Technology Solution Guide

Deploying Ascom i62 with Aruba Networks' Secure Mobility Solution

Ascom i62 Handset and OEM derivatives
Software version 4.3.12

Aruba iAP
92/92/104/105/134/134/175
AOS version 6.2.1.0-3.3.0.2

September 4 2013

WARRANTY DISCLAIMER

THE FOLLOWING DOCUMENT, AND THE INFORMATION CONTAINED HEREIN IS PROVIDED ON AN "AS IS" BASIS. ARUBA MAKES NO REPRESENTATIONS, WARRANTIES, CONDITIONS OR GUARANTEES AS TO THE USEFULNESS, QUALITY, SUITABILITY, TRUTH, ACCURACY OR COMPLETENESS OF THISDOCUMENT AND THE INFORMATION CONTAINED IN THIS DOCUMENT.

DISCLAIMER OF LIABILITY

Aruba Networks, Inc. disclaims liability for any personal injury, property or other damages of any nature whatsoever, whether special, indirect, consequential or compensatory, directly or indirectly resulting from the certification program or the acts or omissions of any company or technology that has been certified by Aruba Networks.

Certification does not mean that the company is a subcontractor or under the technical control or direction of Aruba Networks. In conducting the certification program Aruba Networks is not undertaking to render professional or other services for or on behalf of any person or entity.

Table of Contents

Introduction

This document describes the steps and guidelines necessary to configure Aruba's wireless LAN (AOS version. 6.2.1.0-3.3.0.2) infrastructure to work interoperable with Ascom's i62 handsets.

The guide is intended to be used in conjunction with Aruba and Ascom configuration guides. Please contact the respective company's sales engineering or support groups should additional information be required.

Solution Verified: Ascom Phones

Aruba Product: Aruba Campus WLAN Solution OS version 6.2.1.0-3.3.0.2

Partner Solution Tested: Ascom i62 Handset; Software version 4.3.12

Solution Components

Aruba Campus WLAN Solution

Secure and reliable mobility is the responsibility of the enterprise network, which must support a wide range of converged clients over wireless, wired, and remote access networks. Laptops and smartphones are capable of simultaneously running voice, data, and now video applications, an operating model that breaks traditional dedicated VLAN and SSID architectures. Delivering the quality of service (QoS), bandwidth, and management tools necessary to accommodate these devices on a grand scale – within a campus environment, to users on the road, and in branch offices – requires a specially tailored system design.

Aruba's unique application and device fingerprinting enable the system to detect the types of traffic flows, and the devices from which they originate. The network can then be dynamically conditioned to deliver QoS - on an application-by-application, device-by-device basis - as needed to ensure highly reliable application delivery. Aruba's integrated policy enforcement firewall isolates applications from one another to essentially create multiple dedicated virtual networks, and then allocates the necessary bandwidth for each user and application.

To ensure reliable application delivery in changing RF environments, Aruba's Adaptive Radio Management (ARM) technology forces client devices to shift away from the noisy 2.4GHz band to the quieter 5GHz band, adjusts radio power levels to blanket coverage areas, load balance by shifting clients between access points, and even allocates airtime based on the capabilities of each client device. The result is a superb user experience without any user involvement.

These services are complemented by security systems that ensure the integrity of the network. Rogue detection, wireless intrusion and prevention, access control, remote site VPN, content security scanning, end-to-end data encryption, and other services protect the network and users at all times.

Aruba's extensive portfolio of campus, branch/teleworker, and mobile solutions simplify operations and secure access to unified communications applications and services - regardless of the user's device, location, or network. This dramatically improves productivity, lowering capital and operational costs while providing a superior uninterrupted user experience.

Ascom Solution

The Ascom i62 VoWiFi handset replaces the Ascom i75, offering a sleeker design, high-resolution color TFT display, IP44 compliant construction, and longer battery time. The i62, like other Ascom handsets, can be managed over-the-air (OTA) and is designed to interoperate within a Wi-Fi network. With the Ascom i62 VoWiFi handset, users get a single mobile device for voice conversations, text messaging and alarms from systems throughout their hospital or business.

Certified Product Summary

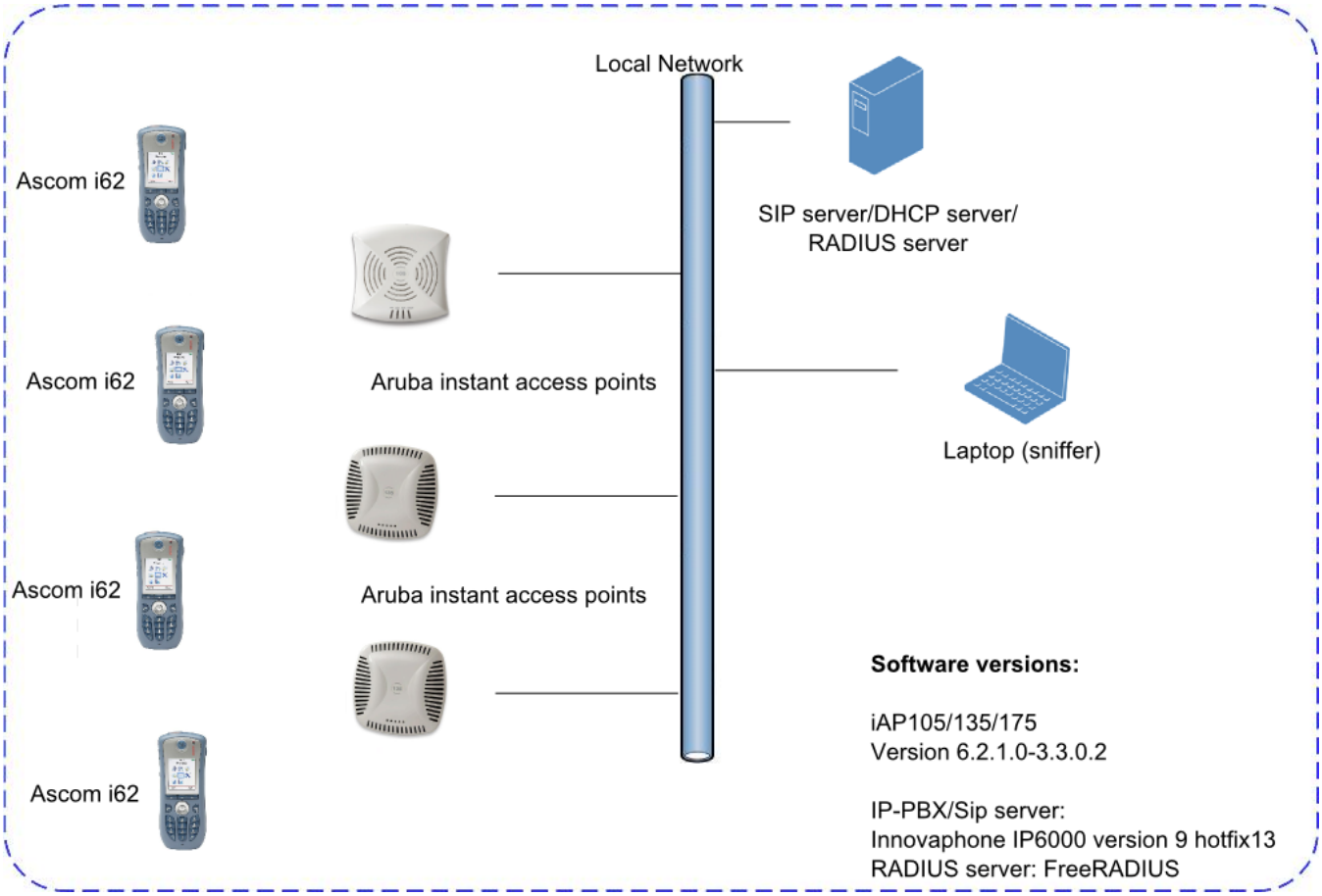
Manufacturer	Ascom Wireless Solutions
Products Certified	Ascom i62 and OEM derivatives
• Hardware Model Numbers	WH1-xxxx
• Software Version Numbers	4.3.12
RF Features Tested	
• Radio Supported	802.11a/b/g/n
QoS Features Supported / Tested	WMM
• Powersave Features Tested	U-APSD
• Encryption Supported	WEP64/128, WPA-PSK, WPA2-PSK, PEAP-MSCHAPv2, EAP-TLS
• Encryption Tested	WPA-PSK, WPA2-PSK, PEAP-MSCHAPv2, EAP-TLS
• 802.11h Supported	Yes
• Key Caching Support for Optimized Roaming	Not supported by iAP
Voice Specific Features	
• Protocols Supported	SIP-UDP, SIP-TCP, H323
• Control Traffic Pattern	Handset to Server and vice versa
• Voice Traffic Pattern	Peer-to-peer (between handsets)
• # of Calls per AP Tested	18 calls (not AP-capacity limited)

