Release Note	Alcatel-Lucent OmniPCX Office

TC0096 Ed.28 **Releases 7.1 and later**

SOFTWARE EVOLUTIONS OF THE VOICE OVER WLAN SOLUTION FOR OMNIPCX OFFICE

This document describes the evolutions of software versions available for the Voice over WLAN solution and the software compatibilities between all Alcatel-Lucent WLAN equipments.

Revision History

Edition 25: April 9, 2012	Release of latest VoWLAN R5.3 offer
Edition 26: April 22, 2013	Update for new VoWLAN R5.4 release
Edition 27: June 17, 2013	Supported infrastructure update
Edition 28: September 26, 2013	Add the iAP new infrastructure support

Legal notice:

Alcatel, Lucent, Alcatel-Lucent and the Alcatel-Lucent logo are trademarks of Alcatel-Lucent.
All other trademarks are the property of their respective owners.
The information presented is subject to change without notice.
Alcatel-Lucent assumes no responsibility for inaccuracies contained herein.

Table of contents

1 Introduction

The **Voice over WLAN release 5.4** introduces infrastructure evolutions in the Voice offer, permits to sustain OmniTouch 8118/8128 WLAN Handsets software and takes in consideration the HW and SW compatibility for the new functionalities.

With the AOS version 6.2.x SW maintenance version of the OmniAccess WLAN, the **VoWLAN R5.4** brings the following features:

- Platform enhancements (ARM, WMM enhancements, DFS channels management, L2/L3 VLAN scalability)
- Embedded spectral analysis enhancements
- Policy Enforcement Firewall (PEF) visibility in dashboard GUI
- RAP serviceability enhancements
- LLDP MIBs enhancements

This release includes the following AP hardware for the VoWLAN topologies **plus the new Instant AP solution support for voice**:

- Outdoor OAW-AP175
- OAW-AP104
- **OAW Instant AP: iAP92/93, iAP104/105, iAP134/135, iAP175 (Outdoor AP)**

2 Compatibilities

The **Voice over WLAN R5.4** offer for OT8118/8128 WLAN Handsets is composed of the following software versions:

- Alcatel-Lucent OmniPCX Office R7.1 and higher
- Alcatel-Lucent OmniTouch 8118/8128 Handsets **4.2.8 SW Version**
- Alcatel-Lucent OmniTouch 8118/8128 WinPDM 3.9.0 SW Version
- Alcatel-Lucent OmniAccess WLAN 5.0.4.2 SW Version
- Alcatel-Lucent OmniAccess WLAN 6.2.1.1 SW Version
- **Alcatel-Lucent InstantOS 6.2.1.0-3.3.0.2 SW version**

Alcatel-Lucent OmniTouch 8118/8128 supports Wi-Fi standard QoS (Standards-Based WMM) and CCXv2 QoS mode.

Warning

Business Partner must take into account that adding OmniTouch 8118 & 8128 WLAN Handsets on existing customer premises installed with IPT 310/610 with/without SVP server ***is no more supported. Replace IPT 310/610 solution by OT81x8 solution.***

3 Alcatel-Lucent OmniTouch 8118/8128 WLAN Handsets

3.1 OT8118/8128 WLAN Handsets Released Software Versions

3.1.1 4.2.8 version

This SW version of the VoWLAN R5.4 offer is a minor release for the OmniTouch 8118/8128 WLAN Handsets. It includes the following fix:

- NCR 22663 - WEP key error with upgrade from 2.6.6 to 4.2.2

⚠ Warning

Limitation: It is not possible to recover after an earlier upgrade to version 4.2.2. WEP keys containing 0x00 byte will be corrupted after upgrade. Examples of non-handled WEP keys: 0x1200345678, 0x00aabbccdd. WEP keys like 0x1002334455 will not be corrupted.

3.1.2 4.2.2 version

This SW version of the VoWLAN R5.4 offer is a minor release for the OmniTouch 8118/8128 WLAN Handsets. It includes the following improvements:

- Configurable automatic key/phone lock timer with timeout and auto key unlock
- Range beep in Sound and Alerts menu is added: handset starts beeping when the signal strength from the AP is low
- Automatic switching between network systems: if the current WiFi network is lost, the handset will try to associate to the next configured network
- Disable permanent mute: it is possible to restrict the user from setting the handset to silent.
- Add reset_cause in NOE EVT_REST message
- Validation of server certificate is now optional for PEAP/MSCHAPv2 and EAP-TLS
- New Hearing Aid Compliance (HAC) mode
- Show WLAN interface version in Device info screen
- Improved echo cancellation for hearing protector headset
- NTP server IP address in DHCP mode

It includes the following corrections:

- NCR 17584 – No beep (or tone) on some digit dialed
- NCR 20056 – EAP-TLS in a Cisco system fails to renew
- NCR 20178 – Wrong encryption key used by handset when using EAP
- NCR 20636 – WEP keys are handled correctly also after restart
- NCR 20838/20742 – Radio sensitive to frequency offset on 5GHz band : tolerance to RF frequency offset between handset and APs improved
- NCR 20958 – Faulty entry in syslog at roam: "From AP" instead of "RSSI: 0 - Ch: 0" fixed
- NCR 21062 – 802.1x Re-authentication issues with Alcatel-Lucent Networks : Encrypted EAPOL frames will pass APs and finally reach the RADIUS server to complete the authentication
- NCR 21908 - Voicemail via menu not working
- NCR 21693 - Wrong value in BA TID trigger (Cisco bug)

For features and fixes details, please refer to the file « mipt8_journal » included with the binaries zip package.

Enhancements on infrastructure: **tested and supported versions and hardware: for configuration and limits, refer to the Technical Documentation for third Party on the Business Partner Portal**:

Meru	
Hardware	**Software**
WLAN Controller: MC500 AP: AP2xx/AP3xx	4.0-150 (MR3)
WLAN Controller: MC1000/5000 AP: AP2xx/AP3xx	5.0-87
WLAN Controller: MC1500/3x00/4x00/**5000/6000** AP: **AP320/332/AP1000**	**5.3.50**
Trapeze/Juniper	
Hardware	**Software**
WLAN Controller: MX/WLC 2/8/200/8x0/2800 AP: MP/WLA **321/322**/371/372/422/522/532	7.6.2.3 **8.0.2.2**
Cisco	
Hardware	**Software**
Autonomous mode AP: AP1230/1240 Autonomous mode AP : AP1140/1250/1260 series	12.3(8)JED1 12.4(25d)JA1
WLAN Controller: WLC 210x/440x series/WISM/550x/3750G AP: AP1130/1140/1230/1240/1250/1260/**2600**/3500/3600 series	**7.3.101**
Motorola/OEM Brocade	
Hardware	**Software**
WLAN Controller : RFS4000/RFS6000/RFS7000/NX9000 AP: AP650/6511/6532/7131	**5.4.0.0**
Aruba	
Hardware	**Software**
WLAN Controller : 3000/6000 AP: AP60/61/65/70/92/93/**104/105**/12x/134/135/**175**	AOS 5.0.x **AOS 6.2.x**
iAP: iAP92/93/104/105/134/135/175	**AOS 6.2.1.0-3.3.0.2**
Aerohive	
Hardware	**Software**
WLAN Controller: **AP: AP120/121/141/330/350**	**HiveOS (5.1r5)**
Avaya	
Hardware	**Software**
WLAN Controller: 8180 **AP: AP8120/8120-E**	**2.0.0.084**
Enterasys	
Hardware	**Software**
WLAN Controller: C20/C25/C2110/C2400/C4110/C5110 **AP: AP3605/3610/3620/3630/3640**	**08.11.06**
Extricom	
Hardware	**Software**
WLAN Controller: MultiSeries 500/1000 **AP: EXRP-30n/-40En**	**4.5.09**
HP	
Hardware	**Software**
WLAN Controller: MSM 710/720/760 **AP: MSM 422/430/460/466**	**5.7.1.0**

