INTEROPERABILITY REPORT

Ascom i62

Extreme Networks

C25 / 35 / C2110 / C5110 / C5210 and V2110

AP 37xx / 38xx / 39xx

i62 and OEM derivatives version 5.5.0

Extreme Networks software version 10.11.04.0008

Ascom, Jan 2017
TABLE OF CONTENT:

INTRODUCTION ........................................................................................................................... 3
Ascom solution .......................................................................................................................... 3
Extreme Networks solution ....................................................................................................... 3
SUMMARY .................................................................................................................................... 5
Known issues ............................................................................................................................ 6
General conclusion ................................................................................................................... 6
Compatibility information .......................................................................................................... 6
APPENDIX A: TEST CONFIGURATIONS .................................................................................... 7
   Extreme Networks V2110 Controller v. 10.11.04 ................................................................. 7
      Overview ............................................................................................................................... 7
      Extreme Networks controller overview ............................................................................ 7
      Security settings (PSK) ....................................................................................................... 8
      Security settings (802.1X / PEAP-MSCHAPv2) ................................................................. 10
      General settings (SSID, QoS, Radio ) ............................................................................. 13
   Ascom i62 network settings ................................................................................................. 22
APPENDIX B: DETAILED TEST RECORDS .............................................................................. 25
INTRODUCTION

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

The guide should be used in conjunction with both Extreme Networks and Ascom’s configuration guide(s).

Ascom solution

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.

Extreme Networks solution

Extreme Networks, Inc. (EXTR) is a software and services-led networking solutions company committed to solving IT’s toughest networking challenges. Extreme Networks is headquartered in San Jose, CA, with more than 14,000 customers in over 80 countries. For more information, visit Extreme's website.

Extreme Networks and the Extreme Networks logo are registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.
SITE INFORMATION

Test Site:
Ascom US
300 Perimeter park drive
Morrisville, NC, US-27560
USA

Participants:
Karl-Magnus Olsson, Ascom Sweden, Gothenburg

TEST TOPOLOGY

Software / Hardware versions:
Enterasys V2110 and AP3715, 3825 and 3935
Version 10.11.04.0008
IP-PBX: Innovaphone IP6000 version 10sr35
Radius server: FreeRADIUS
SUMMARY

Please refer to Appendix B for detailed results.

### WLAN Controller Features

<table>
<thead>
<tr>
<th>High Level Functionality</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Association, Open with No Encryption</td>
<td>OK</td>
</tr>
<tr>
<td>Association, WPA2-PSK / AES Encryption</td>
<td>OK</td>
</tr>
<tr>
<td>Association, PEAP-MSCHAPv2 Auth, AES Encryption</td>
<td>OK</td>
</tr>
<tr>
<td>Association with EAP-TLS authentication</td>
<td>OK</td>
</tr>
<tr>
<td>Association, Multiple ESSIDs</td>
<td>OK</td>
</tr>
<tr>
<td>Beacon Interval and DTIM Period</td>
<td>OK</td>
</tr>
<tr>
<td>PMKSA Caching</td>
<td>OK</td>
</tr>
<tr>
<td>WPA2-opportunistic/proactive Key Caching</td>
<td>OK</td>
</tr>
<tr>
<td>WMM Prioritization</td>
<td>OK</td>
</tr>
<tr>
<td>802.11 Power-save mode</td>
<td>OK</td>
</tr>
<tr>
<td>802.11e U-APSD</td>
<td>OK</td>
</tr>
<tr>
<td>802.11e U-APSD (load test)</td>
<td>OK</td>
</tr>
</tbody>
</table>

### Roaming

<table>
<thead>
<tr>
<th>High Level Functionality</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Roaming, Open with No Encryption</td>
<td>OK (typical roaming time 16ms) *</td>
</tr>
<tr>
<td>Roaming, WPA2-PSK, AES Encryption</td>
<td>OK (typical roaming time 32ms) *</td>
</tr>
<tr>
<td>Roaming, PEAP-MSCHAPv2 Auth, AES Encryption</td>
<td>OK (typical roaming time 33ms)*</td>
</tr>
</tbody>
</table>

*) Measured times is with opportunistic key caching enabled and for 802.11an. For detailed results see Appendix B.
Known issues

- No known issues.

For additional information regarding the known issues please contact interop@ascom.com or support@ascom.com

General conclusion

The verification, including association, authentication and call stability tests generated in general very good results. Roaming times were measured in the range of around 35ms when using both WPA2-PSK/AES and PEAP-MSCHAPv2 (WPA2/AES).