ArubaEdge Solution Qualification

Qualification Objective

Validate the interoperability of the Ascom i62 with the Aruba's wireless LAN infrastructure(version 6.2.1.0-3.3.0.2).

Network Topology



Settings on the Aruba WLAN

The following Aruba Instant Access Point configuration settings are recommended for use with Ascom i62 handsets:

- RF Recommended Settings for Ascom
  - Beacon Interval: 100ms
  - DTIM Period: 5
  - WMM/ U-APSD Enabled
  - 802.11d Regulatory Domain: World Mode
- Encryption and Authentication
  - The handset and the WLAN infrastructure support and were tested with WPA/WPA2 enterprise and PSK. Please refer the Aruba configuration guide for additional information on how the SSIDs and encryption/authentication methods should be configured.
- Adaptive Radio Management
  - Enable ARM, voice aware scanning, WMM / UAPSD, and band steering.

Ascom Settings

The following Ascom i62 Handset configuration settings are recommended for use with Aruba Instant Access Point.

Ascom i62 Configuration:

- World Mode Regulatory Domain set to World mode.
- IP DSCP for Voice: 0xC0 (46) – Expedited Forwarding
- IP DSCP for Signaling: 0x68 (26) – Assured Forwarding 31
- Transmit Gratuitous ARP: Enable

Refer to Appendix A for additional details.

Test Methodology

Summary Test Results

The features and functions listed below were assessed during interoperability testing. The test results are presented in the right-most column

WLAN Features

High Level Functionality	Result
Association, Open with No Encryption	OK
Association, Open with Static WEP64/128	Not tested
Association, WPA-PSK, TKIP Encryption	OK
Association, WPA2-PSK, AES Encryption	OK
Association, PEAP-MSCHAPv2 Auth., TKIP Encryption	OK
Association, PEAP-MSCHAPv2 Auth., AES Encryption	OK
Association, EAP-TLS	OK
Association, Multiple ESSIDs	OK
Beacon Interval and DTIM Period	OK
Preauthentication	N/A
PMKSA Caching	OK
WPA2-Opportunistic/Proactive Key Caching	Not supported by iAP
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 (Avg roaming time 31ms) *
Roaming, WPA2-PSK, AES Encryption	OK (Avg roaming time 42ms) *
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption	NOK (Avg roaming time 300-500ms) */**

*) Stated roaming times were measured using 802.11bg (n). Refer to Appendix B for details.

**) Results observed without Opportunistic Key Caching . Opportunistic Key Caching is not supported by Aruba instant AP. Note that roaming time might be higher than 300-500ms depending on RADIUS server and network topology

Know Limitations

- Opportunistic Key Caching is not supported by Aruba Instant AP. Enterprise/.1X authentication such as PEAP-MSCHAPv2 is therefore not recommended for voice deployments. Recommended security method is WPA/WPA2 - PSK

Conclusion

The verification, including association, authentication, roaming, and load test produced very good results overall. Roaming times were in general good with roaming times of around 40ms both when using WPA2-PSK (TKIP and AES). It was however noted that the instant access points does not support opportunistic key caching. This makes Enterprise/.1X authentication unsuitable for voice deployments with the Aruba instant access points.

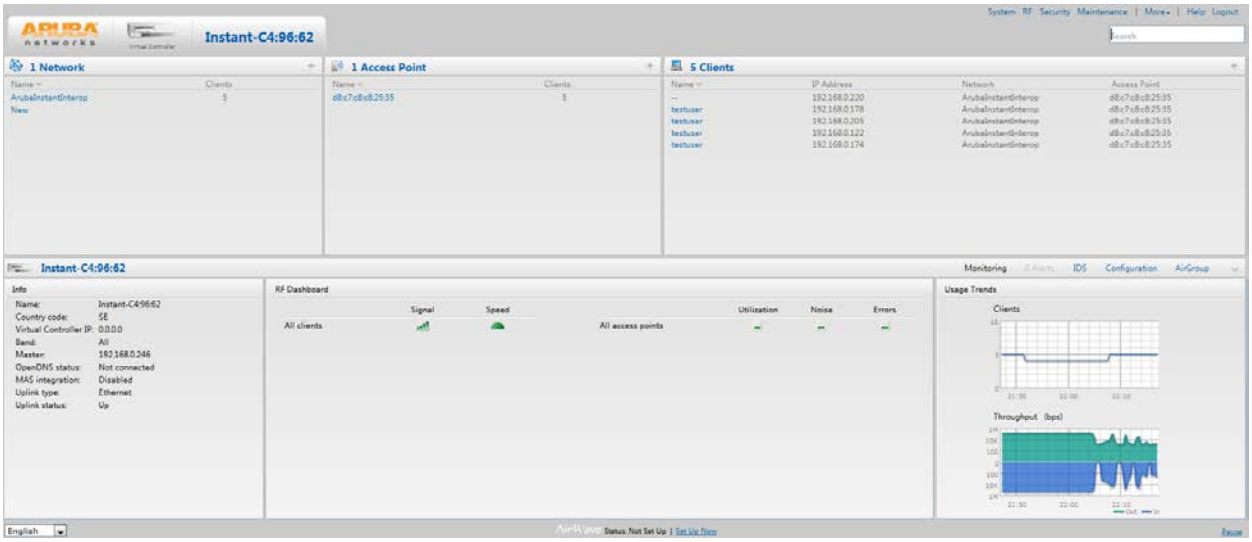
Load testing showed that more than 16 Ascom i62 Handsets could maintain a call via a single Aruba access point when tested both in active and U-APSD modes. Note that the number of 16 was the maximum number of devices tested and not the capacity limit.

