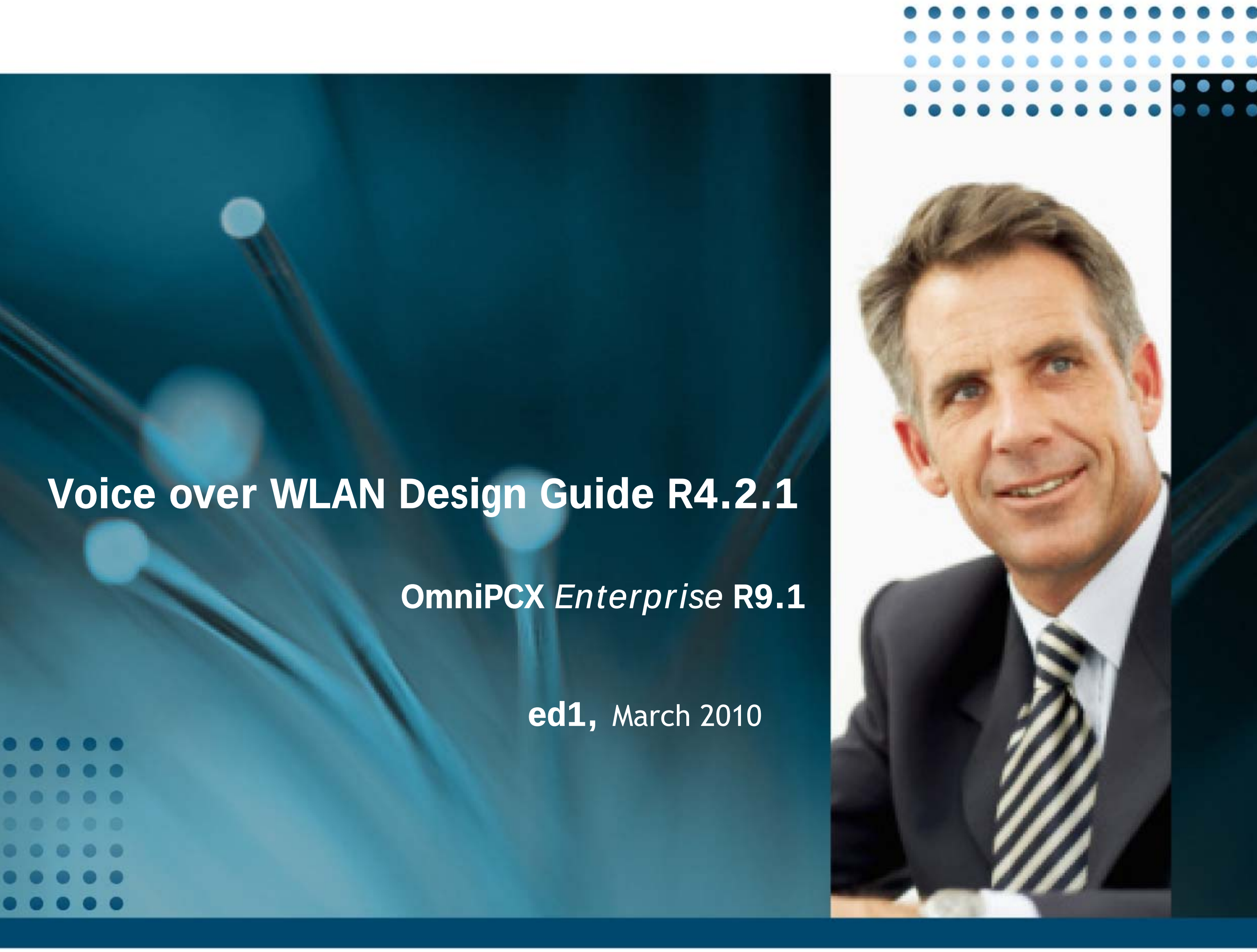


Voice over WLAN Design Guide R4.2.1

OmniPCX *Enterprise* R9.1

ed1, March 2010

Central PreSales

Alcatel-Lucent Corporate Communication Solutions

Central PreSales /DF
Voice over WLAN Design Guide Rel 4.2.1 ed1

1. Introduction & Objectives

It is the intent of this guide to aid Sales Engineers in designing and selling telecommunications solutions Incorporating Alcatel-Lucent’s Mobile IP Touch (MIPT) Voice over Wireless LAN (VoWLAN) solution

This document has been created specifically in the context of an architectural and technical Pre-Sales Design Guide approach. It is clearly understood that a client’s choice of solution components and design options will take into account many factors that will not be explored here (such as financial considerations, deployment constraints, and business process limitations).

Alcatel-Lucent’s MIPT VoWLAN product offering is a multi-stage solution aimed at meeting customer demand for converged voice and data wireless environments based on 802.11 technologies. The MIPT suite is the result of leveraging existing OmniPCX Enterprise features with OEM products available in the Alcatel-Lucent portfolio from Polycom and others.

Technically speaking, the VoWLAN solution can be built on several centralized WLAN topology schemes but must always adhere to the Voice over WLAN operational design restrictions *(For more information on design restrictions, see: section Voice over WLAN Specifications of this document and the ALCATEL-LUCENT OmniPCX Enterprise R9.0 Standard Offer document).*

In this document all descriptions related to Voice over WLAN are linked to OmniPCX Enterprise R9.1

For deployment refer to the Voice Deployment guide, but keeping in mind this document is manufacturer agnostic and thus might be not fully relevant in specific cases when installing ALU VoWLAN solution. Following is the related extract of the Voice deployment guide:

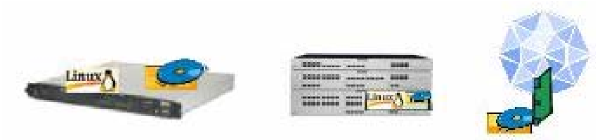
“Scope (Deployment guide extract)

> *This document is handset vendor agnostic and makes general recommendations required to enable voice on the infrastructure.*

1.1. Operational Components

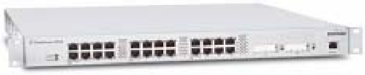
The Alcatel-Lucent MIPT VoWLAN solution offer is comprised of many subcomponents. These components can be easily grouped into their categories defined by their functions and responsibilities.

1.1.1. OmniPCX Enterprise Applications Specific Elements

At the core of Alcatel-Lucent's MIPT VoWLAN offer lays the Alcatel-Lucent OmniPCX Enterprise platform (R9.0) Key to enabling the capabilities of Alcatel-Lucent's VoWLAN solution is the NOE features.	 OmniPCX Enterprise

1.1.2. WLAN Infrastructure (Provided by Alcatel-Lucent)

OmniAccess 4302 Equipped with one Fast Ethernet port (10/100) and one Gigabit Ethernet port (10/100/1000). Used to support: **up to 8 APs (from AOS 3.4)** in overlay mode only. (was up to 6 APs with AOS 3.3 and earlier) There is no POE capability, POE must be provided by a network Switch. Embedded Stateful Inspection firewall options allow for robust security solutions.	 **OmniAccess 4302**
OmniAccess 4304 Used to support: **up to 4 AP** **up to 256 users** Equipped with eight 10/100 Ethernet ports (802.3af capable). Two different models providing either one 1000base-T Gigabit uplink (Copper) or one 1000base-SX Gigabit uplink (Fiber). Embedded Stateful Inspection firewall options allow for robust security solutions.	 **OmniAccess 4304**

OmniAccess 4308 Used to support: **up to 16 AP** **up to 256 users** Equipped with eight 10/100 Ethernet ports (802.3af capable). Two different models providing either one 1000base-T Gigabit uplink (Copper) or one 1000base-SX Gigabit uplink (Fiber). Embedded Stateful Inspection firewall options allow for robust security installations.	 OmniAccess 4308
OmniAccess 4324 Used to support: **up to 48 AP** **up to 768 users** Equipped with twenty-four 10/100 Ethernet ports and two GBIC uplink modules for flexible LAN applications. Embedded Stateful Inspection firewall options allow for robust security solutions.	 OmniAccess 4324
OmniAccess 6000 (Sup Card 1 & 2) Four slot modular chassis used to support: **Up to 512 AP** **Up to 8192 users** **Up to 2 Supervisor Cards** - Supervisor Card 1: **up to 48 or 128 AP** - Supervisor Card 2: **up to 256 AP** **up to 4096 users** Equipped with up to seventy-two 10/100 Ethernet ports and six GBIC uplink modules for flexible LAN applications. Embedded Stateful Inspection firewall options allow for robust security solutions.	 OmniAccess 6000 Sup Card 1 & 2

OmniAccess 6000 (Sup Card 3) Four slot modular chassis used to support: **Up to 2048 AP (LAN Connected)** **Up to 8192 Remote AP/Mesh AP** **Up to 4 Supervisor Cards** **Up to 32768 users** Supervisor Card 3: **up to 512 AP LAN Connected** **up to 2048 Remote AP/Mesh AP** **- 10x 1000Base-X (SFP)** **- 2x 10GBase-X (XFP)** Imbedded Stateful Inspection firewall options allow for robust security solutions.	 **OmniAccess 6000 Sup Card 3**
Family of 3 OmniAccess 4504 4604 4704 Equipped with 4x 10/100/1000BASE-T (RJ-45) or 1000BASE-X (SFP) dual personality ports OmniAccess 4504: **Up to 32 AP (LAN Connected)** **Up to 128 Remote AP/Mesh AP** **Up to 512 users** OmniAccess 4604: **Up to 64 AP (LAN Connected)** **Up to 256 Remote AP/Mesh AP** **Up to 1024 users** OmniAccess 4704: **Up to 128 AP (LAN Connected)** **Up to 512 Remote AP/Mesh AP** **Up to 2048 users** Embedded Stateful Inspection firewall options allow for robust security solutions.	 **OmniAccess 4504 4604 4704**

OmniAccess AP60 and AP61 Single radio (802.11a or 802.11b/g) Wi-Fi Access Points for use with OmniAccess WLAN controllers. - - AP60 model requires external special purpose antenna (no internal antenna) - AP61 offers only internal antennas	 **OmniAccess AP60 & AP61**
OmniAccess AP65 **Dual-radio** Flexible multifunction Access Point provides simultaneous access to both 802.11a and 802.11b/g radios. Dual, integral, tri-band, high-gain, omni-directional antennas with 180 degrees rotational movement. Non-detachable.	 **OmniAccess AP65**
OmniAccess AP70 **Dual-radio** Flexible multifunction Access Point provides simultaneous access to both 802.11a and 802.11b/g radios. Supports built-in and external special purpose antenna.	 **OmniAccess AP70**
OmniAccess AP85 **Dual-radio outdoor** access point. Supports 802.11a and 802.11b/g (200mW). Supports four (4) external antenna connectors (2 for 2.4GHz band and 2 for 5Ghz band. 3 models: AP85TX, AP85FX and AP85LFX AP85TX : Supports one 10/100 Base-T (RJ-45) Ethernet interface supporting 802.3af Power over Ethernet and Serial over Ethernet. AP85FX : Supports one (1) 100 Base-FX (Multi-mode, dual fiber Ethernet - up to 2 Km) Ethernet interface. AP85LX : Supports one (1) 100 Base-LX (Single-mode, dual fiber Ethernet - up to 10 Km) Ethernet interface.	 **OmniAccess AP85**

OmniAccess AP120 and AP121 **Single radio** IEEE 802.11n (draft 2.0) wireless access point with 2 x 10/100/1000Base-T (RJ-45) Ethernet interface (Supports Power over Ethernet) Optional license for operation in **802.11a or b/g** AP120: support for selectable 802.11'B/G/N' or 802.11'A/N' operation, 3x3 MIMO dual-band RP-SMA detachable antenna interfaces. (no internal antenna) AP121: embedded 3x3 MIMO dual-band antenna	 **OmniAccess AP120 & AP121**
OmniAccess AP124 and AP125 **Dual radio IEEE 802.11n (draft 2.0)** wireless access point with 2 x 10/100/1000Base-T (RJ-45) Ethernet interface (Supports Power over Ethernet) Optional license for operation in **802.11a and b/g** AP124: support for selectable 802.11'B/G/N' or 802.11'A/N' operation, 3x3 MIMO dual-band RP-SMA detachable antenna interfaces. AP125: embedded 3x3 MIMO dual-band antenna	 **OmniAccess AP124 & AP125**

1.1.3. Server Elements (DHCP, TFTP, Management)

1.1.3.1. DHCP Server

Customers have two IP address allocation schemes to choose from for MIPT handsets, static mode and dynamic mode. Static mode operation is very simple and requires no expanded explanation. Terminals are simply programmed manually with IP addresses, subnet mask, default gateway, and TFTP server information. Optionally, MIPT Terminals can be configured in a dynamic mode via standard DHCP server options.

Dynamic mode is recommended due to ease of use and speed of reconfiguration. An external or an internal DHCP server (OmniPCX Enterprise) can be used for all MIPT VoWLAN solutions. Alcatel-Lucent does not currently offer the DHCP Server hardware platform and recommends the customers or business partners source this equipment from their usual PC Server supplier.

Alcatel-Lucent has validated the following DHCP Server software platforms for use with MIPT VoWLAN solutions.

Validated DHCP Server software platforms.	
Windows 2000 (Server)	DHCP turbo by Weird Solutions
Linux DHCP Server	

1.1.3.2. TFTP Server

A TFTP Server is mandatory for all MIPT VoWLAN solutions. The TFTP Server is responsible for supplying Binary to the MIPT handsets.

TFTP Server functions can be hosted from the OmniPCX Enterprise Communication Server or external.

There are no unique TFTP Server requirements beyond standard TFTP protocol specifications to support MIPT terminals. It is possible to combine TFTP Server and DHCP Server functions on a single external platform.

Alcatel-Lucent has validated the following TFTP Server platforms for use with MIPT solutions.

Validated TFTP Server software platforms.	
3Com TFTP Server (3CDaemon) V2.0r10	Cisco TFTP Server
TFTP turbo by Weird Solutions	Solar Winds TFTP
Linux TFTP Server	

1.1.3.3. RF Director Management

The initial goal of RF Spectrum Management is to configure and calibrate radio settings for the wireless network. After the radio network is operational, the goal of RF Spectrum Management changes to that of tuning and adjusting radio parameters in order to maintain a high degree of performance. With Alcatel-Lucent, RF Spectrum Management is largely automatic, requiring little configuration or intervention from the administrator. Key components of Alcatel-Lucent's RF Director solution are:

- **Calibration:** Used continuously throughout the life of a wireless network; Calibration functions allow network administrators to optimize power and sensitivity settings of the network on an antenna by antenna basis.
- **Optimization:**
  - <u>Auto Radio Resource Allocation:</u> allows individual access points to monitor for RF changes and, in conjunction with Calibration information, make appropriate channel assignment changes.
  - <u>Self Healing:</u> In the event that an AP fails, surrounding APs can automatically increase their transmit power level to fill in any gaps.
  - <u>Load Balancing:</u> ensures optimum performance by automatically spreading client association in an equitable manner to avoid the premature saturation of a single AP.
- **RF Monitoring:**
  - <u>Coverage Hole Detection:</u> Continuous monitoring of client data access and error rates provides for the identification of coverage holes or areas of diminished service.
  - <u>Interference Detection:</u> notifies network administrators when localized interference becomes sufficient to cause performance degradation.
  - <u>Event Threshold Configuration:</u> provides the ability to configure event thresholds to notify the administrator when certain RF parameters are exceeded.
- **Wireless Intrusion Detection:** can identify and defeat a wide assortment of DoS attacks aimed at Wi-Fi networks.

1.1.4. Mobile IP Touch Terminals

1.1.4.1. General Description

Alcatel-Lucent makes two new models available, one each for office (MIPT 310) and industrial use (MIPT 610). The performance of these two handsets is very similar but their designs and options are focused for use in specific environments. Both of these terminals are products of an OEM partnership between Alcatel-Lucent and Polycom (former SpectraLink)

Main physical changes on MIPT310/610 terminals:

- 802.11a Radio using 5GHz band at 54Mbps (in addition to 802.11 b/g),
- Three models of battery pack,
- Hand-free speakerphone,
- 4-way Navigator and OK physical keys,
- Taller screen and Fonts making the information more readable.

MIPT310

MIPT610

1.1.4.2. Technical characteristics

1.1.4.2.1. General Specification

Radio characteristics	
Radio frequency	802.11b et 802.11g : 2,4GHz-2,4835Ghz 802.11a : 5,15GHz – 5,35Ghz & 5,47-5,725 in Europe 5,15GHz – 5,35Ghz & 5,725-5,825 in US
Transmission type	Direct Sequence Spread Spectrum (DSSS) for 802.11b OFDM for 802.11g/802.11.a
Transmit data rate **(Auto rate selection)**	11, 5.5, 2, 1 Mb/s for 802.11b 54,48,36,24,18,12,9,6,11,5.5,2,1 Mb/s for 802.11g 54,48,36,24,18,12,9,6 Mb/s for 802.11.a
Transmit power	100mW peak max, less than 1mW on average, depending on the radio frequency
Protocol compliance	
VoIP Protocol	New Office Environment (NOE)
Wireless security	WEP, WPA-PSK, WPA2-PSK
QoS Protocol	(WMM+U-APSD+Tspec).
Audio characteristics	
VoIP Protocol	New Office Environment (NOE)
Voice encoding	G711(with A-law and µ-law), G729 AB (with VAD/CNG in compliance G.729 Annex B)
PLC (proprietary packet loss concealment)	Yes, proprietary
Narrow Band capability	Yes
Durability	
MIL STD 810F (IV 516.5) certified	Certified
IP 53 spray and wipe	Certified

1.1.4.2.2. Set features

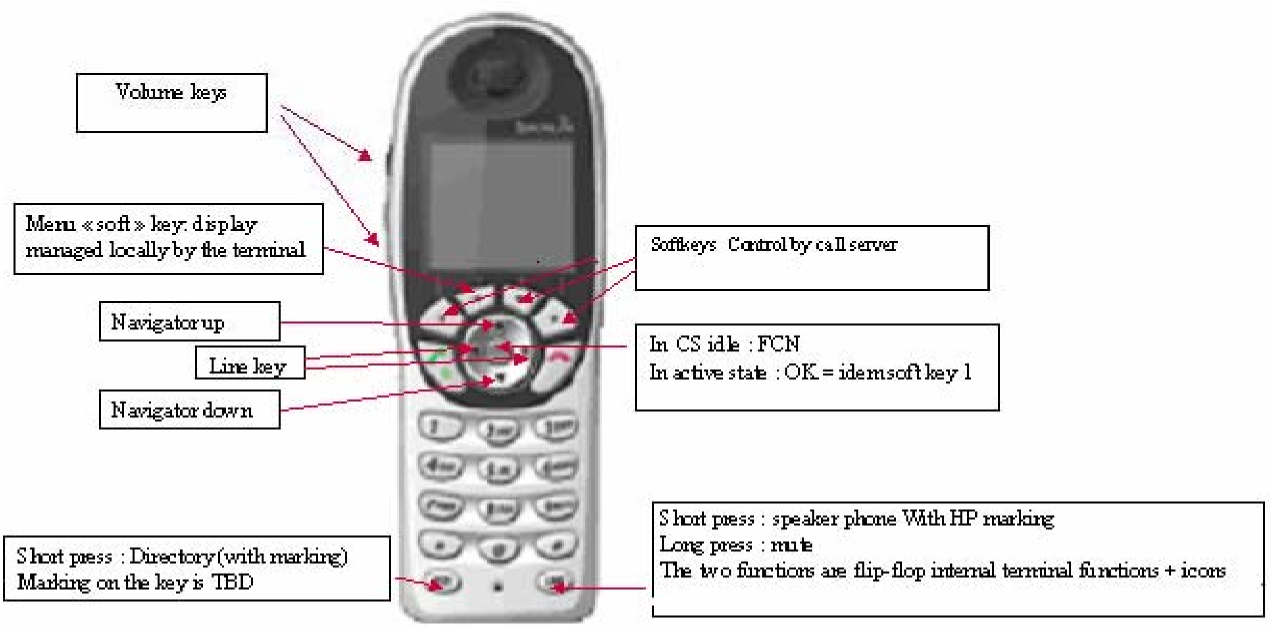
	MIPT310	MIPT610
Physical characteristics		
Dimensions	22x50x137 mm	22x50x145 mm
Weight with standard battery	4.2ounces (110 gr)	6.0 ounces (120 gr)
Vibrator	11000rpm nickel vibrator	
Headset Plug	Micro headset jack	
Hands-free speakerphone	Yes	
Battery types **(Talk time / Standby time / Charge time)**	Standard lithium Ion battery (4H / 80H / 2H) Extended lithium Ion battery (6H / 120H / 3H) Ultra-Extended lithium Ion battery (8H / 160H / 4H)	
Display characteristics		
Graphical display	1 Icon line, 4 text lines (18 characters per line) and 1softkey line	
Size	128x96 pixels (33x25mm)	
Color	Monochrome (Black and White)	
Backlight	Yes (green)	
Icons & status indicators	Signal strength ▂ ▃ ▄ ▅ ▆ Mute 🔒 Battery gauge ▭ ▭ ▭ ▭ Vibrator icon Download Speakerphone 🔊	
Status indicators managed by the PBX	Terminal lock ; Appointment ✓ Forward ; Message ✉	
Call indicators	Only displayed in the first text line Conversation ; ringing ; hold	

	MIPT310	MIPT610
Keypad		
Navigator	4 way navigation key , in WLAN R 4.1, 2 directions only	
Alphabetic keyboard emulation	Yes	
Dialing keyboard	Yes	
Dial-by-name key	Short press on a new marking key	
Validation key (OK)	True navigator Ok key in addition of Ok SWK key	
End key	Yes	
Backspace key	Yes	
Menu key	No, replaced by the 2nd soft key from the left	
Line selection key	No, replaced by left & right navigator key	
Volume keys +/- (Ringing volume control)	Yes (Yes during ringing or idle state)	
Mute key	Mapped on new speaker phone key	
Push-To-talk (PTT)	No	YES (25 channels)
Redial key	No	
Personal directory key	No	
Programmable keys	No	
Help key	No	
Ringing		
Ring Tone, Ring Delay, Ring Cadence and Vibrate Cadence parameters can all be adjusted independently to meet individual call notification preferences	YES	
Ring Volume	YES	

1.1.4.3. MIPT Menu

1.1.4.3.1. Key navigation

The keypad is composed of **16** keys, **5** navigator keys and **3** keys on the side.


Volume keys
Menu « soft » key: display managed locally by the terminal
Navigator up
Line key
Navigator down
Short press : Directory (with marking) Marking on the key is TBD
Softkeys Control by call server
In CS idle : FCN
In active state : OK = idem soft key 1
Short press : speaker phone With HP marking
Long press : mute
The two functions are flip-flop internal terminal functions + icons

Key/Soft Key	Action
Up/Down side key	Display previous/next menu item.
Select side key	Selects the menu item or option.
OK soft key	Selects the menu item or option.
Save soft key	Saves the entry.
Bksp soft key	Backspaces to allow editing of entry.
Cncl soft key	Cancels edit and returns to previous menu level.
Up soft key	Returns to previous menu level
Exit soft key	Exits the menu (at the top level)
Release key	Exits to standby mode (from any level)

1.1.4.3.2. Local standby menu

The Local Standby menu allows the user:

- to customize the phone options (ring parameters, languages, PTT parameters, set contrast, enable/disable keypad lock, etc…),
- to have access to handset configuration information (firmware version, handset IP @, TFTP @, CPU IP @, etc…).

This menu is available in French, English, Spanish, german, dutch, Portuguese and Italian.

The Local Standby menu is only available when the handset is in standby mode (ie. extension number is displayed). While in the standby mode, the [OK] key opens the user options menu.

The Local Standby menu can be exited by different manners :

- a single push on the [release] key exits immediately the menu wherever the user is,
- successive pushes on the [OK] key winds up the menu hierarchy until exit,
- successive pushes on the [Back] soft key winds up the menu hierarchy until exit,
- after 5 seconds without user's activity (key push), the menu is automatically exited.

1.1.4.3.3. Administration menu

The Admin menu allows the setting of configuration options (static dhcp or not, tftp, ess id, wep, wpa, wpa2, QoS type, etc…).

This menu is available in French, English, Spanish, german, dutch, Portuguese and Italian.

When the handset must be powered off, the following combination gives access to the Admin menu:

- First press and hold the [release] and [hook] keys,
- then release the [release] key,
- and finally release the [hook] key.

If a password has been set, the display will require its entry before opening the Admin menu. If no password is set, the display will proceed directly into the Admin menu

The Admin menu can be exited by different methods:

– a single push on the [release] key exits immediately the menu (from any level).

– successive pushes on the [cancel] soft key winds up the menu hierarchy until exit (at the top level).

– after 20 seconds without user's activity (key push), the menu is automatically exited.

1.1.4.3.4. PBX menu

The [Menu] softkey gives access to the menu-driven functions and services proposed by the PBX. The features and services available can be viewed and activated through the displayed menu.

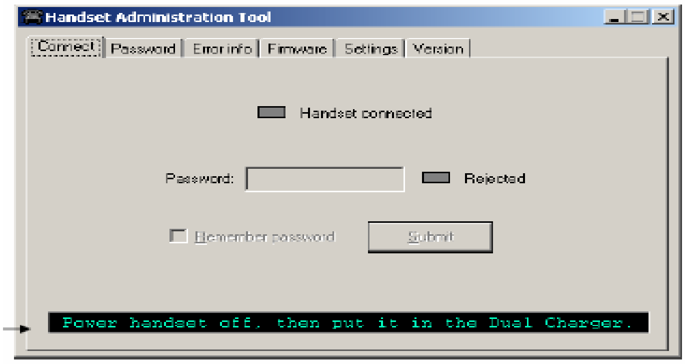
The PBX menu is available when the handset is in the standby mode (ie. extension number is displayed). The PBX displayed supported languages are : French, English , Spanish, German, Dutch, Portuguese, Italian, Cyrillic and Greek.

See section PBX features of this document concerning the description of the menu proposed by the OmniPCX Enterprise.

1.1.4.3.5. Handset Administration Tool for multipleMIPT

The Handset Administration Tool is a software utility installed on a PC with a USB port. During operation, a USB cable must be connected from the PC's USB port to the Dual Charger's USB port, named "cradle tool". The necessary components are provided in the section ALU set and option offers from this document.

The Handset Administration Tool is designed as a time-saving device for rapid administration and configuration of a number of handsets. The Configuration options include setting all options on the "Admin" and "Config" menu, recording error information to assist troubleshooting and upgrading handset software. The tool offers 6 tab labels, named "Connect", "Password", "Error info", "Firmware", "Settings", and "Version".



Power handset off, then put it in the Dual Charger.

Figure 1: Handset administration tool window

The password is a security measure to restrict access to the Admin menu settings.

The Error info tab provides a utility to assist the customer service team to troubleshoot handset errors.

The Firmware tab allows you to copy software updates to the handset's memory after they are downloaded from a website.

The Version tab displays the serial number of the handset and the current version of the Handset Administration Tool software.

The handset has two menus with configurable options – the Admin menu and the Config menu. The Admin menu contains administrative options that can be password protected. The Config menu has options that enable the end user to customize settings for user preferences. The Settings tab allows you to configure both required and optional settings in the Admin and Config menus.

