Interoperability Report

Ascom i62
Aruba
Instant AP Platform
Aruba AOS v. 6.5.4.3
Ascom i62 v. 6.0.6
Gothenburg, Sweden
January 2018
# Contents

Introduction................................................................. 3

About Ascom................................................................. 3

About Aruba, a Hewlett Packard Enterprise company ....................................................... 3

Site Information ................................................................... 4

Interoperability Verification Site ........................................... 4

Participants .......................................................................... 4

Test topology ........................................................................ 4

Summary .............................................................................. 5

General Conclusions ........................................................... 5

Compatibility Information ....................................................... 5

Overview of Results ............................................................... 6

Known limitations ................................................................. 7

Appendix A: Interoperability Verification Configurations .................. 8

Aruba IAP-103/205/215/325, AOS 6.5.4.3 ........................................ 8

Ascom i62 Settings Summary ................................................... 20

Appendix B: Interoperability Verification Records .......................... 22

Test Protocol ........................................................................ 22

Aruba Test Configuration ........................................................ 22

Document History ................................................................. 24
Introduction
This document describes a summary of the interoperability verification results of the Ascom’s and Aruba’s platform, necessary steps and guidelines to optimally configure the platforms and support contact details. The report should be used in conjunction with both Aruba’s and Ascom’s platform configuration guides.

About Ascom
Ascom is a global solutions provider focused on healthcare ICT and mobile workflow solutions. The vision of Ascom is to close digital information gaps allowing for the best possible decisions – anytime and anywhere. Ascom’s mission is to provide mission-critical, real-time solutions for highly mobile, ad hoc, and time-sensitive environments. Ascom uses its unique product and solutions portfolio and software architecture capabilities to devise integration and mobilization solutions that provide truly smooth, complete and efficient workflows for healthcare as well as for industry, security and retail sectors.

Ascom is headquartered in Baar (Switzerland), has subsidiaries in 15 countries and employs around 1,300 people worldwide. Ascom registered shares (ASCN) are listed on the SIX Swiss Exchange in Zurich.

About Aruba, a Hewlett Packard Enterprise company
Aruba, a Hewlett Packard Enterprise company, is a leading provider of next-generation networking solutions for enterprises of all sizes worldwide. The company delivers IT solutions that empower organizations to serve the latest generation of mobile-savvy users who rely on cloud-based business apps for every aspect of their work and personal lives.

To learn more, visit Aruba at http://www.arubanetworks.com . For real-time news updates follow Aruba on Twitter and Facebook, and for the latest technical discussions on mobility and Aruba products visit Airheads Social at http://community.arubanetworks.com .
Site Information

Interoperability Verification Site
Ascom,
Gothenburg,
Sweden

Participants
Matthew Williams, Ascom, Gothenburg

Test topology

Dial Plan:
9xxx - Ascom Handsets, IP Phones
(Not all terminals are shown here)

Software Versions:
Aruba iAP 103/205/215/325,
v. 6.5.4.3 (build 61959)
Ascom i62, v.6.0.6 or later
IP PBX / SIP Server (vendor independent)
Summary

General Conclusions

The verification, including association, authentication, roaming, and load test produced very good results overall. Roaming times were in general good with typical roaming times of approximately 55ms both when using WPA2-PSK/AES and PEAP-MSCHAPv2 (WPA2/AES).

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

Compatibility Information

The following Aruba access point models were selected for this interoperability validation: IAP-103, 205, 215, 325. By testing these access points we are considered to cover a majority of Aruba access points based on chipset compatibility.

Supported Partner Access Points with AOS version 6.5.4.3:

IAP-103, 204, 205, 214, 215, 224, 225

IAP-314, 315, 324, 325
### Overview of Results

Ascom i62, version 6.0.6
Aruba IAP-103/205/215/325, version 6.5.4.3

#### WLAN Compatibility and Performance

<table>
<thead>
<tr>
<th>High Level Functionality</th>
<th>Result</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Association, Open with No Encryption</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Association, WPA2-PSK / AES Encryption</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Association, PEAP-MSCHAPv2 Auth, AES Encryption</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Association with EAP-TLS authentication</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Association, Multiple ESSIDs</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Beacon Interval and DTIM Period</td>
<td>NOK *</td>
<td>IAP103/325 not affected</td>
</tr>
<tr>
<td>PMKSA Caching</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>WPA2-opportunistic/proactive Key Caching</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>WMM Prioritization</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Traffic Specification (TSPEC)</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>802.11 Power-save mode</td>
<td>N/A **</td>
<td></td>
</tr>
<tr>
<td>802.11e U-APSD</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>802.11e U-APSD (load test)</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Roaming, WPA2-PSK, AES Encryption</td>
<td>OK</td>
<td>Typical avg. 40-70 ms</td>
</tr>
<tr>
<td>Roaming, PEAP-MSCHAPv2 Auth, AES Encryption</td>
<td>OK ***</td>
<td>Typical avg. 40-70 ms</td>
</tr>
</tbody>
</table>

*) Refer to the section "Known Limitations" in this report.

