Technology Solution Guide

Deploying Ascom i62 with Aruba Networks’ Secure Mobility Solution

Ascom i62 Handset and OEM derivatives
Software version 5.1.30

Aruba 600/3000/6000/7200 Mobility Controllers
AOS version 6.3.1.3

Aruba
AP92/93/104/105/124/125/134/135
AP114/115/224/225

April 14th 2014
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 THIS DOCUMENT 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 ................................................................................................................................. 3
Solution Components .................................................................................................................... 3
  Aruba Campus WLAN Solution ................................................................................................. 3
  Ascom Solution ......................................................................................................................... 4
ArubaEdge Solution Qualification ............................................................................................... 6
  Qualification Objective .............................................................................................................. 6
  Network Topology ..................................................................................................................... 6
  Test Methodology ...................................................................................................................... 8
  Summary Test Results .............................................................................................................. 8
  Know Limitations ....................................................................................................................... 10
Conclusion .................................................................................................................................... 10
Appendix 1 ................................................................................................................................... 11
  General settings (SSID, Radio and QoS) .................................................................................. 11
  Encryption and Authentication Settings .................................................................................... 14
  Ascom i62 Setting Summary ....................................................................................................... 17
APPENDIX B .................................................................................................................................. 19
  Test Summary ............................................................................................................................ 19
  Aruba Test Configuration File ...................................................................................................... 20
**Introduction**

This document describes the steps and guidelines necessary to configure Aruba’s wireless LAN (AOS version. 6.3.1.3) 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 6.3.x.x

**Partner Solution Tested:** Ascom i62 Handset; Software version 5.1.30

**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 offers a high class telephony, messaging and alarm solution for enterprise business based on the WiFi technology. With offering Voice Over WiFi, only one network is needed to be installed and maintained for all applications running, such as Internet access, e-mail, voice and other business related applications.

The latest 802.11n standard provides the benefits of higher throughput and longer range possibilities which will increase the ability to integrate to other systems and build efficient applications. With the new generation networks and handsets the capacity and versatility outperforms any other on-site wireless technology.

The Ascom i62 offers a unique management tool with central management concept enabling remote management and SW upgrades of the handsets over the air.
### Certified Product Summary

<table>
<thead>
<tr>
<th>Feature</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Manufacturer</strong></td>
<td>Ascom Wireless Solutions</td>
</tr>
<tr>
<td><strong>Products Certified</strong></td>
<td>Ascom i62 and OEM derivatives</td>
</tr>
<tr>
<td><strong>Hardware Model Numbers</strong></td>
<td>WH1-xxxx</td>
</tr>
<tr>
<td><strong>Software Version Numbers</strong></td>
<td>5.1.30</td>
</tr>
<tr>
<td><strong>RF Features Tested</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Radio Supported</strong></td>
<td>802.11a/b/g/n</td>
</tr>
<tr>
<td><strong>QoS Features Supported / Tested</strong></td>
<td>WMM</td>
</tr>
<tr>
<td><strong>Powersave Features Tested</strong></td>
<td>U-APSD</td>
</tr>
<tr>
<td><strong>Encryption Supported</strong></td>
<td>WEP64/128, WPA-PSK, WPA2-PSK, PEAP-MSCHAPv2, EAP-TLS</td>
</tr>
<tr>
<td><strong>Encryption Tested</strong></td>
<td>WPA-PSK, WPA2-PSK, PEAP-MSCHAPv2, EAP-TLS</td>
</tr>
<tr>
<td><strong>802.11h Supported</strong></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Key Caching Support for Optimized Roaming</strong></td>
<td>OKC and PMK</td>
</tr>
<tr>
<td><strong>Voice Specific Features</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Protocols Supported</strong></td>
<td>SIP-UDP, SIP-TCP, SIP-TLS, H.323</td>
</tr>
<tr>
<td><strong>Control Traffic Pattern</strong></td>
<td>Handset to Server and vice versa</td>
</tr>
<tr>
<td><strong>Voice Traffic Pattern</strong></td>
<td>Peer-to-peer (between handsets)</td>
</tr>
<tr>
<td><strong># of Calls per AP Tested</strong></td>
<td>18 calls (not AP-capacity limited)</td>
</tr>
</tbody>
</table>
**ArubaEdge Solution Qualification**

**Qualification Objective**
Validate the interoperability of the Ascom i62 with the Aruba’s wireless LAN infrastructure (version 6.3.1.3).