Appendix 1

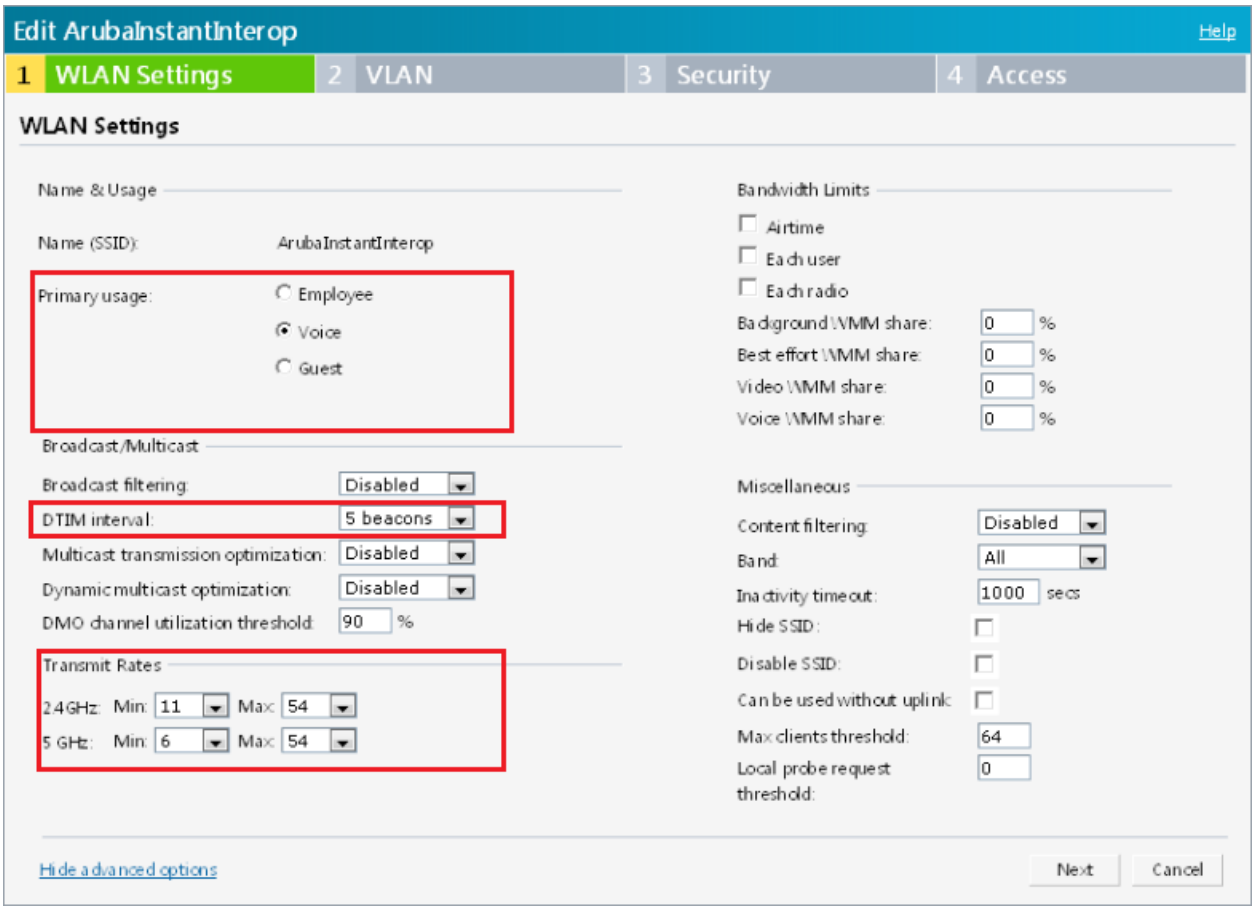
This section includes screenshots and explanations of basic settings required to use Ascom i62 Handsets with Aruba Instant Access Points. Please note the security settings of each test case, as they were modified according to needs of the test cases.

The configuration file is found at the end of this appendix

General settings (SSID, Radio and QoS)