1.1.4.4. PBX services

1.1.4.4.1. PBX features

MIPT set uses integrated NOE features (dial by name, notification for messaging, multi-line, multiple calls, normal/casual conference, enquiry call, transfer, call parking, automatic call back, different forwards, voice mail access, send/read text message, etc…) and as a result can be globally considered as an IP Touch set, but limited by its ergonomics (a part of boss/assistant features , no MLA, no key programming, no interphony, etc…).

For more details see Feature List and Product Limits.

1.1.4.4.2. PBX download

This process is divided into 5 steps: (step 1) terminal initialization, (step 2) IP parameters acquisition, (step 3) software updating, (step 4) configuration file retrieval, and (step 5) start file retrieval.

The MIPT software, developed by *Polycom*, is roughly divided in two parts: the core software and the application software. The core software is responsible for step1 to step3. The application software is responsible for step4 & step5.

The *"spatial redundancy"* feature is available with Voice over WLAN OXE R9.1 including the *"survivability"* feature.

IP parameters acquisition & checking:

This step can be done in static mode or dynamic mode (DHCP).

In *static mode*, IP parameters are: phone IP address, subnet mask, router IP address (if required), TFTP server IP address for download (optional), TFTP primary address (mandatory) and TFTP redundant IP address (if required).

In *dynamic mode*, IP parameters acquired using DHCP are: phone IP address, subnet mask, router IP address, TFTP server IP address for download (mandatory). This TFTP information is provided through *'next server'* field or through "option 66". If both of them are found in the DHCP OFFER, '*next server*' is used.

Software updateserver:

A software delivery is composed of 5 files with size estimation :

slnk_cfg.cfg Config File (1K byte)

pd14cno.bin Functional Code (1024K bytes)

pd14odno.bin Over the air downloader (512K bytes)

pd14udno.bin USB Downloader (192K bytes)

pi1400no.bin Phintl : fonts & labels content (256K bytes)

Only the TFTP server IP address (for download) is used to retrieve the files listed above. The terminal always starts with the "slnk_cfg.cfg" file. There are four attempts to download this file. If it doesn't succeed after four attempts, terminal continues with its initialization (step 4). If the "slnk_cfg.cfg" file does not contain the "TYPE 31" entry, dedicated to MIPT 310/610, the handset skips the step 3 and goes to the step 4.

Configuration file retrieval

The configuration file step consists in downloading the "lanpbx-mipt.cfg" file. This file is in ASCII format. It contains one or more lines and each line provides a call server address (IP_DOWNLOAD) and optionally a redundant call server address (IP_DOWNLOAD_RD).

The content of the "lanpbx-mipt.cfg" file is the same as the "lanpbx.cfg" file. If the "lanpbx.cfg" file size is less than 1KB, the "lanpbx-mipt.cfg" file can be, for example, a symbolic link to the standard "lanpbx.cfg". In the other case, the "lanpbx-mipt.cfg" file must be adapted in order to keep its size below 1Kbytes.

Start file retrieval

The start file step consists in downloading and analyzing the "startmipt-aabbccddeeff" file

(where aabbccddeeff is the terminal Mac address in hexadecimal. This step is independent from the static or dynamic mode.

When the start file is downloaded and parsed without errors, if a CONNECT message is not received after 30 seconds, the terminal must reset.

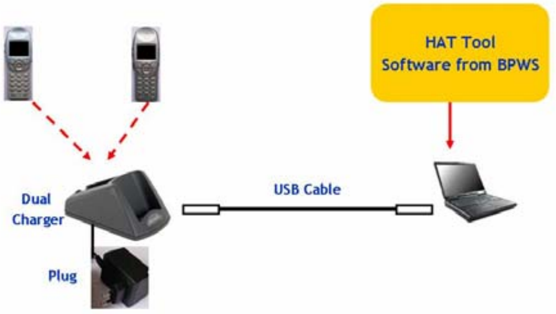
When the CONNECT message is received, signalization link establishment procedure is started. If it fails, the terminal must reset. In case of success, NOE messages exchange can take place.

The terminal will analyse the field QoS_IP_TOS, if present, describing the DSCP value received in the CONNECT message. This optional value (default value Best effort = 0) will be used for setting the DSCP tag for uplink signaling traffic.

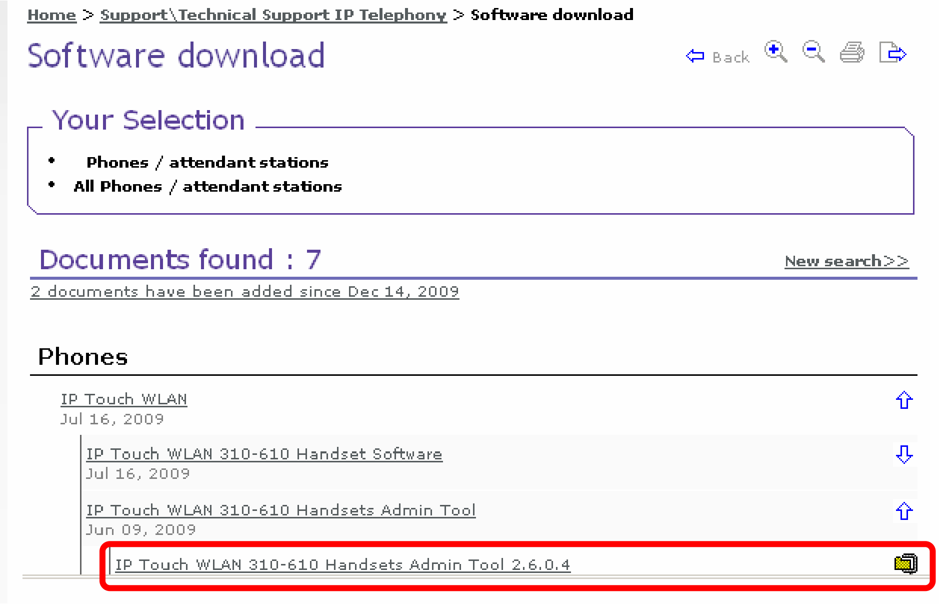
1.1.4.5. Voice over WLAN offers: handset packs and options

Mobile IP Touch 310 Pack: REF 3BN78140AA This pack includes the MIPT 310 handset, the standard battery and the desktop charger. NOTICE: The power supply of the desktop charger must be ordered separately	
Mobile IP Touch 610 Pack: REF 3BN78141AA This pack includes the MIPT 610 handset, the standard battery and the desktop charger. NOTICE: The power supply of the desktop charger must be ordered separately	
Three interchangeable lithium-ion battery packs: Standard battery (Ref: 3BN78145AA), Extended battery (Ref: 3BN78146AA), Ultra extended battery (Ref: 3BN78147AA). Remarks: Each pack is compatible with both MIPT 310 and 610 WLAN handsets.	
Swivel belt clip for: MIPT 310 WLAN handset (Ref: 3BN78148AA), MIPT 610 WLAN handset (Ref: 3BN78149AA)	
Swivel carrying case in black color for: MIPT 310 WLAN handset (Ref: 3BN78150AA), MIPT 610 WLAN handset (Ref: 3BN78152AA).	

Carrying case in black color (Ref: 3BN78151AA) Remarks: the carrying case is compatible with both MIPT 310 and 610 WLAN handsets.	
Lanyard for Alcatel-Lucent IP Touch 310 & 610 WLAN handset (Ref: 3BN78155AA)	
Single charger (Ref 3BN78142AA): In-charger dialing. NOTE: power supply for desktop charger must be ordered separately:(Ref 3BN78120EU)=> Europe (Ref 3BN78120NA)=> North America (Ref 3BN78120UK)=> UK, Hong Kong and Singapore 	
Dual Charger (Ref 3BN78143AA): In-charger dialing LED indicator Designed for easy Battery Pack removal USB port for software updates (see the "MIPT Configuration Tool" chapter) Note: power supply for dual charger must be ordered separately: (Ref 3BN78120EU)=> Europe (Ref 3BN78120NA)=> North America (Ref 3BN78120UK)=> UK, Hong Kong and Singapore 	

Quad charger (Ref 3BN78144AA):: LED indicator Designed for easy Battery Pack removal Wall mounted Note: **Specific** power supply for quad charger. Must be ordered separately: (Ref 3BN78116EU)=> Europe (Ref 3BN78116NA)=> North America (Ref 3BN78116UK)=> UK, Hong Kong and Singapore 	
The necessary components for the Handset Administration Tool (HAT) are: Dual charger (Ref: 3BN78143AA) Specific geographical power supply for dual-charger (Ref 3BN78120xx : see dual-charger above) USB cable for MIPT 310/610 WLAN handset (Ref: 3BN78154AA)	 HAT Tool Software from BPWS Dual Charger USB Cable Plug

Handset Administration Tool is available from BPWS



Home > Support\Technical Support IP Telephony > Software download

Software download

Your Selection

- Phones / attendant stations
- All Phones / attendant stations

Documents found : 7

New search>>

2 documents have been added since Dec 14, 2009

Phones

IP Touch WLAN
Jul 16, 2009

IP Touch WLAN 310-610 Handset Software
Jul 16, 2009

IP Touch WLAN 310-610 Handsets Admin Tool
Jun 09, 2009

IP Touch WLAN 310-610 Handsets Admin Tool 2.6.0.4

2. Architectures

2.1. Non-Alcatel-Lucent WLAN based Architecture

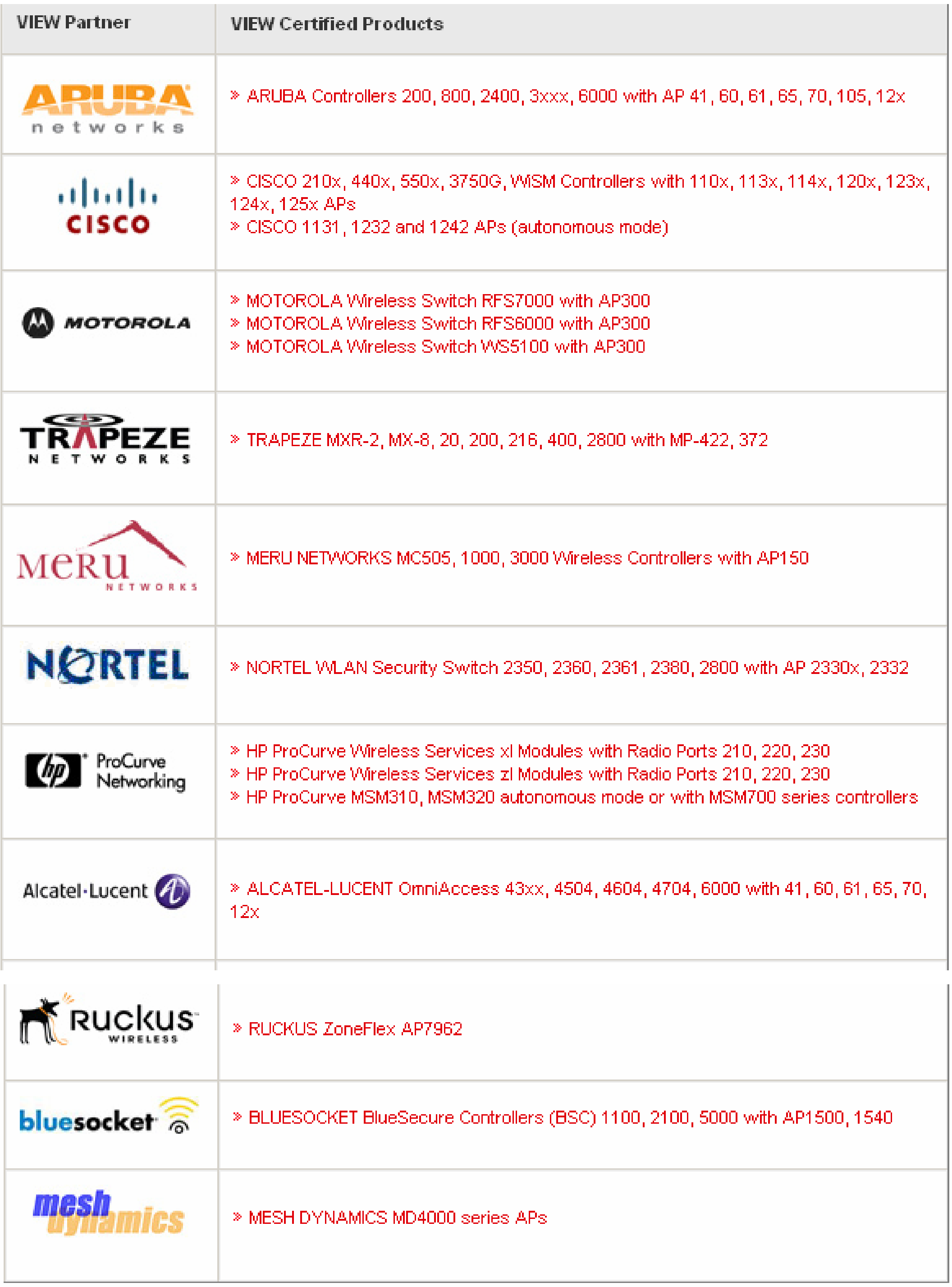
⚠ **Warning: SVP server is still required for Non-ALU WLAN infra**

The implementation of the Alcatel-Lucent VoWLAN solution (MIPT) on a Non Alcatel-Lucent WLAN infra (Aironet, Nortel, Trapeze, etc.) may involve some limitations in terms of VLAN, Roaming & Handover, quantity of calls per AP, QoS, Security etc. Only Alcatel-Lucent WLAN infrastructure and approved third-party infrastructure components are supported. In cases where customers wish to implement Alcatel-Lucent's MIPT VoWLAN solution on an existing non-Alcatel-Lucent wireless LAN infrastructure, a **Premium Customer Support Form (PCS)** must be submitted for evaluation and review prior to customer order.
PCS validation for a VoWLAN multi-vendor project is performed by Alcatel-Lucent and Polycom.

⚠ **Warning: PCS Document is still required for Non-ALU WLAN infra**

Following is Polycom URL for VIEW Certified partners/compatibility list and related configuration notes

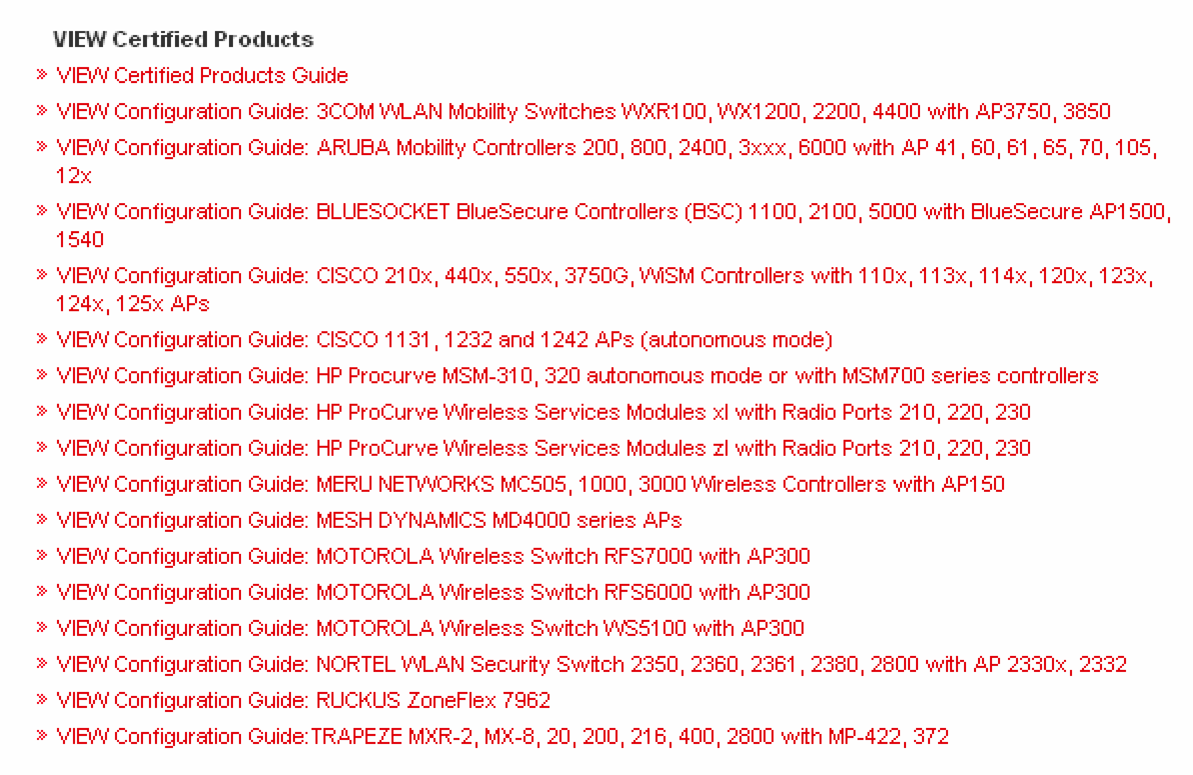
http://www.polycom.com/partners/partner_programs/view_certification_program/view_partners.html



VIEW Partner	VIEW Certified Products
ARUBA networks	» ARUBA Controllers 200, 800, 2400, 3xxx, 6000 with AP 41, 60, 61, 65, 70, 105, 12x
CISCO	» CISCO 210x, 440x, 550x, 3750G, WiSM Controllers with 110x, 113x, 114x, 120x, 123x, 124x, 125x APs » CISCO 1131, 1232 and 1242 APs (autonomous mode)
MOTOROLA	» MOTOROLA Wireless Switch RFS7000 with AP300 » MOTOROLA Wireless Switch RFS6000 with AP300 » MOTOROLA Wireless Switch WS5100 with AP300
TRAPEZE NETWORKS	» TRAPEZE MXR-2, MX-8, 20, 200, 216, 400, 2800 with MP-422, 372
MeRU NETWORKS	» MERU NETWORKS MC505, 1000, 3000 Wireless Controllers with AP150
NORTEL	» NORTEL WLAN Security Switch 2350, 2360, 2361, 2380, 2800 with AP 2330x, 2332
hp ProCurve Networking	» HP ProCurve Wireless Services xl Modules with Radio Ports 210, 220, 230 » HP ProCurve Wireless Services zl Modules with Radio Ports 210, 220, 230 » HP ProCurve MSM310, MSM320 autonomous mode or with MSM700 series controllers
Alcatel·Lucent	» ALCATEL-LUCENT OmniAccess 43xx, 4504, 4604, 4704, 6000 with 41, 60, 61, 65, 70, 12x
RUCKUS WIRELESS	» RUCKUS ZoneFlex AP7962
bluesocket	» BLUESOCKET BlueSecure Controllers (BSC) 1100, 2100, 5000 with AP1500, 1540
mesh dynamics	» MESH DYNAMICS MD4000 series APs

Only VIEW certified topologies from Polycom are supported by Alcatel-Lucent

http://www.polycom.com/support/voice/wi-fi/view_certified.html



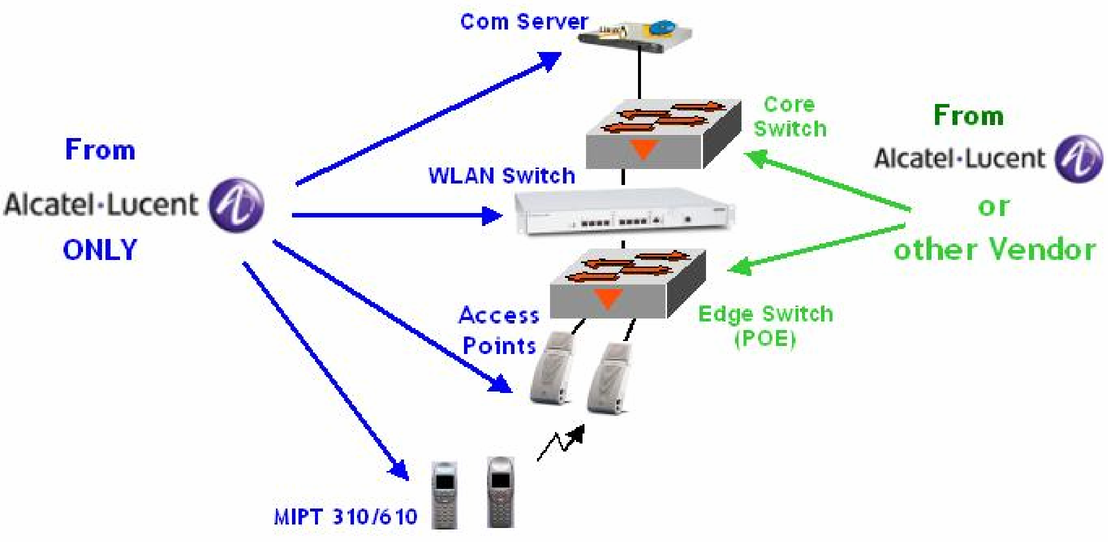
VIEW Certified Products

- » VIEW Certified Products Guide
- » VIEW Configuration Guide: 3COM WLAN Mobility Switches WXR100, WX1200, 2200, 4400 with AP3750, 3850
- » VIEW Configuration Guide: ARUBA Mobility Controllers 200, 800, 2400, 3xxx, 6000 with AP 41, 60, 61, 65, 70, 105, 12x
- » VIEW Configuration Guide: BLUESOCKET BlueSecure Controllers (BSC) 1100, 2100, 5000 with BlueSecure AP1500, 1540
- » VIEW Configuration Guide: CISCO 210x, 440x, 550x, 3750G, WiSM Controllers with 110x, 113x, 114x, 120x, 123x, 124x, 125x APs
- » VIEW Configuration Guide: CISCO 1131, 1232 and 1242 APs (autonomous mode)
- » VIEW Configuration Guide: HP Procurve MSM-310, 320 autonomous mode or with MSM700 series controllers
- » VIEW Configuration Guide: HP ProCurve Wireless Services Modules xl with Radio Ports 210, 220, 230
- » VIEW Configuration Guide: HP ProCurve Wireless Services Modules zl with Radio Ports 210, 220, 230
- » VIEW Configuration Guide: MERU NETWORKS MC505, 1000, 3000 Wireless Controllers with AP150
- » VIEW Configuration Guide: MESH DYNAMICS MD4000 series APs
- » VIEW Configuration Guide: MOTOROLA Wireless Switch RFS7000 with AP300
- » VIEW Configuration Guide: MOTOROLA Wireless Switch RFS6000 with AP300
- » VIEW Configuration Guide: MOTOROLA Wireless Switch WS5100 with AP300
- » VIEW Configuration Guide: NORTEL WLAN Security Switch 2350, 2360, 2361, 2380, 2800 with AP 2330x, 2332
- » VIEW Configuration Guide: RUCKUS ZoneFlex 7962
- » VIEW Configuration Guide:TRAPEZE MXR-2, MX-8, 20, 200, 216, 400, 2800 with MP-422, 372

⚠ **Warning: Check Polycom WEB site regularly for latest updates**

Note : VoWLAN topologies studied in this document are exclusively built on Alcatel-Lucent WLAN infra. For Non-ALU WLAN infra topologies and restrictions please refer to Polycom configuration notes.

2.2. Alcatel-Lucent WLAN based Architecture



Some considerations must be taken under account when implementing the ALU VoWLAN solution. Com Server, WLAN switch, Access Points and MIPT sets must be provided by Alcatel-Lucent. The edge switch must be POE compatible (AP power feeding). The edge switch and the core switch can be either provided by ALU or coming from other vendors.

Nota: SVP server, although still supported, is not needed anymore when using an Alcatel-Lucent WLAN infrastructure.

For SVP server information see annexe

2.2.1. Access Point Modes of Operation

Being as no two customer network environments are exactly the same, it is critical for technology such as VoWLAN to possess a great degree of flexibility. Alcatel-Lucent's MIPT solution is not exempt from this requirement. The following section highlights some MIPT architectural adaptabilities.

2.2.1.1. Direct-Attach Mode

In Direct-Attach operation, the Access Points are directly connected to the 10/100 Ethernet switch interfaces on an Alcatel-Lucent OmniAccess Wireless Switch (model: OA4308, 4324 and/or 6000.) These WLAN Switches have the ability to provide Power over Ethernet (IEEE 802.3af) to Access Point (AP) on all Ethernet ports (Power Class 3 for all ports simultaneously.)

This type of operational mode is desirable and advantageous in the following situations:

1. In small buildings or locations where cables lengths are less than 100m (in order to effectively leverage integrated IEEE 802.3af capabilities.)
2. Where there is no existing data network or the existing data network is already operating at maximum capacity.
3. When existing data network elements lack the ability to provide sufficient IEEE 802.3af power to Access Points.
4. When wireless LAN Access Point controller redundancy is not necessary.
5. For small WLAN environments requiring only a small number of Access Points.
6. To meet requirements for completely independent voice and data networks/backbones.

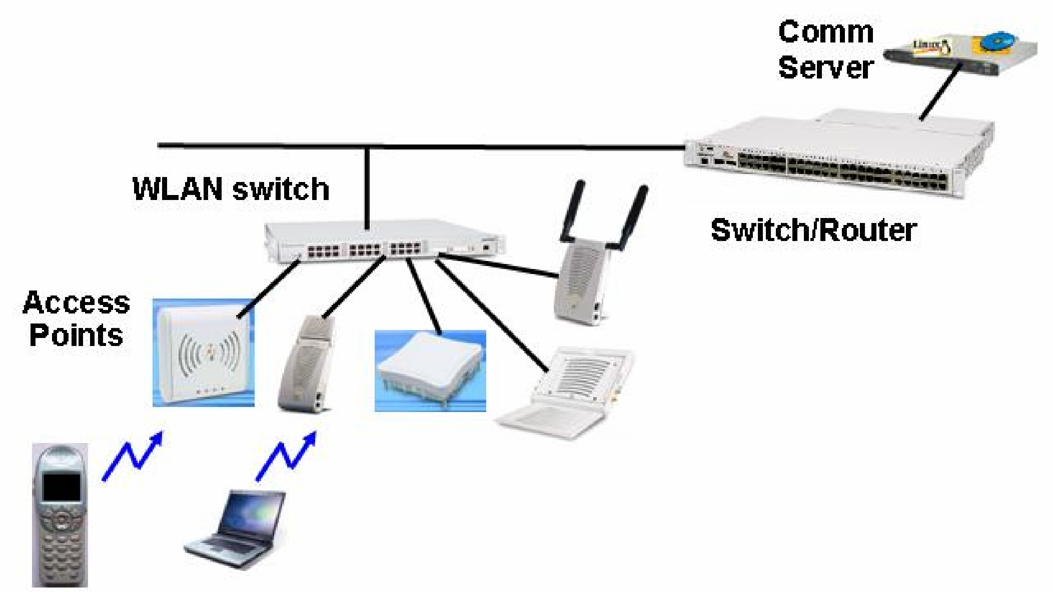


Figure 1: Direct-Attach

2.2.1.2. Overlay Mode

In Overlay Mode operation, Access Points are not directly attached to Alcatel-Lucent OmniAccess Wireless Switches. In this type of operational mode, the Alcatel-Lucent OmniAccess Wireless Switch acts only as an Access Point Controller and does not directly host AP via local 10/100 ports.

This type of operation mode can be highly desirable and advantageous in the following situations:

1. When existing data network elements are present and capable to supporting WLAN Access Points and traffic.
2. In large and/or multi-floor buildings where cables lengths are commonly in excess of 100m from the data switching centers and wiring closets to Access Points, thus causing problems for Inline Power over Ethernet (IEEE 802.3af.)
   In cases such as this, localized power options can be proposed to meet or eliminate the distance limitation and power problems.
3. When system failover/redundancy of the WLAN controller elements is highly desired.