**Network Topology**

![Network Topology Diagram]

**Software versions:**
- Aruba 3400 controller, AP 105, 135, 115, 225
  Version 6.3.1.3
- IP-PBX/SIP server
  Innovaphone IP6000 version 9 hotfix 13
**Settings on the Aruba WLAN**

Enable SNMP v2 on the Aruba Mobility Controller, and configure the community string as follows:

The following Aruba Mobility Controller 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: Country specific

- **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.

- **User Roles and Policies**
  The Ascom phones support SIP and H.323. So enable the voice ACL or the SIP and H.323 ACLs

**Ascom Settings**

The following Ascom i62 Handset configuration settings are recommended for use with Aruba Mobility Controllers

**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 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, Open with Static WEP64/128</td>
<td>Not tested</td>
</tr>
<tr>
<td>Association, WPA-PSK, TKIP</td>
<td>OK</td>
</tr>
<tr>
<td>Association, WPA2-PSK, TKIP / AES Encryption</td>
<td>OK</td>
</tr>
<tr>
<td>Association, PEAP-MSCHAPv2 Auth., TKIP Encryption</td>
<td>OK</td>
</tr>
<tr>
<td>Association, PEAP-MSCHAPv2 Auth., AES Encryption</td>
<td>OK</td>
</tr>
<tr>
<td>Association, EAP-TLS</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>Pre-authentication</td>
<td>N/A</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>Active Mode (load test)</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 (Avg roaming time 24ms) *</td>
</tr>
<tr>
<td>Roaming, WPA-PSK, TKIP Encryption</td>
<td>OK (Avg roaming time 50ms) *</td>
</tr>
<tr>
<td>Roaming, WPA2-PSK, AES Encryption</td>
<td>OK (Avg roaming time 56ms) *</td>
</tr>
<tr>
<td>Roaming, PEAP-MSCHAPv2 Auth, AES Encryption</td>
<td>OK (Avg roaming time 60ms) <em>/</em>*</td>
</tr>
</tbody>
</table>

* ) Stated roaming times were measured using 802.11bg (n) AP225. Refer to Appendix B for detailed test records.

**) Results observed with Opportunistic Key Caching enabled. Results average 400ms without Opportunistic Key Caching.
Know Limitations

- Minor voice disturbances due to incorrect handling of service period after re-transmission. The voice disturbance occurs primarily when BAR (block ack requests) are re-sent multiple times. AP 224/225 only

Workaround/solution: Use 11bg or 11a (legacy) mode to prevent frame aggregation and BAR frames. Problem is addressed and solved and will be incorporated in next i62 release.

Note: AP224/225 only

Refer to Ascom ticket 24687 for details.

- Note that AP224/225 only supports DTIM 1. This will reduce the standby (idle) time from approximately 100 hours to 60 hours.

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 40-60ms both when using WPA2-PSK/AES and PEAP-MSCHAPv2 (WPA2/AES).

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 18 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 an Aruba 3400 Mobility Controller. 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)

Set DTIM Interval to 5 (for AP 224/335 only value 1 is supported). This value is recommended for maximum battery conservation without impacting call quality. Using a lower value will also decrease the standby time slightly.
Ascom recommends disabling the lowest rates and recommends that 11mbits is the lowest supported rate.

Ensure that WMM and U-APSD are enabled. To match the default values in the i62 ensure to use DSCP 46 for Voice, 26 for video and 0 for best effort. It is also recommended that “Max Transmit Attempts” be set to 4.

Note: To further optimize performance it is recommended that 802.11b clients is disallowed from associating by setting the 6 Mbps or 12Mbps as Basic Rates in the 802.11g configuration.

Set “Maximum Transmit Failures” to 25.
“High throughput enable” enables 802.11n capabilities that are supported in combination with Open encryption and WPA2-AES (PSK or Enterprise).

Ascom does support both usage of 40MHz and Very High throughput enabled SSID including 80MHz channels.

Ascom recommends a Beacon Interval of 100ms and advertising 802.11d/h capabilities.