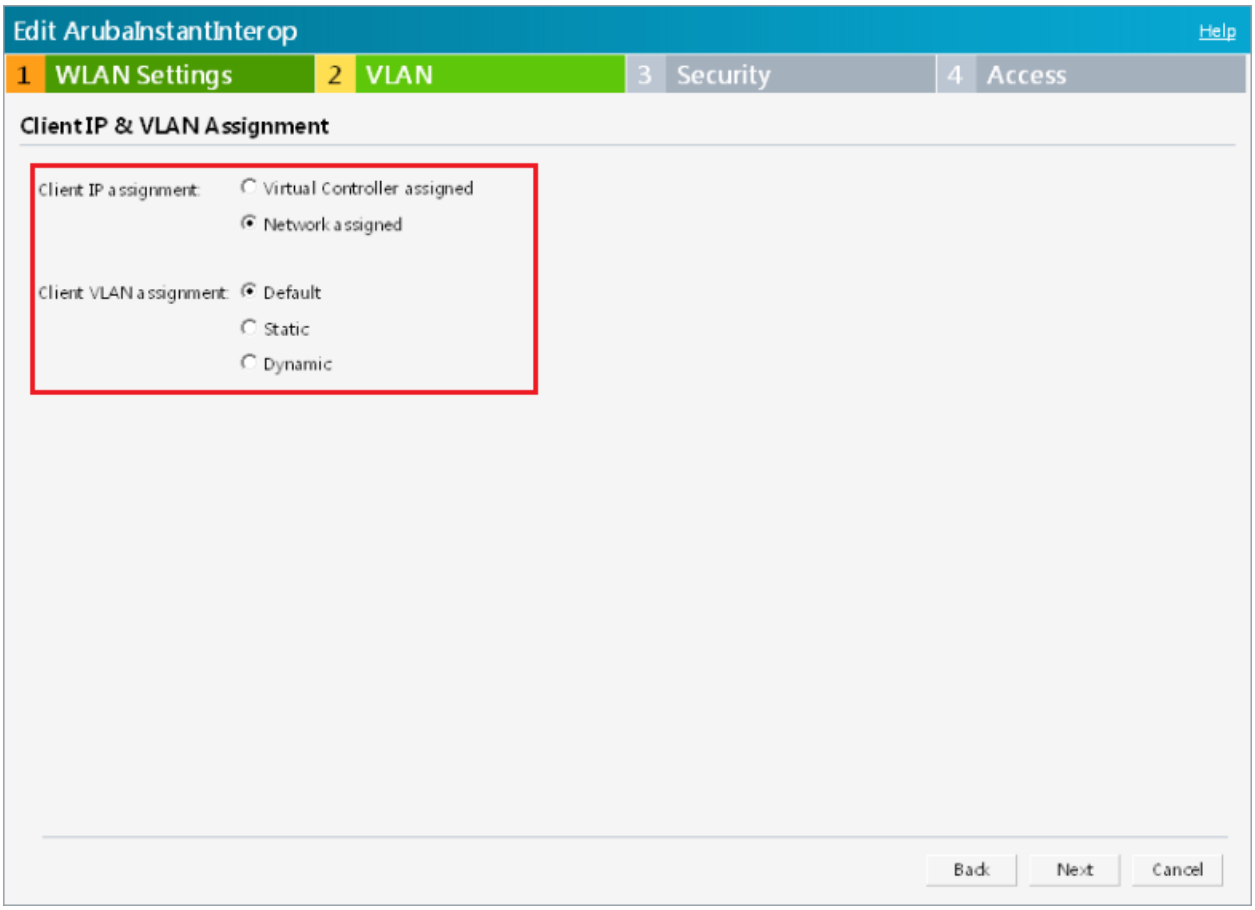


General overview



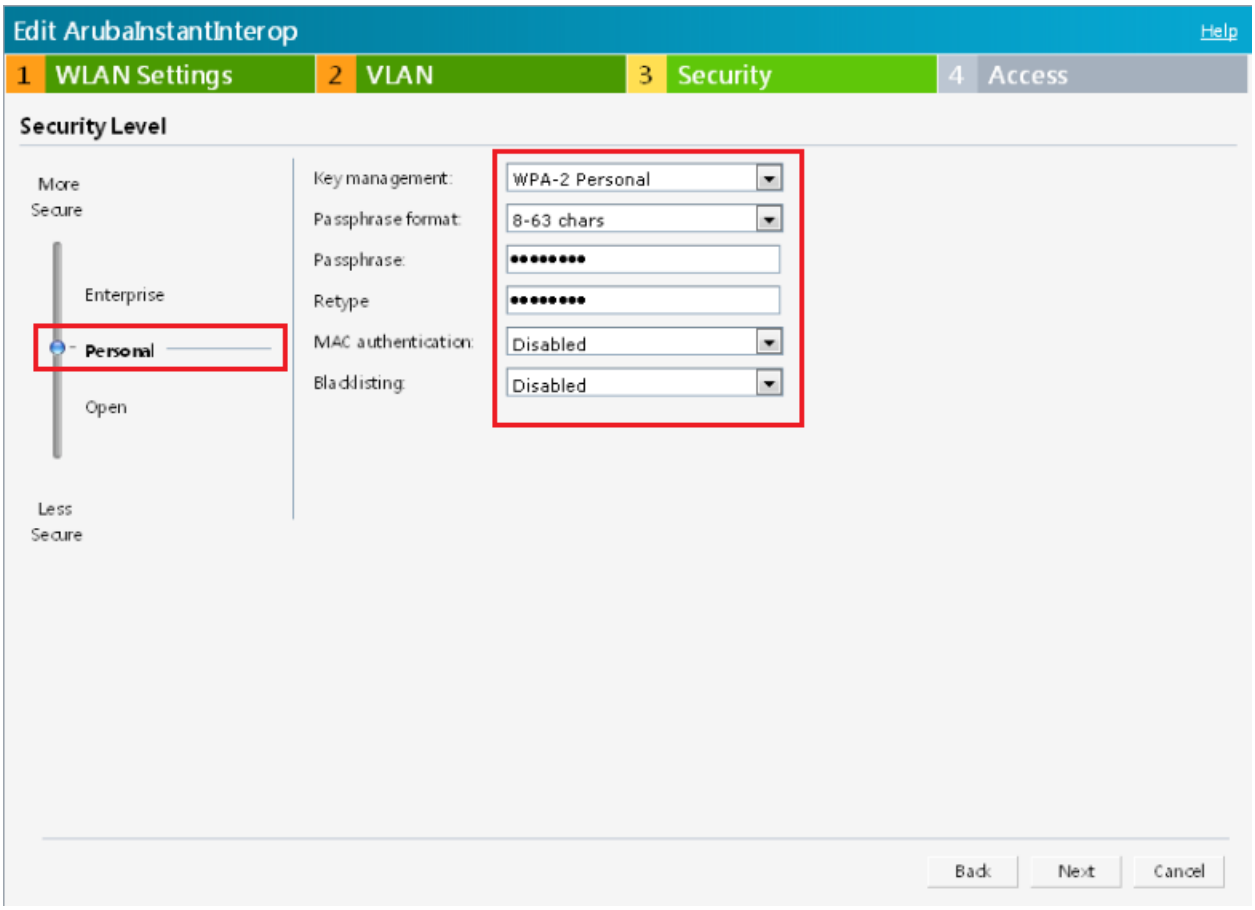
Network configuration -> WLAN settings

- Select Voice as primary usage
- Set DTIM Interval to 5. This value is recommended for maximum battery conservation without impacting call quality. A lower value is possible but will decrease the battery life slightly.
- The default Transmit rates will work fine. To increase the performance it is recommended to disable the lowest data rates.