Ruckus	
Hardware	**Software**
WLAN Controller: ZD 1100/3000/5000 controllers **AP: ZF7963, ZF7363 and ZF7341/7343**	**9.4.2.0**

3.1.3 2.6.8 version

- NCR 20743 – Phone re-associates to the SSID, with network busy notification when receiving a call when TSPEC is activated
- NCR 19370 – UP on signaling data : new parameter added for compatibility with Aruba 800 controller for traffic prioritization
- NCR 20446 - Low volume on notification of second incoming call

3.1.4 2.6.6 version

This SW version of the VoWLAN R5.3 offer is a minor release for the OmniTouch 8118/8128 WLAN Handsets. It includes the following features:

- Added possibility to change WLAN band (already present in WinPDM) from Admin menu > Network setup > 802.11 protocol: choose the 802.11 radio band (b/g, b/g/n, a or a/n)
- Optimized DFS channel scanning: Improved voice performance and positioning in DFS channels. The difference between DFS and non DFS channel operation is reduced. The non DFS channels are still preferable because there are limitations on the DFS channels that might impact the voice quality. Hidden SSID now works on DFS channels.
- Add WLAN keep alive function (Heartbeat): A Null data packet is sent every 125 seconds to insure that the handset stays connected to the infrastructure.
- Added a Site survey mode for Ekahau that will cause location scanning to be performed at shorter intervals: 1 s. Locally enabled from the handset Admin menu > Site survey tool > Location survey.
- TFTP/DHCP survivability enhancement: Shorter time spent in survivability with less retries for config file, start file and binary downloads.
- Change the text "Hide Admin" to "Read only"in the WinPDM view for customization.
- Gain for loudspeaker increased by 3dB on volume level 6, 6 dB on volume level 7 and 10 dB on volume level 8. The maximum sound pressure is not increased on any of the volume levels, only the gain. This means that incoming voice signals that are weak will be played out up to 10 dB stronger. But if the incoming voice signal is strong so that the maximum sound pressure is already reached, there will be no change.

It includes the following corrections:

- U-APSD disabled in WLAN but enabled in handset causes Legacy Power-Save in call: Use active mode (no power save) when U-APSD is enabled in the handset but disabled in the infrastructure.
- When a handset goes out of coverage and tries to reconnect, it gets stuck in "Connecting": PBX connection is restored when the handset regains coverage.
- Handset starts up with "blank" NOE idle screen sometimes: Allow sending an ACK even if the handset is waiting for an ACK for a previously sent DATA packet. Reception of a DATA packet when waiting for CONNECT ACK will now make the session goes into CONNECTED state, so the incoming packets are processed
- Behavior of Call Admission Control: OT81x8 will try a new AP if current AP is refusing the ADDTS request

New WLAN Driver version fixes the followings issues:

- No scanning performed even if RSSI is below -70: Background scanning stopped until network was lost causing gaps during call. This case is now eliminated.
- Firmware hangs for DELTS: Resolved WLAN disconnect issue when terminating call with CAC/TSPEC.
- wpa_supplicant not always able to re-authenticate EAP-FAST with CCKM: Restart resolved. Supplicant sometimes crashed when using CCKM and authentication timed out on RADIUS server.
- Tx maximum spatial stream supported may signal more than 1: Always associates to 802.11n APs with correct number of spatial streams (1).
- Timeout while waiting for power save event: Restart of WLAN driver due to incorrectly missed beacons is now resolved.
- 802.11h power constraint not followed when not roaming: Dynamically changes Tx power when changing Transmit EIRP (802.11h)
- Absence of probe response after directed probe request causes 5 seconds scanning delay: 5 to 10 seconds speech gap due to bad roaming is fixed
- Wrong encryption used by handset: The handset will not lose WLAN connectivity due to use of wrong PTK when regularly updating the PTK
- Handset stops probing issue fix: problem could cause audio disturbance and gaps in call.
- ADDTS and does not comply with CCX requirements: Added missing Traffic Stream Rate Set (TSRS) in the ADDTS Request and (Re) association Request.
- Radio Measurements does not comply with CCX requirements: Accepts radio measurement requests in CCX testing.
- CCX failure: Traffic Stream Metrics (TSM) reports are now sent periodically after each roam.
- 11n with U-APSD bad performance on Cisco WLC: Fixed an issue with aggregation on 802.11n.
-

Enhancements on third party infrastructure: **tested and supported SW versions and HW: for configuration and limits, refer to the Technical Documentation for third Party on the BP Portal**:

Meru	
Hardware	**Software**
WLAN Controller: MC500 AP: AP2xx/AP3xx	4.0-150 (MR3)
WLAN Controller: MC1000/5000 AP: AP2xx/AP3xx	5.0-87
WLAN Controller: MC1500/**3x00**/**4x00** AP: AP3xx/**AP10xx**	**5.1-47**
Trapeze/Juniper	
Hardware	**Software**
WLAN Controller: MX/**WLC 2/**8/200/**8x0**/2800 AP: MP/WLA 371/372/422/522/**532**	**7.6.2.3**
Cisco	
Hardware	**Software**
Autonomous mode AP: AP1230/1240 Autonomous mode AP : AP1140/1250/**1260** series	12.3(8)JED1 **12.4(25d)JA1**
WLAN Controller: WLC 210x/440x series/WISM/550x/3750G AP: AP1130/1140/1230/1240/1250/1260/3500/**3600** series	**7.2.110**
Motorola	
Hardware	**Software**
WLAN Controller : RFS4000/RFS6000/RFS7000/NX9000 AP: AP650/6511/6532/7131	5.1.0.0

Aruba	
Hardware	**Software**
WLAN Controller : 3000/6000 AP: AP60/61/65/70/92/93/105/12x/134/135	AOS 5.0.x AOS 6.0.x AOS 6.1.x

3.1.5 2.3.16 version

This SW version of the VoWLAN R5.2 offer is a major release for the OmniTouch 8118/8128 WLAN Handsets. It includes the following corrections:

- Handset stops probing without reason: slow roaming, connection lost issues fixed
- New WLAN driver version 2.2.1 for Trapeze infra update MP422: Problem with powersave sleep mismatch vs infrastructure fixed
- Loss of connection: Fix for long gaps during start of calls.
- Communication problems with aggregated packets from Cisco 3500: Resolves an issue with aggregated frames (802.11n) on Cisco WLC.

Added functionality and enhancements:

- Continuous ring signal: a new ring signal “Continuous” with continuous ringing is added. It replaces the “Detective” ring signal.
- Ring signal with increased volume: an additional ring signal “Aggressive” is added. This is optimized for the hardware and is composed to breakthrough noisy environment.
- 802.11n support: handset can be configured to use 802.11an or 802.11bgn. If working with 802.11a/b/g AP, the handset will be recognized as 802.11a/b/g client. If working with 802.11n AP, the handset will be recognized as 802.11n client.
- Parameter "Config file TFTP IP address DHCP" is hidden in Local MMI: the parameter is not intended to be changed by the administrator, only changed by software and is now hidden in WinPDM.
- Improved background scanning for positioning purposes: solves a problem with scanning result for positioning (Ekahau)
- Roaming enhancements: Shorter delay before initiating a scan after deauthentication.
- Syslog messages are sent immediately when the log is done.
- Added channel information to WLAN roaming syslog message.
- The handset disassociates from the WLAN when it is switched off.
- Interoperability with Motorola: Corrected some issues found with WMM and sequence numbers.