**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)
Ascom recommends a Beacon Interval of 100ms and advertising 802.11d/h capabilities. For 802.11b/g/n use only channels 1, 6 and 11. For 802.11a/n, use channels in accordance with Aruba’s guidelines and in compliance with local regulations.

**Encryption and Authentication Settings**

WPA2-PSK. Set the security profile to WPA2-PSK, AES encryption.
Deploying Ascom’s i62 VoWiFi handset with Aruba Networks’ Secure Mobility Solution

Enterprise/.1X authentication.

Step 1: When configuring the authentication mode using a Radius server, the IP address and the secret must correspond to the IP address and the credential used by the Radius server. The RADIUS server should be added to a Server Group.

Step 2: Create an 802.1X Authentication Profile.
Step 3: Choose the 802.1X Authentication profile created in previous step and configure the Authentication Server group.

Choose configured AAA Profile and set WPA2/AES as the security mode.

See Appendix B for the controller configuration used for the certification process.
Ascom i62 Setting Summary

Network settings for WPA2-PSK
Network settings for .1X authentication (PEAP-MSCHAPv2)

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 (Validate server certificate under Network settings).*
## APPENDIX B

### Test Summary

<table>
<thead>
<tr>
<th>Description</th>
<th>Runs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tests passed</td>
<td>27</td>
</tr>
<tr>
<td>Tests Not Run</td>
<td>6</td>
</tr>
<tr>
<td>Tests fail</td>
<td>1 (AP224/225)</td>
</tr>
<tr>
<td>Test NA</td>
<td>1</td>
</tr>
<tr>
<td>Total Number of Tests</td>
<td>35</td>
</tr>
</tbody>
</table>
Aruba Test Configuration File

version 6.3
enable secret "7d3988e20126db68084797bcc038534bffc2ced01c24555806"
hostname "Aruba3400"
clock timezone PST -8
location "Building1.floor1"
controller config 714
ip NAT pool dynamic-srnat 0.0.0.0 0.0.0.0
ip access-list eth validuserethacl
permit any
!
net service svc-pcoip2-tcp tcp 4172
net service svc-snmp-trap udp 162
net service svc-netbios-dgm udp 138
net service svc-citrix tcp 2598
net service svc-smb-tcp tcp 445
net service svc-ike udp 500
net service svc-l2tp udp 1701
net service svc-syslog udp 514
net service svc-dhcp udp 67 68 alg dhcp
net service svc-https tcp 443
net service svc-ica tcp 1494
net service svc-pptp tcp 1723
net service svc-telnet tcp 23
net service svc-http-accl tcp 88
net service svc-sccp tcp 2000 alg sccp
net service svc-sec-papi udp 8209
net service svc-fttp udp 69 alg fttp
net service svc-kerberos udp 88
net service svc-sip-tcp tcp 5060
net service svc-netbios-ssn tcp 139
net service svc-pcoip-udp udp 50002
net service svc-pcoip-tcp tcp 50002
net service svc-pop3 tcp 110
net service svc-udp udp 8200
net service svc-cfgm-tcp tcp 8211
net service svc-noe udp 32512 alg noe
net service svc-http-proxy3 tcp 8888
net service svc-ipd-tcp tcp 631
net service svc-msrpc-tcp tcp 135 139
net service svc-rtsp tcp 554 alg rtsp
net service svc-dns udp 53 alg dns
net service vnc tcp 5900 5905
net service svc-vocera udp 5002 alg vocera
net service svc-h323-tcp tcp 1720
net service svc-h323-udp udp 1718 1719
net service svc-http tcp 80
net service svc-nterm tcp 1026 1028
net service svc-sip-udp udp 5060
net service svc-http-proxy2 tcp 8080
net service svc-noe-oxo udp 5000 alg noe
net service svc-papi udp 8211
net service svc-ftp tcp 21 alg ftp
net service svc-natt udp 4500
net service svc-svp 119 alg svp
net service svc-microsoft-ds tcp 445
net service svc-gre 47
net service svc-smtp tcp 25
net service web tcp list "80 443"
net service svc-smb-udp udp 445
net service svc-sips tcp 5061 alg sips
net service svc-netbios-ns udp 137
net service svc-esp 50
netservice svc-cups tcp 515
netservice svc-pcoip2-udp udp 4172
netservice svc-bootp udp 67 69
netservice svc-snmp udp 161
netservice svc-v6-dhcp udp 546 547
netservice svc-icmp 1
netservice svc-ntp udp 123
netservice svc-msrscp-udp udp 135 139
netservice svc-ssh tcp 22
netservice svc-http-proxy1 tcp 3128
netservice svc-v6-icmp 58
netservice svc-lpd-udp udp 631
netservice svc-vmware-rdp tcp 3389
netdestination6 ipv6-reserved-range
  invert
network 2000::/3
  netexthdr default
  !
time-range night-hours periodic
  weekday 18:01 to 23:59
  weekday 00:00 to 07:59
  !
time-range weekend periodic
  weekend 00:00 to 23:59
  !
time-range working-hours periodic
  weekday 08:00 to 18:00
  !
ip access-list session allow-diskservices
    any any svc-netbios-dgm permit
    any any svc-netbios-ssn permit
    any any svc-microsoft-ds permit
    any any svc-netbios-ns permit
  !
ip access-list session control
    any any svc-papi permit
    any any svc-sec-papi permit
    user any udp 68 deny
    any any svc-icmp permit
    any any svc-dns permit
    any any svc-cfgm-tcp permit
    any any svc-adp permit
    any any svc-tftp permit
    any any svc-dhcp permit
    any any svc-natt permit
  !
ip access-list session v6-icmp-acl
  !
ip access-list session validuser
    network 169.254.0.0 255.255.0.0 any any deny
    network 127.0.0.0 255.0.0.0 any any deny
    network 224.0.0.0 240.0.0.0 any any deny
    host 255.255.255.255 any any deny
    network 240.0.0.0 240.0.0.0 any any deny
    any any any permit
    ipv6 host fe80:: any any deny
    ipv6 network fe80::/64 any any permit
    ipv6 alias ipv6-reserved-range any any deny
    ipv6 any any any permit
  !
ip access-list session vocera-acl
    any any svc-vocera permit queue high
  !
ip access-list session v6-https-acl