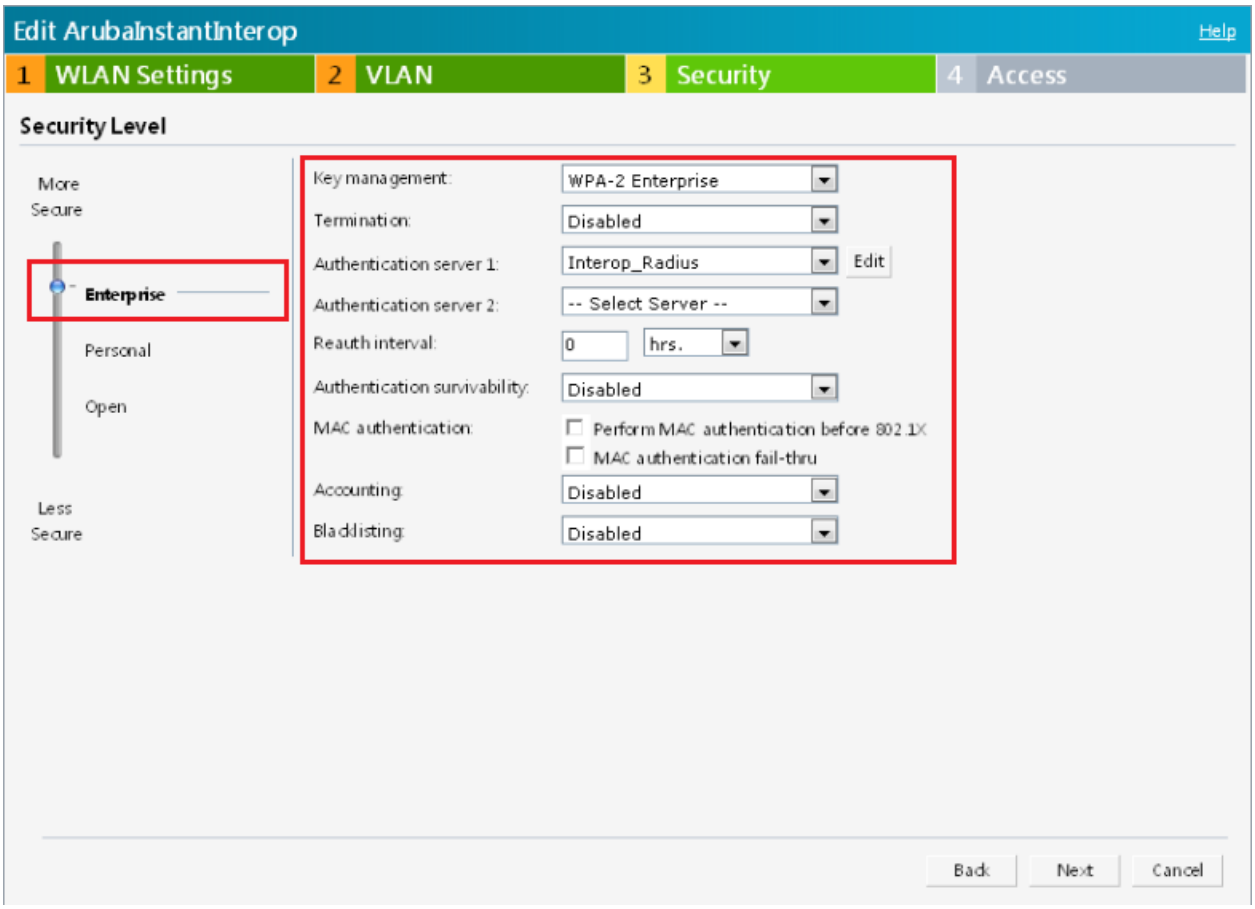
Network configuration -> VLAN settings

- Client IP assignment is handled by the network in the test setup.
- VLAN assignment set to Default



Network configuration -> Security (Personal – WPA2-PSK)

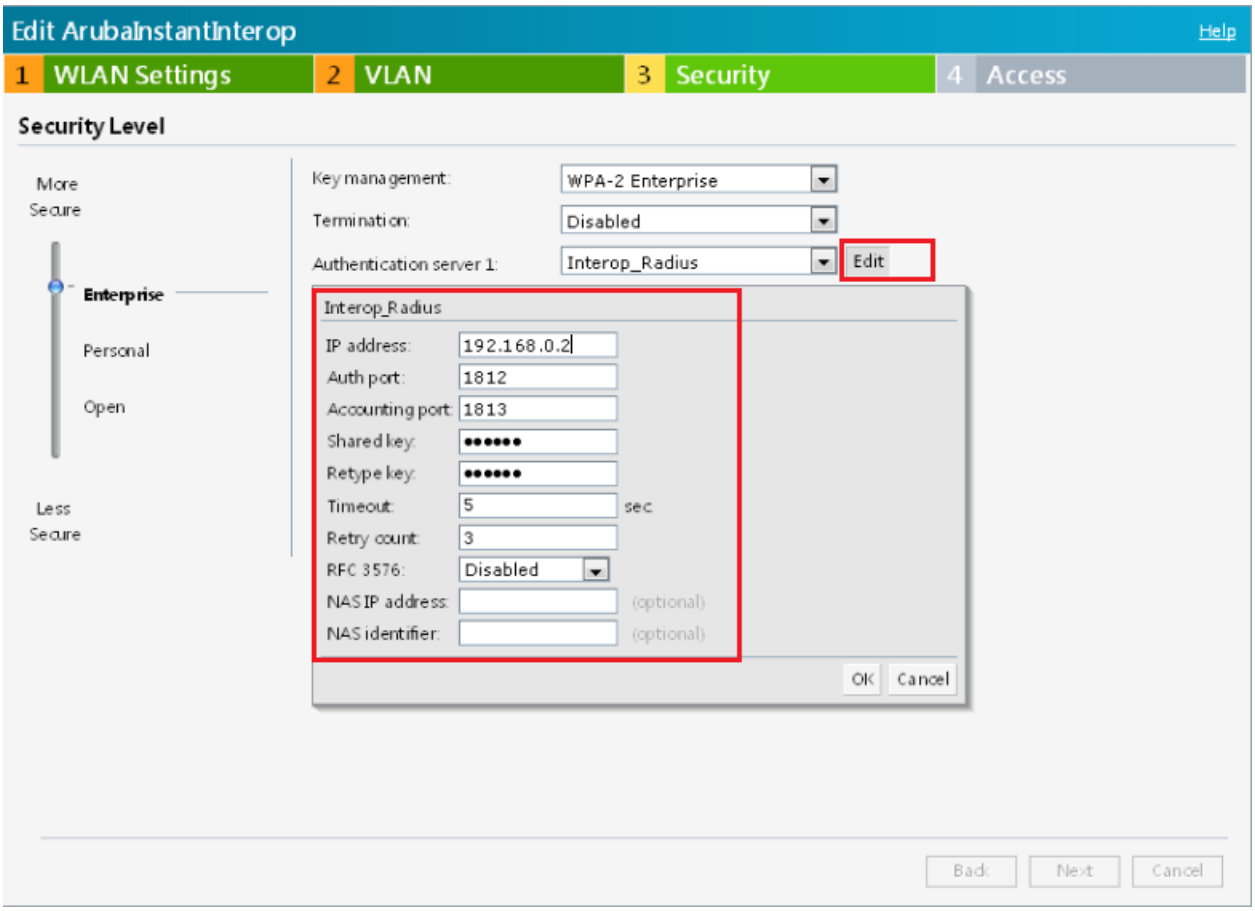
- Key Management set to WPA2. WPA2 also implies that AES/CCMP encryption will be used. (WPA implies TKIP encryption)



Network configuration -> Security (Enterprise/.1X)

- Set Key management to WPA-2 Enterprise
- Configure Authentication server 1. See next picture