Enhancements on third party infrastructure: tested and supported versions and hardware: **for configuration and limits, refer to the Technical Documentation for third Party on the Business Partner Portal:**

Meru	
Hardware	**Software**
WLAN Controller: MC1000\MC3000\MC5000 AP: AP200/AP300	4.0-150 (MR3)
WLAN Controller: MC1500, AP: AP320	4.0-150 (MR3)
Trapeze/Juniper	
Hardware	**Software**
WLAN Controller: MXR-2, AP: MP-422B, MP-372-CN	7.3.4.4.0
WLAN Controller: MX-8/**200/800/2800**, AP: **MP372**/422/**522**	**7.3.4.4**

Cisco	
Hardware	**Software**
Autonomous mode AP: 1130/1230/1240/**1250** series	12.3(8)JED1/**12.4(21a)JY**
Cisco WLC 210x, 440x series, WISM, 550x, 3750G AP (thin mode): 1130/1140/1230/1240/1250/1260/3500 series	7.0.98
Motorola	
Hardware	**Software**
WLAN Controller : RFS4000\RFS6000\RFS7000\NX9000 **AP: AP650/AP6511/AP6532/AP7131**	**5.1.0.0**

3.1.6 2.2.26 version

This SW version for the OmniTouch 8118/8128 WLAN Handsets is a maintenance release. It includes the following corrections:

- The configured IP DSCP for voice value is now correctly used on voice traffic.
- One way speech after received DTMF tones: drop unknown RTP packets to not affect the speech.

3.1.7 2.2.24 version

This SW version for the OmniTouch 8118/8128 WLAN Handsets is a maintenance release introduced with the VoWLAN R5.1. It includes the following corrections and enhancements:

- Possibility to select mode 802.11b/g or 802.11a (without n) added: the parameter “802.11 protocol” is set to its non-802.11n variant at start-up, i.e.:
  - 802.11a/n -> 802.11a
  - 802.11b/g/n -> 802.11b/g
- WinPDM: "Edit certificates" menu is missing on WinPDM v3.8.1: fixed
- Improvement of channels scan
- Handset cannot associate with Alcatel-Lucent AP when configuring with 4 WEP keys: fixed
- Loudspeaker enabled a short time during lock/unlock operation: fixed
- Handset enables Handsfree after some operation of Feature call: fixed
- “No network” issue fixed
- Advanced channel settings has no effect: fixed
- Ringing melody changed after hang-up of the 1st call: fixed
- Handset can hear the ringing back tone when using vibrate or silent profile
- Problem associating if lowest basic rate is 2, 5.5 or 11 Mbit resolved
- Decreased standby time and call time on Trapeze resolved
- Fast Roaming/handover with EAP-FAST CCKM for WPA2 AES-ccmp: handset stucked in "No access/Connecting" fixed
- CAC works in all Cisco environments

Tested and supported versions and hardware: **for configuration and limits, refer to the Technical Documentation for third Party on the Business Partner Portal**:

Meru	
Hardware	**Software**
WLAN Controller: MC1000\MC3000\MC5000 AP: **AP200**/AP300 WLAN Controller: MC1500, AP: AP320	**4.0-150 (MR3)**
Trapeze/Juniper	
Hardware	**Software**
WLAN Controller: MXR-2, AP: MP-422B, MP-372-CN	7.3.4.4.0
WLAN Controller: MX-8, AP: MP422	7.3.4.0.002
Cisco	
Hardware	**Software**
Autonomous mode AP: 1130/1230/1240 series	12.4(10b)JDA3 / 12.3(8)JED1
Cisco WLC **210x**, 440x series, WISM, 550x, 3750G AP (thin mode): 1130/1140/1230/1240/1250/**1260**/**3500** series	**7.0.98**

3.1.8 2.2.9 version

This SW version for the OmniTouch 8118/8128 WLAN Handsets is a maintenance release. It includes the following corrections:

- Roaming in idle does not work efficiently: fixed
- Improved roaming for small cells
- Transmit EAPOL frames with UP7 instead of UP0. Resolves rare gaps when roaming.
- Syslog: Report "Battery status" and "WLAN status" messages at start-up
- Syslog: Report "WLAN Authentication" and "QoS value" messages
- Password inputting box display not proper: fixed
- Text message last character cannot be input properly: resolved
- Headset indication volume changes
- The handset can delete the MUTE & Loudspeaker icons by local administration
- Device switches back to "normal" when taken out of the charger
- "On hook" button works after enter into "More" menu
- Set updates the profile changes correctly
- Screen is lighted up in com each minute as the display changes: fixed
- TSPEC Call Admission Control works with Cisco Autonomous AP1200

Added functionality:

- New parameter for fast EAP reauthentication: in "Network/Advanced", "Fast EAP reauth": can be useful when running two different systems with the same SSID. When the parameter is active, the handset deauthenticates on every roam to avoid the handset to stay as an idle client in the former system.
- Customizable GUI: It is possible to hide menu items for the users via WinPDM:
    - Select Customization > Visibility
    - Select “Hide”, “Show”, or “Hide admin” for the applicable menu item in the dropdown list. If “Hide admin” is selected, the menu item will be visible in the handset, but cannot be edited by the user.

The following items can be hidden: Connections (Network, Headset etc.), Profiles, Settings (Sounds, Display, Language).

And enhancements on third party infrastructure: **for configuration and limits, refer to the Technical Documentation for third Party on the Business Partner Portal:**

- Support of OT81x8 on third party infrastructure: Trapeze/Juniper, Meru
- QoS Mixed configurations (IPT with SVP server & OT 81x8 on WMM): Cisco, Trapeze/Juniper, Meru and ALU Infrastructure.

Tested and supported versions and hardware:

Meru	
Hardware	**Software**
WLAN Controller: MC1000\MC3000\MC5000, AP: AP300	4.0.86
WLAN Controller: MC1500, AP: AP320	4.0.131
Trapeze/Juniper	
Hardware	**Software**
WLAN Controller: MXR-2, AP: MP-422B, MP-372-CN	7.3.4.4.0
WLAN Controller: MX-8, AP: MP422	7.3.4.0.002
Cisco	
Hardware	**Software**
Autonomous mode AP: 1130/1230/1240 series	12.4(10b)JDA3 / 12.3(8)JED1
Cisco WLC 4400 series, WISM, 5500, 3750G + AP (thin mode): 1130/1140/1230/1240/1250 series	5.2.178.0 6.0.196.0

3.1.9 2.1.19 version

This SW version is the first one released for the OmniTouch 8118/8128 WLAN Handsets introduced in the OmniPCX Office R8.0 offer.

Note

The OmniTouch 8118/8128 WLAN Handsets are compatible with previous OmniPCX Office versions but requires the use of external TFTP server for centralized handset's update

These new handsets integrate the following features:

- Radio:
  - 802.11 a/b/g
  - 802.11 h/DFS2
  - Radio Transmit Output Power: adjustable through configuration up to 100mW
- Security:
  - WEP
  - WPA/PSK (TKIP)
  - WPA2-PSK
  - 802.1X with PEAPv0/EAP-MSCHAPV2
  - 802.1x with EAP-TLS
  - 802.1X with EAP FAST (Cisco...)
  - Certificate management: with Handset management tool WinPDM
- Network:
  - IP/ARP/UDP/TCP/RTP
  - Static IP address Configurable
  - DHCP Client

    - DNS Client
    - TFTP Client
- Audio:
    - Hands free (Model 8128)
    - Headset, Microphone, Mute
    - Audio Codec: G.711 a/u, G729 a/bVAD/CNG
    - Ring Mode, Vibrating Mode
    - DTMF Sending
- QoS:
    - WMM (EDCA) + WMMPS (U-APSD)
    - Call Admission Control
    - DSCP local configuration
- System compatibility:
    - Call server backward compatibility: OXO >= R610
    - Firmware update by TFTP server. Terminal type and binary management in OXO >=R8.0
    - Initialization procedure compatibility to CS
    - NOE/UA protocol support
    - MMI compatibility to CS
    - Same level Telephonic services capability as IPT 310/610
- Misc:
    - Keypad Lock
    - User profiles settings
    - RTLS Geo-Location
    - Screen Saver, Contrast, Brightness, Backlight
    - Handset Administration PC: WinPDM
    - Local administration
    - Registration to different WLAN systems
- Infrastructure compatibility:
    - Alcatel-Lucent WiFi Infrastructure compatibility : AOS >= 5.0
    - Cisco CCXv2
- Serviceability:
    - Embedded Site Survey Tool
    - Syslog mode
    - Indicator Icons
    - Configurable battery low warning
- RADIUS server compatibility:
    - Steel-belted
    - Free radius
    - Microsoft IAS
    - ALU 8950
- DHCP server compatibility:
    - Windows 2003 DHCP Server
    - Vital QIP DHCP server