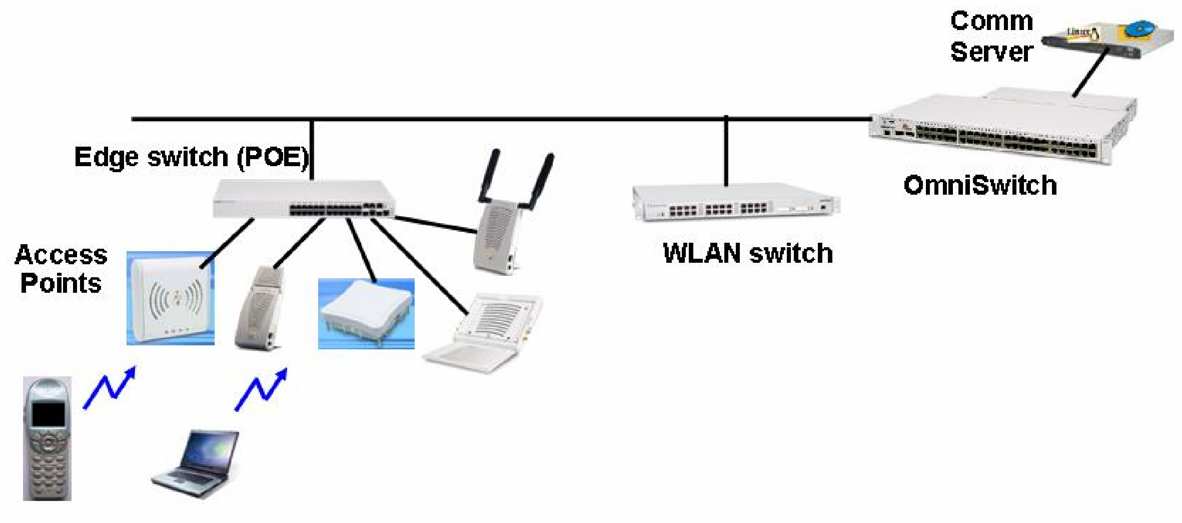


Figure 2: Overlay mode

2.2.1.2.1. *Overlay Mode Operation*

While OmniAccess Wireless Switches can support Direct-Attach mode operation, they can also be used for Overlay mode scenarios. In this way, Access Points can be directly connected to an existing LAN infrastructure Ethernet data switch (from Alcatel-Lucent or third party supplier.) These Access Points can be configured to automatically connect to multiple OmniAccess Wireless Switch (one at a time) using a tunnel protocol optimized for lightweight access points management and traffic transport (GRE, IPSec, and/or L2TP.)

This type of operational mode with OmniAccess Wireless Switches allows for a low cost redundancy proposal for small configurations, particularly with the OmniAccess 4308 model. By being aware of the IP addresses of multiple OmniAccess Wireless Switches, Access Points can perform near-immediate transfer of management responsibilities to backup OmniAccess Wireless Switches and in so doing maintain operation during periods of partial network outage and/or OmniAccess Wireless Switch maintenance.

Since Access Points are not directly attached to OmniAccess Wireless Switches, network connectivity and power options must be provided by an Ethernet switch or other source. It is important to ensure that the desired Ethernet switch is capable of supporting the QoS requirements of the VoIP traffic that it will be forced to carry. The tunnel path between the Access Point and the Wireless Switch must receive high priority to ensure a sufficient level of voice quality.

We can also mix both modes (Direct-Attach and Overlay) but for backup purpose the best solution remains the Overlay mode.

Figure 3: OmniSwitch family with POE (IEEE 802.3af): OS6400-P24/P48 and OS6250-P24

Figure 4: OmniStack family with POE (IEEE 802.3af): OS-LS-6212P/6224P/6248P

Since the Access Points can not benefit from the Inline Power capabilities of the OmniAccess Wireless Switch, the Ethernet switch must be capable of supplying sufficient and standard format power (full 15W limit of IEEE 802.3af.) In the event that this can not be achieved, several options are available:

- The OmniAccess Access Point can be supported via a localized external power supply. This AC/DC transformer is the same type of device used to recharge batteries in PDAs, mobile phones, and some laptop computers. While an available option, the use of localized power is discouraged due to the likely location of Access Point placement and this proximity to AC outlets, fire-code safety concerns, and power autonomy costs.

External Power Supply

- Inline Power Injectors can be used to provide IEEE 802.3af power to individual Access Points. These low-cost, single port (one in, one out) injectors can be used in situations where only one or a few devices require power. These devices require a local AC outlet connection to produce IEEE 802.af power and then inject this power along with the Ethernet traffic that pass transparently through it.

Inline Power Injector

- Ref OAW-AP-AC-xxx : OAW-AP60/61/65/70/120 Series AC Power Adapter Kit (xxx is country dependant)

3. Quality of Service (QoS)

The QoS management responsibilities is shared between the WLAN switch, the AP, the MIPT set and the WLAN switch infrastructure components. The first responsibility of the WLAN Switch is to control the number of simultaneous voice calls permitted per Access Point. While the absolute maximum limit of simultaneous voice conversations per Access Point can be reached, assuming ideal conditions, the actual limits enforced per Access Point must take competition (bandwidth and radio spectrum sharing with data clients) and signal quality (distance from AP and radio obstacles/interference) into consideration.

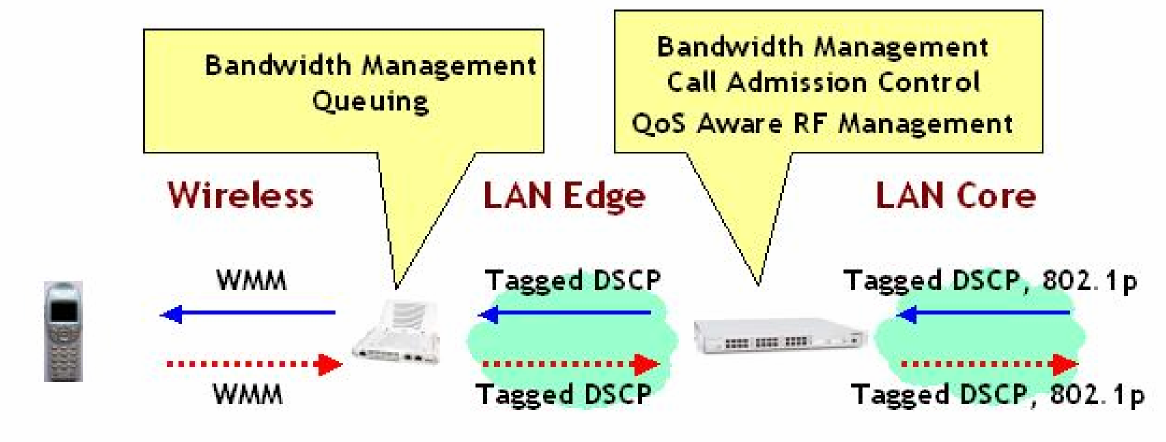


Figure 5: End-to-End QoS

An end-to-end QoS ensures a prioritization or Voice over Data from Wireless to LAN and vice versa. Ensure that network switches and routers do not change the DSCP value set on MIPT or coming from LAN.

4. Security

Security is always a sensitive topic to discuss, and opinions on how best to provide for it vary greatly from one engineer to the next. With this in mind, Alcatel-Lucent is constantly developing the list of security options available within the MIPT VoWLAN solution offer to satisfy as many different opinions as possible.

For the Voice over WLAN R 4.1 solution offer, Alcatel-Lucent makes the following security recommendations:

4.1. SSID Broadcast

When designing and managing a Wireless LAN, engineers must make calculated compromises between performance and ease of use. One such decision is that of whether or not to broadcast the SSID (Service Set Identifier) of a wireless network. Broadcasting the SSID allows clients to “scan” for available network and then attempt to join them. This eliminates the need for users to explicitly know the name of the network that must be defined in their 802.11 client configuration, since it can be learned from the over-the-air broadcasts (excluding MIPT terminals that must be configured manually by design.) Obviously, not broadcasting the SSID provides the opposite: users must know the SSID.

In the above mentioned way, it is commonly thought that we can offer a limited realm of security simply by not broadcasting the SSID of the Wi-Fi environment dedicated to VoWLAN activity. In truth, this practice is often far more troublesome to network administrators than it is to network attackers. The advantages of SSID broadcast usually far exceed the threat of visibility it offers.

Since all MIPT terminals must be manually configured with an SSID, the decision to enable or disable SSID broadcast is of little consequence to Alcatel-Lucent MIPT terminals. There is no impact to ease of use or functionality presented by the state of SSID broadcast. Alcatel-Lucent recommends that customers maintain their current or desired security policies governing this topic.

4.2. Authentication

PEAP (Protected Extensible Authentication Protocol) uses TLS to create an encrypted Tunnel

MIPT uses PEAP for 802.1X Authentication

- A certificate is required on server side (Radius Server)
- No certificate need on client side (MIPT)
- Only the Radius server is authenticated, but not the MIPT
- Avoids using a heavy PKI (Public Key Infrastructure)

Inside the TLS Tunnel two EAP Methods can be used:

EAP-MSCHAP v2 (EAP Microsoft Challenge Handshake Authentication Protocol) on ALU WLAN infra

EAP-FAST (Flexible Authentication via Secure Tunneling) on Cisco WLAN infra

- No certificate is needed (client & server sides)

In order to minimize the re-authentication delay the following methods are used:

- OKC (Opportunistic Key Caching)
    - Available on ALU WLAN infra (OKC on MIPT with WPA2 only)
- CCKM (Cisco Centralized Key Management)
    - Available on Cisco AP only

4.3. Peoria

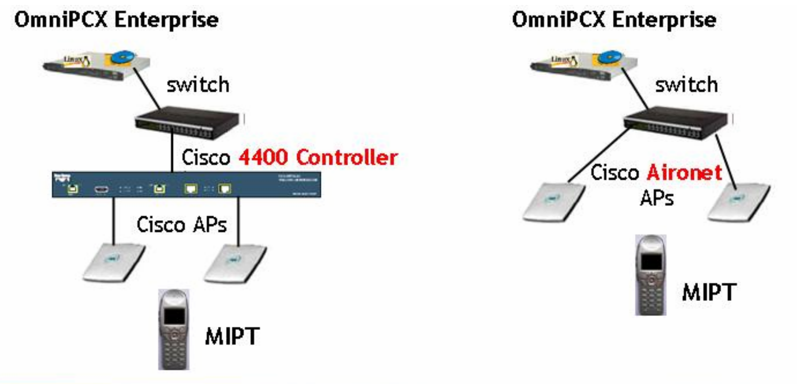
Peoria is a development program for **SVP server removal** on Cisco WLAN infra

Peoria is not under PCS (Premium Customer Support)

Three features are part of Peoria program:

- CCXv4 (Cisco AP only)
- MIPT Precedence and OXE DSCP Tagging
- WMM Admission Control Support

Following are the involved topologies :



For more details concerning supported configuration for Peoria please check the following URL http://www.polycom.com/usa/en/support/voice/wi-fi/wi_fi_interoperability.html

4.4. Ekahau RTLS

Ekahau RTLS (Real-Time Location System) provides a geo-localization of MIPT sets within a building or an outdoor RF covered area, is made of a server (Ekahau Positioning Engine) and a client that is embedded on MIPT set.

Ekahau RTLS solution is **managed via AAPP (Alcatel-Lucent Application Partner Program)** and is only supported on ALU/Aruba WLAN infra.

Ekahau RTLS includes the following features:

Ekahau Tracker: End-user application for real-time tracking and analyzing the location of people

Ekahau Finder: End-user application for real-time grouping, locating and viewing the location of people

Ekahau Engine (dedicated Windows server): Systems and device management through a web-based interface

The EPE (Ekahau Positioning Engine) runs on Windows Server 2000, Windows Server 2003 or under VMWare. Hardware recommendations depend on the number of Tag clients to be serviced.

Ekahau Location Survey for recording reference

For more details see: http://www.ekahau.com/products/real-time-location-system/overview.html

Deployment recommendations:

- Ekahau RTLS and OV3600 cannot be installed on the same physical server

- When using Ekahau EPE with any Ekahau client then their rules for RF design would apply. These rules are common to all RTLS vendors and are basically required to get decent accuracy out of the system. 1 AP at > -65dBm and 2 APs at > -75dBm minimum.

The MIPT 310/610 could be located without the client as well. The client should increase accuracy because of increased frequency of data and increased quantity of data to the location engine.

4.5. Encryption

At present, for the WLAN R 4.1 offer, Alcatel-Lucent provides encryption options based on WEP (Static Key), WPA-PSK and WPA2-PSK (802.11i / AES encryption) personal mode (4-Way handshake authentication method based on pre-shared key). This means that, if selected, wireless traffic for VoWLAN can be encrypted based either on RC4 ciphering techniques (with or without TKIP) or on AES (WPA2), and “Shared Key” authentication mechanisms. Pre Shared Keys must be manually entered in each MIPT terminal at installation. In the case of WPA/WPA2-PSK implementation, the

Pre Shared Key is used for initial authentication and as the seed for Temporal Key Integrity Protocol key rotations.

WEP is recognized as being a weak security option due to the static nature of the encryption key. Derivation of the key is possible through simple passive scanning techniques and data analysis. To counter this problem, the Wi-Fi Alliance has defined a standard known as WPA. WPA, in reality, is WEP enhanced with TKIP key rotation. This prevents key derivation through passive scanning and brute force attacks. WPA-PSK can be implemented in most infrastructure environments through simple software upgrades, making it a universally available, simple and effective scheme for content protection.

Alcatel-Lucent strongly recommends the use of WPA2 (or at least WPA) in order to provide the highest levels of confidentiality and network security. The password length must be greater than twenty characters in order to avoid the brute force attacks.

4.6. MAC Address Filtering

MAC address filtering facilities are provided for within Alcatel-Lucent's OmniAccess product platforms. Alcatel-Lucent strongly encourages the use of Local MAC address filter rules to help ensure that only authorized wireless clients are permitted to join the VoWLAN network.
For more information on MAC address filtering, please refer to the Alcatel-Lucent VoWLAN Engineering Reference.

4.7. Rogue Activity Detection

Rogue Access Points and Rogue Ad-Hoc Wi-Fi activity can seriously degrade VoWLAN voice quality by wreaking havoc with carefully designed and implemented Radio Frequency coverage patterns. For this reason, Alcatel-Lucent strongly recommends the use of the OmniAccess Wireless Protection option to identify and eliminate these potential threats. The nominal cost of this technology option provides an immense amount of investment protection, and the value of Rogue Activity Detection can not be stressed enough.

4.8. Isolation Practices

Network segmentation is seen as a critical core component of any network security design. Separating traffic by type and application scope allows for more sophisticated security methodologies to be later implemented. VPN, Packet Inspection/Filtering, Access Control Lists, and other security technologies generally rely on network segmentation in order to be most effective.

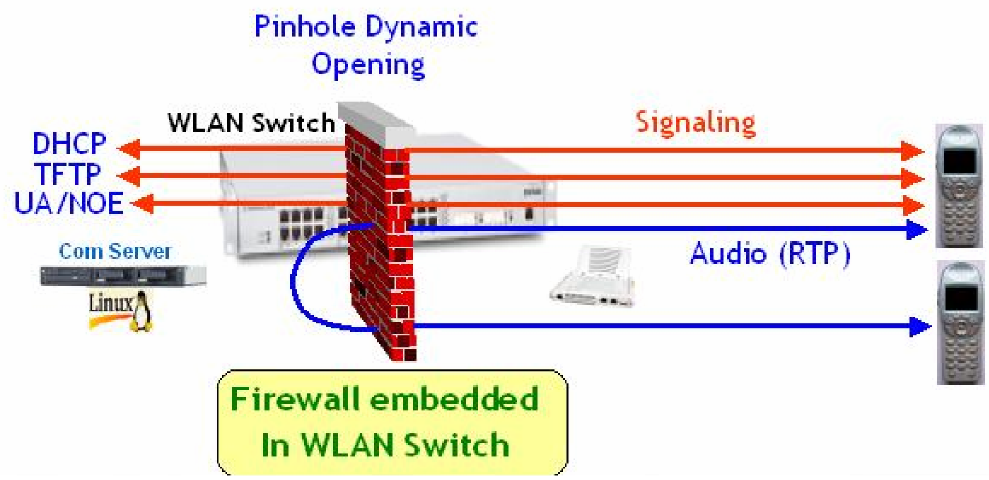
For the above reasons, Alcatel-Lucent strongly suggests a Voice and non-Voice domain separation on VoWLAN equipment. Sharing the VoWLAN environment with non-voice related elements is a compromise in security that does not need to be made. For example at WLAN switch level Alcatel-Lucent recommends to implement first a single **Voice VLAN** dedicated to Voice and a **Data VLAN** dedicated to Wireless Data.

4.9. Layer 3 & 4 Filtering (ACL & Packet Inspection)

It is assumed that the VoWLAN environment will be hosted on a customer network which also supports data networking environments. To assure privacy and system security, security controls should be implemented at network routing points to restrict the ability of non-voice related elements from gaining access to VoWLAN and OmniPCX Enterprise components. These security controls can be delivered in the form of router or route-switch based Access Control Lists or via dedicated Packet Filtering and Packet Inspection platforms.

Alcatel-Lucent’s OmniAccess WLAN 43xx, 4x04 and 6xxx products incorporate integral Stateful Inspection technology (NOE Protocol for VoWLAN). This allows for strong access control policies and network protection.

4.10. ALG (Application Layer Gateway)



ALG process on Firewall allowing dynamic port opening based on UA/NOE protocol
Used to dynamically open UDP ports for RTP traffic)
Firewall is embedded on WLAN Switch
Application Layer Gateway benefit: Reduction of permanently opened ports on Firewall

4.11. Auxiliary Security Measures

In addition to the standard security mechanisms discussed above, some customers may desire to implement specialized security measures that apply specifically to their environment. Use of MAC address controls within the external TFTP server or DHCP server, as well as other application security methods can be very advantageous. Alcatel-Lucent offers none of these server-based features, but encourages customers to explore the security capabilities present in third-party support hardware.

5. Design Process for VoWLAN

5.1. Pre Sale Data Collection

In order to prepare an Alcatel-Lucent VoWLAN solution, several pieces of documentation must be sourced from the customer. The accuracy of a final system proposal is directly related, in most cases, to the amount and quality of information collected prior to initiating design formulation.

5.1.1. Physical Diagram (to include existing wireless technologies)

A clear understanding of the customer's physical network topology is essential in order to properly determine the possible future locations and integration points of VoWLAN support elements. This physical diagram should be as complete as possible and include information related to all existing customer infrastructure (Data Wi-Fi, LAN, MAN, closet switching platforms (to include power feeding abilities), core routing platforms, copper and fiber patching facilities (termination types).) Again, an accurate MIPT VoWLAN solution can not be developed without this information.

The physical diagram is responsible for helping the design engineer in gauging a number of placement and connectivity options from the number of locations where OmniAccess Wireless Switch/Appliance platforms can be housed, to the type of physical connectors needed on the fiber patch cords to connect them to the network. To meet this requirement, the physical diagram must contain as much detail as possible.

This diagram should also detail cable-plant distances and the ability of existing data network switches to support IEEE 802.3af power in sufficient quantity for the proposed solution.

Of a much more complex nature is the presence and status of existing wireless technology. The Physical diagram should detail, in as much detail as possible, the presence of existing or proposed Bluetooth, Wi-Fi, microwave technology, high-gain or industrial radio transmitters, DECT/PWT technologies and other interference or radio spectrum competitors.

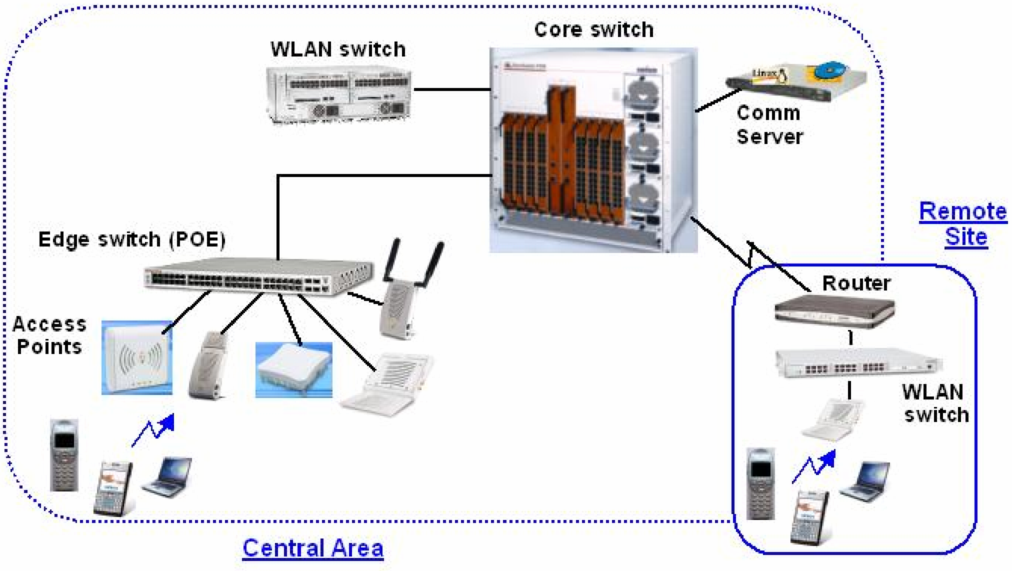


Figure 6: Physical Diagram

5.1.2. Logical Diagram

Logical Diagrams are also critical for complete and accurate solution construction. The logical diagram must include information related to the existing customer VLAN strategy, QoS policies, Security measures, redundancy and fault tolerance schemes, as well as future provisioning and traffic shaping.
Information gathered from the logical diagrams will determine IP addressing schemes, security measures, and VLAN mapping as well as influence certain physical design options (ideal TFTP & DHCP Server location, etc.)

This diagram shows the different domains at layer 2 and 3 currently used in the customer network: VLANs, Broadcast domains, IP subnets and IP addressing Plan.

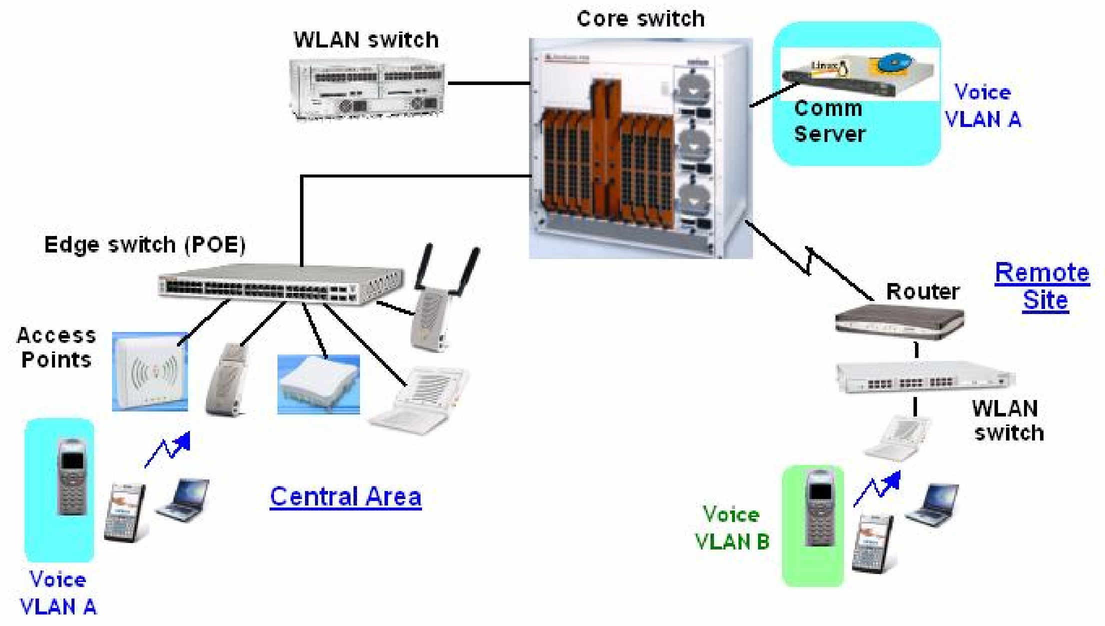


Figure 7: IP Logical Diagram

5.1.3. Floor Level Maps/Diagrams

To complete detailed planning, a floor level diagram is required. This floor level diagram can be used in the design process in two different ways, Prediction Planning and for the Site Survey. This diagram does not necessarily need to include detail on how desks are situated within office and where toilets and potted plants are located within restroom, but walls, dividers, elevators, pillars, windows, doors, and other obstacles should be clearly marked and to scale.

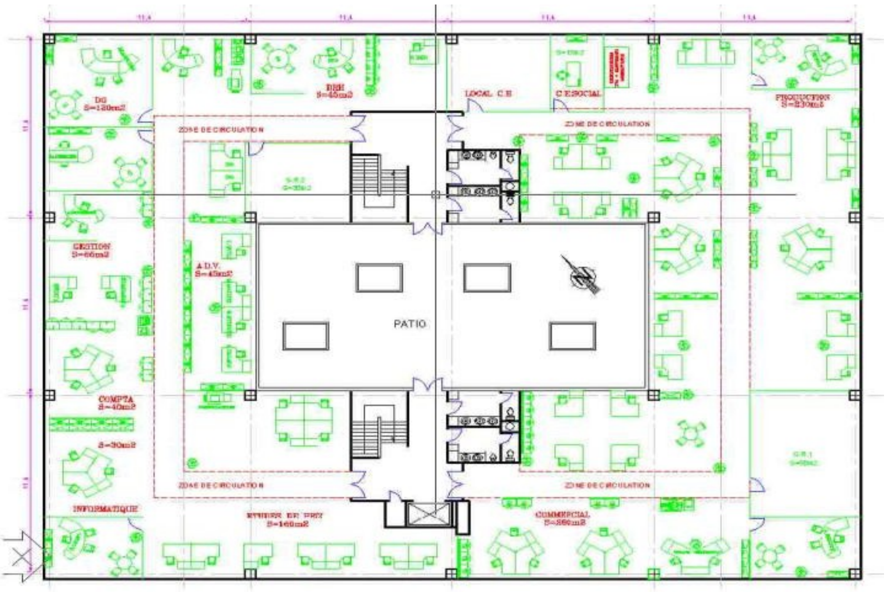


Figure 8: Floor Map (with scale & legend)

6. Customer Specific Application & Design Considerations

Due to the fact that Alcatel-Lucent’s MIPT VoWLAN solution is being offered in a multi-stage fashion with evolving capabilities, it is important for the design engineer to compare expected customer usage patterns against current MIPT release restrictions before proposing an Alcatel-Lucent MIPT VoWLAN solution.

6.1. Network Topologies

When studying VoWLAN topologies it is needed to use some terminology in order to well define the various basic configurations

6.1.1. Campus definition

Network topology where all components (Com Servers, IPMG, Switch/Routers, etc.) are scattered over a large geographic area and are interconnected through High Speed links (such as Fiber Optic cabling), resulting in no delay or bandwidth concerns.

6.1.2. Multi-Node definition

Several OmniPCX Enterprise Nodes belonging to the same Homogenous ABC network.

6.1.3. Multi-Site definition

Topology comprised of a Single OmniPCX Enterprise Node with one or several remote site(s). For instance it can be a headquarter and one or more branch offices.