Deploying Ascom's i62 VoWiFi handset with Aruba Networks' Secure Mobility Solution
Deploying Ascom’s i62 VoWiFi handset with Aruba Networks’ Secure Mobility Solution

```plaintext
! ip access-list session vmware-acl
  any any svc-vmware-rdp permit tos 46 dot1p-priority 6
  any any svc-pcoip-tcp permit tos 46 dot1p-priority 6
  any any svc-pcoip-udp permit tos 46 dot1p-priority 6
  any any svc-pcoip2-tcp permit tos 46 dot1p-priority 6
  any any svc-pcoip2-udp permit tos 46 dot1p-priority 6
!
ip access-list session v6-control
  ipv6 any any svc-papi permit
  ipv6 any any svc-sec-papi permit
  ipv6 user any udp 547 deny
  ipv6 any any svc-v6-icmp permit
  ipv6 any any svc-dns permit
  ipv6 any any svc-cfgm-tcp permit
  ipv6 any any svc-udp permit
  ipv6 any any svc-ftp permit
  ipv6 any any svc-dhcp permit
  ipv6 any any svc-natt permit
!
ip access-list session v6-dhcp-acl
!
ip access-list session allowall
  any any any permit
!
ip access-list session v6-dns-acl
!
ip access-list session lync-acl
  any any svc-sips permit queue high
!
ip access-list session test
!
ip access-list session sip-acl
  any any svc-sip-udp permit queue high
  any any svc-sip-tcp permit queue high
!
ip access-list session https-acl
  any any svc-https permit
!
ip access-list session citrix-acl
  any any svc-citrix permit tos 46 dot1p-priority 6
  any any svc-ica permit tos 46 dot1p-priority 6
!
ip access-list session dns-acl
  any any svc-dns permit
!
ip access-list session ascom
  any any any permit
!
ip access-list session ra-guard
  ipv6 user any icmpv6 rtr-adv deny
!
ip access-list session allow-printservices
  any any svc-cups permit
  any any svc-lpd-tcp permit
```

