Hospitality
Networking Solution Guide

Alcatel·Lucent
Enterprise

Contents

Figures

Tables

1. Introduction

1.1. Purpose

The purpose of this solution guide is to present the requirements and considerations relevant to the hospitality vertical along with design options and ALE features and equipment positioning.

1.1. Audience

This solution guide is intended for network architects and network engineers involved in the design of networks for the hospitality industry. This document is to guide ALE customers in the architecting and design of an ALE network (wired and wireless) capable of delivering today's (and more) hospitality services expected by both guests and staff of a hotel.

To benefit from this document, the reader will have a solid understanding of various networking technologies at the ACPS or similar level.

1.2. Scope

Most hotel properties have basic network needs and are very sensitive to price – they are looking for basic functionality at the lowest price. But some large or luxury hotels consider networks to be more than a commodity and are ready to invest in a differentiating and state of the art network (wired and wireless).

This document covers all requirements in between those two models.

Large resorts that may be seen as real towns by their very nature (an area that is up to hundreds of kilometers square, a population of several thousand guests) and non Ethernet technologies like GPON are out-of scope. They will be discussed in a future and updated version of this document.

This document focuses on Ethernet (IEEE 802.3) and Wi-Fi (IEEE 802.11) technologies, and common hospitality services built and deployed over a network infrastructure based on those technologies.

1.3. Acronyms

ACPS	Alcatel-Lucent Enterprise Certified Pre-Sales
AFN	Application Fluent Network
AP	access point
ARM	Adaptive Radio Management
AWG	American wire gauge
BGP	Border Gateway Protocol

CCTV	closed-circuit television
DHCP	Dynamic Host Configuration Protocol
DPI	Deep Packet Inspection
FC	fiber channel
FCoE	Fiber Channel over Ethernet
GBIC	Gigabit Interface Converter
GPON	Gigabit Passive Optical Network
GRE	Generic Routing Encapsulation
GUI	graphical user interface
HVAC	heating, ventilation and air-conditioning
IEEE	Institute of Electrical and Electronics Engineers
IoT	internet of things
IP	Internet Protocol
IPTV	IP television
LACP	Link Aggregation Control Protocol
LAN	local area network
LLDP	Link Layer Discovery Protocol
MED	media endpoint discovery
MIMO	multiple input multiple output
NMS	network management system
OSPF	Open Shortest Path First
OXO	OmniPCX Office
OXE	OmniPCX Enterprise
PMS	property management system
PoE	Power over Ethernet
PSTN	public switched telephone network
PVC	Primary Virtual Controller
POS	point of sale
PTZ	pan tilt zoom
QSFP	quad small form-factor pluggable
QoS	quality of service
RAP	remote access point
RDA	radio dynamic adjustment
RF	radio frequency
RIP	Routing Information protocol
SFP	small form-factor pluggable
SSID	service set identifier
STP	Spanning Tree protocol
SVC	secondary virtual controller
uNP	User Network Profile
VC	virtual chassis
VFL	virtual fabric link
VoD	video on demand
WLAN	wireless local area network
WLC	wireless LAN controller

1.4. Related documents

[1] Alcatel-Lucent Enterprise Hospitality solutions
- *http://enterprise.alcatel-lucent.com/?solution=Hospitalityandpage=overview*

[2] Alcatel-Lucent Enterprise 2015 Reference Compilation on Hospitality
- *http://enterprise.alcatel-lucent.com/docs/?id=26684*

[3] ALE Succeeds in Hospitality with Vertical Marketing
- *http://www.nojitter.com/post/240170356/ale-succeeds-in-hospitality-with-vertical-marketing*

[4] Alcatel-Lucent Enterprise Equipment documentations (datasheets, user guides...)
- *http://enterprise.alcatel-lucent.com/?product=EnterpriseProductsandpage=directory*

2. Networking Requirements in Hospitality

2.1. Several systems and one converged network

Basically, a converged network is the grouping of telephone, video and data communication within a single network. Designing and managing all of these within one network offers convenience and flexibility that are not possible with separate infrastructures. No longer do properties need different cables for different services.

For example, by delivering a power over Ethernet (PoE) switch, hotels can deliver power and data with the same cable. This can reduce costs and enables the delivery of multiple applications efficiently without having to manage each vendor-specific system installation.

For the hospitality industry specifically, a converged network can include:

- **VoIP**: Delivery of voice and multimedia over IP networks.
- **HSIA**: High speed internet access for staff and guests
- **PMS**: Property management system software at the front-desk
- **IPTV**: Television delivered over Internet Protocol (IP)
- **Mobile POS**: Point-0f-sale services for mobile devices (restaurant, bar, etc.)
- **HVAC**: Allowing the management of air-conditioning in the hotel
- **CCTV**: Video surveillance for safety and security

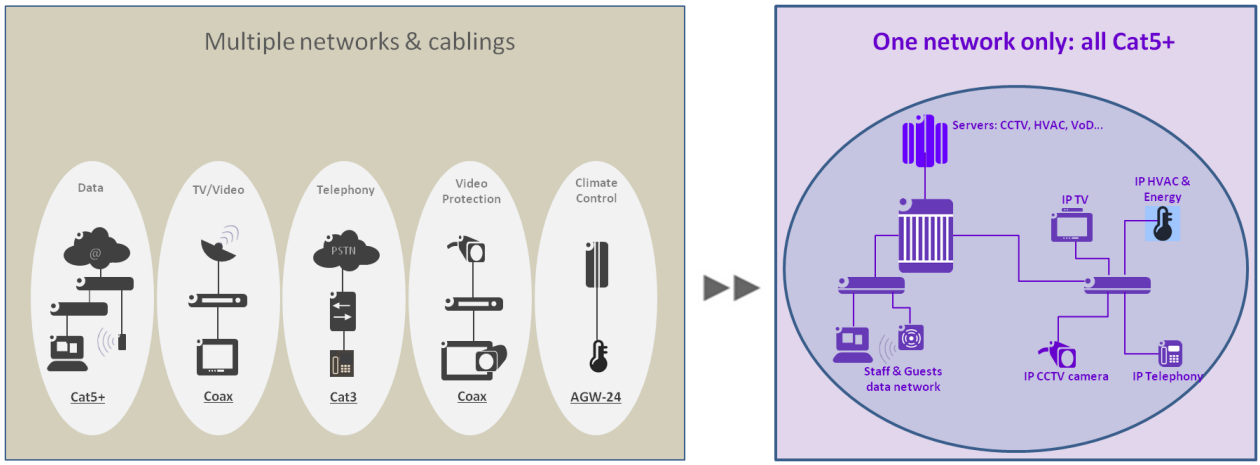


Figure 1: Converged Network

When done correctly (bandwidth capacity planning, quality of service [QoS], etc.), the integration of all these technologies can lead to significant operational efficiencies:

- **Easier network performance management**

  Converged networking allows efficiency and scalability when, for instance, a new service is added. Network performance can be configured and monitored from a single common infrastructure, thus streamlining management and making it easier to identify and address issues.

- **Lower costs due to simplified cabling and hardware infrastructure**

  Cabling once for all systems can mean significant cost savings. By using the same equipment and space for multiple systems, a hotel eliminates redundancy and optimizes the delivery of all services. In addition, once the network is established it is easier to add new services to the existing infrastructure, thus making it more cost effective than laying down a whole new network.

- **Smart management of energy resources**

  A converged network eliminates redundancies in everything from power usage and maintenance costs to reducing overall environmental impact.

- **Elevated customer service**

  Connected to a single and converged network, systems can easily communicate and interoperate. This may be leveraged to improve guests' experience by allowing, for instance, voice over Wi-Fi communications from smartphones.

2.2. High performance

Hospitality networks must be able to deliver consistent and performance even when there are high concentrations of users, for example, in a conference centre or a meeting room.

