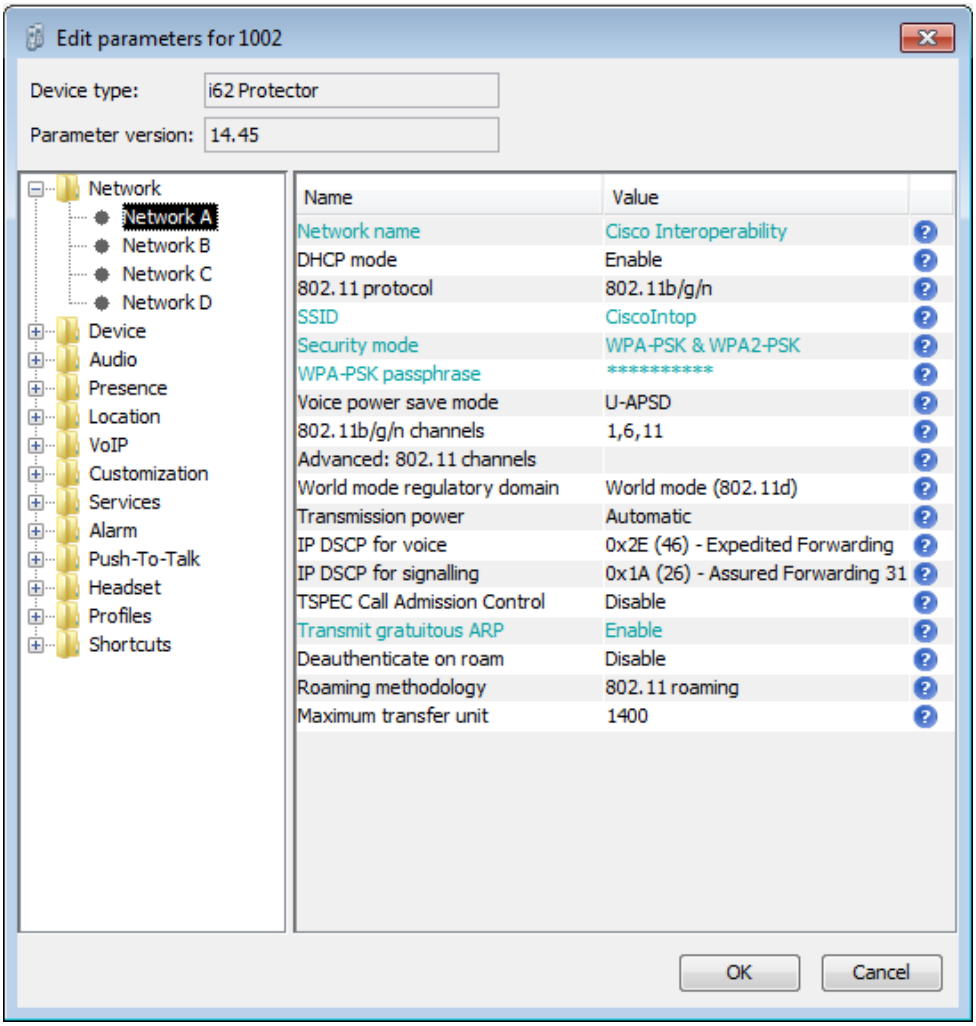


Apply the “Rule” for both incoming and outgoing traffic on the radio interfaces used.