3.2 Known Restrictions

3.2.1 Global restrictions

The following restrictions and limitations have been reported during tests and have been taken into account:

- Handset radio performance can be impacted by interferences produced by other radio devices:
    - A **site survey for voice deployment** must be done on site mainly after environment evolution /handsets adjunction
    - Prefer the use of **802.11a/n band** if possible
    - If 802.11b/g radio is used, some channels may be revised depending on b/g interferers (channel 11 is easily interfered by other devices in blue tooth…)
    - 2x20 MHz mode is not recommended on the 2.4 GHz frequency band (802.11 b/g/n) due to a limited number of non overlapping channels (3 only).
- 802.11a/n: it is recommended to **use non-DFS (36-48 and 149-161**, depending on the regulatory domains). The recommendations made in OAW section for 802.11a/n must be considered if DFS channels use is mandatory.
- Due to DFS channel improvements, the power consumption in call can be higher in 2.6.x compared to 2.3.x when using the default setting for Network, 802.11a/n channels "all" (via WinPDM). For best performance and battery lifetime it is recommended to limit the channels used to the ones actually used in the system.
- ARM (Automatic Radio Management used to have an automatic channel and transmission power configuration) is not recommended. This should be disabled on the controller or set to maintenance mode.
- G.723 codec is not supported by the handset.
- Hidden SSID is not supported.
- SVP server and Standard-Based WMM QoS is no more supprted (IPT no more supported).
- Infrastructure compatibility: Alcatel-Lucent AOS >= 5.0, Cisco CCXv2, Meru, Motorola and Trapeze/Juniper **following the limits given in the Configuration notes on the Business Partner Portal**
- TCLAS (for traffic classification) is not implemented.
- The GUI local menu does not return to idle automatically.
- Audio routing is not supported. The handset will manage the loudspeaker and microphone mute locally.
- No key beep after the 2nd digit dialed, no key tone when have an external call.
- During EAP-FAST authentication, the handset only supports auto provisioning ".PAC" file. Moreover, it will try to download the ".PAC" file at each initialization.
- **802.11k is not supported by OT81x8, deactivate it on infrastructure side**
- **WEP key is lost after an upgrade to 4.2.2 version, the key must be reinitialized manually**
    - **Fixed in version 4.2.8 but it remains impossible to recover after an earlier upgrade to version 4.2.2. WEP keys containing 0x00 byte will be corrupted after upgrade. Examples of non-handled WEP keys: 0x1200345678, 0x00aabbccdd. WEP keys like 0x1002334455 will not be corrupted.**
- The following settings can only be configured via WinPDM tool and the configuration cradle:
    - 802.1x parameters
    - TSPEC Call Admission Control
    - DSCP value for QoS

3.2.2 Restrictions with OmniPCX Office

- OT81x8 hardware type and binary management have not been implemented on OXO release <= R710: upgrade the handset's version via WinPDM or external TFTP server. OT81x8 are seen as MIPT300.

3.2.3 Restrictions with third party infrastructures

Third party infrastructure refers to non Alcatel-Lucent infrastructure such as Cisco, Trapeze, Meru, Motorola…

For an up to date list of supported infrastructure and associated configuration and restrictions, please **refer to the Technical Documentation for third Party on the Business Partner Portal**.

3.3 OT8118/8128 WLAN Handsets Update

The binary files of software version and the WinPDM application can be found on the Business Partner Portal in section *Customer Support > Technical Support > Software download > Phones > OmniTouch 8118/8128*.

When the OmniTouch 81x8 handset starts, it compares its current version with the software available on the TFTP server. If it is a different software version, it will be updated automatically:

- By OmniPCX Office embedded TFTP Server:
- The OmniTouch WLAN Handset software version included in the updated software version of the OmniPCX. The Master VoIP card IP address of the OmniPCX must be configured in the Firmware TFTP IP field available from the administration menu of the handset.

Note

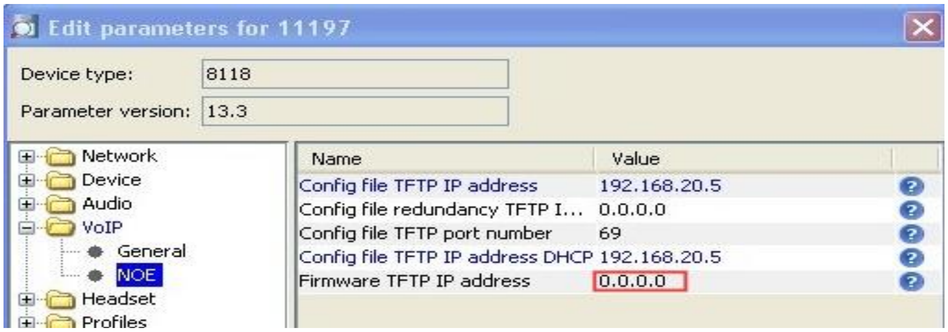
TFTP file from OmniPCX Office cannot be updated

or

- By external TFTP Server on the LAN:
  It is possible to add the software in an external TFTP Server available on the LAN. Its IP address must be configured in the Firmware TFTP IP field available from the administration menu of the handset.

or

- By the WinPDM Tool for PC (without TFTP Server):
  The WinPDM tool permits to update the Omni Touch 8118/8128 WLAN handset's version. In that case, 0.0.0.0 must be configured in the Firmware TFTP IP address field available from WinPDM VoIP > NOE sub-menu of the handset in order to avoid update request to another TFTP Server.