6.1.4. Single OXE Node in a Multi-Site Environment (Campus / Remote Site)

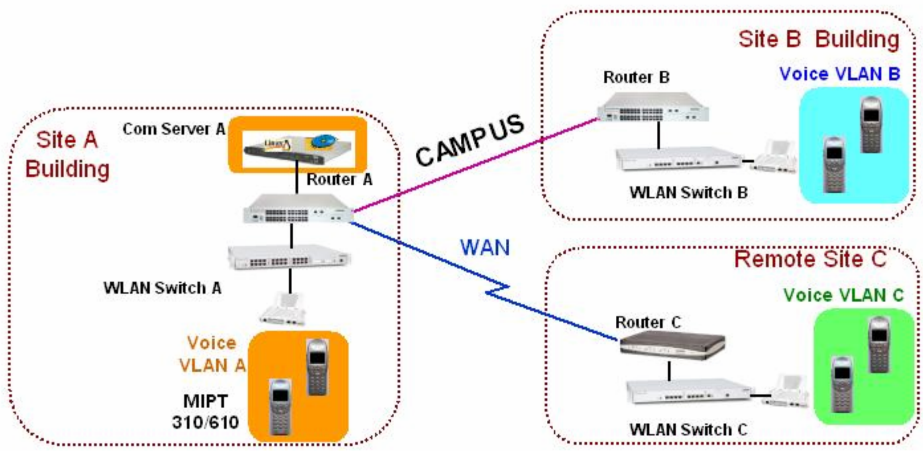


Figure 9: Single-OXE Node and Multi-Site

This topology based on a single OXE node allows a VoWLAN implementation on remote sites.
For Roaming and Handover restrictions in campus or remote site see the chapter dedicated to Roaming & Handover.

6.1.5. Multi OXE Node in a Multi-Site Environment (WAN)

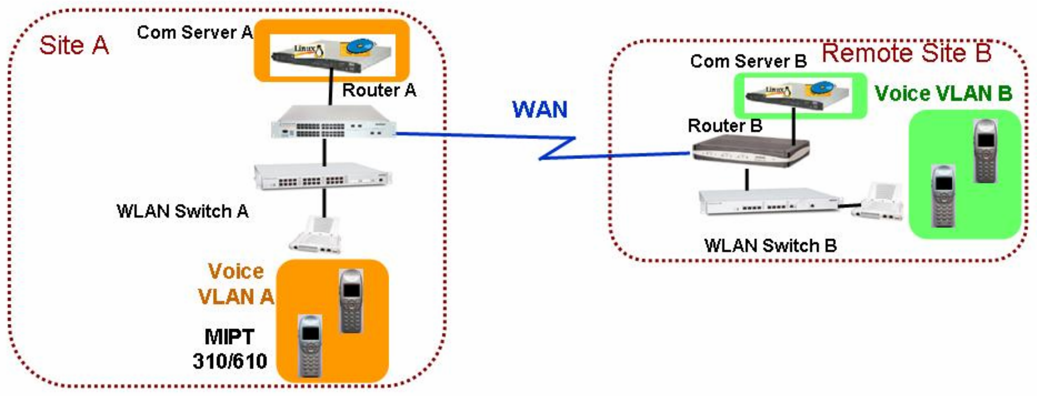


Figure 10: Multi-OXE Node and Multi-Site

Same configuration as previously, but now in an OXE Multi-node OmniPCX topology.
For Roaming and Handover restrictions see the chapter dedicated to Roaming & Handover.

6.1.6. Multi-WLAN Switch Layer 2 Configuration

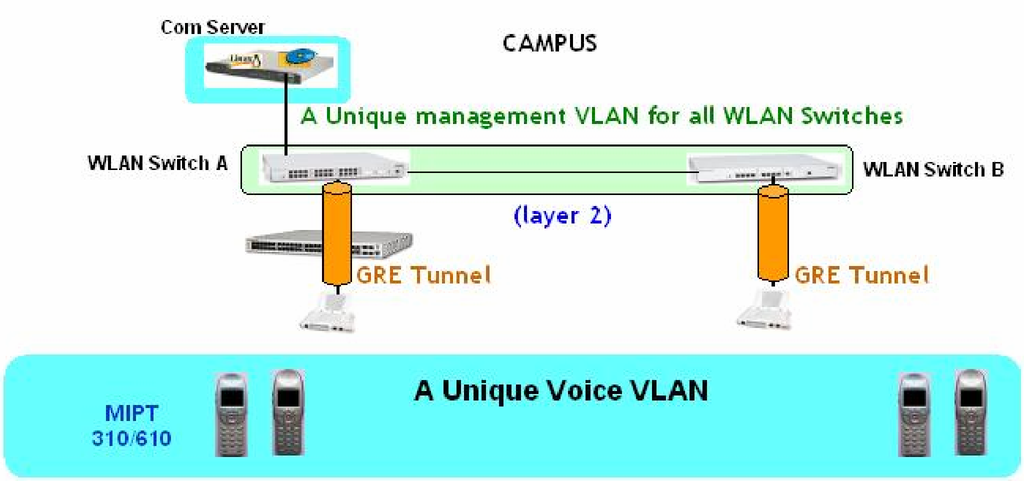


Figure 11: Layer 2 configuration (WLAN switch)

Layer 2 configuration means that all WLAN switches are in a unique VLAN/IP subnet and MIPT sets are all in the same Voice VLAN/IP subnet. This topology allows quick handover.

6.1.7. Multi-WLAN Switch Layer 3 Configuration

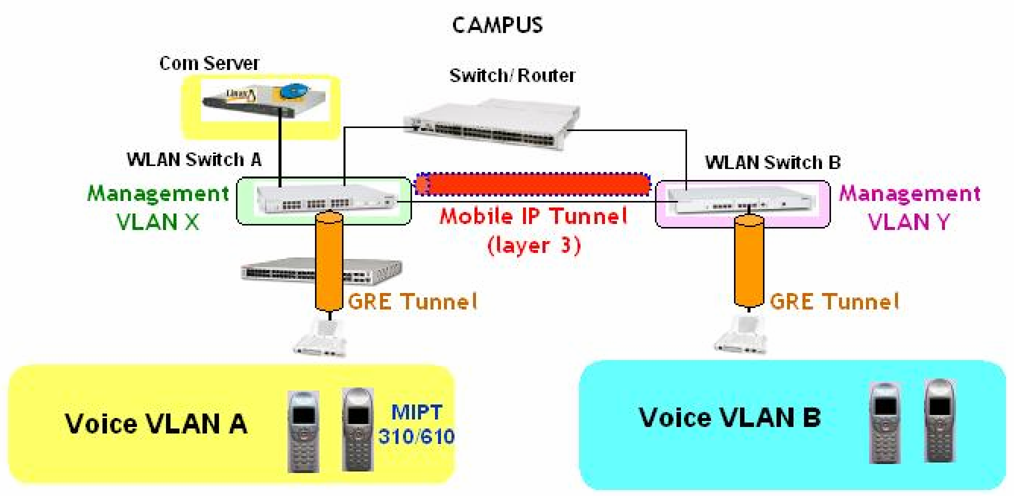


Figure 12: Layer 3 configuration (WLAN switch)

Layer 3 configuration means that each WLAN switch is in a different VLAN/IP subnet and MIPT sets can be spread over several Voice VLANs/IP subnets

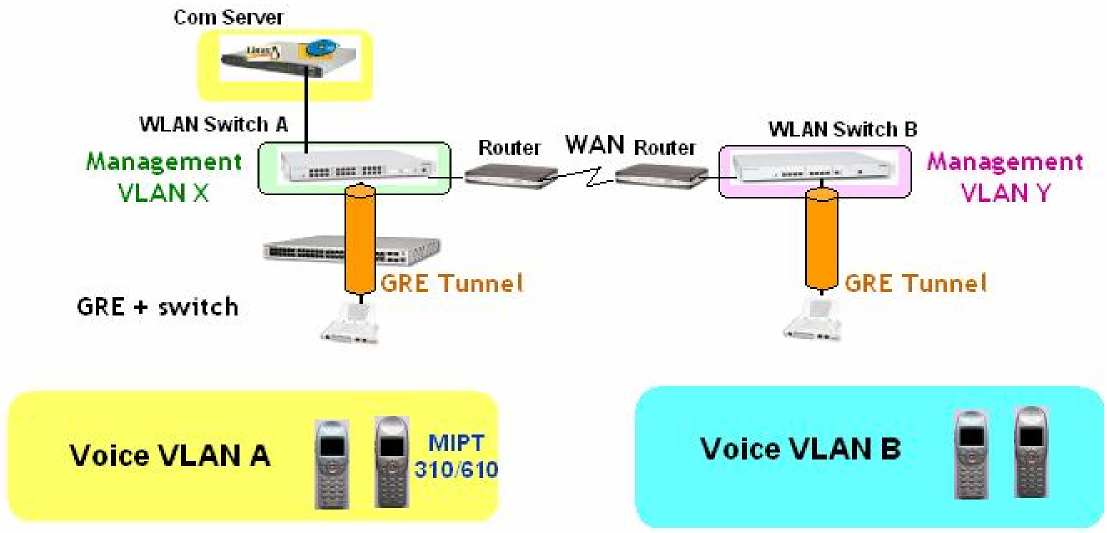


Figure 13: Layer 3 configuration for WAN

Layer 3 configuration is also applicable to WAN topologies

6.2. Remote LAN-connected AP

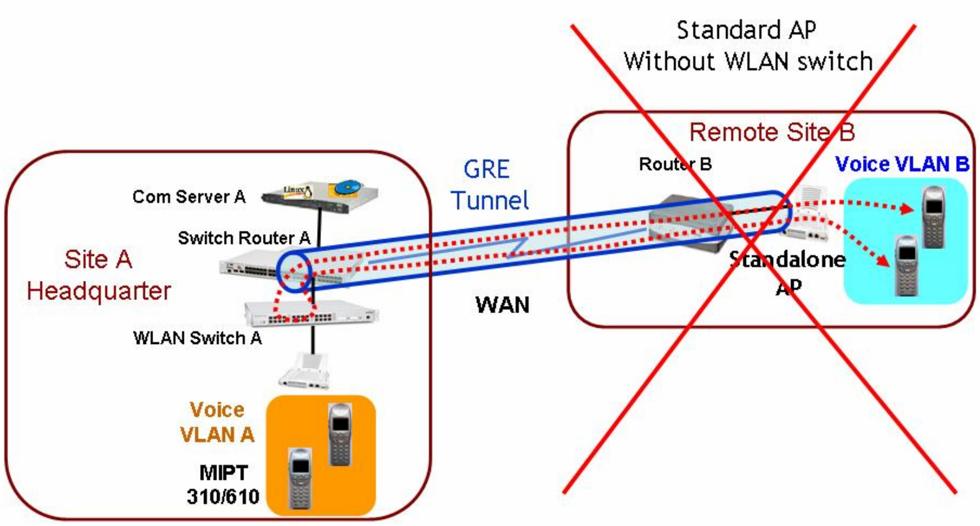


Figure 14 Remote LAN-connected AP

A Remote LAN-connected AP is a standard AP that is installed on a remote site and interconnected to the central WLAN switch via a GRE tunnel. **This configuration is not supported with MIPT** due to voice tromboning over the WAN.

6.3. VoWLAN on Remote AP for Home Worker

6.3.1. Overview

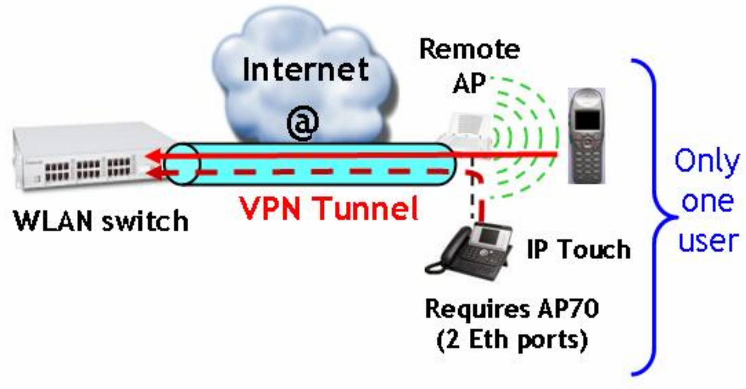


Figure 15: Remote AP for Home worker

A Remote AP is an AP that is installed on a remote site but **with a specific Remote AP license configured on central WLAN switch**. During the provisioning (where the Remote AP is locally connected to the WLAN switch) a VPN tunnel is automatically raised between the Remote AP and the central WLAN switch. There are several modes of operation when the remote AP is used for wireless data

- Tunnel mode: Traffic between Remote AP and WLAN switch goes through the VPN Tunnel
- Local bridging: Traffic between 2 users at remote location remains local and does not go through the VPN tunnel
- Split Tunneling: policy-based forwarding of packets in the VPN tunnel or locally bridge

Only Tunnel mode is supported by Voice over WLAN and for a unique user. An IP Touch set can be connected to the second Ethernet port of the AP70, the RTP and signalling traffic is redirected to the VPN tunnel. The IP Touch and the MIPT must be configured in twinset mode or supervision. It is not allowed to make a call from the MIPT set to IP Touch set (tromboning issue).

Some figures resulting from RAP tests:

- An IP Touch call (in G711) needs approximately 150 Kbps
- A MIPT call (in G711) needs approximately 140 Kbps
- The quantity of calls is WAN bandwidth dependent

PEF licence is required for Voice over WLAN and to create bandwidth contracts for Data (in order to keep bandwidth for Voice).

Nota: If the IP Touch set feature is not needed, the AP70 can be replaced by another Access Point supporting the remote AP feature (i.e. AP60, AP61 or AP65).

6.3.2. Remote AP and Encryption

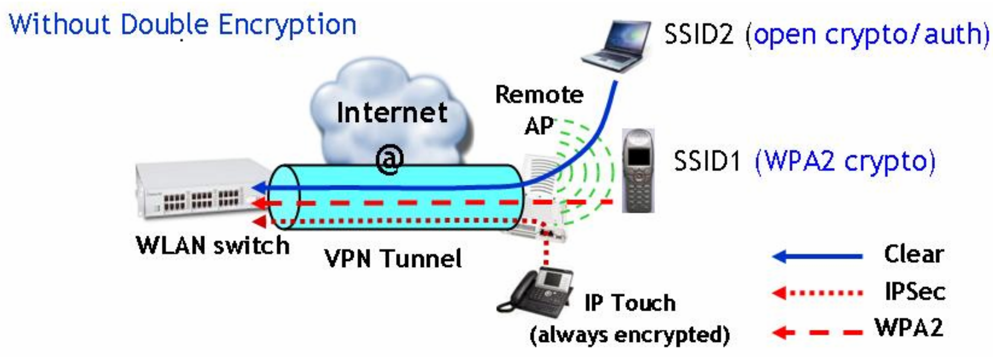


Figure 16: Encryption on Remote AP

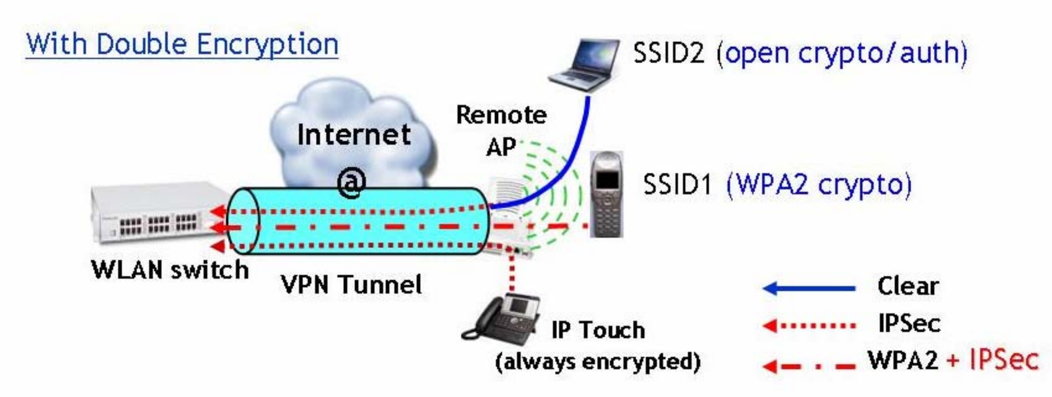


Figure 17: Double encryption on Remote AP

From the above pictures an IP Touch set is plugged into the Eth port 1 of the AP70 (configured as RAP).
Two SSIDs are created:

- SSID1 with WPA2 crypto (MIPT)
- SSID2 with open crypto/auth (Wireless PC)

All traffic from wired users connected to Eth1 is always encrypted – independent of the “double encrypt” configuration. For SSID2, the traffic will be in the clear unless the “double encrypt” option is enabled.
The expected encrypted performance with the AP70/61/65 configured as RAP is in the 3-6 Mbps range (while a LAN-connected AP has about a 20Mbps useful bandwidth).

6.3.3. Implementation with a Corporate Firewall (Security)

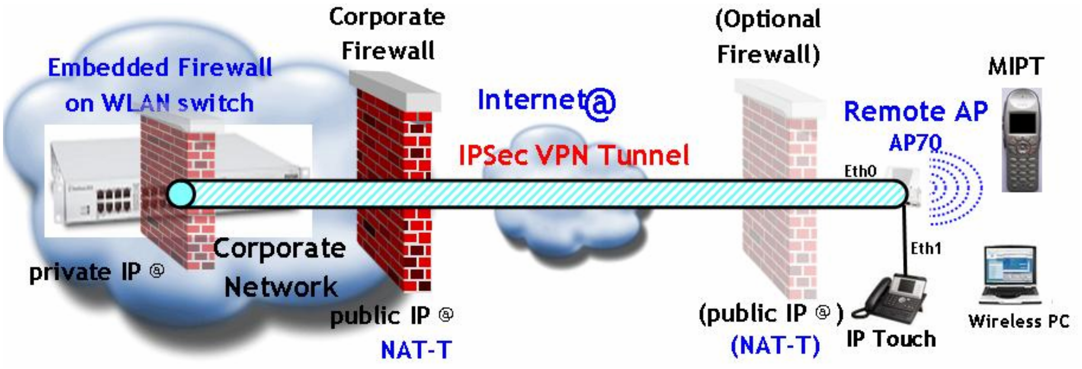


Figure 18: RAP with a corporate Firewall

This above picture shows how to implement a remote AP access with a corporate firewall, the purpose of this topology being to hide the corporate network from the Internet.

The IP Sec VPN Tunnel created between the remote AP and the WLAN switch must go through the Corporate Firewall. A NAT Traversal function for IPSec Tunnel is performed by the firewall. Only the UDP port 4500 (IP Sec Tunnel) is open on Firewall.

The AP70 Ethernet port Access can be protected using 2 possibilities:

- 802.1X Authentication on AP70 Ethernet port 1. The IP Touch must authenticate before acceding to the corporate network.

- Filtering Rules must be entered on WLAN switch Firewall to limit the AP70 Eth1 access

(PEF license required)

6.3.4. Implementation in a DMZ (Security)

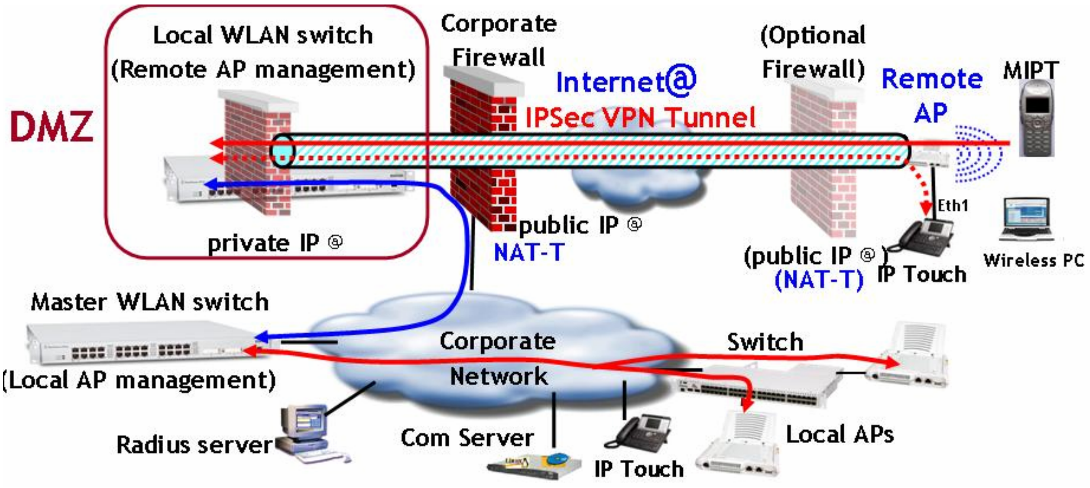


Figure 19: DMZ implementation with RAP

This implementation is fully adapted when the customer requires that any VPN tunnel ends in a DMZ (Demilitary Zone). In this case the Local WLAN switch ensures a VPN termination in DMZ and is in charge of remote APs only. The Master WLAN switch in Corporate Network manages local APs and communicates with the local WLAN switch via the Corporate Firewall.

6.4. VoWLAN Mesh in 802.11a b/g

Mesh function is subdivided in two separate features: Mesh Bridging and Mesh Backhaul.

Indoor mesh or outdoor mesh can be used depending on license installed on WLAN switch (Indoor Mesh Point License or outdoor Mesh Point License)and the type of AP.

For instance an AP70 needs an Indoor Mesh Point license while an AP85 requires an outdoor Mesh Point license.

A mesh license is required whatever the function is, mesh portal or mesh point.

6.4.1. Mesh LAN Bridging

The Mesh Bridging purpose is to extend the LAN through a wireless mesh link. This solution allows VoIP and data users.

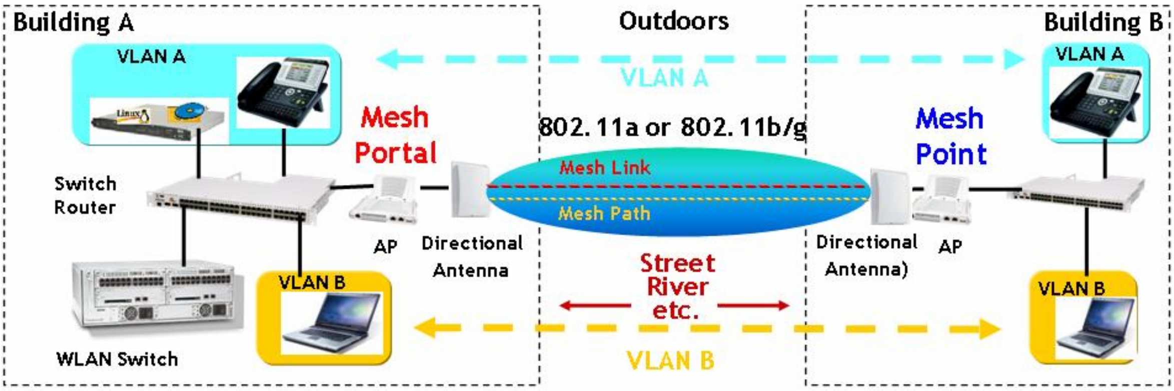


Figure 20: Mesh Bridging with VLANs

Only one radio can be used for the mesh link (802.11a or 802.11b/g, but not both)

It is important to remember a few things:

- Bandwidth on arrival decreases as the distance between the mesh portal and mesh point increases.

- Considering the best situation where a bandwidth of 54 Mbps could be expected, it does not mean that the usable bandwidth is 54 Mbps, but only about 20-24 Mbps due to 802.11 overhead.

Different VLANs can be propagated through the mesh link.

6.4.2. Mesh Backhaul

Mesh Backhaul purpose is to extend RF coverage through a wireless mesh link. WLAN services (local coverage) can be either done on the mesh point only or on the both mesh portal and mesh point.

6.4.2.1. Mesh Backhaul on a single Radio

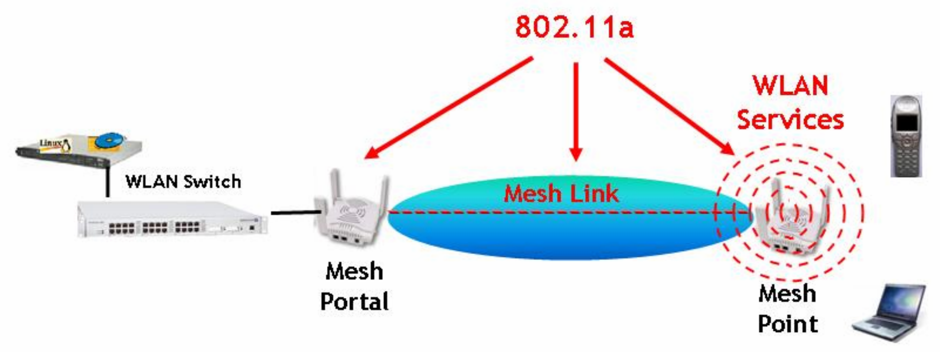


Figure 21: Mesh Backhaul with a Single Radio

Mesh link and WLAN services, the both being on a Single Radio are supported from AOS 3.4.0. Selected radio can be either 802.11a or 802.11b/g. On this above example 802.11a is used for the both Mesh Link and WLAN services. This solution takes advantage of using a single radio AP for Mesh Portal and also for Mesh Point function.

Voice and Data wireless users must share the same Radio.

6.4.2.2. Mesh Backhaul using dual Radio

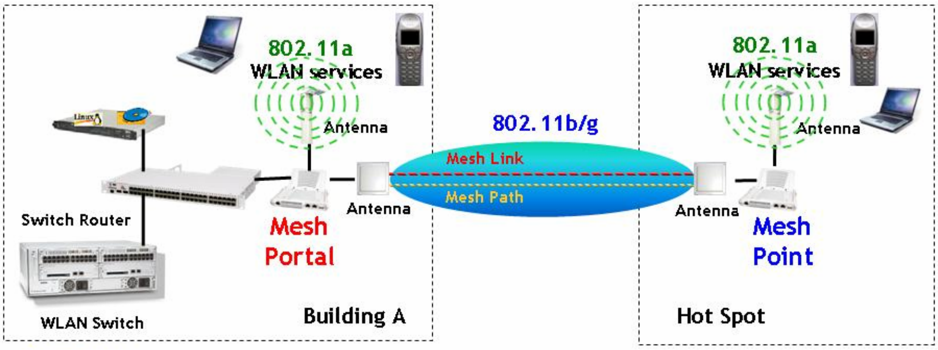


Figure 22: Mesh Backhaul using two Radios

Using one Radio for Mesh Link and another Radio for WLAN Services is still valid:

Mesh link in 802.11b/g with WLAN services in 802.11a, or Mesh link in 802.11a with WLAN services in 802.11b/g. A dual-radio is required for Mesh Point AP. If Mesh Portal AP provides WLAN services a dual-radio AP is required, if not a single-radio AP for Mesh Portal is enough.

Voice and Data wireless users must share the same Radio.