any any svc-lpd-udp permit
!
ip access-list session logon-control
user any udp 68 deny
any any svc-icmp permit
any any svc-dns permit
any any svc-dhcp permit
any any svc-natt permit
any network 169.254.0.0 255.255.0.0 any deny
any network 240.0.0.0 240.0.0.0 any deny
!
ip access-list session vpnlogon
user any svc-ike permit
user any svc-esp permit
any any svc-l2tp permit
any any svc-gptp permit
any any svc-gre permit
!
ip access-list session srcnat
user any any src-nat
!
ip access-list session skinny-acl
any any svc-sccp permit queue high
!
ip access-list session tftp-acl
any any svc-tftp permit
!
ip access-list session v6-allowall
!
ip access-list session clogout
user alias controller svc-https dst-nat 8081
!
ip access-list session dhcp-acl
any any svc-dhcp permit
!
ip access-list session http-acl
any any svc-http permit
!
ip access-list session v6-http-acl
!
ip access-list session captiveportal6
ipv6 user alias controller6 svc-https captive
ipv6 user any svc-http captive
ipv6 user any svc-https captive
ipv6 user any svc-http-proxy1 captive
ipv6 user any svc-http-proxy2 captive
ipv6 user any svc-http-proxy3 captive
!
ip access-list session ap-uplink-acl
any any udp 68 permit
any any svc-icmp permit
any host 224.0.0.251 udp 5353 permit
!
ip access-list session ap-acl
any any svc-gre permit
any any svc-syslog permit
any user svc-snmp permit
user any svc-http permit
user any svc-http-accl permit
user any svc-smb-tcp permit
user any svc-msrpc-tcp permit
user any svc-snmp-trap permit
user any svc-ntp permit
user alias controller svc-ftp permit
!
ip access-list session svp-acl

Deploying Ascom’s i62 VoWiFi handset with Aruba Networks’ Secure Mobility Solution
any any svc-svp permit queue high
user host 224.0.1.116 any permit
!
ip access-list session noe-acl
 any any svc-noe permit queue high
!
ip access-list session v6-ap-acl
 ipv6 any any svc-gre permit
 ipv6 any any svc-syslog permit
 ipv6 any user svc-snmp permit
 ipv6 user any svc-snmp-trap permit
 ipv6 user any svc-ntp permit
 ipv6 user alias controller6 svc-ftp permit
!
  ip access-list session h323-acl
  any any svc-h323-tcp permit queue high
  any any svc-h323-udp permit queue high
!
  ip access-list session v6-logon-control
  ipv6 any network fc00::/7 any permit
  ipv6 any network fe80::/64 any permit
  ipv6 any alias ipv6-reserved-range any deny
!
vpn-dialer default-dialer
  ike authentication PRE-SHARE 085bc5a72755c71f779cfff49b5d892e33f7d65ebe691ad8
!
  dot1x high-watermark 60
  dot1x low-watermark 57
  user-role ap-role
  access-list session ra-guard
  access-list session control
  access-list session ap-acl
  access-list session v6-control
  access-list session v6-ap-acl
!
  user-role denyall
!
  user-role default-vpn-role
  access-list session ra-guard
  access-list session allowall
  access-list session v6-allowall
!
  user-role cpbase
!
  user-role voice
  access-list session ra-guard
  access-list session sip-acl
  access-list session noe-acl
  access-list session svp-acl
  access-list session vocera-acl
  access-list session skinny-acl
  access-list session h323-acl
  access-list session dhcp-acl
  access-list session tftp-acl
  access-list session dns-acl
  access-list session icmp-acl
!
  user-role ascom
  access-list session ascom
!
  user-role default-via-role
  access-list session allowall
  access-list session v6-allowall
!
  user-role guest-logon
  captive-portal "default"
access-list session ra-guard
access-list session logon-control
access-list session captiveportal
access-list session v6-logon-control
access-list session captiveportal6
!
user-role guest
access-list session ra-guard
access-list session http-acl
access-list session https-acl
access-list session dhcp-acl
access-list session icmp-acl
access-list session v6-http-acl
access-list session v6-https-acl
access-list session v6-dhcp-acl
access-list session v6-icmp-acl
access-list session v6-dns-acl
!
user-role stateful-dot1x
!
user-role authenticated
access-list session ra-guard
access-list session allowall
access-list session v6-allowall
!
user-role logon
access-list session ra-guard
access-list session logon-control
access-list session captiveportal
access-list session vpnlogon
access-list session v6-logon-control
access-list session captiveportal6
!
!
interface mgmt
    shutdown
!
dialer group evdo_us
init-string ATQ0V1E0
dial-string ATDT#777
!
dialer group gsm_us
init-string AT+CGDCONT=1,"IP","ISP.CINGULAR"
dial-string ATD*99#
!
dialer group gsm_asia
init-string AT+CGDCONT=1,"IP","internet"
dial-string ATD*99***1#
!
dialer group vivo_br
init-string AT+CGDCONT=1,"IP","zap.vivo.com.br"
dial-string ATD*99#
!
no spanning-tree