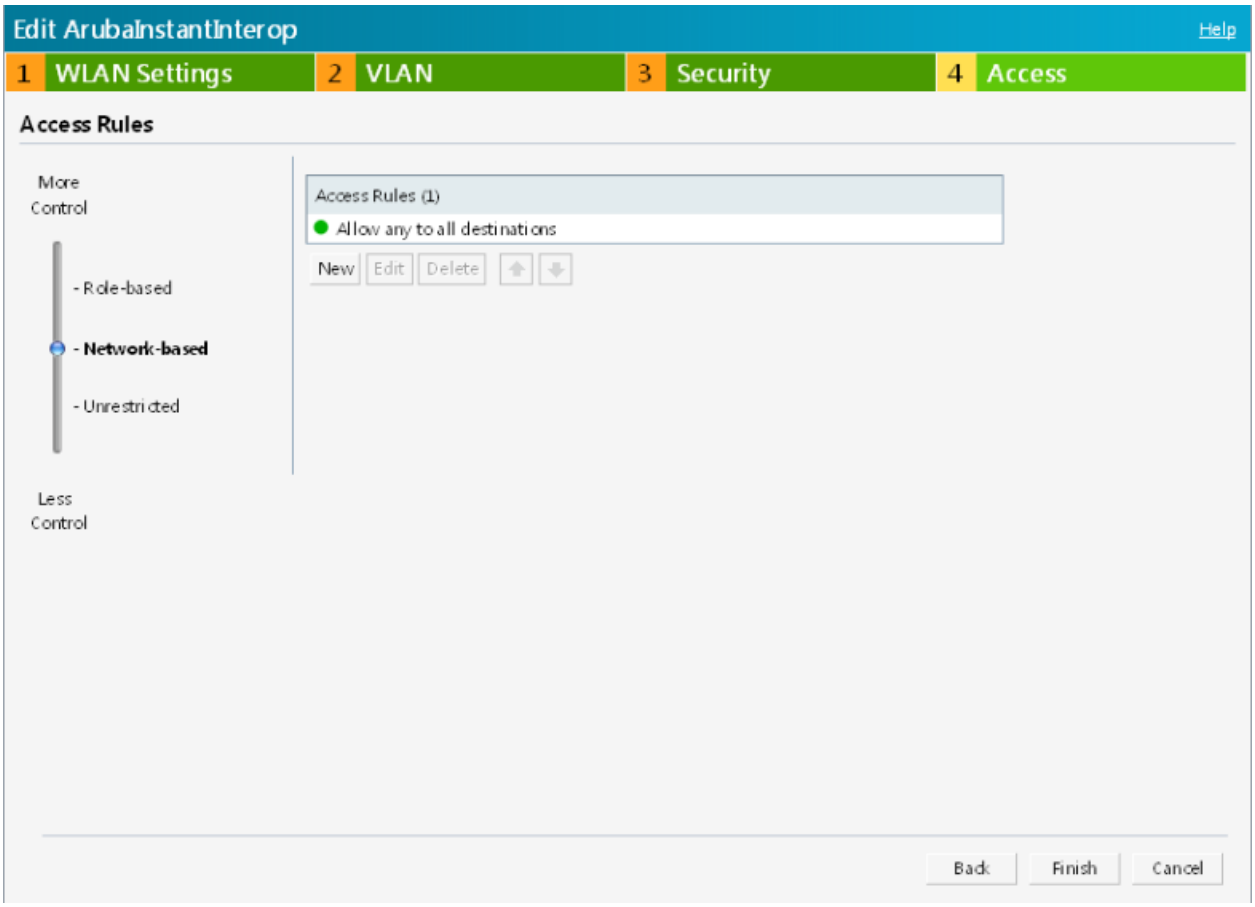
Note. Enterprise (.1X) authentication is not recommended due to lack of Opportunistic Key Caching



Network configuration -> Security (Enterprise/.1X)

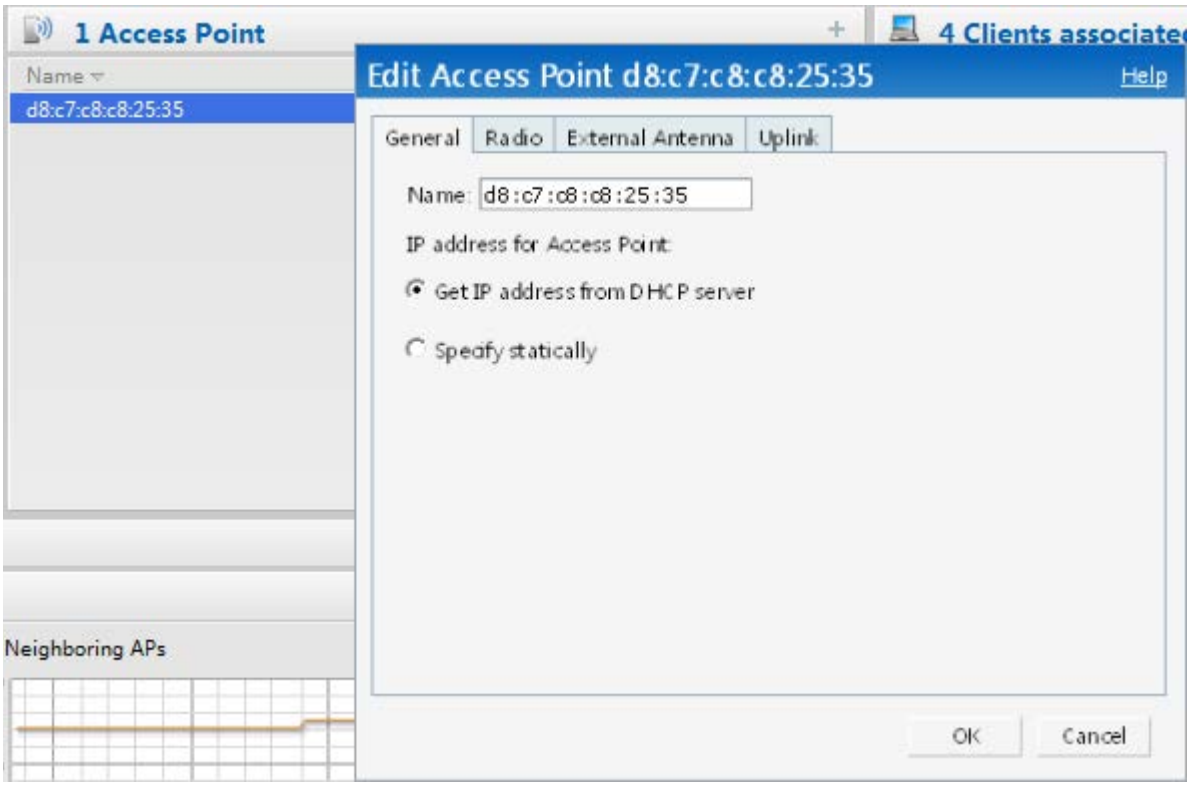
- The IP address and the secret must correspond to the IP address and the credential used by the Radius server.

Note. Enterprise (.1X) authentication is not recommended due to lack of Opportunistic Key Caching