Load tests showed that it was possible to maintain 12 simultaneous calls on one access point (radio) when using the minimum basic rate set to 12Mbps for both 802.11bgn. The same number of simulations calls could be maintained also for 802.11an.

The majority of the test cases were performed in B@AP mode.

Compatibility information

All tests were done on AP3715, AP3825 3935 on a v2110 controller. Due to similar chipsets in other access points we consider all access points listed below supported. All Extreme Networks controllers are considered to be covered based on testing towards V2110.

Supported access points with Extreme Networks version 10.11.04:

AP3705, 3710, 3715, 3765, 3767
AP3801, 3805, 3825, 3865
AP 3935

Supported controller platforms with Extreme Networks version 10.11.04:

C25
C35
V2110
C5110
APPENDIX A: TEST CONFIGURATIONS

Extreme Networks V2110 Controller v. 10.11.04

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

Overview

Extreme Networks controller overview.
Security settings (PSK)

General SSID settings.
Security profile WPA2-PSK, AES encryption
Security settings (802.1X / PEAP-MSCHAPv2)

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 in order to allow faster roaming between access points.
Configuration of authentication using external Radius sever (Step 2). Select the server to use. The server is created/configured in next step.
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. Server certificate validation can however be overridden in version 4.1.12 and above per handset setting.

Note. To enable fast inter-controller roaming with opportunistic key caching, the “pair” option under “Wireless controller -> availability” has to be enabled. Please consult Extreme Networks for details.
General settings (SSID, QoS, Radio)

Make sure that WMM. In this example U-APSD is enabled which is strongly recommended in order to increase battery performance.
Ascom recommended settings for 802.11g/n are to use 3 channel plan (channel 1, 6 and 11). Due to the limited number of non-overlapping channels using 802.11g/n it is recommended to use 20MHz channel width.

Note that Tx Power was adjusted in order to test roaming.
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. A lower DTIM value is possible but will impact the standby time negatively.

It is recommended to set the Min Basic Rate to 11Mbps to increase the performance.

Radio 2 -> Advanced (continued). Additional settings left as default.
Configuration of 802.11a/n/ac: Refer to general guidelines on page 18.

Note that Tx Power was adjusted in order to test roaming.
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. A lower DTIM value is possible but will impact the standby time negatively.
Configuration of 802.11a/n/ac: Refer to general guidelines on page 18.

Note that Tx Power was adjusted in order to test roaming.
General guidelines when deploying Ascom i62 handsets in 802.11a/n/ac environments:

1. **Enabling more than 8 channels will degrade roaming performance. Ascom 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. **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)
Virtual Network set up including the Roles.

Voice role configuration.
Controller configuration

See attached file (controller_config.cli) for controller configuration.
Ascom i62 network settings

Ascom i62 Network configurations (WPA2-PSK)

Note. Refer to general guidelines on page 18 concerning 802.11a/n channels. It’s important that the channels in the handset match the channel plan used in the system.

Note. FCC is no longer allowing 802.11d to determine regulatory domain. Devices deployed in USA must set Regulatory domain to “USA".
i62 network settings for 802.1X authentication (PEAP-MSCHAPv2)

Note. Refer to general guidelines on page 18 concerning 802.11a/n channels. It's important that the channels in the handset match the channel plan used in the system.

Note. FCC is no longer allowing 802.11d to determine regulatory domain. Devices deployed in USA must set Regulatory domain to “USA”.
802.1X Authentication requires a root certificate to be uploaded to the phone by "right clicking" -> Edit certificates. EAP-TLS will require both a root and a client certificate.

Note that both a root and a client certificate are needed for TLS. Otherwise only a root certificate is needed. Server certificate validation can be overridden in version 4.1.12 and above per handset setting.
APPENDIX B: DETAILED TEST RECORDS

VoWIFI

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Pass</td>
<td>17</td>
</tr>
<tr>
<td>Fail</td>
<td>0</td>
</tr>
<tr>
<td>Comments</td>
<td>0</td>
</tr>
<tr>
<td>Untested</td>
<td>2</td>
</tr>
<tr>
<td>Total</td>
<td>19</td>
</tr>
</tbody>
</table>

See attached file (WLANinteroperabilityTestReport_Extreme_networks.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):
## Document History

<table>
<thead>
<tr>
<th>Rev</th>
<th>Date</th>
<th>Author</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>2016-12-16</td>
<td>SEKMO</td>
<td>Draft 1</td>
</tr>
<tr>
<td>R1</td>
<td>2017-01-13</td>
<td>SEKMO</td>
<td>Updates after review. Revision R1</td>
</tr>
</tbody>
</table>