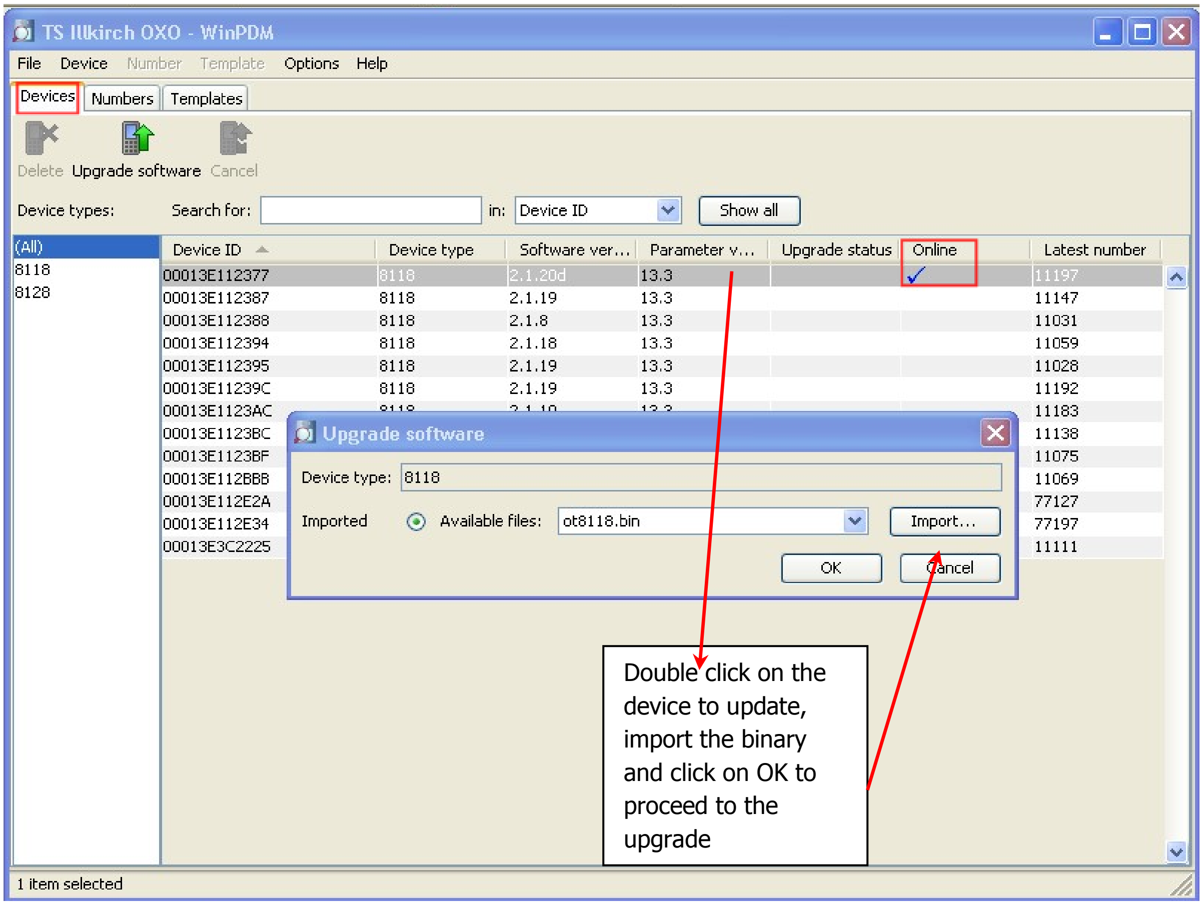


Device type: 8118

Parameter version: 13.3

Name	Value
Config file TFTP IP address	192.168.20.5
Config file redundancy TFTP I…	0.0.0.0
Config file TFTP port number	69
Config file TFTP IP address DHCP	192.168.20.5
Firmware TFTP IP address	0.0.0.0

Then, the new version can be uploaded: in the Devices tab, check the 'Online' flag for the handset to upgrade, double click on the device, import the right binary file (.pkg) and accept. Download is pending and when finished, the handset shuts down and restarts.



TS Illkirch OXO - WinPDM
File Device Number Template Options Help
Devices Numbers Templates
Delete Upgrade software Cancel
Device types: Search for: in: Device ID Show all
(All)
8118
8128

Device ID	Device type	Software ver...	Parameter v...	Upgrade status	Online	Latest number
00013E112377	8118	2.1.20d	13.3		✓	11197
00013E112387	8118	2.1.19	13.3			11147
00013E112388	8118	2.1.8	13.3			11031
00013E112394	8118	2.1.18	13.3			11059
00013E112395	8118	2.1.19	13.3			11028
00013E11239C	8118	2.1.19	13.3			11192
00013E1123AC	8118	2.1.19	13.3			11183
00013E1123BC						11138
00013E1123BF						11075
00013E112BBB						11069
00013E112E2A						77127
00013E112E34						77197
00013E3C2225						11111

Double click on the device to update, import the binary and click on OK to proceed to the upgrade

A software delivery is composed of several files:

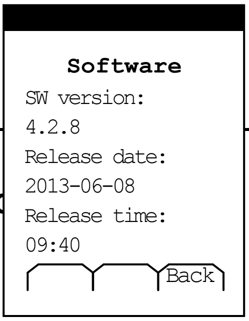
• ot8118.bin	Binary for handset 8118
• ot8128.bin	Binary for handset 8128
• 8118_4.2.8.pkg	8118 package with definition file for WinPDM tool
• 8128_4.2.8.pkg	8128 package with definition file for WinPDM tool
• miptr3bin	Only used by OXE TFTP server

The software version of 81x8 phones can be verified:

- Through the Local Menu: Enter the local menu by pressing the [ok] key, then navigate through the link Settings > Device info and then Software menu. The Software version screen displays the version (ie. x.y.z) plus other information (release date, etc…).

or

- With the handset powered off, switch on the OmniTouch. When the progress bar is finished and the set is 'Searching' for its network, dial the 40022 administration code to enter in the Admin menu: access to the Device info and Software menus:



Software
SW version:
4.2.8
Release date:
2013-06-08
Release time:
09:40

3.4 OT8118/8128 WLAN Handsets WinPDM Administration Tool

The WinPDM application on PC permits to manage and configure the OmniTouch 8118/8128 WLAN handsets through a PDM Configuration cradle. This specific cradle has a self-supplied USB connection to the PC and is required to configure the handset and to update its software with the WinPDM software.

3.4.1 WinPDM 3.9.0 version

The WinPDM delivery includes setup files and driver files:

- Support for Windows 7 (32 bits and 64 bits)
- New column for last login
- Move columns in the GUI and remember their locations
- Possible to change case for string parameters

3.4.2 WinPDM 3.8.1 version

This SW version is a minor release including:

- Support for Windows 7
- Signed executable and USB drivers for Windows 7 32-bit and 64-bit

3.4.3 WinPDM 3.6.5 version

This SW version is the first released version of the WinPDM Administration Tool, which gives the ability to configure Alcatel-Lucent OmniTouch 8118/8128 WLAN Handset from a computer.

Note

The following settings can only be configured via WinPDM tool and the configuration cradle:

- 802.11 radio mode
- 802.1x parameters
- TSPEC Call Admission Control
- DSCP value for QoS

4 Alcatel-Lucent OmniAccess Wireless LAN switch

The VoWLAN R5.4 is the latest released offer of the VoWLAN solution.

4.1 Licenses

In Campus deployment I.E. Campus APs managed by a WLAN controller, licenses are mandatory. Information about AOS-W 6.2 licenses and procedure to obtain them are described in detail in the "Software Licenses" chapter of AOS-W 6.2 User Guide. Ensure to follow the instructions carefully to obtain and install the AOS-W 6.2 licenses in the switch.
Mandatory licenses for the Voice over WLAN:

- Access Point license (LAP) (calculated on AP quantity)
- PEF New Generation license (PEFNG) (calculated on AP quantity)

The Instant AP solution is a controllerless WLAN solution based on a Virtual Controller (VC) and does not require any license.

4.2 Software and hardware compatibilities for VoWLAN

The VoWLAN R5.4 is covering the following list of WLAN products:

OAW Products	**AP Products**
OAW-4306	OAW-AP92
OAW-4306G	OAW-AP93
OAW-4504XM	OAW-AP104
OAW-4604	OAW-AP105
OAW-4704	OAW-AP124
OAW-6000-PS4	OAW-AP125
OAW-S3-0-2X10G	OAW-AP134
	OAW-AP135
	OAW-AP175
	OAW-iAP92
	OAW-iAP93
	OAW-iAP104
	OAW-iAP105
	OAW-iAP134
	OAW-iAP135
	OAW-iAP175

Warning

Only listed items and topologies are supported, other items not in the list are not supported.

Warning

Reminder: the following types of HW are in phase out: OAW-4302, OAW-4304, OAW-4308, OAW-4324, OAW-6000-PS2, OAW-SC-1-48/128 & SC-2-256 and OAW-LC-2G/F/FP, OAW-AP60, OAW-AP61, OAW-AP65, OAW-AP70, OAW-AP85, OAW-4306, OAW-4306GW, OAW-4504, OAW-AP12x series, OAW-RAP2WG and OAW-RAP5WN.
Please refer to WLAN Data support site for associated support life cycle and end of support date.