interface gigabitethernet 1/0
Deploying Ascom’s i62 VoWiFi handset with Aruba Networks’ Secure Mobility Solution

interface gigabitethernet 1/1
    description "GE1/1"
    trusted
    trusted vlan 1-4094

interface gigabitethernet 1/2
    description "GE1/2"
    trusted
    trusted vlan 1-4094

interface gigabitethernet 1/3
    description "GE1/3"
    trusted
    trusted vlan 1-4094

interface vlan 1
    ip address 192.168.0.13 255.255.255.0

ip default-gateway 172.20.106.1
ip default-gateway 192.168.0.50
uplink disable

ap mesh-recovery-profile cluster Recovery3Y7svy9npuyoWT2 wpa-hexkey
d25a708d7d02f5ec290fd3f63c7469a82956f320e49128942716f6e08bd3aeeb42497de39ee46f812270211997d9c92de5bf2af6fea707e475e642
9147af7ab955f0b3a8ad44819aee39f97f035ac9
crypto isakmp policy 20
    encryption aes256

    crypto ipsec transform-set default-boc-bm-transform esp-3des esp-sha-hmac
    crypto ipsec transform-set default-rap-transform esp-aes256 esp-sha-hmac
    crypto ipsec transform-set default-aes esp-aes256 esp-sha-hmac
    crypto dynamic-map default-dynamicmap 10000
    set transform-set "default-transform" "default-aes"

    crypto isakmp eap-passthrough eap-tls
    crypto isakmp eap-passthrough eap-peap
    crypto isakmp eap-passthrough eap-mschapv2

vpdn group l2tp

vpdn group pptp

tunneled-node-address 0.0.0.0

adp discovery enable
adp igmp-join enable
adp igmp-vlan 0
voice rtcp-inactivity disable
voice alg-based-cac enable
voice sip-midcall-req-timeout disable
ap ap-blacklist-timeout 3600
ap flushr1-on-new-r0 disable

mgmt-user admin root 5436b5a101681372db26d314e974065944317cd3e1fe6a5534

no database synchronize
ip mobile domain default
!
!
!
airgroup "enable"
!
airgroup location-discovery "enable"
!
!
airgroup active-wireless-discovery "disable"
!
airgroupservice "airplay"
  id ".airplay._tcp"
  id ".raop._tcp"
  id ".appleavd-v2._tcp"
  description "AirPlay"
!
airgroupservice "airprint"
  id ".ipp._tcp"
  id ".pdl-datastream._tcp"
  id ".printer._tcp"
  id ".scanner._tcp"
  id ".universal._ipp._tcp"
  id ".universal._ipp._tcp"
  id ".printer._http._tcp"
  id ".http._tcp"
  id ".http-alt._tcp"
  id ".ipp-tls._tcp"
  id ".fax-ipp._tcp"
  id ".rionusprint._tcp"
  id ".cups._ipp._tcp"
  id ".cups._fsox-fax-ipp._tcp"
  id ".ica-networking._tcp"
  id ".ptp._tcp"
  id ".canon-bjnp1._tcp"
  id ".ippss._tcp"
  id ".ica-networking2._tcp"
  description "AirPrint"
!
airgroupservice "itunes"
  id ".home-sharing._tcp"
  id ".apple-mobdev._tcp"
  id ".dpap._tcp"
  id ".dackp._tcp"
  description "iTunes"
!
airgroupservice "remotemgmt"
  id ".ssh._tcp"
  id ".sftp-ssh._tcp"
  id ".ftp._tcp"
  id ".telnet._tcp"
  id ".rfb._tcp"
  id ".net-assistant._tcp"
description "Remote management"
!
airgroupservice "sharing"
id "_odisk_tcp"
id "_afpovertcp_tcp"
id "_xgrid_tcp"
description "Sharing"
!
airgroupservice "chat"
id "_presence_tcp"
description "Chat"
!
airgroupservice "allowall"
description "Remaining-Services"
!
airgroup service "airplay" enable
!
airgroup service "airprint" enable
!
airgroup service "itunes" disable
!
airgroup service "remotemgmt" disable
!
airgroup service "sharing" disable
!
airgroup service "chat" disable
!
airgroup service "allowall" disable
!