Today's guests expect to feel at home in their hotel and arrive with an average of three devices: A laptop, smartphone, and tablet. Mobile devices are used everywhere (restaurant, gym room, etc.) and data use has become increasingly varied and complex: Online gaming, voice and video communications, social media, video streaming, etc. Moreover, storage is no longer on the device, but in the cloud, needing constant access to the internet. Networks must ensure that data-hungry guests cannot take over the network, crowding out everyone else.

For these reasons, high bandwidth will be considered -- from the access network (wired and wireless) up to the core of the network.

2.3. Network security and segmentation

The hospitality industry is a high value target for hackers and both the hotel operational network and the guests' network, wired or wireless, are concerned.

The hotel's operational network will be completely separated from the guest network. Additional network segments (physical or logical) may be required for conference rooms and meeting areas, and sometimes up to the guest room for VIP guests.

Balancing the ease of access for guests with appropriate security is a difficult task. The wired network is often "open" and wireless access is poorly protected (open Wi-Fi, or connection information given on a piece of paper). This is no longer an option.

Additionally, the network must be able to serve several different user groups, each with different needs. Required for allowing a single network to serve multiple user groups is the ability to authenticate users and to provide custom levels of access and security to each group. Guests and visitors may only need Internet access while the hotel corporate staff needs full access to the WLAN in order to access secure locations such as share drives and printers.

2.4. Mobility and unified user experience

Hotel management is now done by employees while on the move with tablets. However, a wired connection is still expected by guests for security reasons. The user experience cannot be different whether wired or wireless.

Wired and wireless networks are increasingly unified, improving network operations with a single management (one set of policies, etc.) and a unique and seamless user experience (wired or wireless).

2.5. Network analytics and business insight

Analytics should be leveraged to optimize business performance and employee productivity and can offer the personalized experience guests expect today.

Analytics will provide hotel IT with detailed visibility into the applications being used and bandwidth consumed, and with the ability to immediately enforce policies to control prioritization, QoS and security of these applications right at the edge of the network.

Additionally, analytics may be used to build targeted promotional campaigns, and combined with location based services, it can market to guests in new and inventive ways.

2.6. Wi-Fi and PMS integration

Not all hotel Wi-Fi networks are capable of integrating with existing hotel PMSs. Lack of integration leads to providing open and free access to all guests or requires the hotel staff to manage credentials and billings manually (errors, missed billing, etc.) This may be a difficult task in some situations where, for instance, the hotel faces a massive number of guest arrivals.

Integration of the network with the hotel PMS allows to generate automatic and personalized Wi-Fi credentials and to send billing information directly to the PMS to bill the guest at the time of checkout.

2.7. Location-based services

Today, hotels seek to benefit from location-based services in order to provide premium services to their guests. Beyond way-finding applications, hotels aspire to engage the guests in a very personalized way as a result of the understanding and the interaction that become possible when using location-based services. For instance, a hotel may use location-based services to send a welcome message to a guest upon his arrival or push a relevant promotional offer to a guest who is passing by the bar or any shop in the hotel property. Access to recreation and services that enhance the guest's stay is a way to encourage loyalty to the hotel chain whose technology enabled a more seamless and personalized guest experience.

2.8. Monetizing the network

Some guests are still willing to pay for a high quality internet connection and the hotel will have the option to charge for a basic service or up sell to a higher speed. The network and especially the Wi-Fi Internet access offers customizable billing options with online payment services providers (for example, *PayPal*) or with the PMS of the hotel (for example, Micros Opera, Protel, etc.)

In addition, advertising can be sold for appearing on the guest portal or on digital signs throughout the grounds, providing direct access to guests for local advertisers and relevant content to guests.

2.9. The Internet of Things

The *internet of things* (IoT) is about to impact strongly the hospitality industry in order to better serve customers and also increase the efficiency of its operations.

For example, a hotel can use IoT to provide integrated services such as application driven devices and automated triggers like automated door locks, set-top-boxes, thermostats, telephones, light switches, electric blinds and other devices that are connected on a common network to enable the services that guests want.

The employees will also be able to provide a better housekeeping service, facilities maintenance, room service and carry out energy conservation. Implementation of IoT solutions for hospitality industry enables owners to optimize the front desk, concierge, room service, and employees to address customer requirements through data-driven triggers and alerts. If a hotel can automate various sensors with guest data or employee information, it can provide a better experience and gain more guest loyalty.

But, while IoT opens up new possibilities, it also introduces new challenges and risks, especially in terms of security. For example, an HVAC system that is IoT enabled could be hacked and every air conditioning unit could be turned up on high with maximum negative impact on a guests' personal comfort.

3. Alcatel-Lucent Enterprise Solution Overview and Portfolio

3.1. General approach

Alcatel-Lucent Enterprise has developed an approach called ***Application Fluent Network (AFN)*** that answers challenges the hospitality industry may face: mobility, security, IT virtualization, mission-critical applications...

The *Application Fluent Network* approach is based on a resilient architecture with automatic controls capable of dynamically tuning the network performance, and streamlined operations that reduce network complexity. This Application Fluent Network is user, device and application aware. Most importantly, it makes automatic adjustments based on that understanding. It provides Unified Access, where network services are transparently offered resulting in a consistent User Experience over both Wired and Wireless networks for both staff and guests.

With an *Application Fluent Network*, a hotel can enjoy a network that understands devices as well as associated applications. Contextual understanding of conversations between devices and applications makes it possible for the network to optimize the user experience and network performance, while lowering capital and operating expenses.

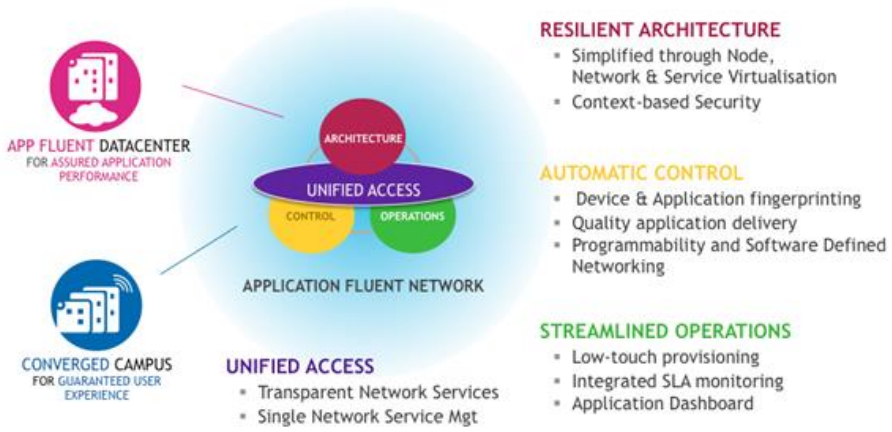


Figure 2: Alcatel-Lucent *Application Fluent Network* approach

The Unified Access solution provides a common set of network services, a policy framework, authentication scheme and a single authentication database that is applied to users accessing the network with either wired or wireless devices of the Alcatel-Lucent Enterprise portfolio, ensuring a seamless user experience for both guests and staff of the hotel and allowing simplification of the operations thanks to a common wired and wireless Network Management System (NMS).

Wireless access is provided by the OmniAccess® series that offers a variety of Wi-Fi access points (APs) including instant/controller-less APs or controller-based APs for larger deployments.

3.2. LAN equipment

The Alcatel-Lucent Enterprise *Application Fluent Network* Solution is built on a high-performance wire- rate up to 10GE/40GE network. The Alcatel-Lucent Enterprise Ethernet Switching port-folio provides solutions for core and access. The core network includes the market-leading Alcatel-Lucent Enterprise OmniSwitch® 6900 Stackable LAN Switch and the OmniSwitch 10K and 9900 Modular LAN Chassis models. Wireline access is provided by stackable LAN switches like the advanced Alcatel-Lucent Enterprise OmniSwitch 6860, the value OmniSwitch 6450 and the Gigabit Ethernet OmniSwitch 6350.