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

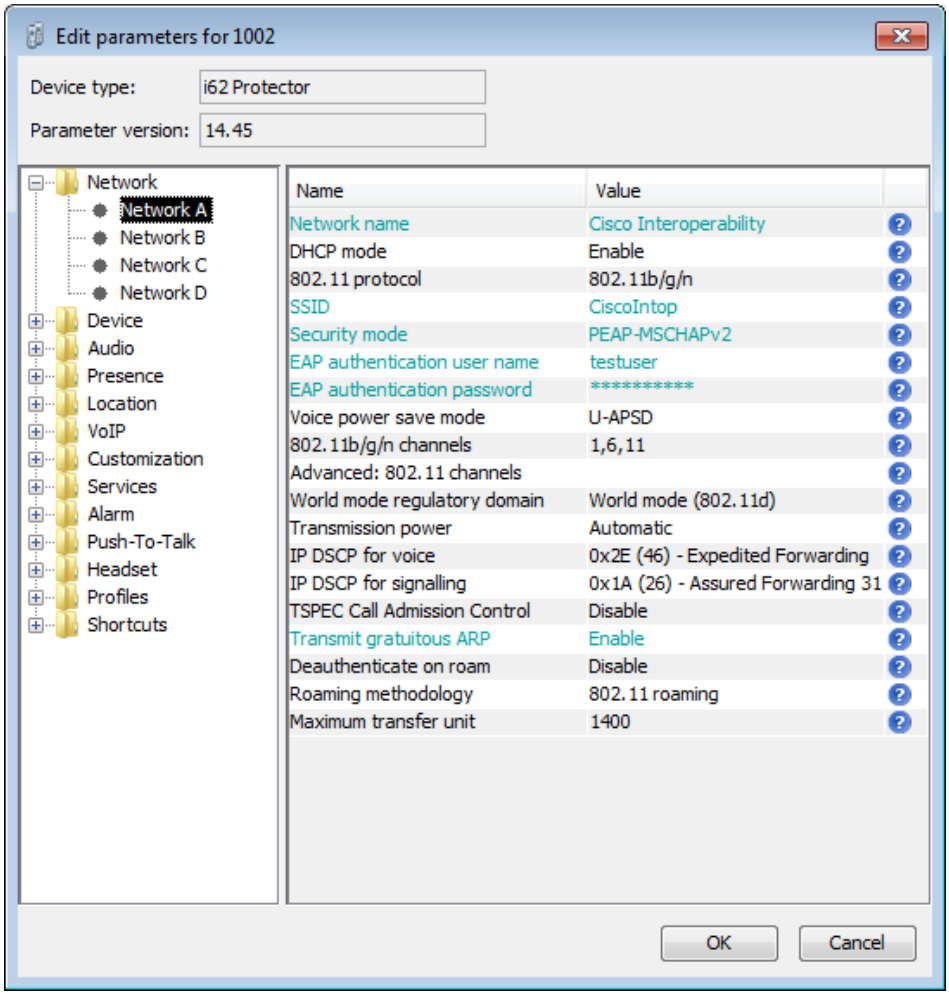
Ascom i62



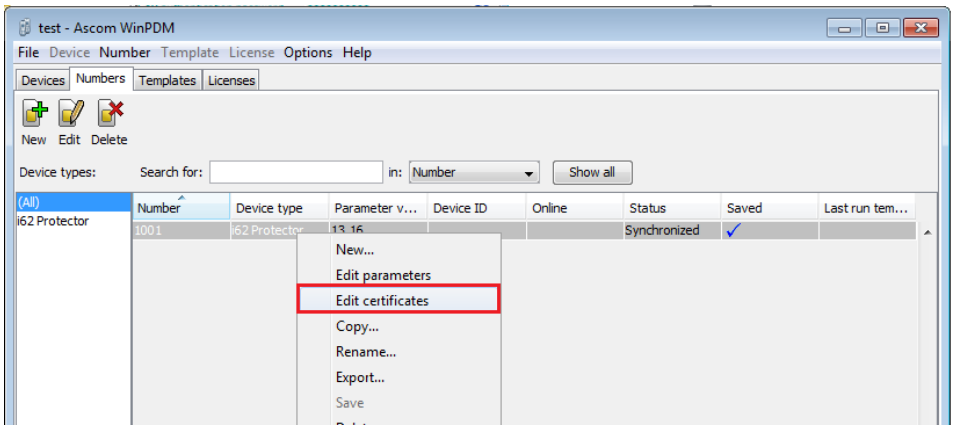
i62 network settings for WPA2-PSK

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.