Validation test results:

OXE: 8 MIPTs in conversation   Codec: G.711   Framing: 20ms

Radio: 802.11a on mesh link and 802.11g for WLAN services

MIPT: 802.11g only/WPA2-PSK/WMM-AC

Wireless Data client: 802.11g

Scenario	TCP-Downstream	TCP-Upstream	UDP-Downstream	UDP-Upstream
Data traffic with 8 concurrent MIPT calls	5.5 Mbps	5.5 Mbps	3.5 Mbps	4Mbps

6.4.3. VoWLAN Mesh Rules

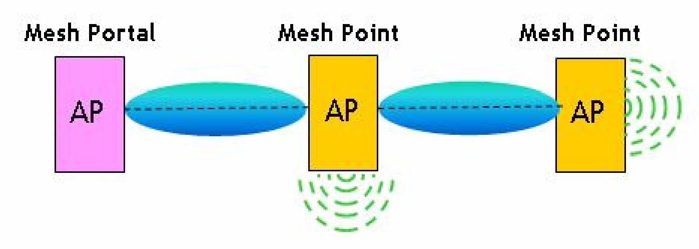


Figure 23: First VoWLAN Mesh rule

First rule: 2 Voice Mesh Hops max.

Let us consider the above topology (made of one mesh portal and 2 successive mesh points) and assume that the true bandwidth is 20 Mbps between mesh portal and the first mesh point, this bandwidth will be divided by 2 when reaching the second mesh point. It is due to the fact that the first mesh point has 2 mesh links to manage.

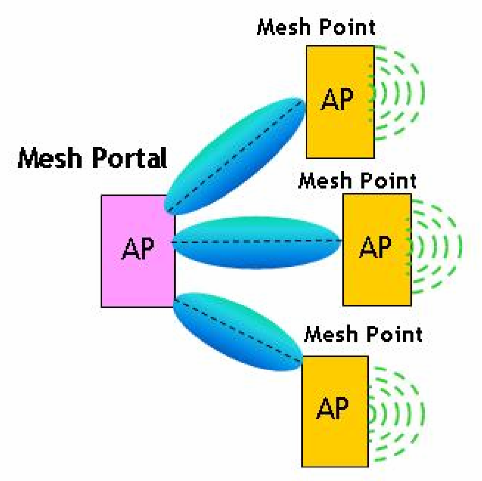


Figure 24: Second VoWLAN mesh rule

Second rule: 3 Voice Mesh directions max.

In this topology if we consider an identical bandwidth for the 3 directions, the available bandwidth at a given mesh point will be equivalent to the mesh portal bandwidth divided by 3.

A Mesh portal has a max transit capacity of about 20 MIPT calls shared between the 3 Mesh points. Each mesh point can handle up to 10 MIPT calls in 802.11g and up to 12 MIPT calls in 802.11a; however the global quantity of MIPT calls must stay in the limit of the mesh portal capacity.

Third rule: a Mesh portal supports up to 6 Mesh points max

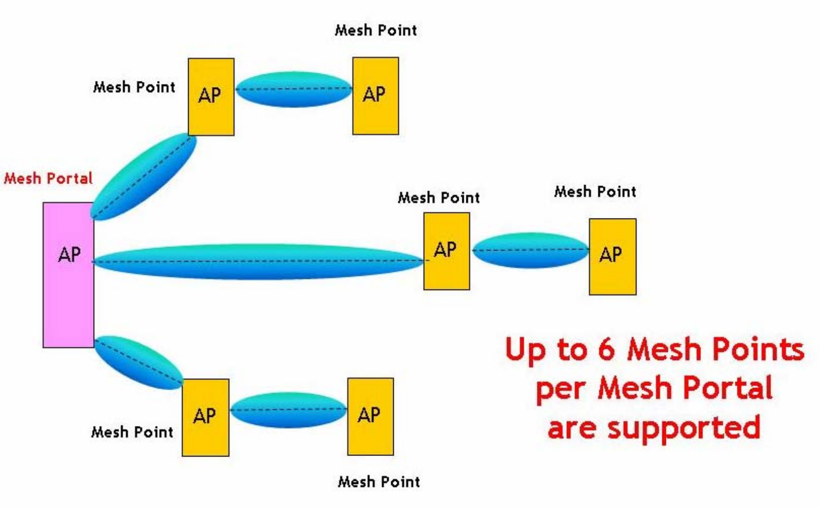


Figure 25: Third VoWLAN mesh rule

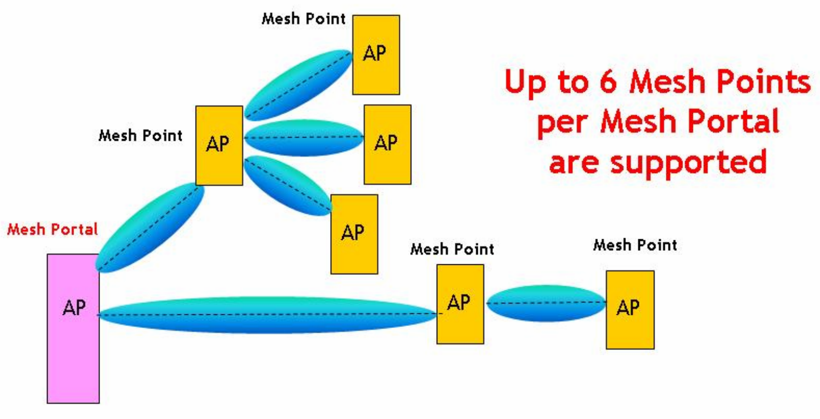


Figure 26: Combining VoWLAN mesh rules

All combinations are possible as long as the 3 rules are observed:
3 directions max, 2 hops max and up to 6 Mesh Points.

Warning: The Global call transit capacity of the Mesh Portal AP has to be shared between all Mesh Points

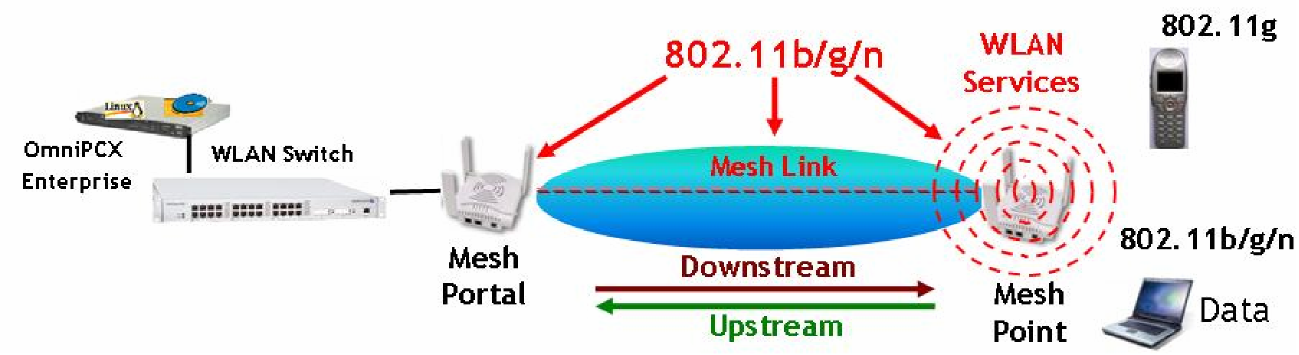
6.5. VoWLAN Mesh in 802.11n

802.11n is available for Mesh from AOS 3.4.0 for Backhaul and LAN Bridging solutions

802.11n Mesh can be based either on 802.11 a/n (5 GHz) or 802.11 b/g/n (2.4 GHz)

802.11n Mesh Backhaul can either use a single Radio for the both Mesh Link and WLAN services, or one Radio for Mesh Link and another radio for WLAN services

802.11n Mesh Benefit is throughput improvement. Following are some test results performed by Alcatel-Lucent validation.



Validation test results: Throughput in 802.11b/g/n

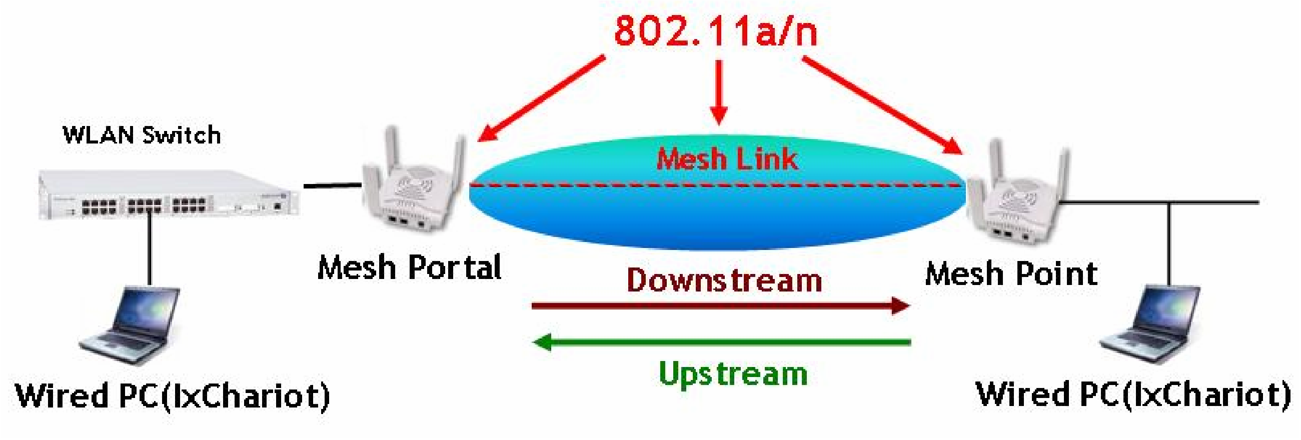
MIPT: 802.11g only/WPA2-PSK/WMM-AC

OXE: 12 MIPTs in conversation   Codec: G.711   Framing: 20ms

Radio: 802.11b/g/n on mesh link and 802.11b/g/n for WLAN services

Wireless PC: 802.11b/g/n (802.11g-HT)

Scenarios	TCP-Downstream	TCP-Upstream	UDP-Downstream	UDP-Upstream
Data traffic with 12 concurrent MIPT calls	13 Mbps	6 Mbps	5 Mbps	5.5 Mbps
Data traffic alone	28 Mbps	19 Mbps	20 Mbps	18 Mbps



Validation test results: Data throughput in 802.11 a/n

Radio: 802.11a/n on mesh link

Scenario	TCP-Downstream	TCP-Upstream	UDP-Downstream	UDP-Upstream
Data traffic alone	64 Mbps	52 Mbps	23 Mbps	22 Mbps

6.6. VoWLAN on AP85

AP85 is available for Voice over WLAN (MIPT) for the following topologies:

- Outdoor LAN-Connected AP
- Outdoor Mesh Backhaul
- Outdoor Mesh LAN bridging

AP85 can operate in 802.11a and 802.11bg simultaneously. On each radio 2 connectors are available in order to perform diversity.

6.7. 802.11n

6.7.1. Overview

802.11n is a standard supplement to increase the throughput in 2.4 GHz & 5 GHz radio bands in order to reach very high data rate up to 300Mbps. 802.11n technology is based on MIMO (Multiple-Input-Multiple-Output) technology that takes advantage of multipath effects.

MIMO is defined as MxN: e.g. 2x2, 3x3 and up to 4x4

M = number of transmit antennas   N = number of antennas at the receiver.

802.11n improves RF coverage of 30% when using 802.11n clients only and can run in 2.4 GHz and 5 GHz in 2 modes (40 MHz channel and 20 MHz channel. 802.11n is backward compatible with 802.11a/b/g (MIPT) but not at "n" speed.

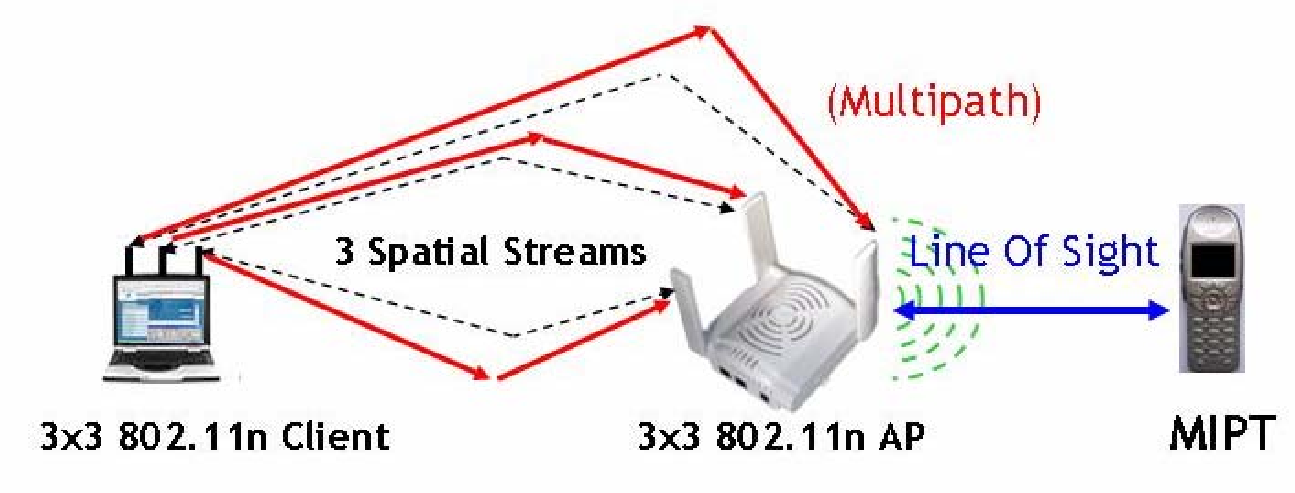


Figure 27: MIMO principle

This picture shows a 802.11n client that is associated to a 802.11n AP using a 3x3 MIMO mode and taking advantage of multipath reflections while the MIPT set can only support 802.11a or b/g , but not 802.11n. MIPT uses line of sight to reach the AP and uses diversity provided by this 802.11n AP.

6.7.2. 2.4 GHz channel aggregation for 802.11n

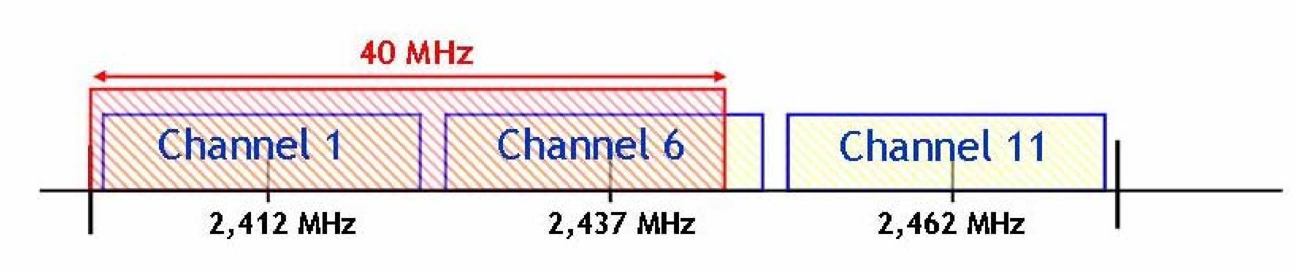


Figure 28: Channel aggregation in 2.4GHz

802.11n can operate either in 20 MHz or 40 MHz. Channel aggregation made of 2 channels is possible in 2.4 GHz (802.11 b/g /n) but makes the AP implementation difficult to avoid interferences between APs. As a reminder channels 1, 6 and 11 must not interfere. If channels 1 and 6 are aggregated in the same AP, the only remaining channel is 11, and it becomes difficult to ensure at the same time a correct coverage and avoid interferences between APs using the same channel number (i.e. channels 1 & 1, 6 &6 and channels 11 & 11).

6.7.3. 5 GHz channel aggregation for 802.11n

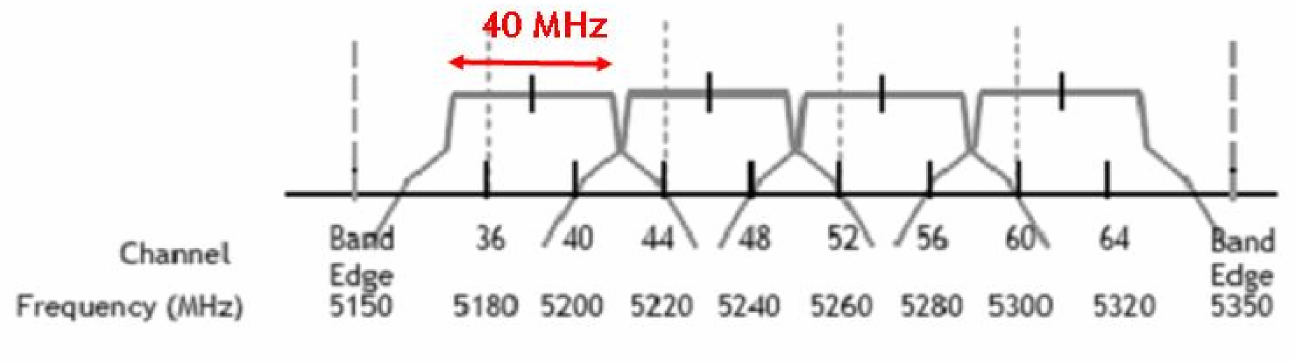


Figure 29: Channel aggregation in 5 GHz

5 GHz radio (802.11 a /n)offers many more channels making possible a 802.11n operation in 40 MHz (aggregation of 2 channels on the same AP). In this example 20 MHz channels 36 and 40 have been aggregated in order to create a 40 MHz channel.

6.7.4. MIPT interoperability between 802.11n and “Non n” APs

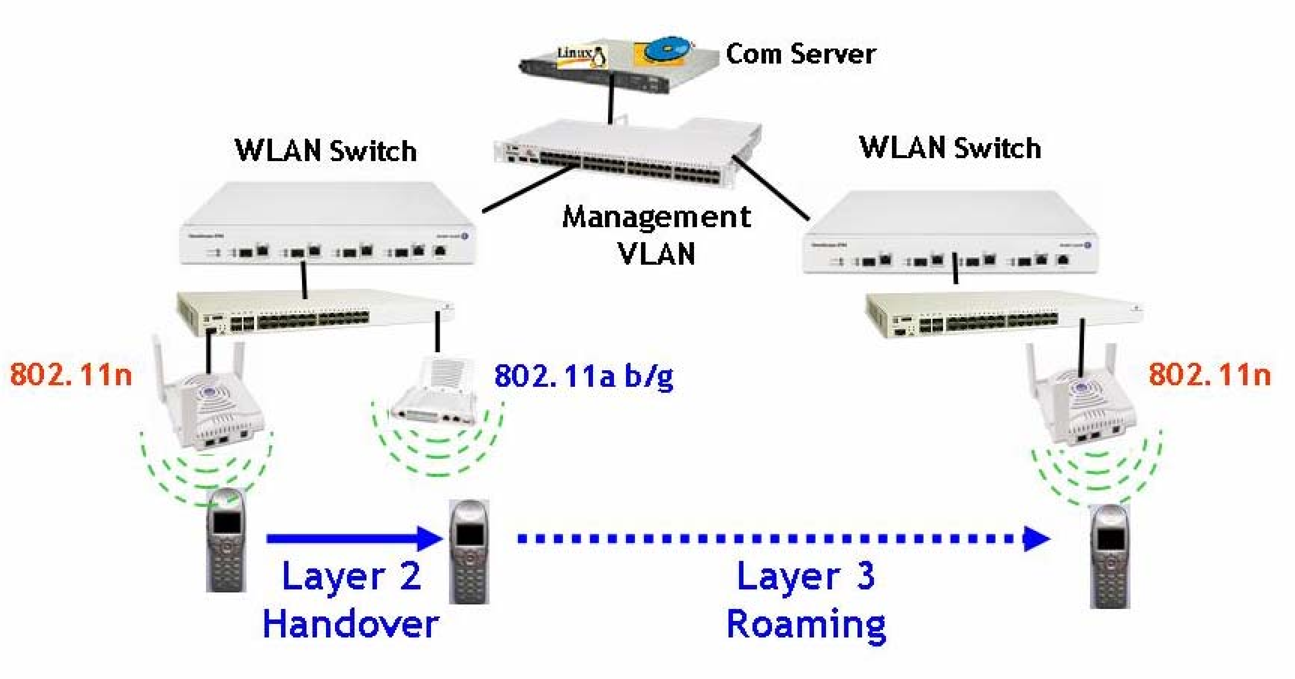


Figure 30: Interoperability 802.11n and 802.11a b/g

MIPT is not a 802.11n client and so does not support native 802.11n operation. Due to the fact that 802.11n AP is backward compatible with 802.11 a b/g, a MIPT set supporting 802.11 a b/g can interoperate with a 802.11n AP.

802.11n does not increase bandwidth for MIPT, because the MIPT still operates in 802.11a or b/g.

6.7.5. General Recommendations for a 802.11n Deployment

802.11n implementation should be a green field allowing fewer APs as long as all clients are native 802.11n.

Gigabit support is mandatory for AP Ethernet connection due to the larger bandwidth involved by MIMO operation and channel aggregation:

- GB Ethernet ports, GB Ethernet cabling, GB controller throughput

New access points to support 802.11n: AP120, AP121, AP124 & AP125

New power sources for 40MHz support (Dual-channel): PoE+ followed by 802.3at

New drivers may be involved: Driver maturity must be considered (Wireless clients)

New channel planning approach related to Channel Bandwidth: 40MHz instead of 20MHz (channel distribution).

6.7.6. MIPT Recommendations for a 802.11n Deployment

- MIPT sets are configured in 802.11a with a CAC limiting the quantity of simultaneous calls (about 8 calls -to be tuned-)
- Wireless PCs operate in 802.11 a/n
- Non-802.11n legacy wireless PCs if any, can be configured in 802.11g

Advantages:

- Due to the fact that 802.11a requires a slightly higher AP density for Voice coverage, it is not necessary to reach the full capacity of 12 simultaneous MIPT calls per AP. This keeps room for 802.11 a/n wireless PCs that can optimize AP throughput by using 40 MHz channel aggregation.

- Using 802.11a for MIPT avoids Bluetooth interference and 802.11g protected mode issue.

- Gigabit Ethernet ports with POE are required to feed the AP125s

- A Voice Site survey must be performed in 802.11a with a minimum available Received Signal Strength (RSSI)of **- 60 dBm**

6.7.7. VoWLAN Use Case in 802.11n

Purpose of this section is to describe an implementation scenario mixing WiFi customer needs in 802.11a, 802.11b/g and 802.11n.

In a recent past (before 802.11n) the recommendation was having Voice over WLAN (MIPT) in 802.11a and wireless data in 802.11b/g, provided the fact that dual-radio access points were deployed. Today 802.11n implementation modifies a little bit the rules.
Following is a scenario example:

6.7.7.1. Customer requirements (use case)

- Voice should be preferably in 802.11a (802.11b/g being currently used by legacy PCs)
- Legacy PCs in 802.11 b/g (about 50% of the total quantity of wireless PCs)
- 802.11n need for new PCs (about 50 % of the total quantity of wireless PCs)
- Customer R&D labs also uses 802.11a

6.7.7.2. Radio band allocation (use case)

- 802.11n can not be based on 802.11b/g (i.e. 802.11 b/g/n mode) in a deployment made of many adjacent APs, because only two channels remain available (the aggregated channel for 802.11n and the third available channel), resulting in interference occurrence between adjacent APs.

  The only possible choice is 802.11n based on 802.11a (i.e. 802.11a/n mode).

  Due to customer requirements, **Voice and Data clients must share the same 802.11a radio band.**
  As a result **the simultaneous voice call quantity per Access Point has to be limited** to about 6 or 7 calls (value to be tuned), in order to keep enough bandwidth for 802.11n data users.
  Voice & Data sharing on the same radio has a direct impact on the allowed density of voice/data users per AP.

  Note: *The alternative solution with Voice alone in 802.11b/g is not possible due to the legacy wireless PCs also working in 802.11b/g. This alternative solution (sharing Voice & data in 802.11 b/g) has not been retained by the customer.*

- Voice over WLAN (MIPT sets) must be configured in 802.11a
- 802.11n Data Wireless PCs must be configured in 802.11a/n
- Legacy Data Wireless PCs must be configured in 802.11g

- All 802.11a Access Points handling Voice over WLAN must use exclusively the four NON-DFS channels (Dynamic Frequency Selection) **ch 36, 40 ,44 and 48** to avoid Radar interference.
- In order to minimize interference risks between the existing customer R&D labs working in 802.11a and the new VoWLAN network also operating in 802.11a, customer R&D must use 802.11a channels that are out of these four first channels, **starting from channel 56 and upper** (in order to maintain a gap with VoWLAN channels).

6.7.7.3. Voice site survey (use case)

- A Voice site survey must be performed in 802.11a with a minimum RSSI level of **-60 dBm**.
- Floor maps for involved buildings must be provided and also the areas to be covered in WiFi
- Quantity of voice/data users per zone/area or room are also required.

6.7.7.4. Recommendations for the deployment (use case)

- Access Points must be visible (not hidden behind false ceiling)
- Staircases must be covered with access points
- Even if all users are expected to arrive in one shot, it is preferable starting the MIPT deployment in a first step with just a few targeted users to check the good operation with final tuning, and in a second step extend to all VoWLAN users.

6.8. Roaming and Handover

6.8.1. Roaming definition

Refers to the ability to be reached (ie: making and receiving calls) in a different Site or Network. Inside a site or a network, provides a wireless device the capability to associate to an AP after a power-on or a reset of this device.

6.8.2. Handover definition

Refers to the ability to move from one AP coverage area to another AP without service disruption or loss in connectivity.

6.8.3. Handover and Roaming restrictions

This table is a summary of roaming and handover capabilities according to the different VoWLAN topologies.

Roaming and handover capabilities are linked directly to the WLAN switch configuration:
- layer 2 or layer 3, and Single-WLAN switch or multi-WLAN switch

VoWLAN Topologies	Roaming	Handover
OXE Single-Node (Campus) WLAN switches in layer 2	**OK**	**OK**
OXE Single-Node (Campus) WLAN switches in layer 3	**OK**	**OK**
OXE Single-Node (WAN) WLAN switches in layer 3	**OK**	Not Applicable
O XE Multi-Node (WAN) WLAN switches in layer 3	Not Supported (except if no bandwidth restriction on WAN)	Not Applicable

MIPT Roaming between headquarter and a Remote Site is possible only if:
- There is enough bandwidth on WAN to ensure additional bandwidth involved by MIPT roamers
- The SSID and the encryption keys (WEP, WPA orWPA2) are the same between the Headquarter and the Remote Site.

6.8.3.1. Handover and Roaming in Layer 2 (Single or Multi-WLAN switch)

MIPT Layer 2 Handover and Roaming are supported on a single or a multi-WLAN switch topology

6.8.3.2. Handover and Roaming in Layer 3 (Single or Multi-WLAN switch)

MIPT Layer 3 Handover and Roaming are supported on a single or a multi-WLAN switch topology

Note: in the recent past, there was a Multi-Switch handover issue with AOS 3.3 and earlier releases when configured in layer3, CAC value on AP was not correctly decremented and incremented during a MIPT handover between 2 APs belonging to 2 different WLAN switches.

Layer 2 configuration solved the CAC issue, but did not allow the Firewall context to follow the MIPT during an inter-switch handover.