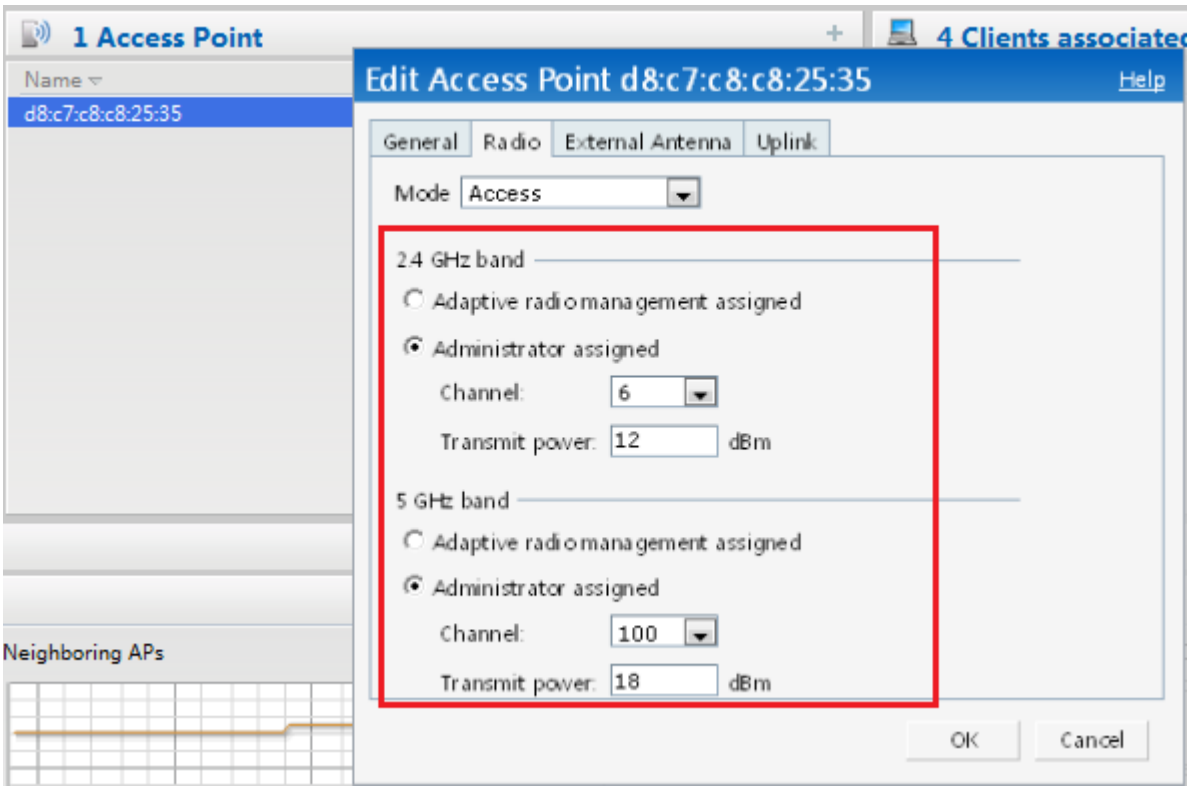
Network configuration -> Access

- Access rules set to default (Network-based)



Configuration of Access Points.

- The access points will get their IP address assigned by a DHCP server.



Configuration of Access Points.

- For test purpose the channel and transmit power was assigned manually.

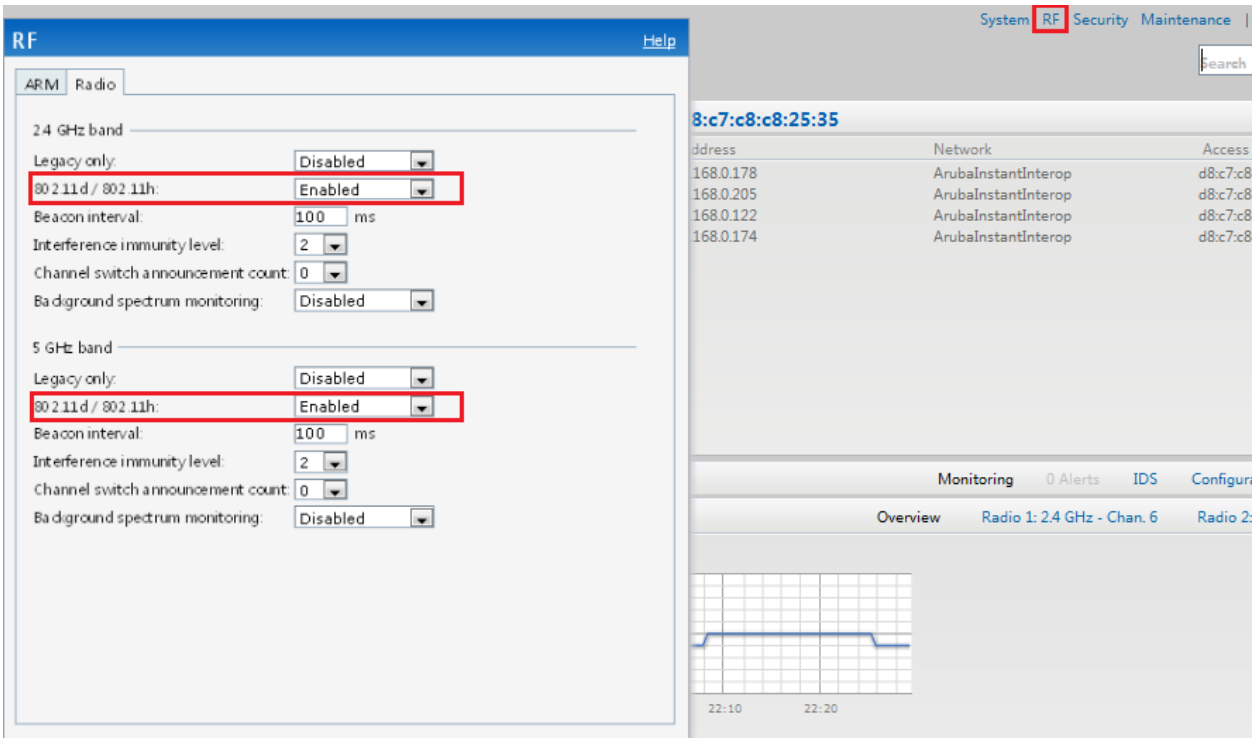
General guidelines when deploying Ascom i62 handsets (SW version 2.5.7 or later) in 802.11a/n environments:

1. ***Enabling more than 8 channels will degrade roaming performance. Ascom strongly recommends against going above this limit.***

2. ***Using 40 MHz channels (or "channel-bonding") will reduce the number of non-DFS* channels to two in ETSI regions (Europe). In FCC regions (North America), 40MHz is a more viable option because of the availability of additional non-DFS channels. The handset can co-exist with 40MHz stations in the same ESS.***

3. ***Make sure that all non-DFS channel are taken before resorting to DFS channels. The handset can cope in mixed non-DFS and DFS environments; however, due to "unpredictability" introduced by radar detection protocols, voice quality may become distorted and roaming delayed. Hence Ascom recommends avoiding the use of DFS channels in VoWIFI deployments.***