The switches come with the same operating system (AOS) on all models, providing a consistent look and feel when configuring core or access functionality. The whole portfolio is fully SNMP manageable; every single CLI command can be performed through SNMP. Also the Web interface is fully implemented; with this GUI everything that is configurable through CLI can be configured through the Web GUI.

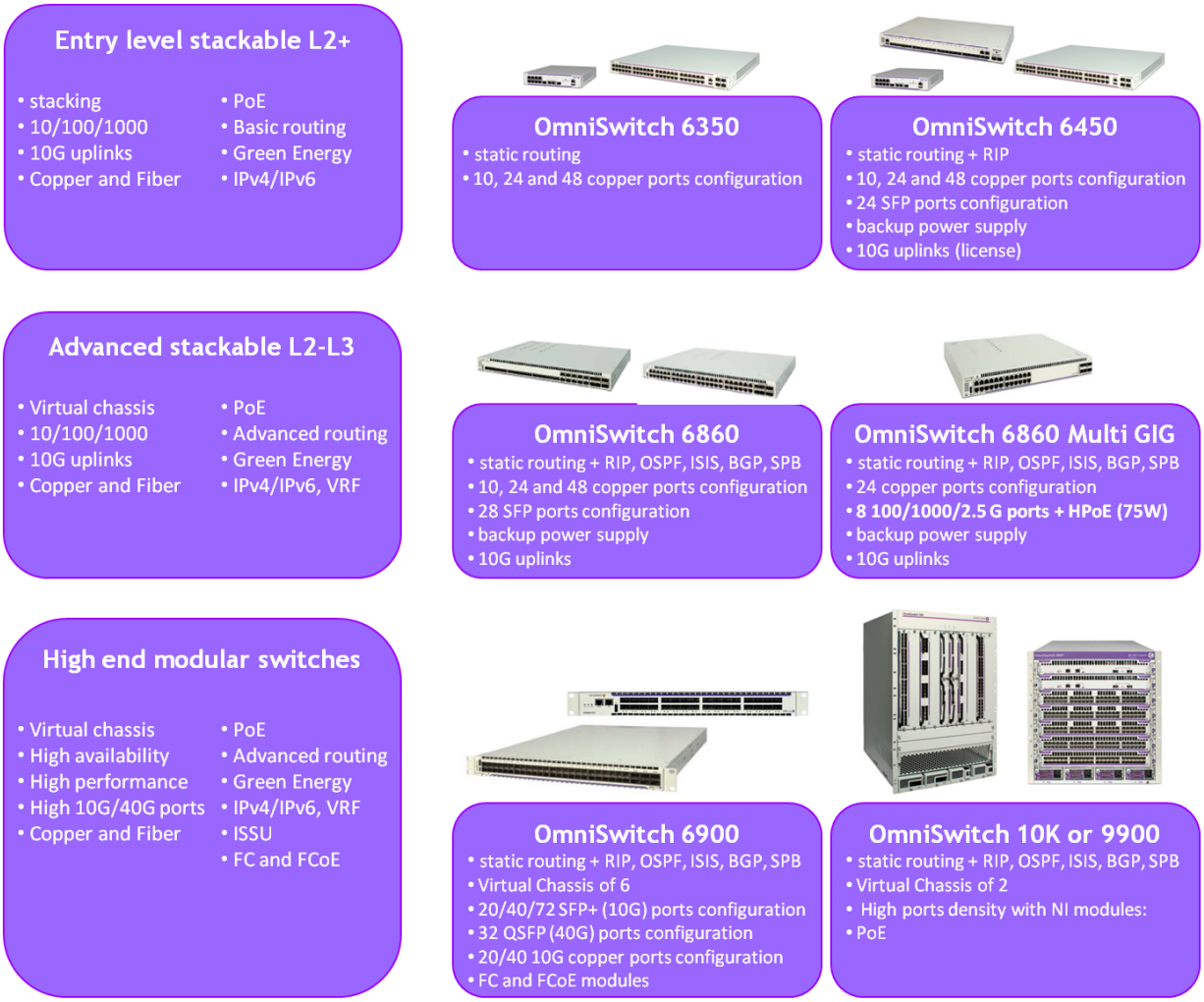


Figure 3: LAN Equipment portfolio

The *Application Fluent Network* approach allows a hotel to deploy a network that is simplified and flattened, with just two layers instead of the traditional three. Indeed, the switches used in the *Application Fluent Network* feature wire-rate and non-blocking capacity as well as a high port density, along with the ability to provide Layer 3 switching functionality in a Layer 2 network.

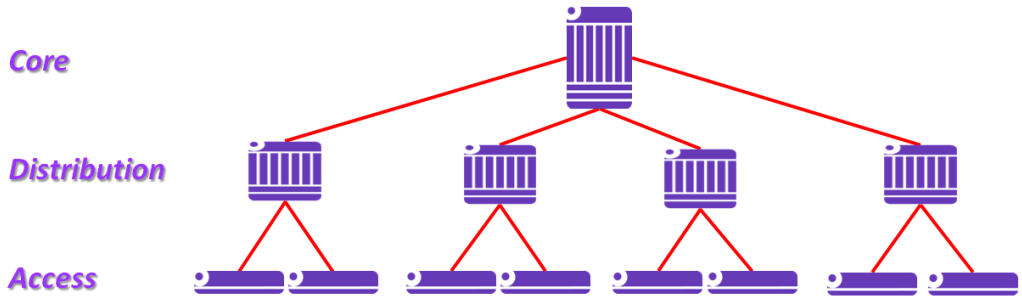


Figure 4: Traditional three-tiered network

The removal of the aggregation layer is also critical to achieving a lower latency network and to support real-time applications like voice and video with high quality expected today by guests in a hotel.

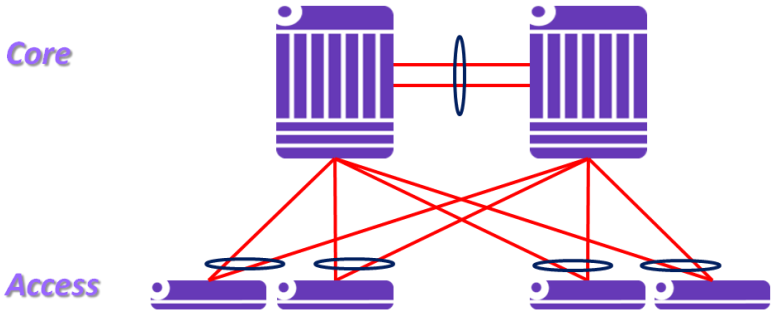


Figure 5: Simplified two-tiered network

Moreover, traditional approach foresees dual uplinks from the access to the aggregation network that need a network protocol like Spanning Tree to avoid Layer 2 loops, resulting in one of the two uplinks to be (partially) inactive. With the concept of "Node virtualization: Network optimization, costs savings, and more" that is detailed in following chapter and Link Aggregation (IEEE 802.3ad LACP protocol), this can now be avoided: Both uplinks are fully active providing double the uplink bandwidth.

Naturally, Alcatel-Lucent Enterprise products and solution would comply with any specific topology requirement like a traditional three-tiered or ring topology that may be dictated by cable topology constraints in the case, for instance, of a hotel revamping.

3.3. WLAN equipment

3.3.1. Medium and large deployments

The Alcatel-Lucent **OmniAccess** series offers a variety of equipment enabling the deployment of appropriate sized solutions to fit the needs of any hotel. The OmniAccess WLAN solution supports a true user-centric network experience, delivering follow-me connectivity, identity-based access, and application continuity services. The solution features a scalable design, mobile voice over IP, integrated network management in a secure network environment.