ip igmp
!

ipv6 mld
!

no firewall attack-rate cp 1024
ipv6 firewall ext-hdr-parse-len 100
!

firewall cp
!
ip domain lookup
!
country US
aaa authentication mac "default"
!

aaa authentication dot1x "Arubalntop-dot1x_prof"
!

aaa authentication dot1x "ascom"
 machine-authentication enable
 machine-authentication machine-default-role "ascom"
 machine-authentication user-default-role "authenticated"
 reauthentication
termination enable
termination eap-type eap-peap
termination inner-eap-type eap-mschapv2
!

aaa authentication dot1x "default"
!

aaa authentication dot1x "freeradius"
 machine-authentication enable
 machine-authentication machine-default-role "ascom"
 machine-authentication user-default-role "authenticated"
aaa authentication-server radius "Intop"
    host "192.168.0.2"
    key bbdf593b6398e54784c19d823672ab7d
! aaa server-group "ascom"
    auth-server Internal
! aaa server-group "default"
    auth-server Internal
    set role condition role value-of
! aaa server-group "intop"
    auth-server Intop
! aaa profile "ascom"
    initial-role "ascom"
    authentication-dot1x "ascom"
    dot1x-default-role "authenticated"
    dot1x-server-group "ascom"
! aaa profile "default"
! aaa profile "default-dot1x"
    initial-role "ascom"
    authentication-dot1x "freeradius"
    dot1x-default-role "authenticated"
    dot1x-server-group "intop"
! aaa profile "default-dot1x-psk"
    initial-role "ascom"
    authentication-dot1x "default-psk"
    dot1x-default-role "authenticated"
! aaa authentication captive-portal "default"
! aaa authentication wispr "default"
! aaa authentication vpn "default"
! aaa authentication vpn "default-rap"
! aaa authentication mgmt
! aaa authentication stateful-ntlm "default"
! aaa authentication stateful-kerberos "default"
! aaa authentication stateful-dot1x
    server-group "intop"
! aaa authentication wired
! web-server
! guest-access-email
! voice logging
! voice dialplan-profile "default"
! voice real-time-config
! voice sip
! aaa password-policy mgmt
control-plane-security
  no cpsec-enable
!
ids wms-general-profile
poll-retries 3
!
ids wms-local-system-profile
!
valid-network-oui-profile
!
upgrade-profile
!
license profile
!
activate-service-whitelist
!
ifmap cppm
!
ap system-profile "default"
!
ap regulatory-domain-profile "default"
  country-code US
valid-11g-channel 1
valid-11g-channel 6
valid-11g-channel 11
valid-11a-channel 36
valid-11a-channel 40
valid-11a-channel 44
valid-11a-channel 48
valid-11a-channel 149
valid-11a-channel 153
valid-11a-channel 157
valid-11a-channel 161
valid-11a-channel 165
valid-11g-40mhz-channel-pair 1-5
valid-11g-40mhz-channel-pair 7-11
valid-11a-40mhz-channel-pair 36-40
valid-11a-40mhz-channel-pair 44-48
valid-11a-40mhz-channel-pair 149-153
valid-11a-40mhz-channel-pair 157-161
!
ap wired-ap-profile "default"
!
ap enet-link-profile "default"
!
ap mesh-ht-ssid-profile "default"
!
ap lldp med-network-policy-profile "default"
!
ap mesh-cluster-profile "default"
!
ap lldp profile "default"
!
ap mesh-radio-profile "default"
!
ap wired-port-profile "default"
!
ids general-profile "default"
!
ids unauthorized-device-profile "default"
!
ids profile "default"
!
rf arm-profile "default"
assignment disable
Deploying Ascom's i62 VoWiFi handset with Aruba Networks' Secure Mobility Solution
Deploying Ascom’s i62 VoWiFi handset with Aruba Networks’ Secure Mobility Solution

```plaintext
call-handoff-reservation 30
!
wlan ht-ssid-profile "default"
!
wlan hotspot anqp-venue-name-profile "default"
!
wlan hotspot anqp-nwk-auth-profile "default"
!
wlan hotspot anqp-roam-cons-profile "default"
!
wlan hotspot anqp-naI-realm-profile "default"
!
wlan hotspot anqp-3gpp-nwk-profile "default"
!
wlan hotspot h2qp-operator-friendly-name-profile "default"
!
wlan hotspot h2qp-wan-metrics-profile "default"
!
wlan hotspot h2qp-conn-capability-profile "default"
!
wlan hotspot h2qp-op-cl-profile "default"
!
wlan hotspot anqp-ip-addr-avail-profile "default"
!
wlan hotspot anqp-domain-name-profile "default"
!
wlan wmm-traffic-management-profile "Ascom"
enable-shaping
!
wlan edca-parameters-profile station "default"
 voice aifsn 2 ecw-min 2 ecw-max 3 txop 47 acm 1
!
wlan edca-parameters-profile ap "default"
 voice aifsn 1 ecw-min 2 ecw-max 3 txop 47 acm 1
!
wlan dot11k-profile "default"
!
wlan ssid-profile "--NEW--"
 essid "ArubaIntop2"
 wmm-vo-dscp "56"
 wmm-vi-dscp "40"
 wmm-be-dscp "24"
 wmm-bk-dscp "8"
!
wlan ssid-profile "default"
 essid "ArubaIntop"
opmode wpa2-psk-aes
dtim-period 5
g-basic-rates 6
g-tx-rates 12 18 24 36 48 54
max-retries 4
wmm
wmm-vo-dscp "46"
wmm-vi-dscp "40"
wmm-be-dscp "26"
wmm-bk-dscp "0"
wepkey1 14ceffb539b44c2c4e50928edbe578b3e17c19e0d93c5
wpa-passphrase e4069775e5237233abf77e826c95ba34cd681b8b43f6d2c
max-tx-fail 25
edca-parameters-profile station "default"
edca-parameters-profile ap "default"
!
wlan ssid-profile "test"
opmode wpa2-psk-aes
wmm-vo-dscp "56"
wmm-vi-dscp "40"
```