From AOS 3.4.0 Multi-Switch handover in layer 2 and layer 3 is supported

Note: Multi-switch layer 3 configuration is required when using Firewall rules on WLAN switches

6.9. G711 considerations

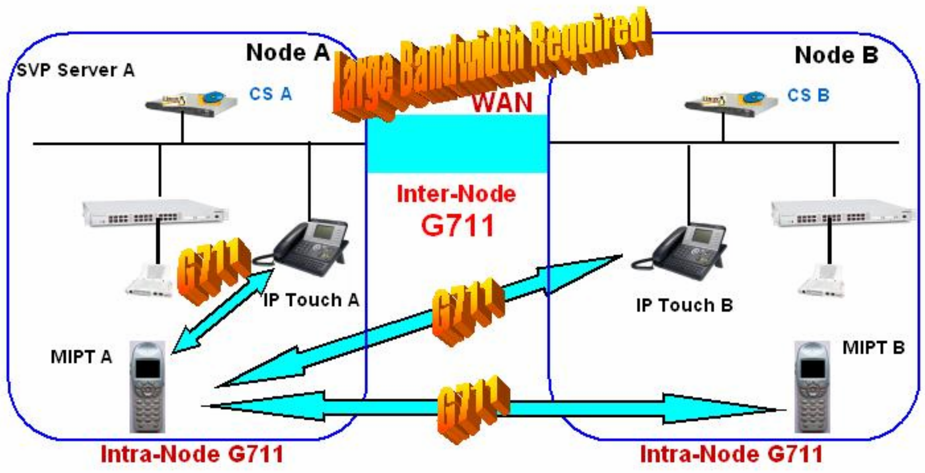


Figure 31: G711

This topology fully based on G711 does not contain any compression.
This configuration is supported but requires a large bandwidth on WAN (no Voice compression).
In this example G711 is permanently used whatever the call destination is (intra-node or extra-node).

6.10. G729 considerations

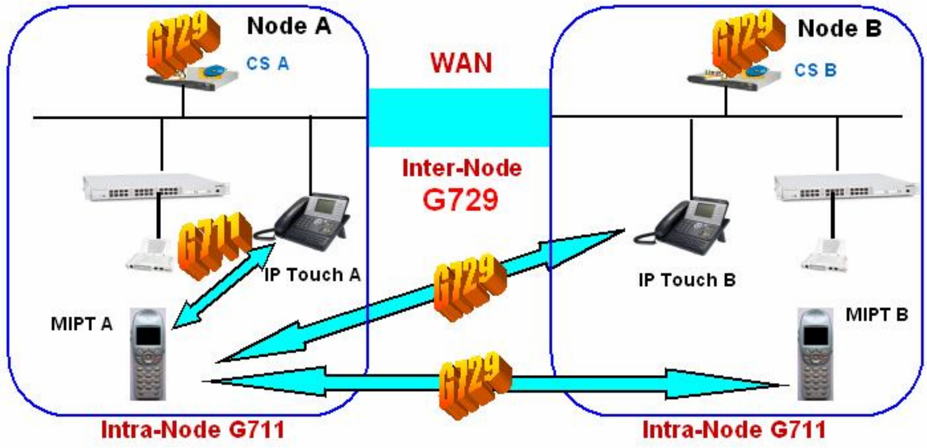


Figure 32: G729

This topology based on G729 allows compression on wan for MIPT 310/610 sets.
(MIPT set supports G711 and G729 only, but not G723). Generic rules:

- The OXE Network must be homogeneous in G729
- G729 must be set on all OXE nodes
- When compression is required (i.e. on WAN), G729 must be used by both MIPT & IP Touch sets.

6.11. Voice over WLAN Design Rules (Alcatel-Lucent WLAN infra)

Alcatel-Lucent MIPT 310 and MIPT 610 VoWLAN terminals support the following radios:

- 802.11b
- 802.11g
- 802.11a

No SVP server need

As a reminder legacy MIPT 300/600 are not supported without SVP server

6.11.1. Recommended AOS for VoWLAN

As part of VoWLAN 4.2.1 the AOS 3.4.1.1 has been used by validation.

Please check from BPWS the latest recommended AOS version to use for VoWLAN

6.11.2. G711 and G729A

Used in Multi-Site configuration (One Comm Server)
- G711 in Intra-domain and G729A in Inter-Domain (WAN)

Used in Multi-Node Configuration
- G711 in Intra-domain and G729A in Extra-Domain (WAN)

For more details about MIPT restrictions see Feature List and Product Limit for OmniPCX Enterprise 9.1.

6.11.3. Security

WEP (128 bits)
WPA (PSK with TKIP) Personal mode only
802.1X PEAP authentication is supported on MIPT wireless sets
WPA2 (PSK with AES) Personal mode only
802.1X PEAP authentication is supported on MIPT wireless sets).
WPA2 is supported on 802.11a and b/g

6.12. WLAN Licensing

Some important changes occurred in the way to apply WLAN licenses, depending on the type of WLAN switch family that is involved.

6.12.1. WLAN Licensing with Original WLAN switch Family (AOS 3.4.1)

6.12.1.1. Licenses Overview (Original Switch Family)

OAW-4324-XSC:	– xSec Module (48 AP License)
OAW-4324-VPN:	– VPN Server Module (48 AP License)
OAW-4324-WIP:	– Wireless Intrusion Protection Module (48 AP License)
OAW-4324-PEF:	– Policy Enforcement Firewall (48 AP License) **is Mandatory for VoWLAN**
~~OAW-4324-VOC~~:	– **VOC license is deprecated**, all Voice functionality is now integrated in PEF license

OAW-AP-MAPx:	– Outdoor Mesh Point License (x AP)
OAW-AP-RAPx:	– Remote access point software module (x AP)

Cumulated quantity of AP + MAP + RAP must not exceed switch capacity limit

OAW-4302	< or = 8
OAW-4304	< or = 4
OAW-4308	< or = 16
OAW-4324	< or = 48
OAW-6000 with Supervisor card 1	< or = 48
OAW-6000 with Supervisor card 1	< or = 128
OAW-6000 with Supervisor card 2	< or = 256

6.12.1.2. License Main Rules (Original Switch Family)

MAP and RAP

LAN-connected AP, MAP and RAP, each counts for 1 AP

Mesh Portal and Mesh Point count for 1 AP each

Redundancy

Licenses are also required on Redundant switch

6.12.1.3. License Calculation Example with OAW-4324

OAW-4324 has a capacity of 48 (LAN-connected) APs

48 LAN-connected AP, or 48 RAP, or 48 MAP

24 LAN-connected AP + 16 RAP + 8 MAP   (24 + 16 + 8 = 48)

Multiple possible combinations…

6.12.2. WLAN Licensing with New WLAN Switch Family (AOS 3.4.1)

6.12.2.1. Licenses Details (New Switch Family)

OAW-SSN-XSCx: – xSec Module License (x Sessions)

OAW-SSN-VPN: – VPN Server Module License (x Sessions)

OAW-USR-PEFx: – Policy Enforcement Firewall Module License (x Users) **is Mandatory for VoWLAN**

OAW-~~USR-VOC~~x: – **VOC license is deprecated**, all Voice functionality is now integrated in PEF license

OAW-AP-WIPx: – Wireless Intrusion Protection Module License (x APs)

OAW-AP-LAPx: – Access Point License (x APs)

OAW-AP-MAPx: – Outdoor Mesh Point License (x APs)

OAW-AP-RAPx: – Remote access point software module (x APs)

Cumulated quantity of LAP + MAP/4 + RAP/4 must not exceed switch capacity limit

OAW-4306	< or = 8
OAW-4306G	< or = 16
OAW-4306GW	< or = 16
OAW-4504	< or = 32
OAW-4604	< or = 64
OAW-4704	< or = 128
OAW-6000 SC3	< or = 512

6.12.2.2. License Main Rules (New Switch Family)

MAP

Rule 1: Each outdoor Mesh Portal or Mesh Point requires a MAP license

Rule 2: Additional LAP license is required if WLAN services is added to Mesh

- Mesh Portal doing WLAN services (local coverage in addition to mesh function)
- Mesh Point in LAN bridging and doing WLAN services (local coverage in addition to mesh function)

LAP MAP and RAP

While LAP counts for 1 (AP), MAP and RAP count for ¼ (AP) each

LAP is not included in Base OS

Redundancy

Licenses are also required on redundant switch

A common rule for New Switch Family Licensing:

As soon as a “User-based License” (PEF) is applied on WLAN switch, all involved (voice or data) wireless devices must be included in the license calculation.

6.12.2.3. License Calculation Example with OAW-4504

Here are non-exhaustive simple combinations:

32 LAP ---- 32 x 1 = 32 or 128 RAP -> 128 x ¼ = 32

or 128 Mesh (No WLAN services on Mesh Portal and on Mesh Point if LAN bridging)

---- 128 x ¼ = 32

or 16 LAP + 32 RAP + 32 MAP (LAN Bridging with No WLAN services on Mesh Portal and on Mesh Point)

---- (16 x 1) + (32 x ¼) + (32 x ¼) = 16 + 8 + 8 = 32

or 30 LAP + 1 RAP + Mesh Backhaul (1 Mesh Portal + 2 Mesh Points) with WLAN services on Mesh Portal (counts for 1 additional LAP)

---- (30 x 1) + (1 x ¼) + (3 x ¼) + 1 = 32

or 29 LAP + 2 RAP + Mesh LAN Bridging (1 Mesh Portal + 1 Mesh Point) with WLAN services on Mesh Portal and on Mesh Point (counts for 2 additional LAPs)

---- (29 x 1) + (2 x ¼) + (2 x ¼) + 2 = 32

6.12.3. WLAN License Rules Summary (Release Notes 3.4.0 & 3.4.1 extract)

VOC license is deprecated from AOS 3.4.1, all Voice functionality is now integrated in PEF license.

Voice Aware Scan feature is moved to the Base OS (from AOS 3.4.1).

IMP functionality—All Indoor Mesh functionality is now supported in the base OS and therefore does not require a separate license (from AOS 3.4.0).

ESI—All ESI functionality is now provided with in the PEF license. (from AOS 3.4.0)

6.12.3.1. WLAN License Interactions (from AOS 3.4.0)

The various licenses used to enable features in AOS-W do require some equity and other important interactions.

- AP/RAP and WIP must be equal. If the number of WIP AP licenses is less than the number of AP/RAP licenses, the number of AP/RAP licenses is reduced to equal the number of WIP licenses.
- All Alcatel-Lucent APs run WIP services, including RAPs.
- Mesh portals/mesh points with no virtual-APs do not consume WIP licenses.
- It is not possible to designate APs for WIP/non-WIP operations.
- Outdoor mesh points or mesh portals consume one mesh license.
- It is not possible to designate APs for WIP/non-WIP operations.
- If a mesh node is also configured for client service (i.e. advertises a BSSID), it consumes one AP license.
- RAPs consume only RAP licenses. AP licenses is not needed nor consumed for the normal operations of RAPs.

6.12.4. Roaming and Handover

Roaming and Handover are topology dependent (see chapter Roaming and Handover)and require:

- A common SSID
- Common Security rules to be applied to all WLAN switches
  (Same WEP key or WPA/WPA2 passphrase)

6.12.5. Converged Wireless Environments (Voice & Data Combinations)

One of the most significant reasons that businesses look to use wireless LAN technology to support voice is the desire to have a single infrastructure for both voice and data services. While this may at first sound like a very simple thing to implement, it often is far more complex to design than most customers originally anticipate. Alone, a VoWLAN environment has some challenges that must be overcome. Combined with a need to coexist with data client service, VoWLAN environments can face a tremendous amount of competition that requires special planning to minimize.

One of the major complexity factors faced during the design stage is the varied nature of the standards that can be used to support a data WLAN, and the affects each method has on voice quality and performance.

6.12.5.1. Voice alone on 802.11b

This implementation although possible has become obsolete due to the new capability of handling 802.11g and 802.11a radios on MIPT 310/610.

6.12.5.2. Voice & Data on 802.11g eliminating 802.11b (Shared AP & Bandwidth)

Sharing Voice and Data on the same radio (802.11g) minimizes the cost of implementation by using single radio Access Points (AP 60 or 61) but provided the fact that there is no 802.11b user sharing the same AP.

On the other hand choosing a single radio AP blocks a future evolution to a topology using concurrently the both radios (802.11a & 802.11g).

Nevertheless this implementation becomes fully relevant in countries or areas where local WLAN regulations do not allow 802.11a use.

Protected mode allows a 802.11b wireless device (using DSSS modulation) to recognize a 802.11g device as a real user participating in bandwidth sharing (and not just noise), by adding an extra header on 802.11g frame (OFDM modulation) that is understandable by an 802.11b user (the transmitting device should precede any OFDM transmission with a CTS frame).

MIPT wireless phones do not support “Protected mode”, so when sharing Voice and Data on the same AP, 802.11b Voice and data wireless devices must be forbidden.

Another factor to be considered is the fact that 802.11g uses 2.4 GHz radio that is prone to environmental noises (Bluetooth, microwave oven, etc.).

6.12.5.3. Voice on 802.11g, Data on 802.11a

This implementation is still possible but may be not fully adapted as many laptops and wireless PCs are still equipped with embedded 802.11g wireless cards.

6.12.5.4. Voice on 802.11a, Data on 802.11g

Because IEEE 802.11a utilizes the 5 GHz wireless spectrum that fits VoWLAN needs, it offers no direct radio competition to Data Wireless solutions that require use of the 2.4 GHz IEEE 802.11g realm. This is an ideal situation that offers the greatest benefit for both voice and data subscribers. As a result of the lack of frequency competition, Data wireless elements are free to utilize the full theoretical 54 Mbps of the IEEE 802.11g network. Congestion and competition is reduced or eliminated, resulting in the highest possible levels of service and voice quality.

This full separation of networks is also of great advantage to Voice subscribers to take benefit greatly from the density and coverage capabilities of the 10-13 non-overlapping channels (depending on local market restrictions) it makes available.

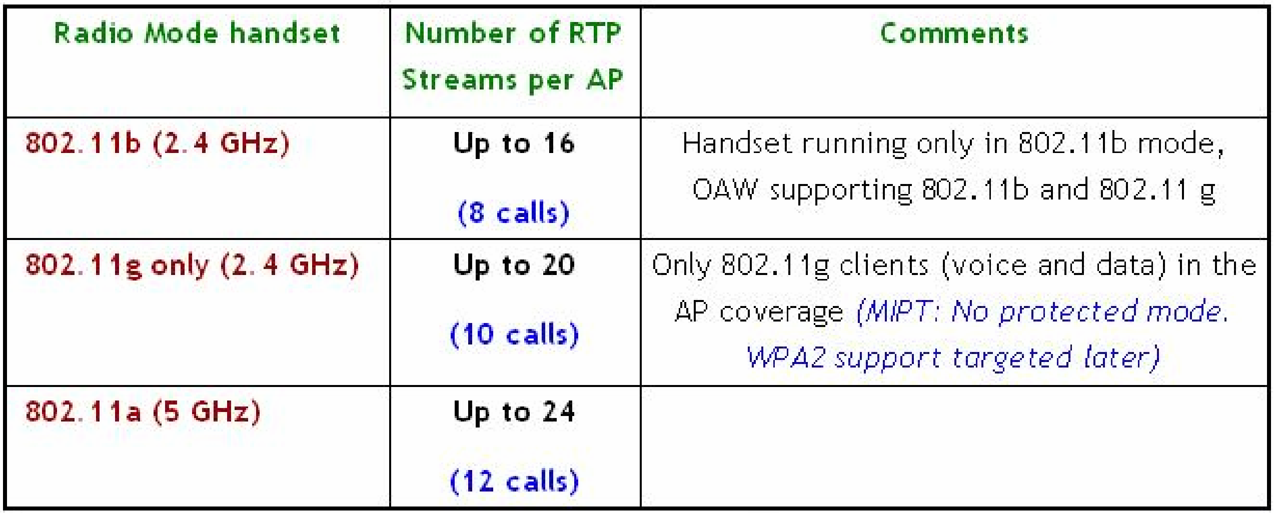
Customers seeking this type of solution can unify the infrastructure elements by using Alcatel-Lucent's OmniAccess product suite for both Wi-Fi formats. Alcatel-Lucent's OmniAccess 65 and 70 Access Point can be effectively leveraged to construct networks for both 2.4 GHz (802.11b/g) and 5 GHz (802.11a) networks simultaneously. For more detailed product information, visit : http://www.alcatel-lucent.com/wps/portal/enterprise.

Another advantage is the fact that there is no environmental interference from Bluetooth and microwave oven in 802.11a. In addition to that 802.11 b/g radio is more common on PCs than 802.11a.

On the other hand 802.11a radio may be prone to RADAR interference at 5 GHz (DFS, 802.11h) and might be not allowed by local law.

This implementation based on 802.11a for Voice and 802.11g for data remains, (when 802.11a is allowed), the most optimized VoWLAN solution in terms of bandwidth for Voice and Data users.

6.12.5.5. Simultaneous Calls per AP with a concurrent Data traffic of 5Mbps



Radio Mode handset	Number of RTP Streams per AP	Comments
802.11b (2.4 GHz)	Up to 16 (8 calls)	Handset running only in 802.11b mode, OAW supporting 802.11b and 802.11 g
802.11g only (2.4 GHz)	Up to 20 (10 calls)	Only 802.11g clients (voice and data) in the AP coverage *(MIPT: No protected mode. WPA2 support targeted later)*
802.11a (5 GHz)	Up to 24 (12 calls)	

This table shows the test results done with a concurrent Data traffic of 5 Mbps on the same Radio in each case (Bandwidth sharing between Voice and Data on 802.11b, 802.11g and 802.11a) .

6.12.5.6. Partially Overlapping Voice and Data Networks on 802.11b/g (isolated applicability)

In some cases, a customer may implement 802.11 g for voice and choose to restrict Wi-Fi data client access for security or productivity reasons. This same customer may decide that Wi-Fi data access is desirable in very specific and isolated environments (a shipping dock, cafeteria, large auditorium, etc.) For cost control and access flexibility the customer may desire to service these isolated data applications with IEEE 802.11b. This can present channel overlap challenges.

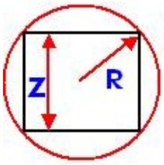
Similar situations can be encountered when a customer network closely neighbors another Wi-Fi environment. Hot-Spots, Cyber Café, or Wi-Fi radio propagation from the building across the street can all present direct channel competition. Due to the distinct channel selection options available, with careful planning it is usually possible to adapt to these types of network settings. Care must be taken to ensure that the data environment does not pose significant impact to the voice solution.

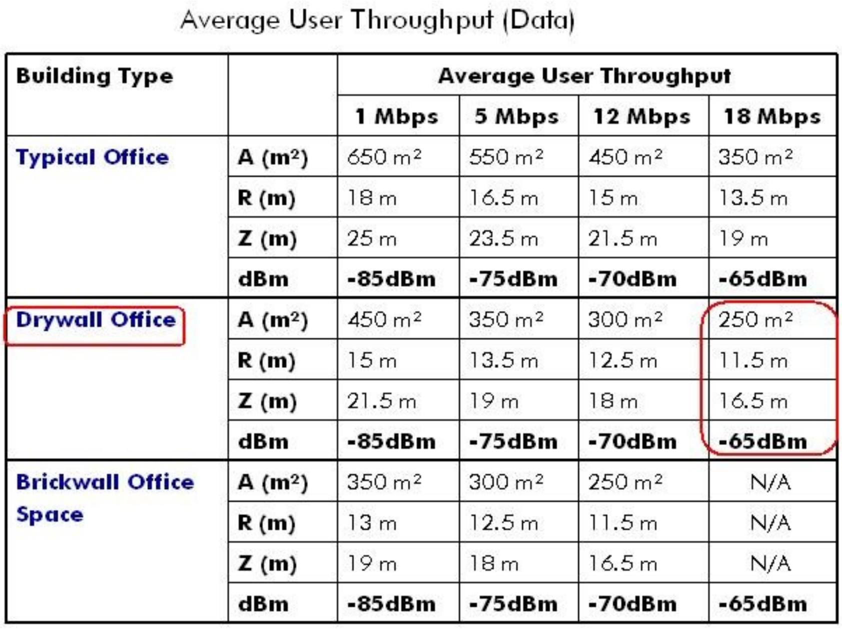
6.13. Predictive Environment Solution Options (Responding to RFx)

When answering an RFP or RFI, normally, there is little possibility of scheduling a Site Survey for various reasons: Building under construction or not yet built, short delay to answer the RFP, fair competition clause, etc. In these cases we can make a compromise between absolute accuracy of design and ease of offer presentation by trying to evaluate the user environment and theorize the required quantity of Access Points. It is essential to never forget to clearly indicate on the RFP, or unsolicited bid, that a compulsory Site Survey is required to verify the correct quantity of AP and their related locations.

6.13.1. Manual Calculation of Predictive Coverage

The following predictive method can be used to produce a budgetary design. Many environment variables like wave propagation, type of building, wall structure, interferences, etc. may, unexpectedly- affect the size quality, and complexity of the RF (Radio Frequency) coverage plan.





Average User Throughput (Data)

Building Type		Average User Throughput			
		1 Mbps	5 Mbps	12 Mbps	18 Mbps
Typical Office	A (m^2)	650 m^2	550 m^2	450 m^2	350 m^2
	R (m)	18 m	16.5 m	15 m	13.5 m
	Z (m)	25 m	23.5 m	21.5 m	19 m
	dBm	-85dBm	-75dBm	-70dBm	-65dBm
Drywall Office	A (m^2)	450 m^2	350 m^2	300 m^2	250 m^2
	R (m)	15 m	13.5 m	12.5 m	11.5 m
	Z (m)	21.5 m	19 m	18 m	16.5 m
	dBm	-85dBm	-75dBm	-70dBm	-65dBm
Brickwall Office Space	A (m^2)	350 m^2	300 m^2	250 m^2	N/A
	R (m)	13 m	12.5 m	11.5 m	N/A
	Z (m)	19 m	18 m	16.5 m	N/A
	dBm	-85dBm	-75dBm	-70dBm	-65dBm

Figure 33: User Throughput (type of Wall) for 802.11g

In the above chart:

R=”The coverage radius provided by an AP and is used to define a perimeter or radial-footprint.”
Z=”The coverage square contained within the perimeter(R).”
A=”The area of (Z^2) covered in square meters.”

For the following example (Drywall construction office building), use of the above defined calculation table results in an estimated bandwidth average of roughly 18 Mbps for data 802.11g Wi-Fi traffic. We can apply the same calculation strategy to VoWLAN simply by focusing on the performance of 802.11b at an estimated signal strength of -65dBm (target limit for voice.)

Calculating Access Point Quantity

- **Drywall building with a theoretical bandwidth of 18 Mbps for 802.11a (-65dBm)**
- **Determine Radius & Z factors: R=~11.5m Z=~16.5m Z²=~250m² (approximated with margin of error)**
- **Divide the building floor in rectangles and calculate the number of AP by dividing the area of each rectangle by Z²:**

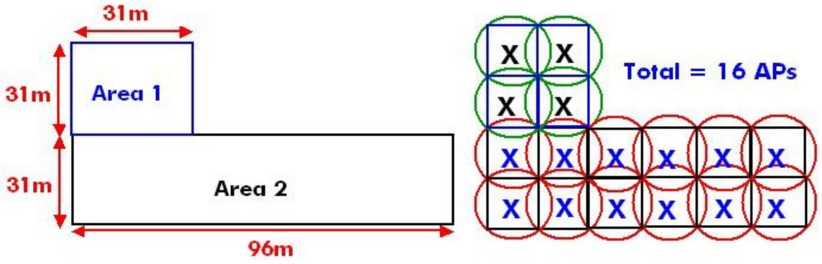
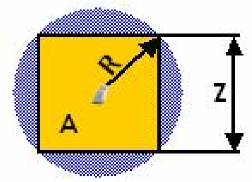


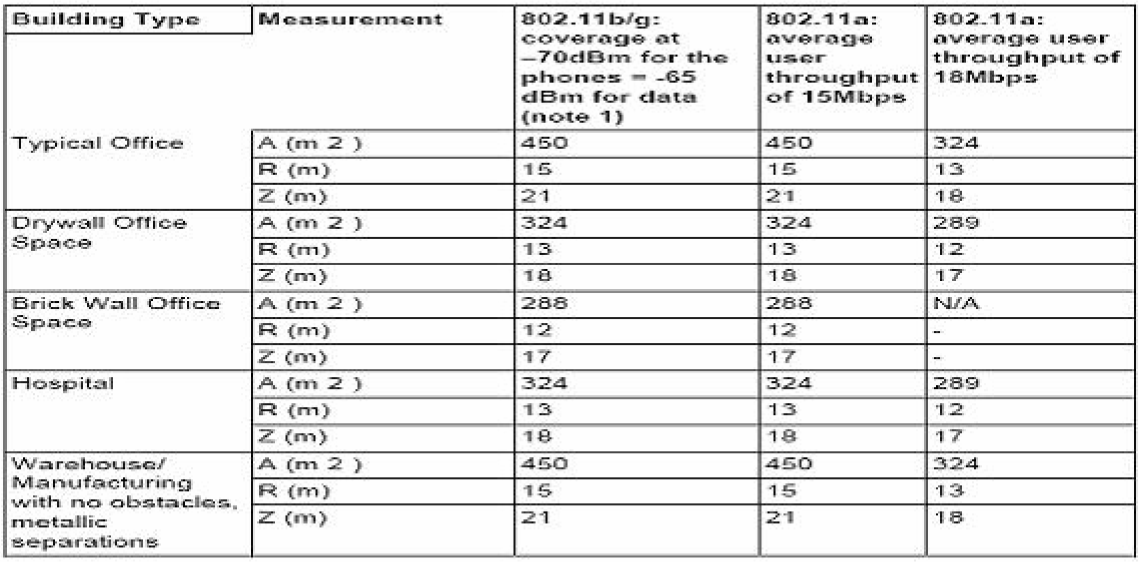
Figure 34: Predictive Method: AP Calculation

Example Results:
Area 1 => Quantity of AP = (31 x 31)/250 = 3.84 => 4 AP (rounded up to next highest whole number)
Area 2 => Quantity of AP = (31 x 96)/250 = 11.9 => 12 AP

Note: This calculation remains an approximation . Only a Voice over WLAN site survey can determine the exact quantity of APs to be installed in order to ensure a correct RF coverage.