Alcatel-Lucent OmniAccess Access Points (APs) are small, lightweight and can be securely deployed in a variety of locations such as on walls, cubicles, desktops, and in the ceiling. The AP antenna diversity allows for the best possible signal processing using dual, omni-directional antennas.

Alcatel-Lucent OmniAccess APs are dual band APs (2.4GHZ and 5GHZ) and work with Alcatel-Lucent OmniAccess Wireless LAN (WLAN) switch/controllers to provide a high performance wireless mobility solution for hotels. Alcatel-Lucent OmniAccess APs have an extended lifespan because they automatically configure themselves across any L2/L3 network using discovery, allowing easy upgrades when new features, capabilities, or standards emerge.

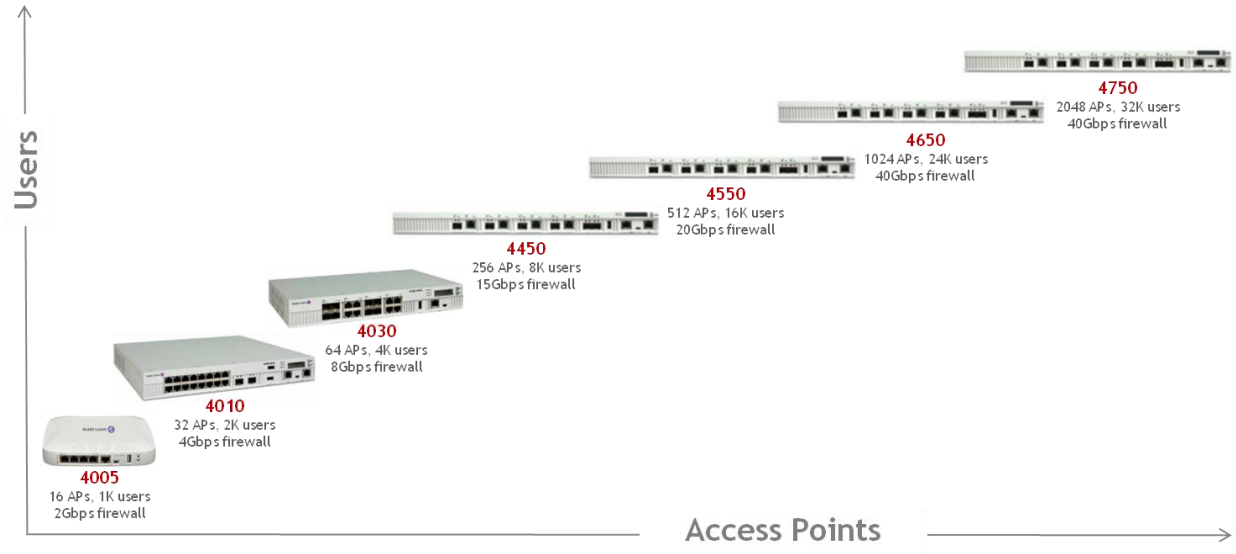


Figure 6: WLAN controllers

Three access point types are available:

- **Campus access points or access points:** Alcatel-Lucent OmniAccess Access Points provide enterprise-class access capable of supporting multiple functions including wired and wireless access, air monitoring/wireless intrusion detection and prevention. These access points deliver secure user-centric network services and applications. They require a WLAN switch/controller and software licenses.

- **Instant Access Points:** Alcatel-Lucent OmniAccess Instant Access Points make Alcatel-Lucent OmniAccess Mobility Controller capabilities virtual on 802.11ac access points (APs) creating a feature-rich, enterprise-grade wireless LAN (WLAN) that delivers the affordability and simplicity of an entry-level Wi-Fi network. No WLAN switch/controller is required and software licenses are included.

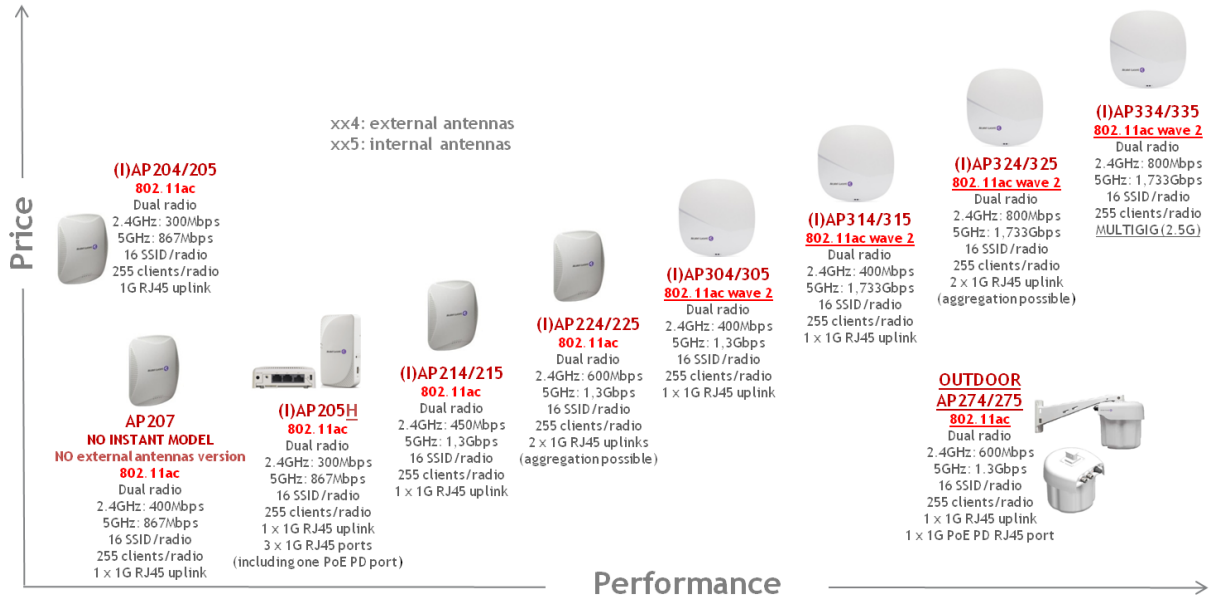


Figure 7: WLAN Access Points or Instant Access Points

In a **controller-based deployment**, the Campus APs are driven by a centralized mobility controller that manages the APs (configuration, firmware, licenses, and more) and coordinates the APs by dynamically adjusting their settings like the Radio Frequency parameters (channel selection, transmit power, and more). The mobility controllers are available as network appliances systems that scale to meet the needs of the **largest properties**:

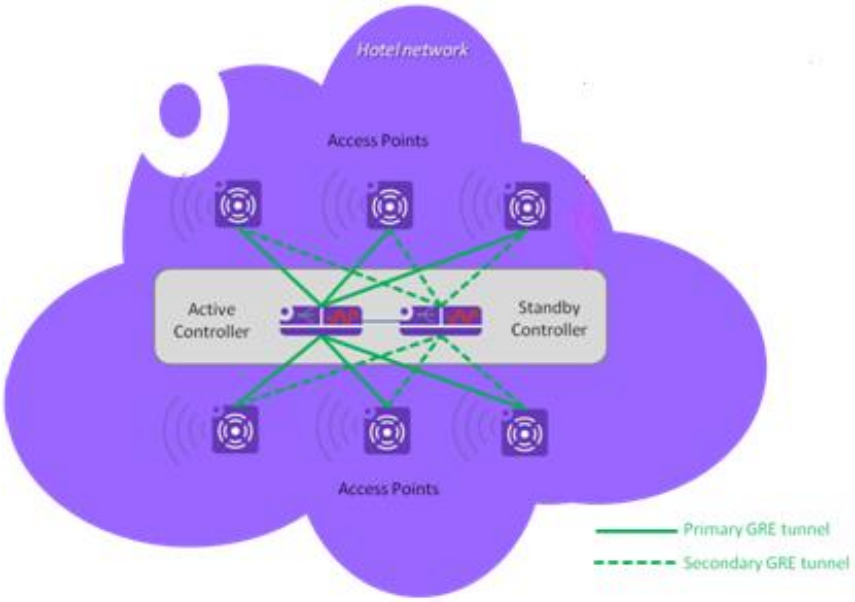


Figure 8: WLAN controller-based architecture (large deployment)

In such a deployment, the controllers are deployed in a central location (typically, the server room or technical room of the hotel) and the access points may be deployed in mass in any

location of the property, providing they have a Layer 3 network connectivity allowing contact with the WLAN controllers and to establish GRE tunnels.