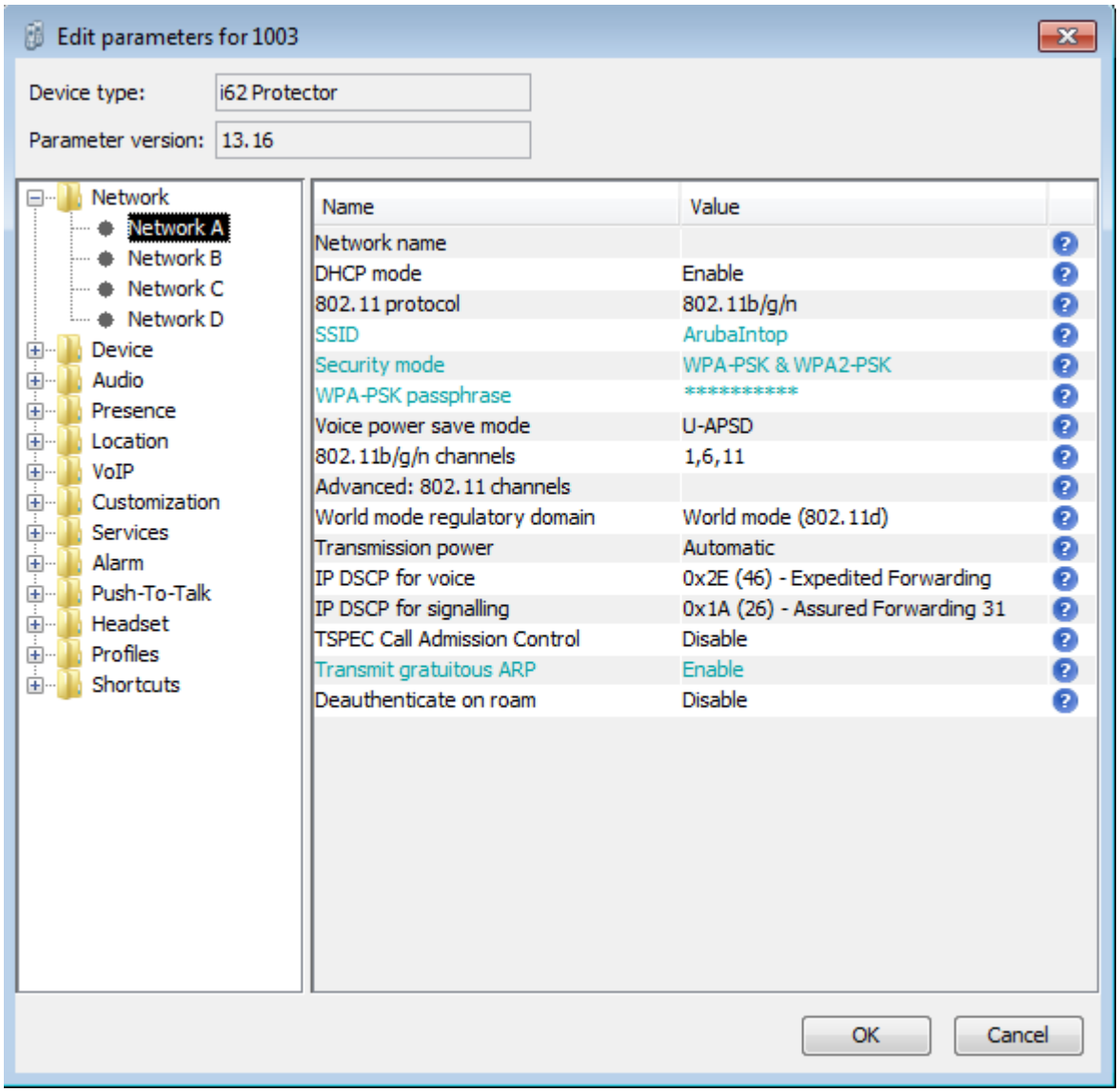
***) Dynamic Frequency Selection (radar detection)**



RF settings

- 802.11d/802.11h has to be enabled if regulatory domain is set to “world mode” in the i62

Ascom i62 Setting Summary



The table above summarizes the Ascom i62 settings.

APPENDIX B

Test Summary

Description	Runs
Tests passed	23
Tests Not Run	8
Tests fail	0
Test NA	0
Total Number of Tests	31

See attached excel document “WLANinteroperabilityTestReport_Aruba iAP.xls” for detailed test records.

Aruba Test Configuration File

```
version 6.2.1.0-3.3.0
virtual-controller-country SE
virtual-controller-key 2c4a7a170163b4698733f1009dca8cba27cec121e894c33783
name Instant-C4:96:62
terminal-access
clock timezone none 00 00
rf-band all

allow-new-aps
allowed-ap 24:de:c6:c4:96:62
allowed-ap 24:de:c6:c4:96:1f
allowed-ap 24:de:c6:c7:1a:58
allowed-ap d8:c7:c8:c8:25:35



arm
 wide-bands 5ghz
 min-tx-power 18
 max-tx-power 127
 band-steering-mode prefer-5ghz
 air-time-fairness-mode fair-access
rf dot11g-radio-profile
 dot11h

rf dot11a-radio-profile
 dot11h


syslog-level warn ap-debug
syslog-level warn network
syslog-level warn security
syslog-level warn system
syslog-level warn user
syslog-level warn user-debug
syslog-level warn wireless




mgmt-user admin 9054ce271fd611a670013fb49edc0596

wlan access-rule ArubaInstantInterop
 rule any any match any any any permit

wlan access-rule default_wired_port_profile
 rule any any match any any any permit
```

```
wlan access-rule wired-instant
 rule 192.168.0.246 255.255.255.255 match tcp 80 80 permit
 rule 192.168.0.246 255.255.255.255 match tcp 4343 4343 permit
 rule any any match udp 67 68 permit
 rule any any match udp 53 53 permit

wlan ssid-profile ArubaInstantInterop
 enable
 index 0
 type voice
 essid ArubaInstantInterop
 wpa-passphrase 782d23146cbf9095bbd6f11b02f8560db4e8ca8491227ca6
 opmode wpa-psk-tkip,wpa2-psk-aes
 max-authentication-failures 0
 auth-server Interop_Radius
 rf-band all
 captive-portal disable
 dtim-period 5
 inactivity-timeout 1000
 broadcast-filter none
 g-min-tx-rate 11
 dmo-channel-utilization-threshold 90
 local-probe-req-thresh 0
 max-clients-threshold 64

auth-survivability cache-time-out 24



wlan auth-server Interop_Radius
 ip 192.168.0.2
 port 1812
 acctport 1813
 key ab0be3b1ce242b97e03376b86ebc4dd6

wlan external-captive-portal
 server localhost
 port 80
 url "/"
 auth-text "Authenticated"


blacklist-time 3600
auth-failure-blacklist-time 3600

ids classification

ids
 wireless-containment none


wired-port-profile wired-instant
```

```
 switchport-mode access
 allowed-vlan all
 native-vlan guest
 no shutdown
 access-rule-name wired-instant
 speed auto
 duplex auto
 no poe
 type guest
 captive-portal disable
 no dot1x

wired-port-profile default_wired_port_profile
 switchport-mode trunk
 allowed-vlan all
 native-vlan 1
 shutdown
 access-rule-name default_wired_port_profile
 speed auto
 duplex full
 no poe
 type employee
 captive-portal disable
 no dot1x


enet0-port-profile default_wired_port_profile

uplink
 preemption
 enforce none
 failover-internet-pkt-lost-cnt 10
 failover-internet-pkt-send-freq 30
 failover-vpn-timeout 180


airgroup
 disable

airgroupservice airplay
 disable
 description AirPlay
 id _airplay._tcp
 id _raop._tcp

airgroupservice airprint
 disable
 description AirPrint
 id _ipp._tcp
 id _pdl-datastream._tcp
 id _printer._tcp
 id _scanner._tcp
 id _universal._sub._ipp._tcp
```

id _printer._sub._http._tcp
id _http._tcp
id _http-alt._tcp
id _ipp-tls._tcp
id _fax-ipp._tcp
id _riousbprint._tcp
id _cups._sub._ipp._tcp
id _cups._sub._fax-ipp._tcp
id _ica-networking._tcp
id _ptp._tcp
id _canon-bjnp1._tcp