6.13.1.1. Predictive Coverage chart example for 802.11 b/g and 802.11a





Building Type	Measurement	802.11b/g: coverage at –70dBm for the phones = -65 dBm for data (note 1)	802.11a: average user throughput of 15Mbps	802.11a: average user throughput of 18Mbps
Typical Office	A (m 2)	450	450	324
	R (m)	15	15	13
	Z (m)	21	21	18
Drywall Office Space	A (m 2)	324	324	289
	R (m)	13	13	12
	Z (m)	18	18	17
Brick Wall Office Space	A (m 2)	288	288	N/A
	R (m)	12	12	-
	Z (m)	17	17	-
Hospital	A (m 2)	324	324	289
	R (m)	13	13	12
	Z (m)	18	18	17
Warehouse/ Manufacturing with no obstacles, metallic separations	A (m 2)	450	450	324
	R (m)	15	15	13
	Z (m)	21	21	18

This chart provides additional indications about building coverage for 802.11b/g and 802.11a for data, but keeping in mind the RSSI levels required for Voice over WLAN

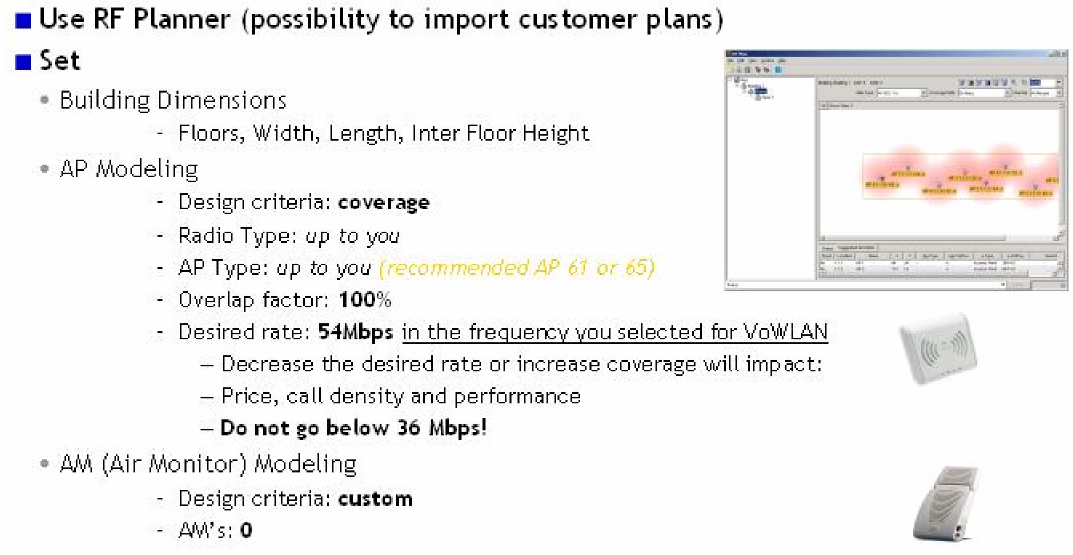
For more details see the chapter:

Required RSSI levels for a Voice Site Survey (VoWLAN)

6.13.2. Predictive Tool Coverage Planning

In the interest of easing predictive planning for large sites, or sites not yet fully constructed, several predictive coverage planning tools are available. These tools focus almost exclusively on the service requirements of 802.11 data clients with typical power and sensitivity specifications. It is for this reason that the use of predictive planning tools is not currently recommended by Alcatel-Lucent. Even in the case of Alcatel-Lucent's predictive planning tool, the unique operational characteristics of MIPT handsets can not be taken into full consideration, resulting in often flawed and under-engineered proposals. When the use of such tools is absolutely mandatory, it is recommended that a coverage plan of 160% or better be used in order to ensure proper plan overlap at the desired -65 dB level (802.11b). It is assumed that future versions of predictive coverage planning tools will be more accurate, and capable of calculating plans based on VoWLAN characteristics.

6.13.2.1. RF Planner (available from BPWS)



- Use RF Planner (possibility to import customer plans)
- Set
  - Building Dimensions
    - Floors, Width, Length, Inter Floor Height
  - AP Modeling
    - Design criteria: **coverage**
    - Radio Type: *up to you*
    - AP Type: *up to you* *(recommended AP 61 or 65)*
    - Overlap factor: **100%**
    - Desired rate: **54Mbps** in the frequency you selected for VoWLAN
      - Decrease the desired rate or increase coverage will impact:
      - Price, call density and performance
      - **Do not go below 36 Mbps!**
  - AM (Air Monitor) Modeling
    - Design criteria: **custom**
    - AM's: **0**

The offline RF Plan application provides tools for pre-deployment RF planning. RF Plan allows you to determine access point placement based on your specified coverage and capacity requirements without impacting the live network. Using this tool, you can design new wireless network areas, such as campuses, buildings, and floors, and enter settings to provision and connect access points (APs) and/or air monitors (AMs) within the areas. This tool does not incorporate VoWLAN requirements but is helpful for a first approach on AP placement (building not existing yet, working from maps, etc.).

7. Environment Verification & Validation

After collecting information on the customer data networking environment from both a logical and physical perspective, and evaluating the customer voice communications needs; it becomes important to verify and validate the collected information. These operations are not meant to be insulting to a customer or business partner, nor are these practices meant to be “revenue generation” tactics. The processes outlined below are incredibly important steps required to ensure customer satisfaction and to provide for baseline references for support contracts and service level agreements.

7.1. Compliance with VoWLAN Offer

As previously stated, the MIPT VoWLAN solution offer is being delivered in a multi-stage format. Proposed designs must be built with a clear knowledge and respect for the present offer restrictions. For example, networking criteria should be carefully analyzed. Please ensure that the proposed solution does not violate the list of restrictions provided in section Voice over WLAN Design Rules above.

7.2. Pre Install VoWLAN Radio Coverage Audit (Site Survey)

It s recognized that in many situations, a customer may be unwilling or unable to perform a wireless audit before the establishment of budgetary costs (RFP/RFQ.) Regardless of whether or not predictive tools were used to define a “budgetary” topology design, a Radio Coverage Audit (also known as a Site Survey) is mandatory for all MIPT VoWLAN solutions prior to installation. Voice quality and coverage continuity can not be guaranteed without this compulsory environmental evaluation.

In ideal situations, this audit would be performed as the first step towards building a VoWLAN solution. The results of the audit could be used to strategically identify ideal locations for Access Points to maximize coverage and minimize radio spectrum conflict. By working backwards from the Access Points, we could easily see where best to place and how best to size Wireless Switches and/or Wireless Appliances.

VoWLAN Radio Coverage Audits are very specific in that they focus on the requirements of 802.11b, g or a based wireless clients. Being small, handheld, battery operated devices; Mobile IP Touch terminals possess unique radio sensitivities. Where a typical Wi-Fi enabled PC could find the ability to maintain a useful connection with a signal as weak as -80dBm, MIPT terminals lose reliable communications capabilities beyond (approximately) -65dBm in 802.11b. It is for this reason that typical Wi-Fi surveys, as well surveys for other digital wireless technologies, can not be used for VoWLAN solutions. Again: A VoWLAN Radio Coverage Audit is mandatory for all solutions prior to installation.

Alcatel-Lucent’s OmniAccess platform family can be used to support data as well as voice. For solutions that propose both voice and data coverage, it is important to distinguish between the needs of the voice and data elements. If voice and data are to share 802.11b/g Access Points, bandwidth consumption and client saturation need to be incorporated into the overall audit results. If the data will utilize 802.11a Access Points, a completely different wireless audit may be required.

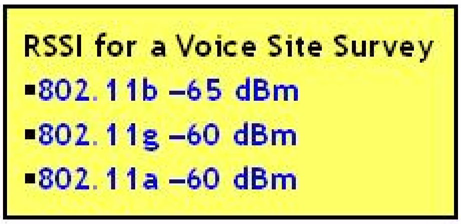
The specificity of VoWLAN audits requires a certain level of solution specific training and knowledge. For the benefit of Alcatel-Lucent customers and business partners, Alcatel-Lucent’s Professional Services organization can provide VoWLAN and WLAN Radio Coverage Audits at a competitive price. For more details on this service, please contact Alcatel-Lucent Professional Services.

7.3. Post Install Survey

Wireless networks are often changing to meet new application demands, business processes, or in response to external influences (neighboring networks and other spectrum disturbing sources.) For this reason, Alcatel-Lucent recommends regular radio coverage surveys in order to continuously revalidate system operation. This is not a mandatory process, but a recommended one as proactive network modification is often less costly and disruptive than reactionary engineering to sudden holes or degradations in the RF coverage plan.

The regularity by which a customer should consider RF coverage re-evaluation depends greatly on network size, radio spectrum competition, sensitivity to degraded voice quality, rate of user population growth, and other factors. As a general rule, Alcatel-Lucent recommends re-evaluation whenever new technology demand is generated or roughly every 18 months. Some customers may be able to happily use VoWLAN technology in a static environment for many years without a renewed survey, others may find that continuous evolution of network demands require a validation every six months. It is recommended to set proper customer expectations before they decide to implement VoWLAN technology.

7.3.1. Required RSSI levels for a Voice Site Survey (VoWLAN)



RSSI for a Voice Site Survey

- 802.11b –65 dBm
- 802.11g –60 dBm
- 802.11a –60 dBm

Here are the RSSI (Received Signal Strength Indication) levels to be applied when doing a Voice Over Wireless LAN Site Survey. Note that a stronger level (-60 dBm or better) is required for MIPT operation
in 802.11a and 802.11g.

These above RSSI levels related to 802.11b, 802.11g and 802.11a must be applied when doing a Voice over WLAN site survey.

7.4. ALU Professional Services Offer

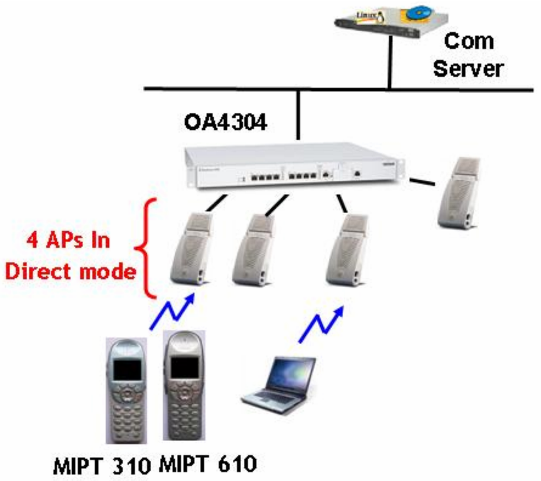
Specific service offer is available from ALU Professional Services to provide a Voice Site Survey with on-site deployment of Access Points (accurate positions resulting from the Site survey) and also WLAN switch configuration.

Send your request to: Professional.Services@alcatel-lucent.com

8. Design Examples

8.1. Configuration for up to 4 AP & 8 AP (Demo & small area coverage)

This configuration example depicts a model well adapted to a Demo context for up to 4 AP without a customer need for WLAN controller redundancy.



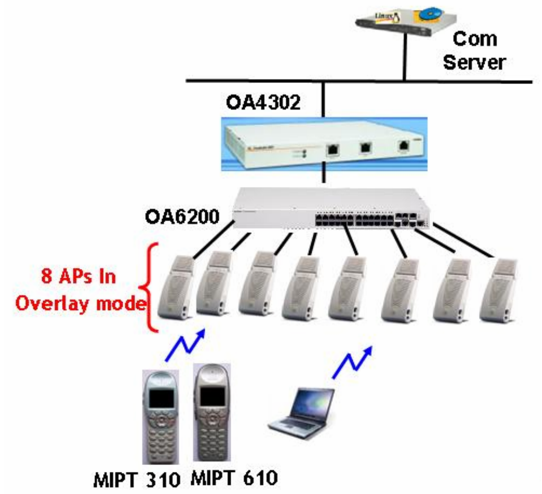


Figure 35: Config for up to 4 AP (no redundancy)

Figure 36: Config for up to 8 AP (no redundancy)

8.2. Configuration for up to 16 AP (No redundancy)

This example depicts a model for up to 16 AP without a customer need for WLAN controller redundancy.

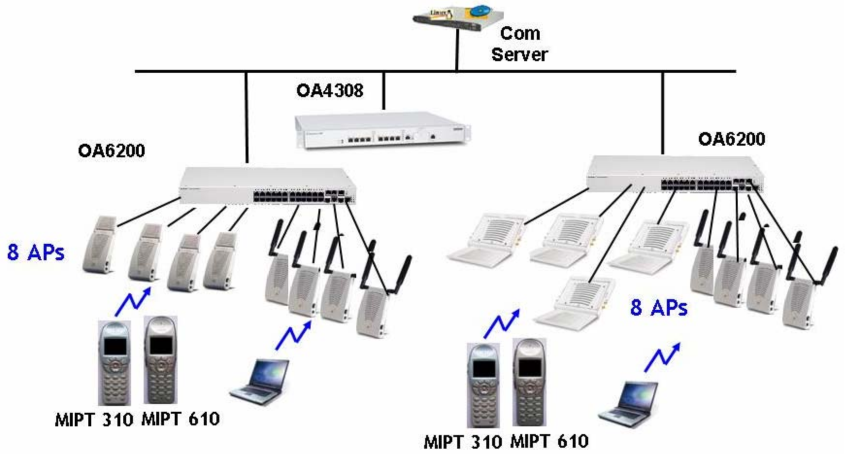


Figure 37: Configuration for up to 16 AP (no redundancy)

Depending on needed bandwidth a Fast-Ethernet port or a Gigabit port can be used to join LAN.

8.3. Configuration for up to 16 AP (with redundancy)

This example depicts a model for up to 16 AP with WLAN controller redundancy.

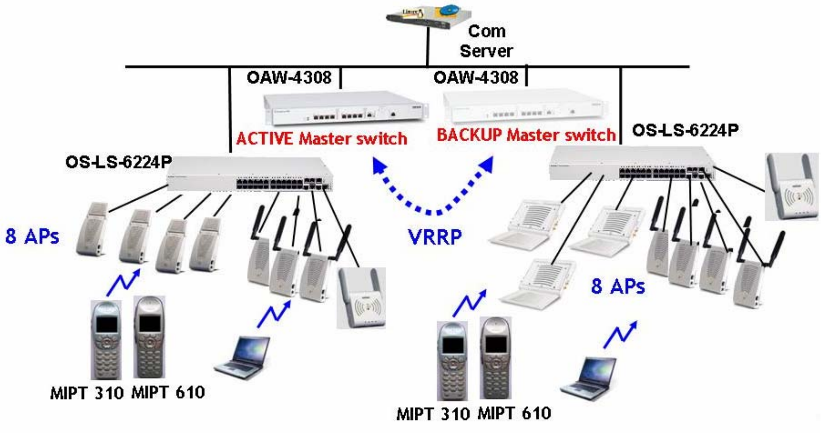


Figure 38: Configuration for up to 16 AP (with redundancy)

In this scenario, the backup process takes place between the 2 WLAN Switches OA4308. In order to insure a full backup, the total quantity of AP must not exceed the maximum number of AP supported by one OmniAccess 4308. Depending on the global Bandwidth a Gigabit port can be used on both OA4308.

Note: The backup Master switch does not manage any Access point as long as the active Master switch is operational (no AP load balancing)

8.4. WLAN Switch Redundancy

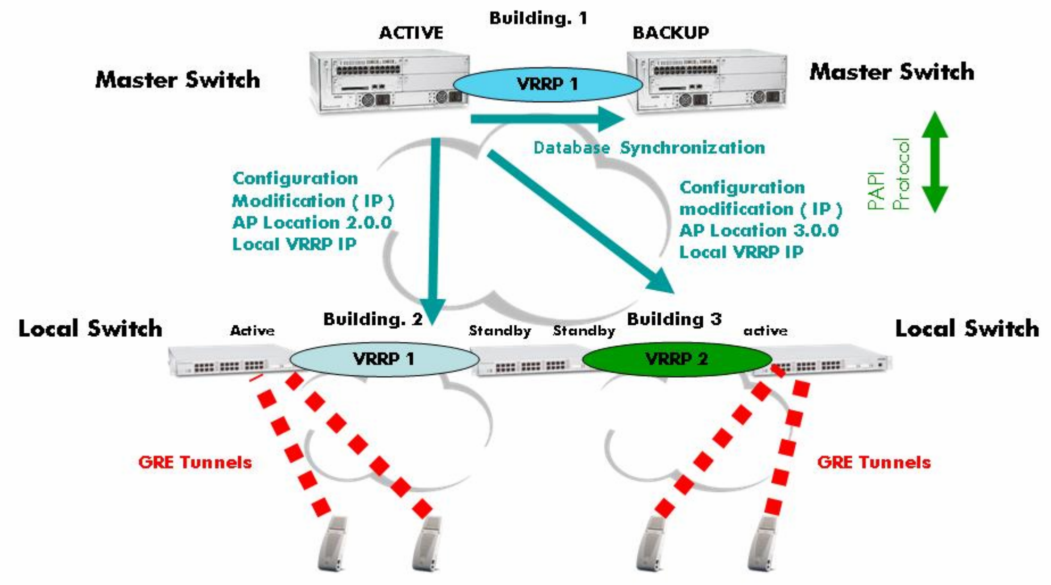


Figure 39: WLAN Redundancy (VRRP)

8.4.1. Master Switch Redundancy (Active-Backup only) based on VRRP

Active Master switch and Backup Master switch must be both in the same IP subnet due to VRRP operation. Same consideration for the Active Local switch and the Standby Local switch that must be both in the same IP subnet (VRRP).

Note: Active-Active redundancy is not supported on Master switch

8.4.2. Local Switch Redundancy (Active-Standby) based on VRRP

The Active and Standby WLAN switches must be both part in the same IP subnet to ensure VRRP operation. A “1 to n” redundancy is also possible for Local WLAN switch as showed on the above picture.

8.4.3. Local Switch Redundancy (Active-Active) based on VRRP

Another alternative is the Active-Active redundancy mode for Local switch (VRRP).

In this model both the OmniAccess WLAN switches are serving access points and clients in the normal mode of operation. Each switch acts as a backup for the access points and clients on the other switch. This places some restrictions on the load that can be placed on each switch (when both are active) to ensure that each of the switches can still serve the total number of access points and users in a failure scenario.

8.4.4. WLAN Redundancy with Local Mobility Switch (LMS)

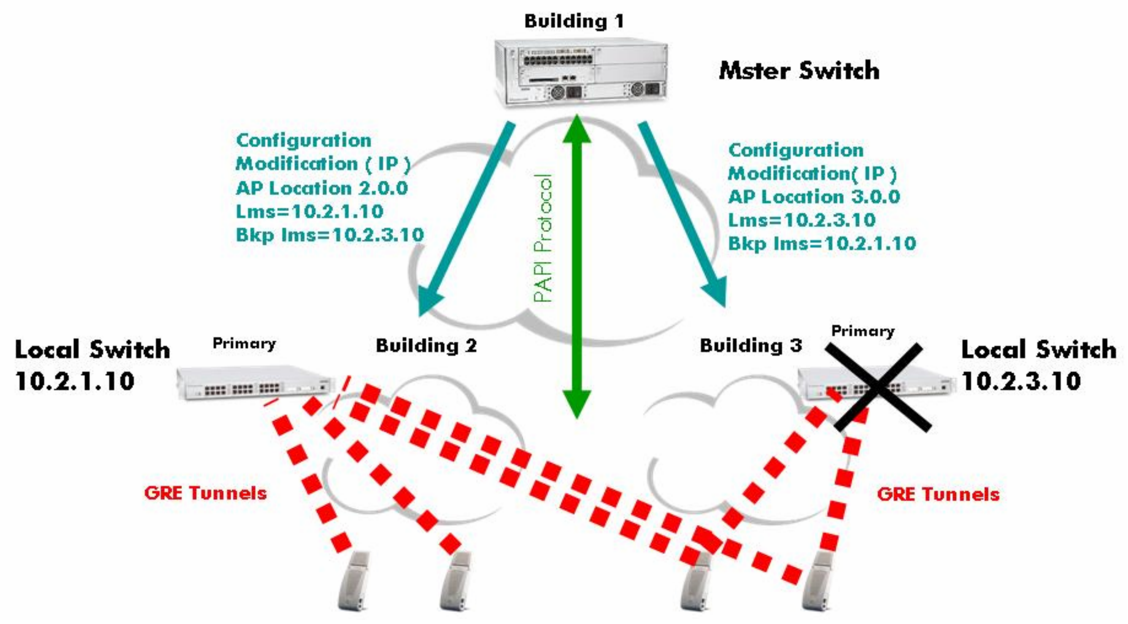


Figure 40: WLAN Redundancy with LMS

LMS-IP/BACKUP-LMS-IP
Each access point is managed by an OmniAccess WLAN mobility controller/switch. This switch is then called the “LMS” (Local Mobility Switch) for this access point and the IP address used by the access point to connect to is referred to as the “LMS-IP”. It is also possible to specify the IP address of a different switch that the access point can connect to if it is unable to connect (or loses its connection) to the “LMS”. This IP address is referred to as the “Backup-LMS-IP”.

This solution allows having the both Local WLAN switches in different IP subnets, but is not so efficient as redundancy solutions based on VRRP. This LMS solution should be used as a spare solution when VRRP cannot be used (local switches being in different IP subnets.

8.4.5. Local WLAN Switch operation in case of Master WLAN Switch Failure

In case of Master WLAN Switch failure, a Local WLAN can continue to operate but with limited capabilities:

- No possibility to modify the Local switch configuration
- If an Access Point is turned off or disconnected from Local switch it can not boot anymore
- 802.1X authentication cannot be applied to new users on Local switch even if there is a local Radius server.
- A Local WLAN switch reboot leads to a total loss of all attached Access Points

Just to highlight the fact that a Master WLAN Switch redundancy is recommended

8.4.6. Alcatel-Lucent Recommended Solutions for WLAN Redundancy

Even though the LMS solution (in different IP subnets) may be applicable in some cases Alcatel-Lucent recommends using the WLAN redundancy solutions based on VRRP.

9. Quotes & Orders

Unfortunately, the quotation process for the Voice over WLAN solution is not fully automated within ACTIS as many of Alcatel-Lucent's other voice technologies. For this reason, engineers are strongly encouraged to complete the framework of the target VoWLAN design prior to beginning the ACTIS process. All hardware components must be manually selected from the VoWLAN SERVERS and IP MOBILE SETS menus (within Mobility Others page.)

Design engineers should pay special attention during the quotation process to insure that necessary items are not accidentally omitted. For instance, an MIPT subscriber is not complete with a terminal, battery, charging stand, charging stand power plug, and some form of clothing attachment. Each of these items must be selected separately within ACTIS (or in bundle package combination.) Infrastructure items are no less attention demanding. Design engineers should pay special attention to power cords, uplinks options, and mounting hardware.

Since Wi-Fi networks are constantly evolving environments, Alcatel-Lucent recommends that customers seriously consider the deployment of Access Points capable of supporting IEEE 802.11a, IEEE 802.11b/g as well as IEEE 802.11n. Alcatel-Lucent also recommends that a measurable portion of Access Points deployed within the framework of most solutions be capable of supporting external antenna connection. The nominal increases in cost that these options may bring to a solution should be viewed as very inexpensive insurance against unforeseen future needs.

For more detailed information on the QUOTING process for VoWLAN solutions, refer to VoWLAN section of the PreSales Presentations:

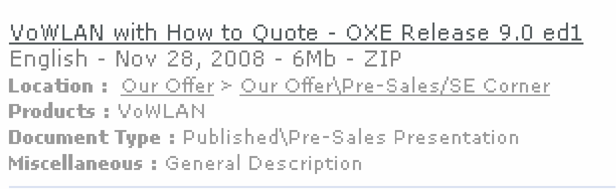
10. Reference Documents

The documents related to the MIPT VoWLAN solution can all be found on the Business Partner Web Site. Here are the related links:

10.1. VoWLAN section of the PreSales Presentations:

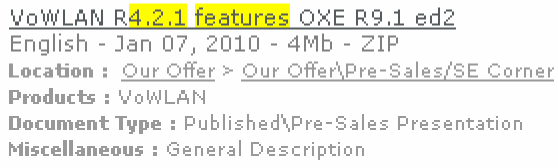
BPWS Path:

- KD_13_VoWLAN_Features_R4-1 OXE_9-0_ed2.ppt (includes How to Quote section)



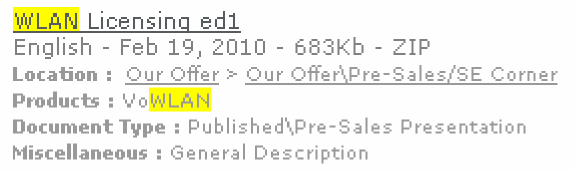
VoWLAN with How to Quote - OXE Release 9.0 ed1
English - Nov 28, 2008 - 6Mb - ZIP
Location : Our Offer > Our Offer\Pre-Sales/SE Corner
Products : VoWLAN
Document Type : Published\Pre-Sales Presentation
Miscellaneous : General Description

- KD_14_VoWLAN_Features_R4-2-1_OXE_9-1_ed2



VoWLAN R4.2.1 features OXE R9.1 ed2
English - Jan 07, 2010 - 4Mb - ZIP
Location : Our Offer > Our Offer\Pre-Sales/SE Corner
Products : VoWLAN
Document Type : Published\Pre-Sales Presentation
Miscellaneous : General Description

- KD_15_WLAN_licensing_ed1

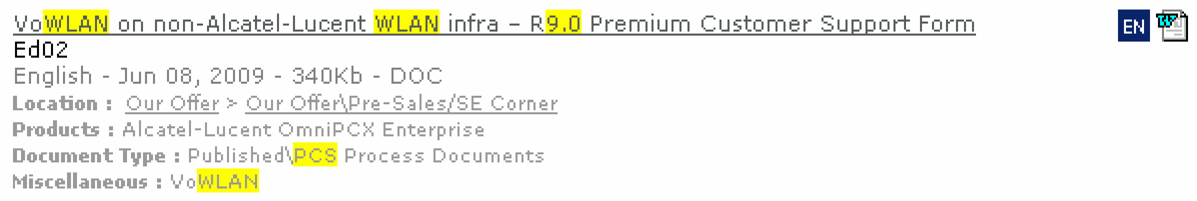


WLAN Licensing ed1
English - Feb 19, 2010 - 683Kb - ZIP
Location : Our Offer > Our Offer\Pre-Sales/SE Corner
Products : VoWLAN
Document Type : Published\Pre-Sales Presentation
Miscellaneous : General Description

10.2. VoWLAN section of the PCS Process (non-Alcatel-Lucent WLAN infra):

BPWS Path:

- VoWLAN PCS Process Information Form

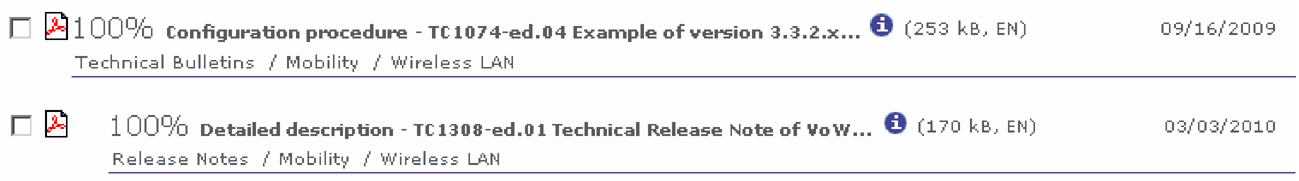


VoWLAN on non-Alcatel-Lucent WLAN infra – R9.0 Premium Customer Support Form EN
Ed02
English - Jun 08, 2009 - 340Kb - DOC
Location : Our Offer > Our Offer\Pre-Sales/SE Corner
Products : Alcatel-Lucent OmniPCX Enterprise
Document Type : Published\PCS Process Documents
Miscellaneous : VoWLAN

10.2.1. Multi-Vendor section for compatibility:

- http://www.spectralink.com/consumer/resources/wifi_compatibility.jsp

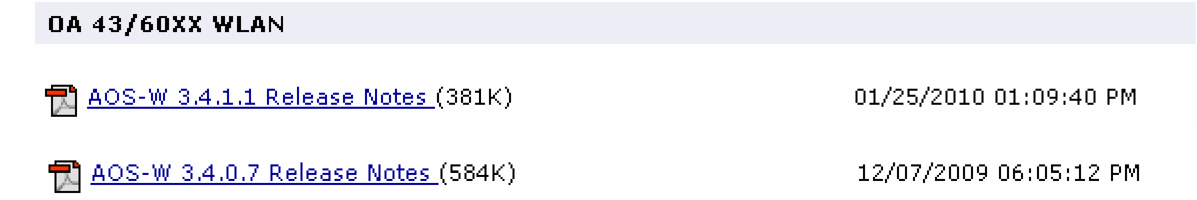
10.3. Technical Knowledge base (Technical Communications)



□ 100% **Configuration procedure** - **TC1074-ed.04 Example of version 3.3.2.x...** (253 kB, EN) 09/16/2009
Technical Bulletins / Mobility / Wireless LAN