A controller can also act as an IPSec VPN concentrator (which requires additional licenses) to connect through Internet a remote location or a "home worker" equipped with a remote AP. The IPSec tunnel established between the central controller and the RAP allows extending the private network of the hotel by offering a set of copper 10/100/1000 ports and by broadcasting the various hotels' SSIDs up to the connected remote location.

Opposite of a controller-based wireless network, an **instant-based wireless network** made of instant APs (a cluster) does not require an external mobility controller to regulate and manage the Wi-Fi network. Instead, one IAP in the cluster assumes the role of *virtual controller*. It coordinates, stores, and distributes the settings required to provide a centralized functionality to regulate and manage the Wi-Fi network. The virtual controller is the single point of configuration and firmware management. The virtual controller also functions like any other AP with full RF scalability, and is dynamically designated according to a "master election protocol" that enables IAPs in a cluster to elect an IAP to take on a virtual controller role and allow graceful failover to a new virtual controller when the existing virtual controller is not available. An administrator can also enforce a particular instant AP to act as a master.

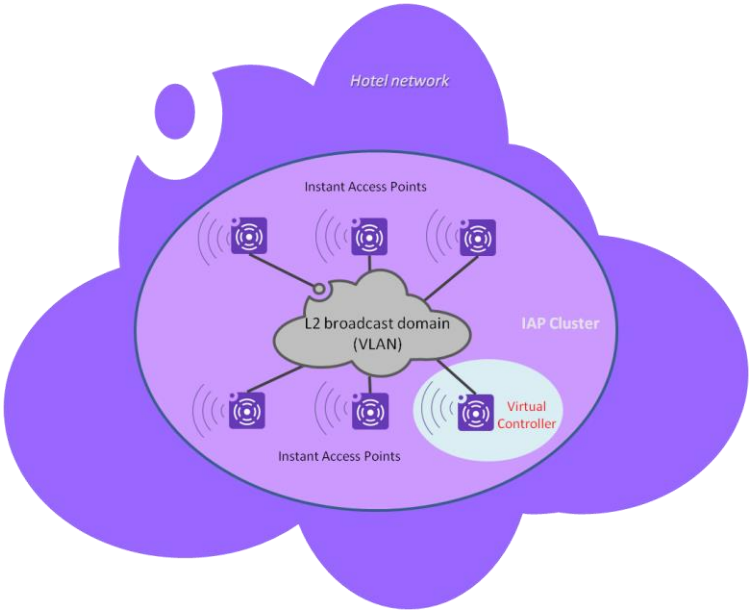


Figure 9: WLAN instant based (medium deployment)

Both controller based and Instant based architectures support features expected today to deliver a state of the art wireless network for large and/or medium hotel deployments:

- Centralized management
- Network access authentication
- Stateful packet inspection firewall
- Network access control through user based firewall policies
- Dynamic radio management and user load balancing over (I)APs
- Bandwidth management (at user, group of users, or application level) and quality of service

- Wireless intrusion protection
- Live RF power levels visualization (“heat map”)
- Voice over wireless LAN (VoWLAN)
- And more

The main differentiating criteria to be considered when deciding to go with a controller based or instant based design is **scalability**. Whereas an instant based deployment is limited to 128 (I)APs and 2048 concurrent clients (best practices, no hardware or software limits), a controller-based deployment can scale from 16 APs and 1024 concurrent clients (OmniAccess 4005 WLC model) to 2048 APs and 32768 concurrent clients (OmniAccess 4750 WLC model). Additionally, an instant based deployment requires that every IAP is connected to a common VLAN (L2 domain) in order to allow intra-cluster communications between IAPs, which does not fit a large multi-site hotel.

Even if an IAP cluster offers main of the features a modern hotel WLAN network would expect today, some features are nevertheless only available on WLAN controllers:

- Embedded captive portal for guests management
- Advanced routing protocols (OSPF)
- IPSec VPN server function to allow Remote AP connections
- And more

3.3.2. Small deployments

For small hotels, ALE has developed and designed the **AP1101** access point. The AP1101 is a dual-radio 802.11ac 2x2 MIMO, indoor wireless access point that provides high throughput and a seamless user experience (up to 1.2Gb/s wireless data rate and 64 simultaneous clients associations) with maximum simplicity for deployment and management.

Figure 10: AP1101 Access Point (small deployment)

The OmniAccess AP1101 works in a fully redundant AP-group architecture to provide simplified plug-and-play deployments. The AP-group is similar to the previous “instant cluster” concept. It is an autonomous system that consists of a group of OmniAccess AP1101s and a virtual controller, which is a selected access point, for AP-group management. **One AP-group supports up to 16 OmniAccess AP1101s, 256 concurrent clients, and 16 WLANs SSIDs**.

The AP-group architecture ensures simplified and quick deployment. A wizard is available to configure the first AP. Once the first AP is configured, the remaining APs in the network will come up automatically with an updated configuration. This ensures that the whole network is up and functional within a few minutes.

The AP1101 provides advanced features such as a fine-tuned QoS, advanced security mechanisms (for example, rogue AP detection) dynamic RF parameters adjacent (channel selection, transmit power, and more) and a built-in customizable (logo and background pictures, terms of use, etc.) captive portal (with an internal user database) which enables a small hotel to deploy its own Wi-Fi guest access solution with minimum cost and effort.

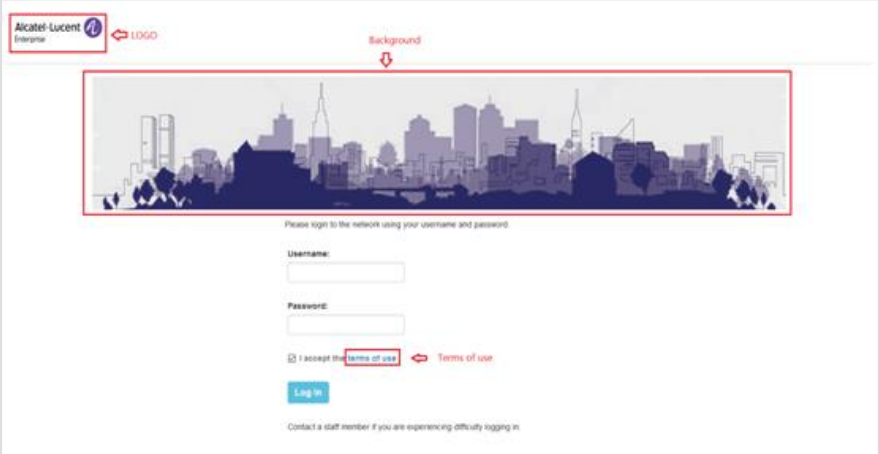


Figure 11: AP1101 embedded captive portal

3.4. Policy Manager and Guest Management

ClearPass Policy Manager is a hardware or virtual appliance made of several and optional modules providing extremely smart user/role and device network access control for staff, contractors and guests across the wired and wireless infrastructure deployed by a hotel. ClearPass embeds a context-based policy engine that supports RADIUS and TACACS+ protocol and that goes beyond traditional AAA solutions to deliver device profiling, posture assessment, staff device on-boarding (BYOD) and guest access options:

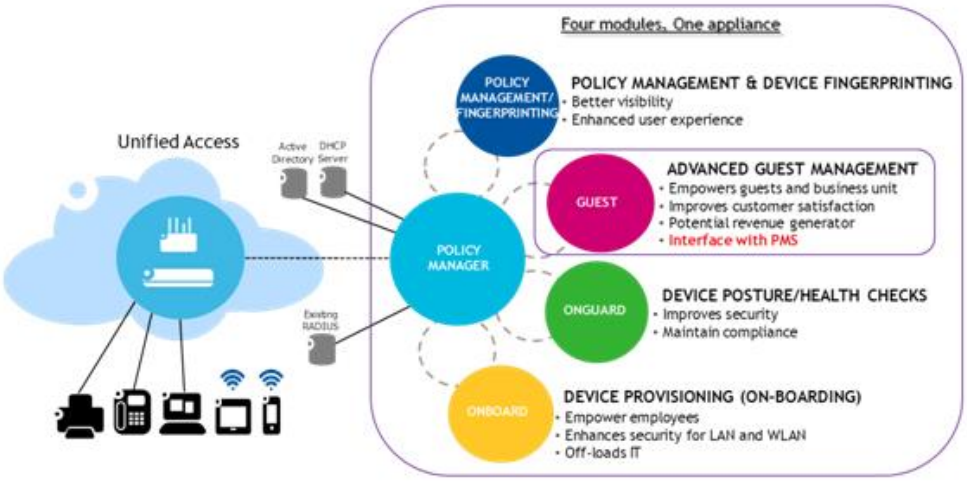


Figure 12: ClearPass Policy Manager

This document will focus on the ClearPass Guest module that answers one of the main critical network challenges today in hospitality: **Guests network (wireless or wired) access management**.

ClearPass Guest solution offers the security and automation to support hundreds or thousands of guests with unique and personal credentials while offering maximum IT or hotel staffs (receptionist) off-load. The guests may indeed self-register to generate their own personal credentials in case of free internet access or their credentials may be generated by a payment service provider (for example, *PayPal*) if the hotel decides to charge internet access. ClearPass integrates with leading property management systems in order to automate guests' credentials creation upon arrival.

Guest credentials and access privileges can be customized to enforce bandwidth limits, access to specific resources and length of connections. MAC caching can be also be used to ensure that guests are not repeatedly asked to enter login and passwords each time they re-connect to the guest network for a set period of time.

ClearPass Guest captive portal offers customizable login pages that provide the ability to display the latest corporate branding, messaging and promotional offers. ClearPass embeds a built-in advertisement module allowing a hotel to easily promote special offers each time a guest registers for credentials.

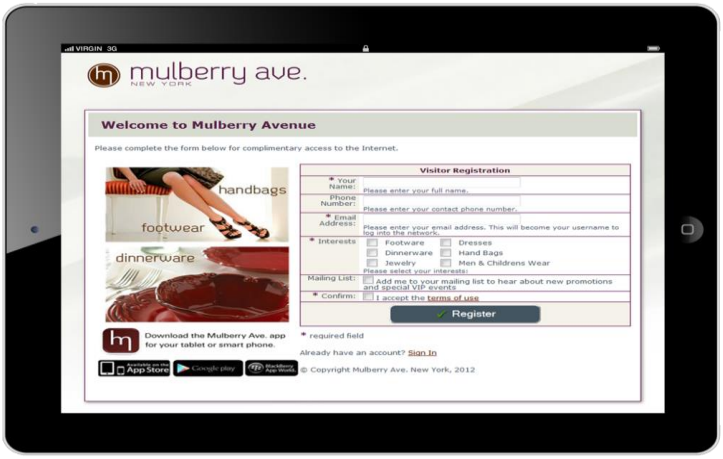


Figure 13: ClearPass captive portal with self-registration and built-in advertising

3.5. Unified management

Hotels usually have a limited number of IT staff and a common complaint by IT administrators is the proliferation of tools for monitoring and managing the network infrastructure. AlcatelA:E helps relieve this problem by:

- Consolidating many network management functions into a single management tool. IT staff can access this system remotely, allowing them to monitor and control the network from any location, at any time.
- Enabling management of the network infrastructure as virtualized segments, (for example, all switches on one floor of a building would be treated as one virtualized complex), rather than as individual network elements.
- Including application traffic monitoring tools allowing network operators to collect statistics such as loss, jitter, latency, response time, and packet loss.

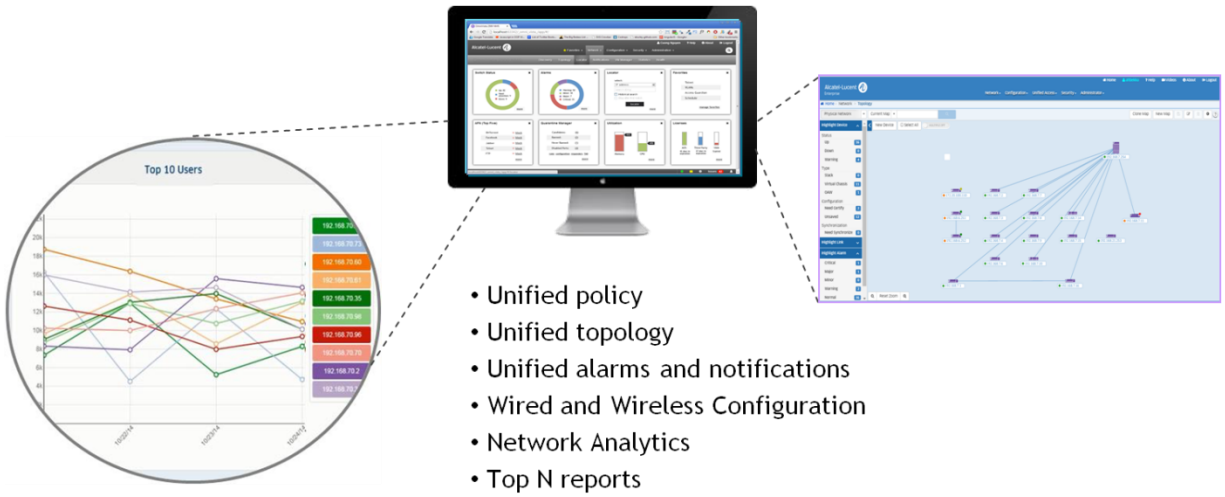


Figure 14: Unified OmniVista 2500 Network Management System

OmniVista® 2500 is ALE's network management system for both wired and wireless networks. It is a virtual appliance bundled with Linux OS image and OmniVista 2500 application for full turnkey operation. OmniVista 2500 provides much needed support to hotel IT managers and network administrators dealing with a deployment of converged, mission-critical applications and challenged with upholding service level agreements (SLAs) for existing services. Its application dashboard provides a real-time overview of all the applications running over the network and on what device. From here, the Application Fluent Network can be realized over the wired and wireless network so that the mission-critical applications always have priority over the network.

For both wired and wireless networks, OmniVista 2500 offers:

- Unified policy (defining a policy once for application on both wired and wireless equipment)
- Unified topology
- Unified applications visibility (what applications are running on the network? how much bandwidth they are taking, etc.)
- Unified alarms and notifications
- Wired and wireless configuration
- Network analytics (giving users and/or applications behavior allowing detecting potential attacks, planning expansion of the network, etc.)