**) Ascom requires that U-APSD is enabled in the WLAN.

***) Observed times are with Opportunistic/Proactive Key Caching enabled.
## Known limitations

<table>
<thead>
<tr>
<th>Description and Consequence</th>
<th>Workaround</th>
<th>Ticket(s) raised</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ascom i62 does not handle 802.11K info correctly which affects the roaming negatively.</td>
<td>Do not advertise the 802.11K capabilities for the Ascom i62 SSID.</td>
<td></td>
</tr>
<tr>
<td>802.11ac-capable iAP205/215 advertises a DTIM interval of 1 irrespective of configuration (5), which marginally increases the battery consumption of the Ascom i62 in idle mode (observed standby time: &gt;65 hours). IAP103/325 do not exhibit the issue.</td>
<td>No workaround available.</td>
<td></td>
</tr>
<tr>
<td>During testing, it was occasionally noted that an Ascom i62 associated to a WLAN on the 5GHz band couldn't immediately switch to 2.4GHz.</td>
<td>As a workaround, “Band Steering Mode” can be changed from “Prefer 5GHz” to “Disabled”.</td>
<td></td>
</tr>
</tbody>
</table>

For additional information regarding the known limitations please contact [interop@ascom.com](mailto:interop@ascom.com) or [support@ascom.com](mailto:support@ascom.com).

For detailed test results, refer to Appendix B: Interoperability Verification Records.
Appendix A: Interoperability Verification Configurations

Aruba IAP-103/205/215/325, AOS 6.5.4.3

This section includes screenshots and explanations of basic settings required to use Ascom i62 Handsets with an 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 Appendix B.

General settings (SSID, Authentication, Radio and QoS)

General Overview
Network configuration -> WLAN settings

- Select Voice as primary usage
- Set broadcast filtering to ARP. This implies that access points drop all broadcast and multicast frames, except ARP and DHCP. In addition, ARP requests will be converted to unicast and sent to the associated station.
- 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.
- Ascom recommends disabling the lowest transmit rates and recommends that 12mbits is the lowest basic rate.
- To match the default values for the i62 ensure to use DSCP 46 for Voice, 26 for video and 0 for best effort. Ensure that WMM and U-APSD are enabled (default).
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, while WPA implies TKIP encryption. The latter is not recommended.

Note: The Ascom i62 does not support fast roaming.
Network configuration -> Security (Enterprise/1X)

- Set Key management to WPA-2 Enterprise
- Ensure that Opportunistic Key Caching is enabled.
- Configure Authentication server 1. See next picture.
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.
Network configuration -> Access

- Access rules set to default (Network-based)
Configuration of Access Points -> General

- This AP was selected as Preferred Master.
- The access points will get their IP address assigned by a DHCP server (default).
Configuration of Access Points -> Radio

- For testing purposes, the channel and transmit power were assigned manually.
RF settings -> Radio

- 802.11d/802.11h has to be enabled if regulatory domain is set to "world mode" on the Ascom i62.
**RF settings -> ARM**

- For testing purposes, available channels and wide channel support were set statically.

**Note:** Ascom recommends a Beacon Interval of 100ms and advertising 802.11d/h capabilities. Recommended settings for 802.11b/g/n are to use only channel 1, 6 and 11. For 802.11a/n/ac use channels according to the infrastructure manufacturer, country regulations and per guidelines below.
General guidelines when deploying Ascom i62 handsets in 802.11a/n/ac environments:

1. Enabling more than 8 channels will degrade roaming performance. In situations where UNII1 and UNII3 are used, a maximum of 9 enabled channels can be allowed. Ascom does not recommend exceeding 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. Ascom do support and can coexist in 80MHz channel bonding environments. The recommendations is however to avoid 80MHz channel bonding as it severely reduces the number of available non overlapping channels.

4. 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 if possible avoiding the use of DFS channels in VoWIFI deployments.