□ 100% **Detailed description** - **TC1308-ed.01 Technical Release Note of VoW...** (170 kB, EN) 03/03/2010
Release Notes / Mobility / Wireless LAN

10.4. Release Notes (AOS)



OA 43/60XX WLAN

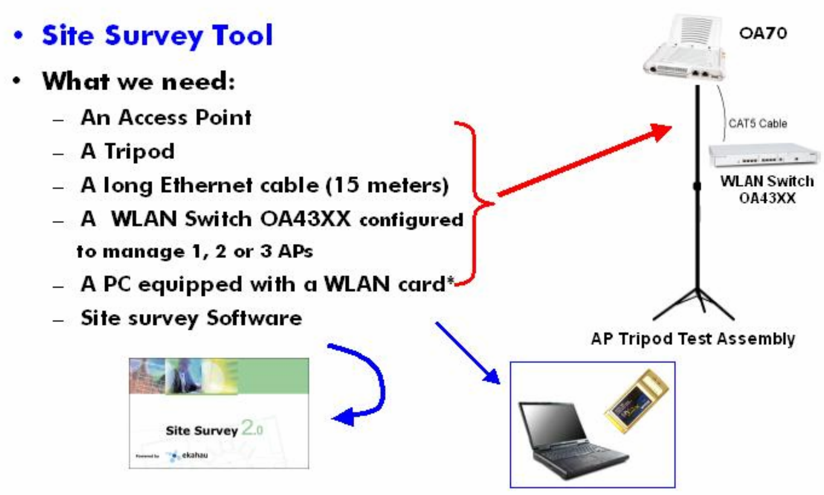
AOS-W 3.4.1.1 Release Notes (381K)	01/25/2010 01:09:40 PM
AOS-W 3.4.0.7 Release Notes (584K)	12/07/2009 06:05:12 PM

11. Annex

11.1. Site Survey Tool

•The Site Survey Tool is a portable engineering tool for measuring and monitoring the air interface of Wireless Local Area Networks (IEEE 802.11). This Tool helps to determine:

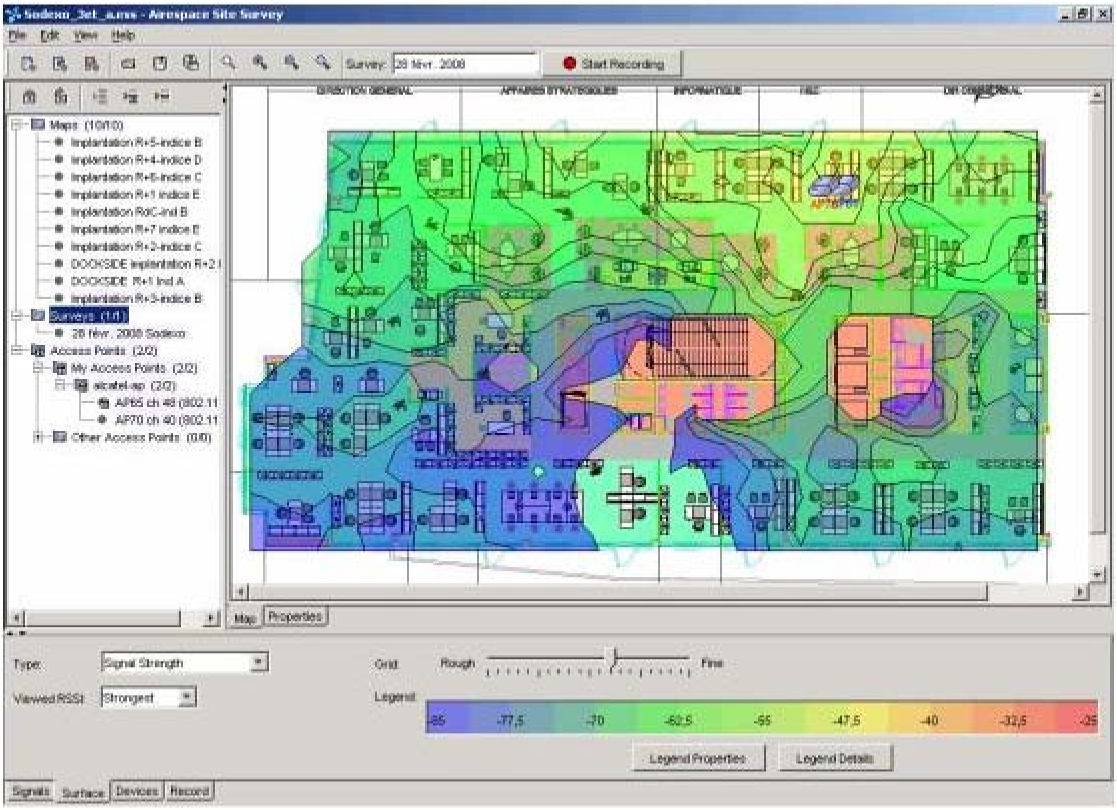
- The quantity of needed Access points
- The correct placement for these Access Points



- Site Survey Tool
- What we need:
  - An Access Point
  - A Tripod
  - A long Ethernet cable (15 meters)
  - A WLAN Switch OA43XX configured to manage 1, 2 or 3 APs
  - A PC equipped with a WLAN card*
  - Site survey Software

Figure 41: Site Survey components

The Site Survey tool is mainly used by Alcatel-Lucent Professional Services and Business Partners. A site Survey is required every time it is needed to perform a quotation for VoWLAN implementation. A VoIP audit is also necessary. A WLAN Switch OA4304/08, OA4324 or OA6000 is needed to manage and feed 1, 2 or 3 APS (Chan 1 , 6 and 11 being configured in manual mode). WLAN adapter must be compliant with Survey Soft



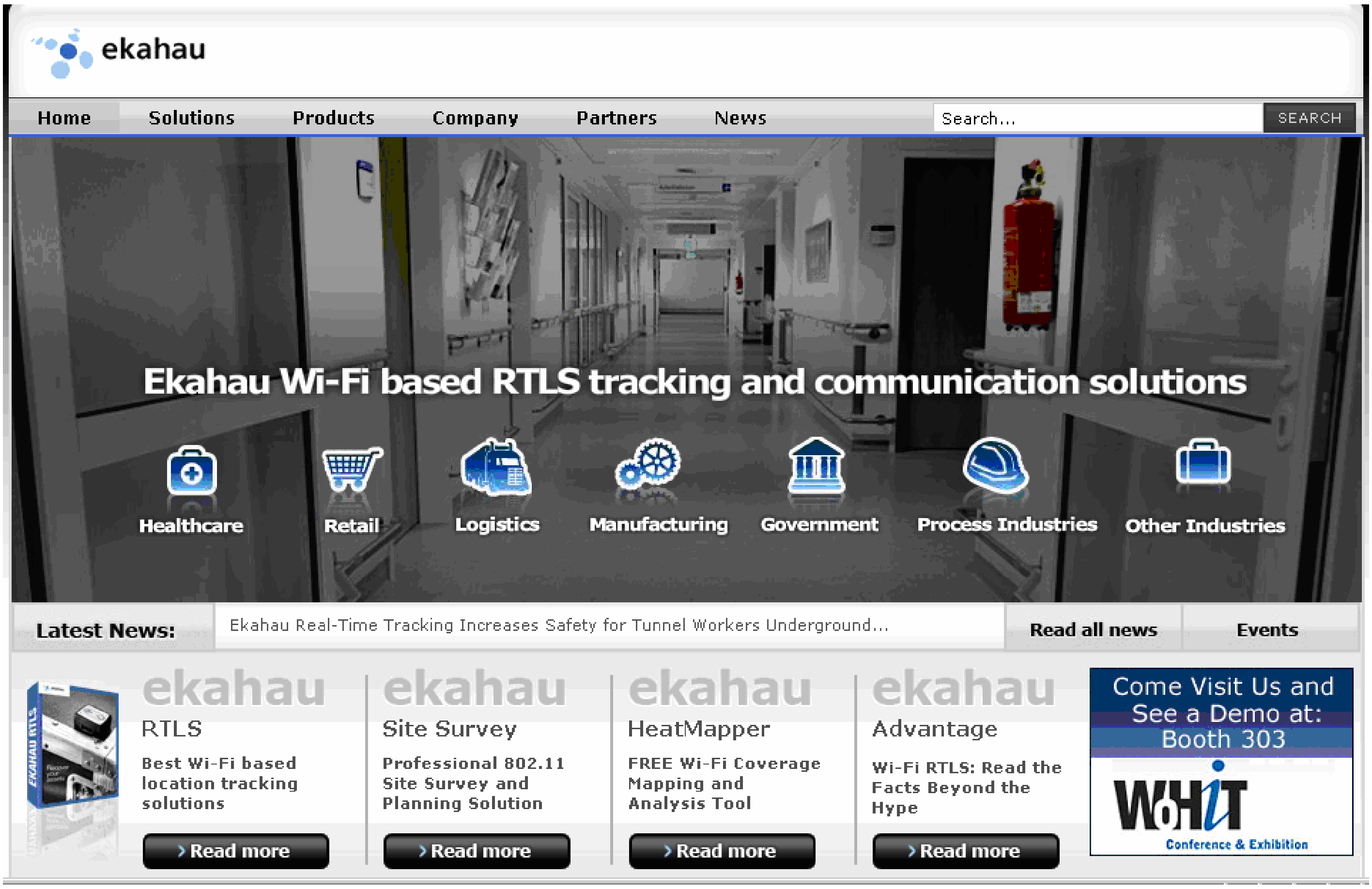
Type: Signal Strength

Viewed RSSI: Strongest

Figure 42: Survey Result

The above picture shows a site survey result done in 802.11a. Just compare the color to the scale. The Target is to obtain a signal strength of **-60 dBm** or better required for MIPT set operation.

11.2. Site Survey Tool Example



ekahau

Home | Solutions | Products | Company | Partners | News | Search... | SEARCH

Ekahau Wi-Fi based RTLS tracking and communication solutions

Latest News: Ekahau Real-Time Tracking Increases Safety for Tunnel Workers Underground... | Read all news | Events

ekahau RTLS
Best Wi-Fi based location tracking solutions
› Read more

ekahau Site Survey
Professional 802.11 Site Survey and Planning Solution
› Read more

ekahau HeatMapper
FREE Wi-Fi Coverage Mapping and Analysis Tool
› Read more

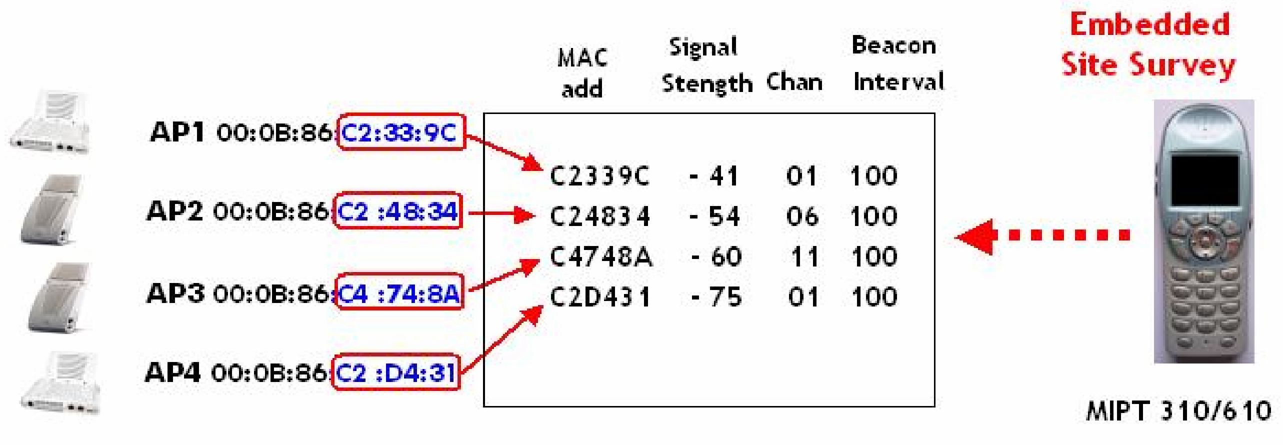
ekahau Advantage
Wi-Fi RTLS: Read the Facts Beyond the Hype
› Read more

Come Visit Us and See a Demo at: Booth 303

http://www.ekahau.com/

Note: This Site Survey software is not orderable from Alcatel-Lucent

11.3. Embedded Site Survey on MIPT 310 and 610



MAC add	Signal Stength	Chan	Beacon Interval
C2339C	- 41	01	100
C24834	- 54	06	100
C4748A	- 60	11	100
C2D431	- 75	01	100

The MIPT embedded Site Survey is also present on MIPT 310 and 610. This mode requires to reboot the MIPT (offline mode). The MIPT site survey mode provides the RSSI level of up to 4 neighboring APs. It can be used at any time to evaluate coverage by testing signal strength, to gain information about an AP, and to scan an area to look for all APs regardless of SSID.

This MIPT embedded site survey is not intended to replace the VoWLAN Site Survey tool, but provides additional diagnostics (handover capability).

12. SVP Server Rules (Reminder)

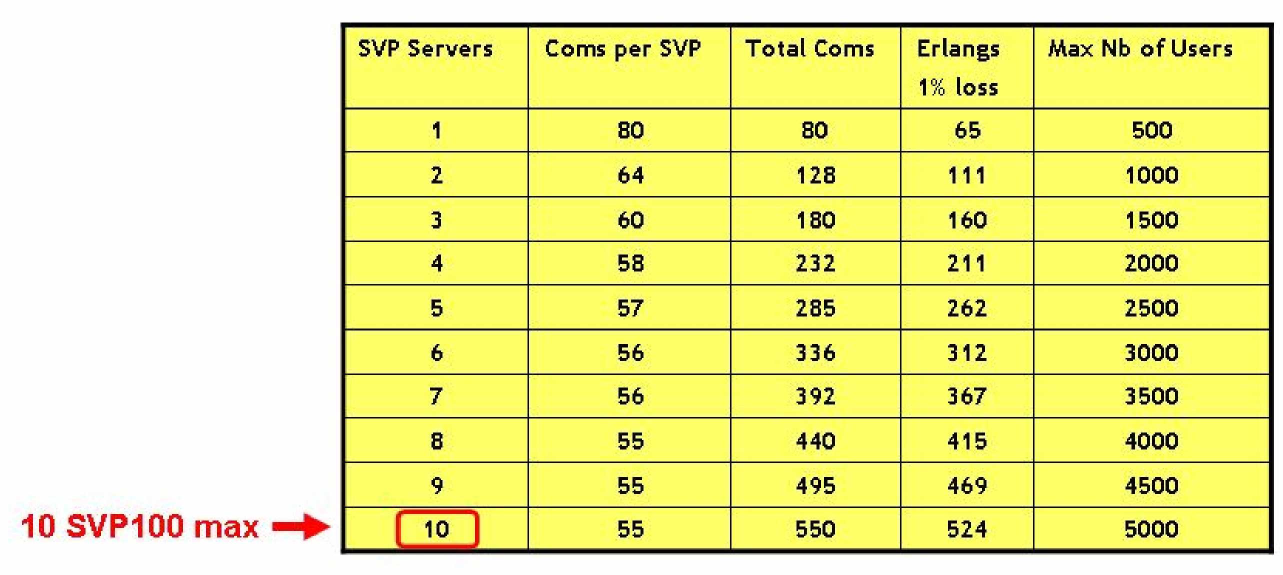
12.1. DHCP Server

Important remark: In addition to standard and common parameters (IP Address, Subnet Mask, Default Gateway IP Address, TFTP Server IP Address), the external DHCP server must be able to provide the MIPT terminal with the IP address of the SVP Server. This makes the optional DHCP fields for "Vendor Specific Options" mandatory for use with MIPT handsets. For Windows 2000 Server, the Vendor Specific Option field is known as "Special Option N°151" (for the SVP Server).

12.2. SVP Server Cascading

In order to increase the quantity of MIPT users several cascading solutions can be proposed with some related rules:

12.2.1. SVP Server 100



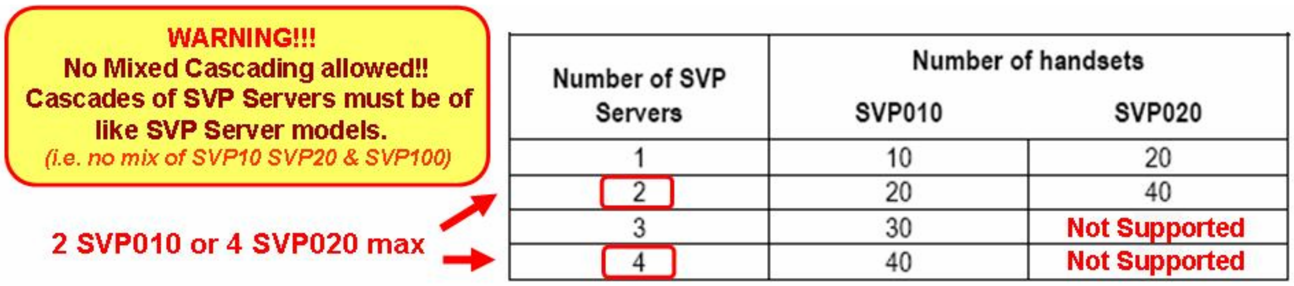
SVP Servers	Coms per SVP	Total Coms	Erlangs 1% loss	Max Nb of Users
1	80	80	65	500
2	64	128	111	1000
3	60	180	160	1500
4	58	232	211	2000
5	57	285	262	2500
6	56	336	312	3000
7	56	392	367	3500
8	55	440	415	4000
9	55	495	469	4500
10	55	550	524	5000

10 SVP100 max

Figure 43: Cascading with SVP100

A maximum of 10 SVP Servers 100 can be cascaded in order to reach 5000 users. The above picture shows the maximum quantity of simultaneous calls depending on the quantity of cascaded SVP Servers.

12.2.2. SVP Server 10 and 20



WARNING!!!
No Mixed Cascading allowed!!
Cascades of SVP Servers must be of like SVP Server models.
(i.e. no mix of SVP10 SVP20 & SVP100)

2 SVP010 or 4 SVP020 max

Number of SVP Servers	Number of handsets	
	SVP010	SVP020
1	10	20
2	20	40
3	30	Not Supported
4	40	Not Supported

Figure 44: Cascading using SVP 010 or SVP 020

A maximum of 4 SVP Servers 10 and a maximum of 2 SVP Server 20 can be cascaded in order to match the quantity of users. Only one SVP Server model can be used for cascading (SVP Server 10 or SVP Server 20 or SVP Server 100). No mixed cascading allowed.

12.2.3. SVP Cascading Rules Summary

- One group of cascaded SVP Servers per Site
- Up to 4 (four) SVP010 => (40 MIPT users max)
- Up to 2 (two) SVP020 => (40 MIPT users max)
- Up to 10 (ten) SVP100 => Up to 15000 MIPT users per Comm Server
- Only like SVP Server models in cascades. (No mixing of SVP Server models)
- SVP Cascading components (SVP Servers) must be part of the same IP subnet/VLAN

- A Cascading SVP Server configuration MUST be hosted in a single IP Domain
- SVP Servers belonging to separate sites must be set in different IP Subnets/VLANs
- The Max quantity of SVP Server groups is limited to the total quantity of Voice IP Domains

12.2.4. Self Healing SVP Functionality

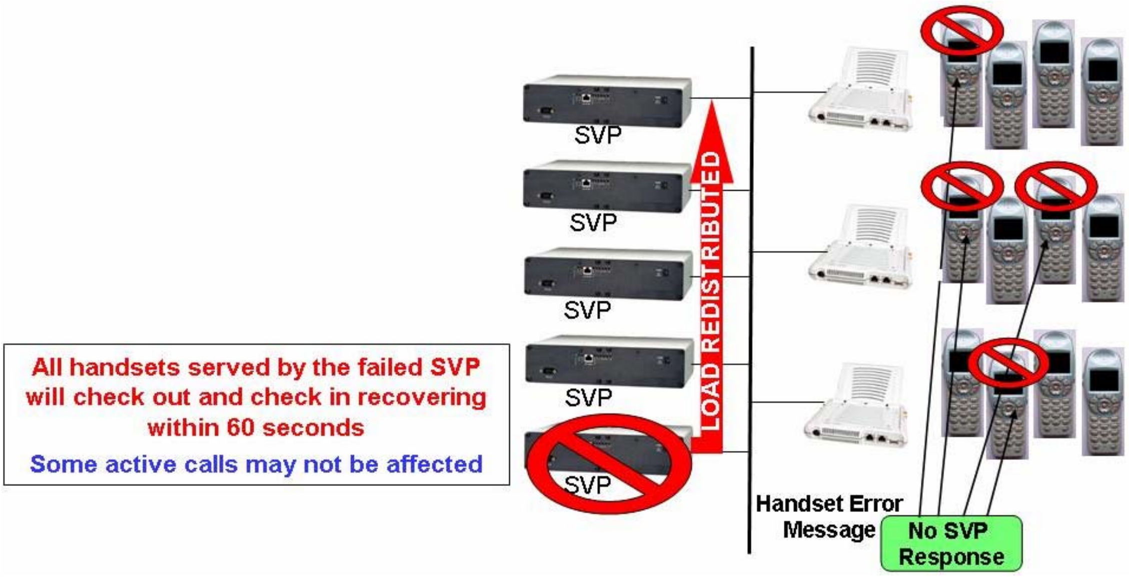

SVP
SVP
SVP
SVP
SVP
LOAD REDISTRIBUTED
All handsets served by the failed SVP will check out and check in recovering within 60 seconds
Some active calls may not be affected
Handset Error Message
No SVP Response

Figure 45: Self Healing on SVP server

SVP server Self-Healing is based on the automatic election of a new Master SVP in case of Master SVP server failure (A slave SVP server becomes the Master SVP). SVP Server code 17x.035 is required to support self-healing feature.

12.2.5. SVP server code evolution (17x.037)

Reminder:
For a long time Alcatel-Lucent prerequisite for SVP server code was frozen to 17x.028 code with no evolution. In the meantime some new features have appeared like Self Healing and implying a SVP code update to support this feature. Decision has been taken by Alcatel-Lucent to follow server code evolution and integrate Polycom new features and bug corrections.
Required for VoWLAN implementation on Non-ALU WLAN infra with SVP server cascading
Also applicable for a standalone SVP Server topology

Some SVP server Codes examples:
SVP server Software (17x.037) Bug Correction
SVP server Software (17x.036) New Feature (MIPT Load Balancing versus SVP, etc.)
SVP server Software (17x.035) Bug Correction
SVP server Software (17x.034) Bug Correction
SVP server Software (17x.033) New Feature (Self-Healing functionality)

12.2.6. Topology Reminder with SVP server

12.2.6.1. Non-Cascaded Mode

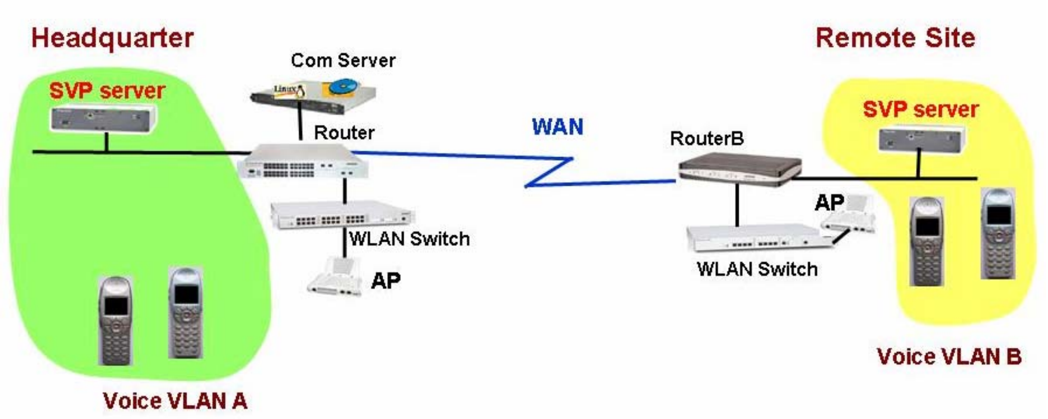


Figure 46: SVP server Topology (non-cascaded)

This topology allows VoWLAN implementation on a remote site
At least one SVP is required on remote site in addition to a WLAN switch in order to avoid tromboning over the WAN.
.

12.2.6.2. Cascaded Mode

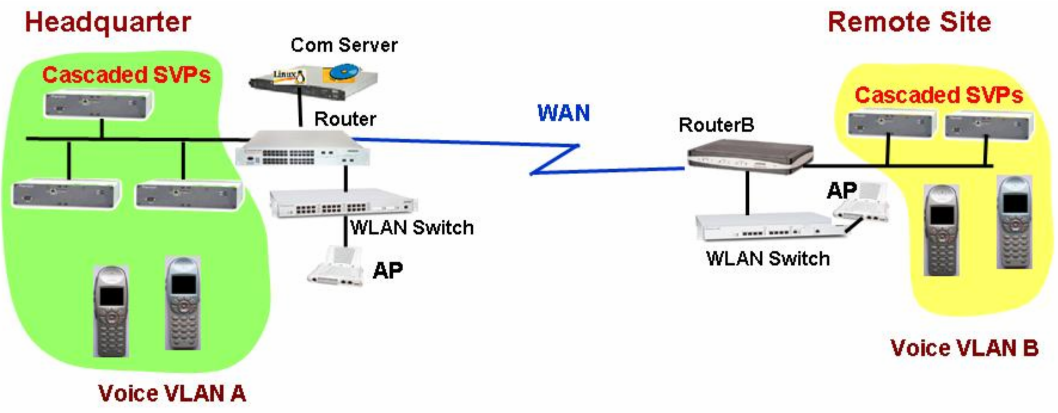


Figure 47: SVP server Topology (Cascaded)

When SVP server capacity is not enough in terms of users, cascaded mode can be applied.

13. Glossary

AES Advanced Encryption Standard

ALG Application Layer Gateway

AP Access Point

ARM Adaptative RF Management

CAC Call Admission Control

DFS Dynamic Frequency Selection

DoS deny of Service

DSCP Differentiated Services Code Point

IEEE 802.1X is an IEE standard for port-based Network Access Control

IEEE Institute of Electrical and Electronics Engineers

IETF Internet engineering Task Force

IMP Indoor Mesh Point license

L2 Layer 2 (MAC level)

L3 Layer 3 (IP level)

LAP Access Point license (LAN Connected AP)

MAC Medium Access Control

MAP Outdoor Mesh Point license

MIPT Alcatel Mobile IP Touch 300/600

OFDM Orthogonal Frequency Division Multiplexing

PEF Policy Enforcement Firewall (WLAN license)

PoE Power over Ethernet

PSK Pre shared key

PTT Push To Talk

RAP Remote Access Point

RF Radio Frequency

SSID Service Set Identifier

TKIP Temporal Layer Security

TSpec Traffic Specifications

U-APSD Unscheduled Automatic Power Save Delivery

UP User Priority

VLAN Virtual Local Area Network

VoWLAN Voice over WLAN

VRRP Virtual Router Redundancy Protocol

VOC (VSM) Voice Services Module (WLAN license)

WIP Wireless Intrusion Protection (WLAN license)

WEP Wired equivalent Privacy

WMM Wi-Fi Multi Media

WPA Wi-Fi protected Access

WPA2 Wi-Fi protected Access

Alcatel·Lucent

www.alcatel-lucent.com