ALE realizes that the network is abundant with real-time information to help the IT administrator. OmniVista collects and analyzes the data that can educate the IT administrator with detail views, summary views and in some cases trending of real-time and historical data:

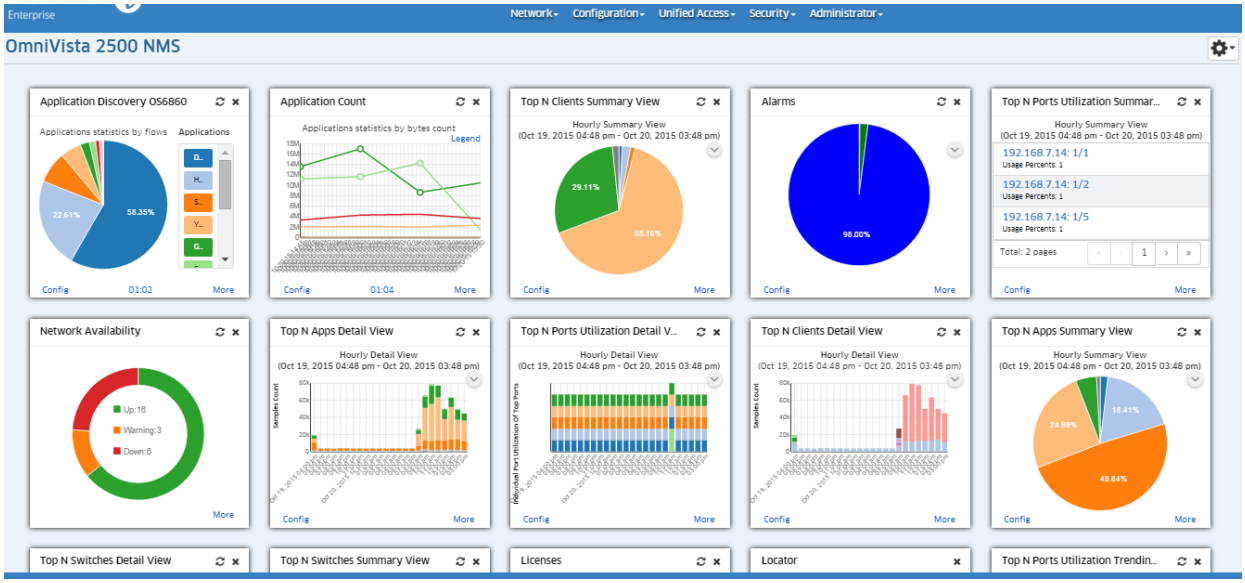


Figure 15: OmniVista 2500 dashboard and Network Analytics

4. Business and technical use cases

A lot of hotels have basic network needs and are very sensitive to price – looking for basic functionality at the lowest price. But some large or luxury hotels do not consider network as commodities only and are ready to invest in a differentiating and state of the art network (wired and wireless). ALE is able to address all requirements in-between those two models.

ALE offers four business and technical use cases where any design element may be selected to build a tailored network for a specific customer.

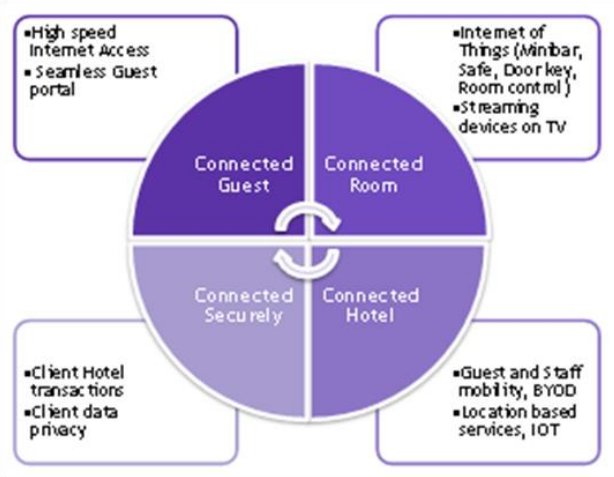


Figure 16: the ideal network for hospitality

4.1. Small or two-star hotel – Use case 1

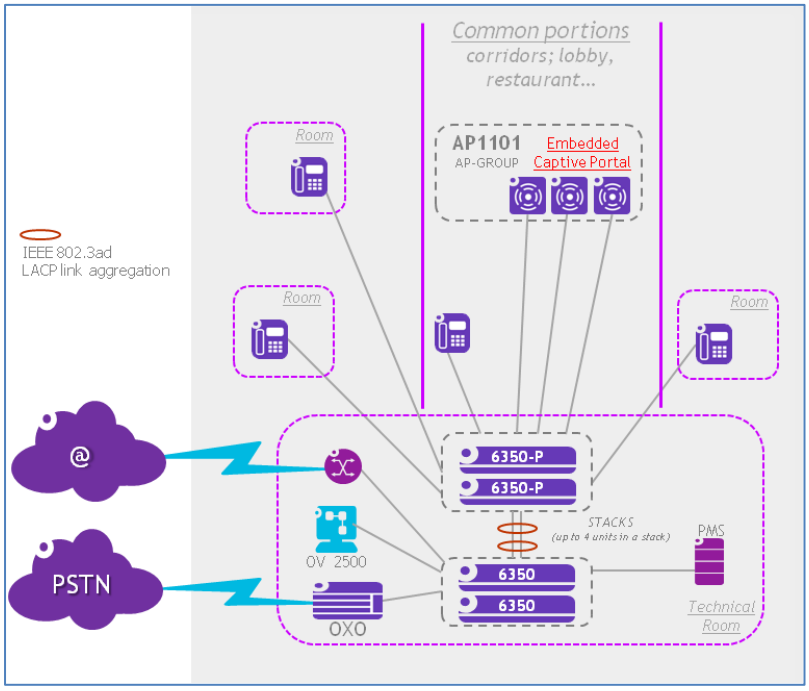


Figure 17: Small or two-star hotel use case

The size of the hotel and number of rooms are limited, and no other digital service than IP telephony (IP phones) are deployed in guest rooms. Required wired ports density (RJ45) can be provided by switches (core and access) deployed in a single central location (the technical room of the hotel) and guests rooms are directly connected to the technical room with UTP copper cabling (up to 100 meters).

Such a network will be based on the OmniSwitch 6350 model for the access and the core layers. Distinct access and core layers will be deployed to maximize fault tolerance by limiting the impact of any issue or outage at the access layer on the core layer that connects critical hotel assets like the PMS, the IP telephony server (Alcatel-Lucent OXO server) and the Internet access modem.

The OmniSwitch 6350 switch supports static routing and provides power over Ethernet (PoE) to deliver electrical power to the IP phones in the guests' rooms and to the Wi-Fi access points deployed in common portions like the hotel reception, corridors or the restaurant. Several (up to four) 6350 switches may be "stacked" in order to build one single logical switch at management, control and forwarding plane, thus reducing administration complexity ("less" equipment to be managed) and improving network stability in case, for instance, of Spanning Tree re-convergence.

Wi-Fi OmniAccess 802.11ac AP1101 access points are deployed as a cluster in common portions of the property (up to 16 APs in a cluster), providing an embedded captive portal for guests' internet access. Such a captive portal relies on an internal data base that needs to be manually provisioned with guests credentials (no PMS integration for automated provisioning).

The OXO server that delivers IP telephony services embeds a TFTP/FTP/HTTP and DHCP servers that allow auto-configuration of both OS6350 switches and AP1101 APs.

The hotel may be equipped with an OmniVista 2500 server for wired and wireless network management which is free for up to 10 nodes.