Deploying Ascom’s i62 VoWiFi handset with Aruba Networks' Secure Mobility Solution
Deploying Ascom's i62 VoWiFi handset with Aruba Networks' Secure Mobility Solution

wmm-be-dscp "24"
wmm-bk-dscp "8"
wpa-passphrase 01f99aa9676847ef32e5781a52a9dccc5c33204e22e1a4b6

wlan hotspot advertisement-profile "default"
wlan hotspot hs2-profile "default"
wlan virtual-ap "default"
  aaa-profile "default-dot1x"
ap provisioning-profile "default"
rf arm-rf-domain-profile
  arm-rf-domain-key "49868e8b02680a8f03980ea4288197a4"
ap-group "default"
  virtual-ap "default"
    dot11a-radio-profile "ch 40"
    dot11g-radio-profile "channel-6"
ap-name "00:1a:1e:ca:2c:1a"
    dot11a-radio-profile "ch 36"
    dot11g-radio-profile "channel-11"
ap-name "00:1a:1e:ca:2c:76"
    dot11a-radio-profile "ch 36"
    dot11g-radio-profile "channel-1"
ap-name "00:24:6c:cb:f8:b1"
ap-name "00:24:6c:cb:f9:00"
    dot11a-radio-profile "ch44"
    dot11g-radio-profile "channel-11"
ap-name "24:de:c6:ca:ca:bc"
    dot11a-radio-profile "ch149"
    dot11g-radio-profile "channel-1"
ap-name "3400-ap-61-a"
    dot11g-radio-profile "channel-6"
ap-name "3400-ap-61-b"
    dot11g-radio-profile "channel-6"
ap-name "9c:1c:12:0:0:3:bc"
    dot11a-radio-profile "ch 36"
    dot11g-radio-profile "channel-6"
ap-name "d8:c7:c8:0:a1:68"
    dot11a-radio-profile "ch 36"
    dot11g-radio-profile "channel-1"
airgroup cppm-server aaa
logging level warnings security subcat ids
logging level warnings security subcat ids-ap
snmp-server enable trap
firewall-visibility
process monitor log
end