An equivalent for WLAN products can be found in the table:

WLAN EOS products	Suggested alternate products
Controllers	
OAW-4302, OAW-4304	OAW-4306G
OAW-4308, OAW-4306, OAW-4306GW	OAW-4306G
OAW-4324	OAW-4604
OAW-4504	OAW-4504XM
OAW-6000-PS2	OAW-6000-PS4
OAW-LC-2G/GF/GFP	Not required with S3
OAW-SC-1-48/128 & SC-2-256	OAW-S3-0-2X10G
Access Points	
OAW-AP60/61/65/70	OAW-AP92/93, OAW-AP104/105, OAW-AP134/135
OAW-AP120/121	OAW-AP92/93, OAW-AP104/105
OAW-AP124/125	OAW-AP134/135
OAW-AP85	OAW-AP175
OAW-RAP2WG	OAW-RAP3WN (not supported for voice)
OAW-RAP5	OAW-RAP3WN (not supported for voice)
OAW-RAP5WN	OAW-RAP109, OAW-RAP155 (not supported for voice)

Supported AOS releases (verify the exact voice version)	End of SW support*
>= AOS 5.0.x	31-May-16
>= AOS 6.1.x	1-May-14
>= AOS 6.2.x	31-May-15
>= InstantOS 6.2.1.0-3.3	22-Oct-13

Note

*Refer to WLAN Data offer for the product life cycle and HW end of support

4.3 Released versions of the OmniAccess Wireless LAN infrastructure

4.3.1 6.2.1.0-3.3.0 version for iAP

This SW version of the iAP solution is the first released for VoWLAN use in the Voice over WLAN R5.4 Solution. This InstantOS version and the following Instant AP models have been validated using OT81x8 solution:

- iAP92/93, iAP104/105, iAP134/135 & iAP175

Warning

OT81x8 solution on **Mesh Instant AP** has not been validated and as a result is **not supported today (in project).**

4.3.2 6.2.1.1 version

This AOS 6.2.1.1 SW is a maintenance version of OAW for the Voice over WLAN R5.4 Solution and has been tested with the OmniTouch™ 8118 & 8128 WLAN handsets.

This OAS 6.2.1.1 version adds some enhancements:

- Platform enhancements (ARM scanning, WMM-DSCP and WMM-AC mapping, ETSI DFS new standard support, L2/L3 VLAN scalability)
- Embedded spectral analysis enhancements

- Policy Enforcement Firewall (PEF) visibility on the dashboard GUI: PEF summary of all the sessions in the controller aggregated by users, devices, destinations, applications, WLANs and roles.
- RAP serviceability enhancements
- Controller capacity alerts

This release includes the following additional AP hardware for the VoWLAN topologies.

- Outdoor OAW-AP175
- OAW-AP104

4.3.3 6.1.3.6 version

This SW of the OAW infrastructure is released with the Voice over WLAN R5.4 Solution. It has been tested with the OmniTouch™ 8118 & 8128 WLAN handsets.

4.3.4 6.1.3.2 version

This SW of the OAW infrastructure is released with the Voice over WLAN R5.3 Solution. It has been tested with the OmniTouch™ 8118 & 8128 WLAN handsets. This version adds:

- Performance, client, AP, WLAN and security dashboard GUI
- Spectrum analysis dashboard GUI
- Support of IPv6 interfaces
- NOE CAC issue fix: remaining issues related to NOE ALG and CAC are fixed in OAS 6.1
- VoWLAN split-tunnelling for uplink on RAP-105/125
- Includes the new default SSL/TLS certificate "securelogin.arubanetworks.com" that replaces the expiring certificate included in previous releases.

Warning

AOS 6.x does not support "legacy" controllers.

This SW version supports the following new equipments for voice:

- OAW-AP92
- OAW-AP93
- OAW-AP134
- OAW-AP135

4.3.5 5.0.4.2 version

This SW version of the OAW infrastructure is a maintenance release. It has been tested with the Alcatel-Lucent IP Touch 310 & 610 and OmniTouch 8118 & 8128 WLAN handsets.

4.3.6 5.0.3.2 version

This SW version of the OAW infrastructure is a maintenance release. It has been tested with the Alcatel-Lucent IP Touch 310 & 610 and OmniTouch 8118 & 8128 WLAN handsets.

The software image contains a new default SSL/TLS certificate "securelogin.arubanetworks.com" that replaces the expiring certificate (expire on June 29, 2011).

4.3.7 5.0.3.0 version

This SW version of the OAW infrastructure is released with the Voice over WLAN R5.0 Solution. It has been tested with the IP Touch 310 & 610 and OmniTouch 81x8 WLAN handsets. This version adds Remote Networking enhancements (RAP Uplink Bandwidth Reservation, RAP Local Client Access, Remote Mesh Portal) and a new licensing model: MAP, VPN were merged into base AOS, RAP was merged into AP license and PEF (user basis) was converted to PEFNG (AP basis).

It also includes the following correction related to voice:

- Controller will lost the NOE voice clients after a while: Voice clients disappear from the voice-client table but stay in the user-table
- WLAN handset cannot connect to network after CAC overflows

This SW version supports the following new equipments:

- OAW RAP 2WG
- OAW RAP 5WN

4.4 Known Restrictions

This section gives the restrictions and limitations reported during tests and taken into account:

4.4.1 General restrictions

- If using "g only mode", there shall be no 802.11b clients on the infrastructure. All 802.11b data rates (1, 2, 5.5 and 11Mbps) must be shut down.
- DAS (distributed antenna system) is not supported for voice
- IGMP multicast requires the use of a multicast aware router and the proxy IGMP management on the OAW
- ARM (Automatic Radio Management) is not recommended. This should be disabled and a manual channel planning must be done.
- 802.11a:
  - Use only the non-DFS (Dynamic Frequency Selection (radar detection)) channels (36-48 and 149-161, depending on the regulatory domains). 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 Alcatel-Lucent recommends avoiding the use of DFS channels in VoWIFI deployments.
  - Enabling more than 8 channels will degrade roaming performance. Alcatel-Lucent strongly recommends against going above this limit.
  - 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), 40 MHz is a more viable option because of the availability of additional non-DFS channels. The handset can co-exist with 40 MHz stations in the same ESS.
  - The channel 165 is not implemented on handset, do not use it.
- OAW embedded DHCP server does not provide all the necessary settings required for WLAN handsets. A dedicated DHCP server should be used instead. In case of use WLAN handsets in DHCP mode, ensure that the OAW DHCP server does not provide IP addresses in the handset's VLAN. If the OAW DHCP in the same IP range of the handsets is to be used, the handsets must be put in IP static mode.
- Max authorized WLAN handsets on the same AP=9, in com at the same time=7

- Not possible to mix security types within a specific SSID
- Not possible to mix QoS methods
- VOIP TSPEC Enforcement parameter in QoS profile must be disabled (or set to 100 (to avoid "Service unavailable" message and reboot)
- AOS 5.0 CAC issues:
  - CAC value is not updated immediately after the call release (30s delay for the call status update)
  - If the call count based CAC is set to n, only n-1 calls will be allowed on that AP. For call count based CAC, set the call-capacity to (n + 1) to ensure that n calls are allowed. For bandwidth based CAC, set the bandwidth capacity to that required by (n+1) calls to ensure that n calls are allowed.
- AOS CAC recommendations:
  - Limits: 12 calls can be done correctly (without data): belong this limit, there may have "no network", impact on other calls, dropped calls.
  - The recommended limit is 7 to ensure that data will not be impacted by voice priority.
  - Possible impact on data between 7 and 12 calls.
- From AOS 6.0.x , if "Control Plane Security" is enabled to send certificates to APs, each AP's information of campus APs and RAP should be manually added to the campus AP whitelist or RAP whitelist. Otherwise, AP cannot connect with the controller.
- From AOS 6.0.x, when making inter-nodes or external call to an analog trunk, the audio can be blocked by OAW controller. AOS-5.x doesn't have this issue. **Workaround**: Modify the user-role for the handsets to allow the UDP-PORT used for communication. Add the following rules in the user role:

  ip access-list session rtp-acl

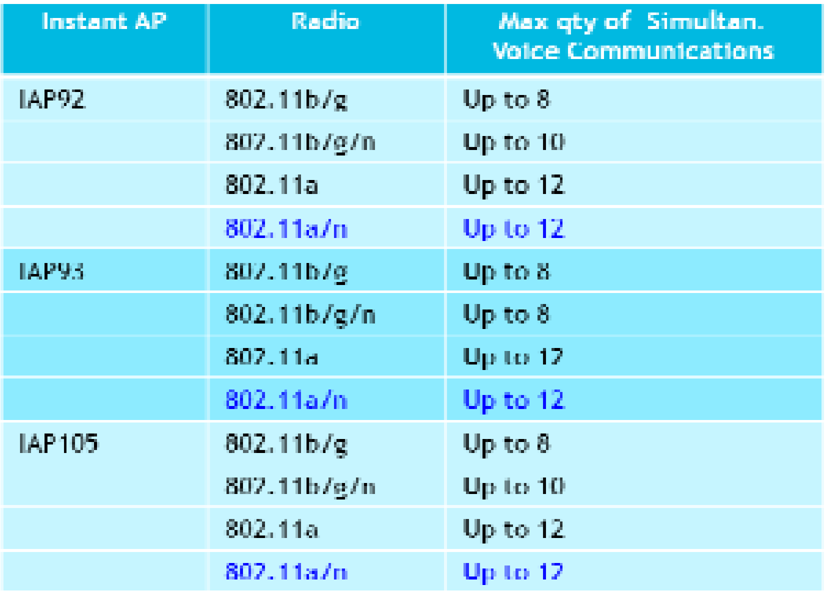
  any any udp 32000 to 32200 permit queue high
- Upgrade OAW to version 6.2 requires intermediate steps depending on the current AOS version. Refer to AOS-W related documentation to see the procedure and restrictions (AOS-Release Note, Upgrade guide).
- **802.11k is not supported by OT81x8 side, do not activate it on the controller**