*) Dynamic Frequency Selection (radar detection)

See Appendix B for the “virtual” controller configuration used for the certification process.
Ascom i62 Settings Summary

Network settings for WPA2-PSK

- Select frequency band according to system setup (here 802.11b/g/n).
- Select only the channels used in the system (here channels 1, 6, 11).

Note: FCC is no longer allowing 802.11d to determine regulatory domain. Devices deployed in the USA must set Regulatory domain to “US”.
Network settings for .1X authentication (PEAP-MSCHAPv2)

- Select frequency band according to system setup (here 802.11b/g/n).
- Select only the channels used in the system (here channels 1,6,11).

Note: FCC is no longer allowing 802.11d to determine regulatory domain. Devices deployed in the USA must set Regulatory domain to "US".
Appendix B: Interoperability Verification Records

Test Protocol
Refer to attached Excel file for detailed test results.

The test specification containing information about each test case can be found here (requires login):

Aruba Test Configuration

version 6.5.4.0-6.5.4
virtual-controller-country SE
virtual-controller-key 473d214b0129b787eb61c537eb1cc5a846f060f960ba6ddcda
name instant-C5:78:B6
terminal/access
clock timezone none 00 00
rf-band all
allow-new-aps
allowed-ap f0:5c:19:c5:78:b6
allowed-ap f0:5c:19:c8:2a:c4
allowed-ap f0:5c:19:c1:03:b0
allowed-ap f0:5c:19:ca:40:24

arm
wide-bands none
a-channels 36,40,44,48,36+,44+,36E,52E
g-channels 1,6,11
min-tx-power 18
max-tx-power 127
band-steering-mode disable
air-time-fairness-mode fair-access
client-aware
scanning

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

extended-ssid

mgmt-user admin 9d6367563cb73174a33a4720eba6baef

wlan access-rule default_wired_port_profile
index 0
rule any any match any any any permit

wlan access-rule wired-SetMeUp
index 1
rule masterip 0.0.0.0 match tcp 80 80 permit
rule masterip 0.0.0.0 match tcp 4343 4343 permit
rule any any match udp 67 68 permit
rule any any match udp 53 53 permit

wlan access-rule CompTest80211
index 2
rule any any match any any any permit

wlan access-rule CompTest
index 3
rule any any match any any any permit

wlan ssid-profile CompTest80211
enable
index 0
type voice
essid CompTest80211
wpa-pwd password 91507e499869661ca211e37756f6af1be3a478444835a6b450948b7cf53f62d
opmode wpa2-psk-aes
max-authentication-failures 0
rf-band all
captive-portal disable
l2-auth-failthrough
dtim-period 5
broadcast-filter arp
g-min-tx-rate 12
a-min-tx-rate 12
dmo-channel-utilization-threshold 90
local-probe-req-thresh 0
max-clients-threshold 64
wmm-background-dscp "8"
wmm-best-effort-dscp "24"
wmm-video-dscp "26"
wmm-voice-dscp "46"
okc

wlan ssid-profile CompTest
enable
index 1
type voice
essid CompTest
wpa-pwd password 2ca2ee6b10f80c4a93d04f2cc17e26180ec81771819144ef6a8044a145ecc76d
opmode wpa2-psk-aes
max-authentication-failures 0
rf-band all
captive-portal disable
dtim-period 5
broadcast-filter arp
dmo-channel-utilization-threshold 90
local-probe-req-thresh 0
max-clients-threshold 64
auth-survivability cache-time-out 24

wlan auth-server FreeRadius
ip 10.11.24.98
port 1812
acctport 1813
key 127ce940c29288e0ec9d325377fe89a6d

wlan external-captive-portal
server localhost
port 80
url ""
auth-text "Authenticated"
auto-whitelist-disable
https

blacklist-time 3600
auth-failure-blacklist-time 3600
ids
wireless-containment none

wired-port-profile wired-SetMeUp
switchport-mode access
allowed-vlan all
native-vlan guest
no shutdown
access-rule-name wired-SetMeUp
speed auto
duplex auto
no poe
no dot3bz
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
no dot3bz
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

airgroupservice airprint
disable
description AirPrint

Document History

<table>
<thead>
<tr>
<th>Rev</th>
<th>Date</th>
<th>Author</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PA1</td>
<td>2018-01-18</td>
<td>SEMW</td>
<td>First draft</td>
</tr>
<tr>
<td>PA2</td>
<td>2018-01-23</td>
<td>SEMW</td>
<td>Updated version (after internal peer review)</td>
</tr>
<tr>
<td>R1</td>
<td>2018-01-24</td>
<td>SEMW</td>
<td>Final version</td>
</tr>
</tbody>
</table>