4.4.2 Restrictions on Remote AP

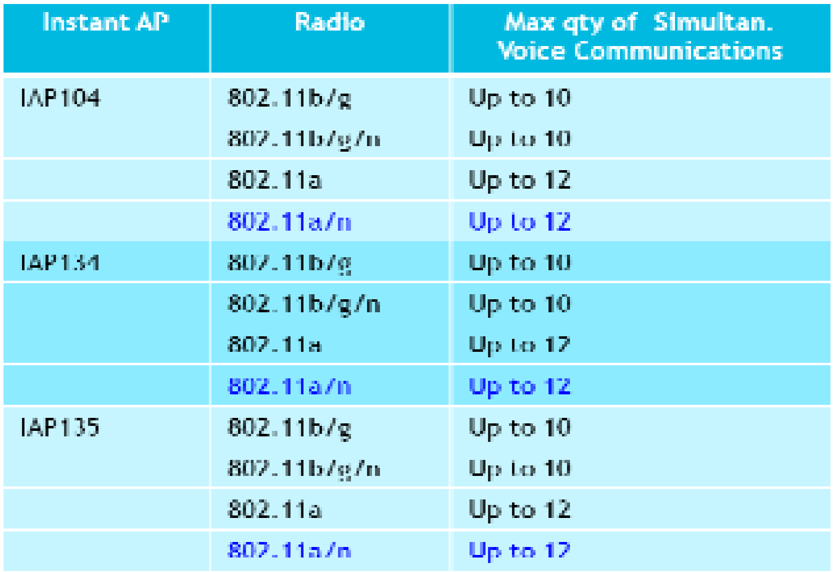
- Split-tunnel mode is recommended for RAP configuration
- TSPEC is not supported in "Split Tunnel" mode
- WPA2-PSK and 802.1x are recommended to be used: issue with WPA-PSK
- If tunnel mode has to be used for RAP, limit the data traffic by setting the bandwidth contract (ex: if the total uplink bandwidth is 1000kbps, the data traffic limitation should be defined as 1000 – 300 = 700kbps (two calls in G711 codec need around 300kbps (one 2-way call reserve 150k)): configuration done in the user-role bandwidth settings
- "Bridge mode" is not supported in Remote AP environments
- CAC during roaming between 2 Remote APs does not work properly (CAC is not required in RAP network environments): CAC is suggested to be disabled
- The voice quality is impacted at RAP side when there is heavy TCP data traffic from HQ to Remote site: limit the bandwidth for data traffic by configuring the bandwidth contract.
- When AP125 acts as Remote AP, Enet1 cannot be used if PoE is running on Enet0
- Handover and OmniTouch 8118/8128 Handsets have not been tested.
- FTP service must be included into the ap-role access list to enable the 6.2 AP remote firmware upgrade.

4.4.3 Restrictions on Instant AP

- **Opportunistic Key Caching (OKC) is not supported by Instant AP. Enterprise/.1X authentication such as PEAP-MSCHAPv2 is therefore not recommended for voice deployments. Recommended security method is WPA/WPA2-PSK**
- **Mesh is not supported**
- **iAP group limits:**
  - **iAP92/93: up to 16 iAPs & 256 users per iAP group**
  - **iAP104/105, iAP134/135 & iAP175: up to 64 iAPs & 1024 users per iAP group**
  - **Limited to 16 iAPs when mixing iAP92/93 with other iAP models**
- **Voice Communication Capacity per Instant AP: (maximum number of simultaneous Voice communications, source: validation tests, <u>without data traffic</u>): values given for information only and not contractual, depending on the real deployment on site:**



Instant AP	Radio	Max qty of Simultan. Voice Communications
IAP92	802.11b/g	Up to 8
	802.11b/g/n	Up to 10
	802.11a	Up to 12
	802.11a/n	Up to 12
IAP93	802.11b/g	Up to 8
	802.11b/g/n	Up to 8
	802.11a	Up to 12
	802.11a/n	Up to 12
IAP105	802.11b/g	Up to 8
	802.11b/g/n	Up to 10
	802.11a	Up to 12
	802.11a/n	Up to 12



Instant AP	Radio	Max qty of Simultan. Voice Communications
IAP104	802.11b/g	Up to 10
	802.11b/g/n	Up to 10
	802.11a	Up to 12
	802.11a/n	Up to 12
IAP134	802.11b/g	Up to 10
	802.11b/g/n	Up to 10
	802.11a	Up to 12
	802.11a/n	Up to 12
IAP135	802.11b/g	Up to 10
	802.11b/g/n	Up to 10
	802.11a	Up to 12
	802.11a/n	Up to 12

  - **The best result is for 802.11a/n with up to 12 simultaneous voice calls per iAP**
  - **802.11a/n operation is recommended for VoWLAN to avoid interferences existing in the 2.4 GHz radio band (Bluetooth, microwave oven, intruder detection systems, etc.), nevertheless 802.11b/g/n can also be used.**

4.4.4 Limitations with wireless Mesh

- No more than 2 hops for mesh
- No more than 6 APs per mesh portal
- WMM Qos must be enabled on mesh links and on mesh APs
- A good signal strength is necessary to make mesh (at least -50 to -60dBm)
- Line of sight for the mesh points preferred

4.4.5 Limitation with Remote Mesh

- Only RAP5WN can work as remote mesh portal
- Client support on mesh radio feature is necessary as RAP5WN is a single radio AP
- For legacy AP to be used as remote mesh point, it should be configured as Remote AP

4.4.6 Restrictions of controllers

- OAW-4306GW controller:
  - The internal AP can operate as an AP, Mesh Portal or an Air Monitor, but NOT as a remote AP, a mesh point or an RF Protect sensor
  - To reboot the embedded AP, the 4306GW controller has to be rebooted as well
  - The internal AP of the controller is deactivated by AOS 6.2
  - Upgraded with AOS 6.2, the 4306GW controller appears as a 4306G-1 and 4306GW-8 as a OAW-4306-9 controller for the AOS-W
- OAW-4504 controller:
  - 4504 controller with its default memory is not supported by AOS 6.2
  - AOS 6.2 supports the controller OAW-4504XM and all OAW-4504 controllers installed with the OAW-4504-MEM-UG memory kit.

4.4.7 Restriction of AP

- OAW-AP105: AP owns a single Ethernet Port (so can be irrelevant with some RAP topologies)

4.4.8 Restriction on 802.1x

- If the forwarding mode on AP12x series is changed from tunnel to split-tunnel, the switch must be rebooted for 802.1x clients to complete the EAP exchange
- WPA2-Enterprise 802.1X authentication type requires the use of a RADIUS authentication server to validate user specific credentials.
- Microsoft IAS RADIUS does not support EAP-FAST authentication.

- Cisco ACS RADIUS server is not supported.
- WPA2-Enterprise 802.1X authentications use requires an onsite intervention. The certificates installations on OmniTouch are done with the winPDM tool and a cradle and must be done on each phone.

⚠ **Warning** The use of 512 or 1024 bit certificates is recommended for optimal performance.

4.4.9 Restrictions of 802.11n

- AP reboot issue during high data traffic
- "UDP Lost Re-init timeout Phone Restarting" issue
  - **Workaround**: enable Convert Broadcast ARP requests to unicast in Virtual AP Profile
- AP125 in HT mode only supports Open and WPA2-PSK security mode
  - **Workaround**: to support WEP / WPA-PSK TKIP in HT mode on AP12x, enable allow-weak-encryption in ht-ssid-profile
- Do not connect Hub and APs on AP125 Enet1
- 2x20 MHz mode is not recommended on the 2.4 GHz frequency band (802.11 b/g) due to a limited number of non overlapping channels (3 only).
- 2x40 MHz mode is not recommended on the 5 GHz frequency band (802.11 a/n) when the 4 non-DFS channels are used only.

4.4.10 Restrictions in multi-switch mode

- Mesh not supported
- **The use of default PSK key for IPSec tunneling will not work after an upgrade of OAW to 6.x release: change the default PSK key value before the 6.x upgrade.**
- ALG only works if the VLAN for the voice is not the same on each switches (L3 mobility is enabled), if the VLAN for the voice is the same on all the switches => DO NOT USE THE ALG NOE
- Master switch VRRP redundancy: when Master controller is down, the Backup controller switches to Master. If the WLAN handset user is in conversation and the Master controller goes down at that time, the call will not be dropped and:
  - If rtp-acl has been used in user-role
    - The audio will recover as soon as the Backup controller switches to Master
  - If rtp-acl has not been used in user-role
    - The audio can NOT recover after the Backup controller switches to Master

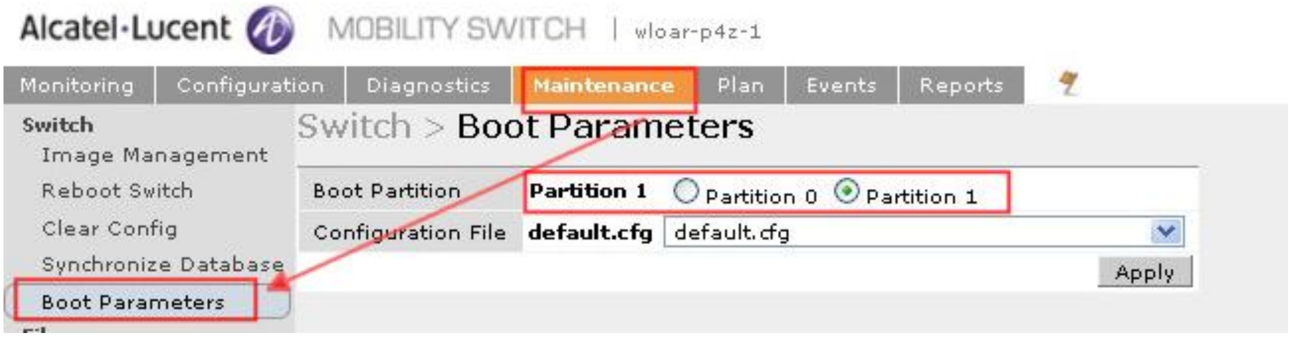
4.5 Upgrade Of The OmniAccess Wireless LAN Controller

The OmniAccess software version is available on the Business Partner Portal under:
Support > Technical Support IP Networking > Technical Resource Center > Downloads > OA 43/60xx/OA4x04 WLAN.

To update the controller, refer to the AOS-W related documentation to see the procedure and the restrictions (AOS-Release Note, Upgrade guide).

The SW upgrade can be done with TFTP or FTP servers. The AP will automatically be updated from the controller.

First check the OAW boot parameters:



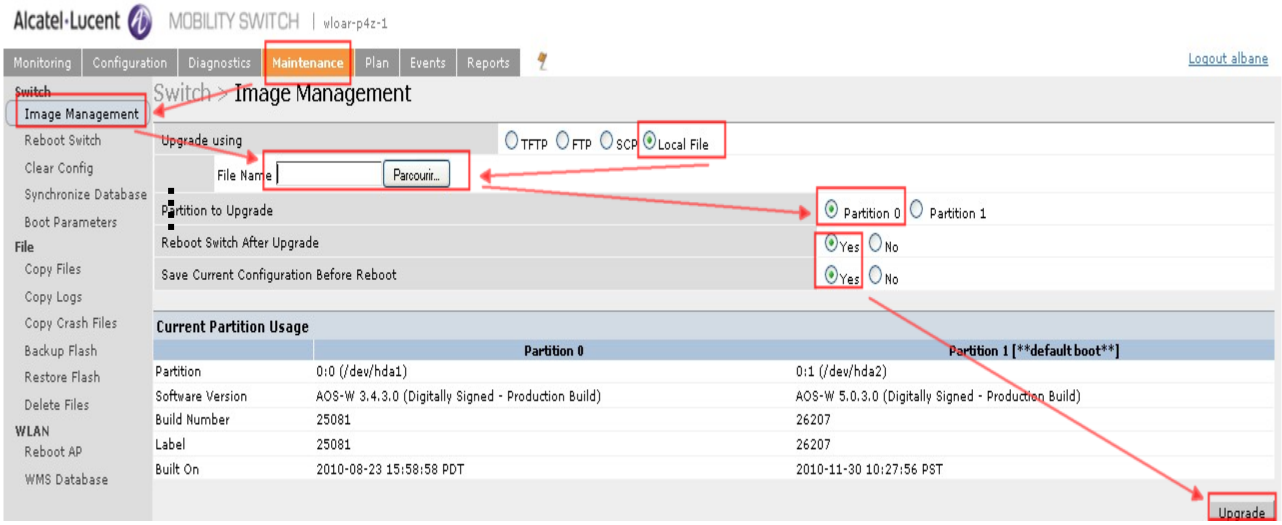
Switch > Boot Parameters

Boot Partition	Partition 1	○ Partition 0 ● Partition 1
Configuration File	default.cfg	default.cfg

Note

Advice: When loading a new firmware version on OAW, upload the new firmware version on the partition not used as default boot (if some problem occurs with the new firmware, this will allow to switch on the partition used previously).

Upload new firmware with TFTP server, FTP server (add login and password for FTP connection) or load a local file:



Switch > Image Management

Upgrade using ○ TFTP ○ FTP ○ SCP ● Local File
File Name
Partition to Upgrade ● Partition 0 ○ Partition 1
Reboot Switch After Upgrade ● Yes ○ No
Save Current Configuration Before Reboot ● Yes ○ No

Current Partition Usage

	Partition 0	Partition 1 [**default boot**]
Partition	0:0 (/dev/hda1)	0:1 (/dev/hda2)
Software Version	AOS-W 3.4.3.0 (Digitally Signed - Production Build)	AOS-W 5.0.3.0 (Digitally Signed - Production Build)
Build Number	25081	26207
Label	25081	26207
Built On	2010-08-23 15:58:58 PDT	2010-11-30 10:27:56 PST

After reboot, check if the switch is running on the good partition, change boot parameter if necessary (OAW boot parameter).

Follow us on Facebook and Twitter

Stay tuned on our Facebook and Twitter channels where we inform you about:

- New software releases
- New technical communications
- AAPP InterWorking Reports
- Newsletter
- Etc.

twitter.com/ALUEnterpriseCare

facebook.com/ALECustomerCare

Submitting a Service Request

Please connect to our eService Request application.

Before submitting a Service Request, make sure that:

- In case a Third-Party application is involved, that application has been certified via the AAPP
- You have read through the Release Notes which lists new features available, system requirements, restrictions etc. available in the Technical Documentation Library
- You have read through the Troubleshooting Guides and Technical Bulletins relative to this subject available in the Technical Documentation Library
- You have read through the self-service information on commonly asked support questions, known issues and workarounds available in the Technical Knowledge Center

- END OF DOCUMENT -