OmniSwitch 6350 Access and Core	• Static routing • Power over Ethernet • Stacking of up to 4 units for a single logical switch and 192 user ports • 4 one gigabit Ethernet SFP uplink ports
OmniAccess AP1101 802.11ac wave1	• Up to 16 OmniAccess AP1101 in an AP-group (single point of management) • Up to 16 SSIDs and 256 concurrent clients • Distributed control functions: dynamic RF management, rogue AP detection, etc. • Embedded captive portal
Zero-Touch Provisioning	• OXO embedded TFTP and DHCP servers allow auto-configuration of switches and APs
OmniVista 2500	• Network management; free for up to 10 nodes

Table 1: Small or two-star hotel – use case 1 technical specifications

4.2. Medium or three-star hotel - Use case 2

The size of the hotel, the number of rooms and the deployment of connected TVs (IPTV) in gests rooms in addition to IP phones require access switches to be deployed at each floor and in common portions of the property.

Such a network will rely on the OmniSwitch 6350 model for the access layer and the OS6450 model for the core layer deployed in the central technical room. Access switches will be doubly connected with IEEE 802.3ad LACP Link Aggregation to the core layer for additional bandwidth and maximum resiliency. Aggregated links shall be connected to different switch members of a same stack, for maximum resiliency.

Access switches are connected to the central technical room with 1Gb/s uplinks that may be UTP copper cables or optical fiber in case of long distance (>100m)

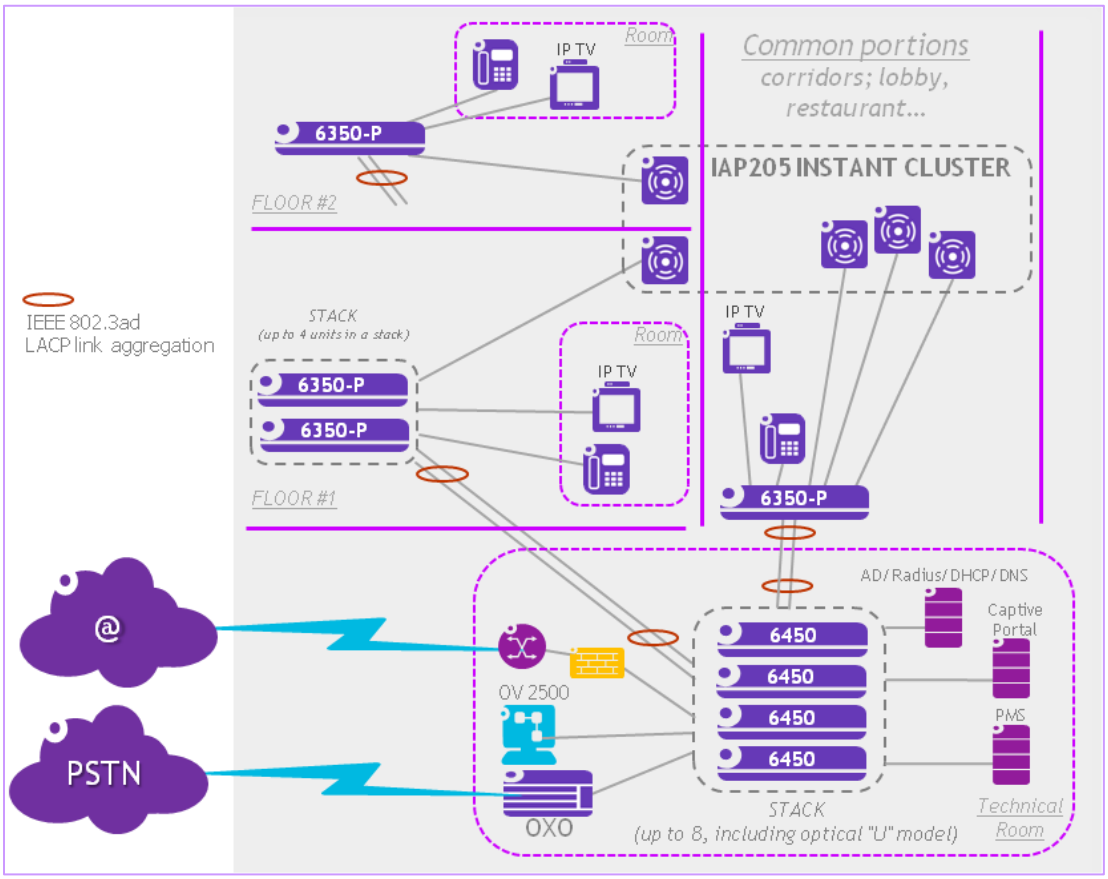


Figure 18: Medium or three-star hotel use case

The OmniSwitch 6350 switch provides power over Ethernet (PoE) to deliver electrical power to the IP phones in the guestrooms and to the Wi-Fi Access Points deployed in common portions like the hotel reception, corridors or the restaurant.

The OmniSwitch 6450 switch is available in a PoE version, supports the RIP routing protocol in addition to static routing and may be equipped with backup power supplies. Several (up to

eight) OS6450 switches may be “stacked” in order to build one single logical switch at management, control and forwarding planes, thus reducing administration complexity (“less” equipment to be managed) and improving network stability in case, for instance, of Spanning Tree re-convergence. Indeed, node virtualization combined with IEEE 802.3ad LACP link aggregation removes layer-2 loops.

The OS6450 switch supports remote stacking over long distances (several kilometers) if the hotel has several buildings and wishes a single management/control/forwarding plane spread over all buildings.

The 802.11ac Wi-Fi OmniAccess IAP 205s are deployed as a cluster in common portions of the property (up to 128 APs in a cluster), in an instant-based architecture (controller-less). Such an option does not offer any captive portal options and requires a third-party captive portal to be acquired and deployed.

The hotel may be equipped with an OmniVista 2500 server for wired and wireless network management which is free for up to 10 nodes.

OmniSwitch 6350 Access	• Static routing • Power over Ethernet • Stacking of up to 4 units for a single logical switch and 192 user ports • Four one gigabit Ethernet SFP uplink ports
OmniSwitch 6450 Core	• Static routing and dynamic RIP routing • Power over Ethernet • Stacking of up to 8 units and mix of "U" units (24 SFP ports) and non "U" models is possible • Backup power supplies
OmniAccess IAP205 802.11ac wave1	• Up to 128 OmniAccess IAP205 in a cluster (single point of management) • Up to 16 SSIDs and 2048 concurrent clients • Distributed control functions: dDnamic RF management, rogue AP detection, etc.
OmniVista 2500	• Network management; free for up to 10 nodes

Table 2: Medium or three-star hotel – use case 2 technical specifications

4.3. Large or four-star hotel - Use case 3

Such a network will rely on the OmniSwitch 6450 model for the access layer and the OS6860 model for the core layer deployed in the central technical room.

The size of the hotel, the number of rooms and the deployment of connected TVs (IPTV) in gests rooms in addition to IP phones require access switches to be deployed at each floor and in common portions of the property. Access switches will be doubly connected with IEEE 802.3ad LACP link aggregation to the core layer for additional bandwidth and maximum resiliency. Aggregated links shall be connected to different switch members of a same stack or virtual chassis, for maximum resiliency.

Both OmniSwitch 6450 and OS6860 switches are available in a PoE version and may be equipped with backup power supplies. Whereas the 6450 model supports only the RIP routing protocol in addition to static routing, the OS6860 switch supports advanced routing protocols like OSPF and BGP. Both models support "node virtualization" in order to build one single logical switch at management, control and forwarding planes made of several physical switches (up to eight) thanks to the "stacking" technology for the OS6450 model on one hand, and the "virtual chassis" technology for the OS6860 on the other hand. Both models also support "remote" stacking over several kilometers. The OS6860 model is available in a "U28" version offering 28 1G SFP ports (to build uplinks connecting access switches) and may be a member of a virtual chassis with other non-optical OS6860 switches.

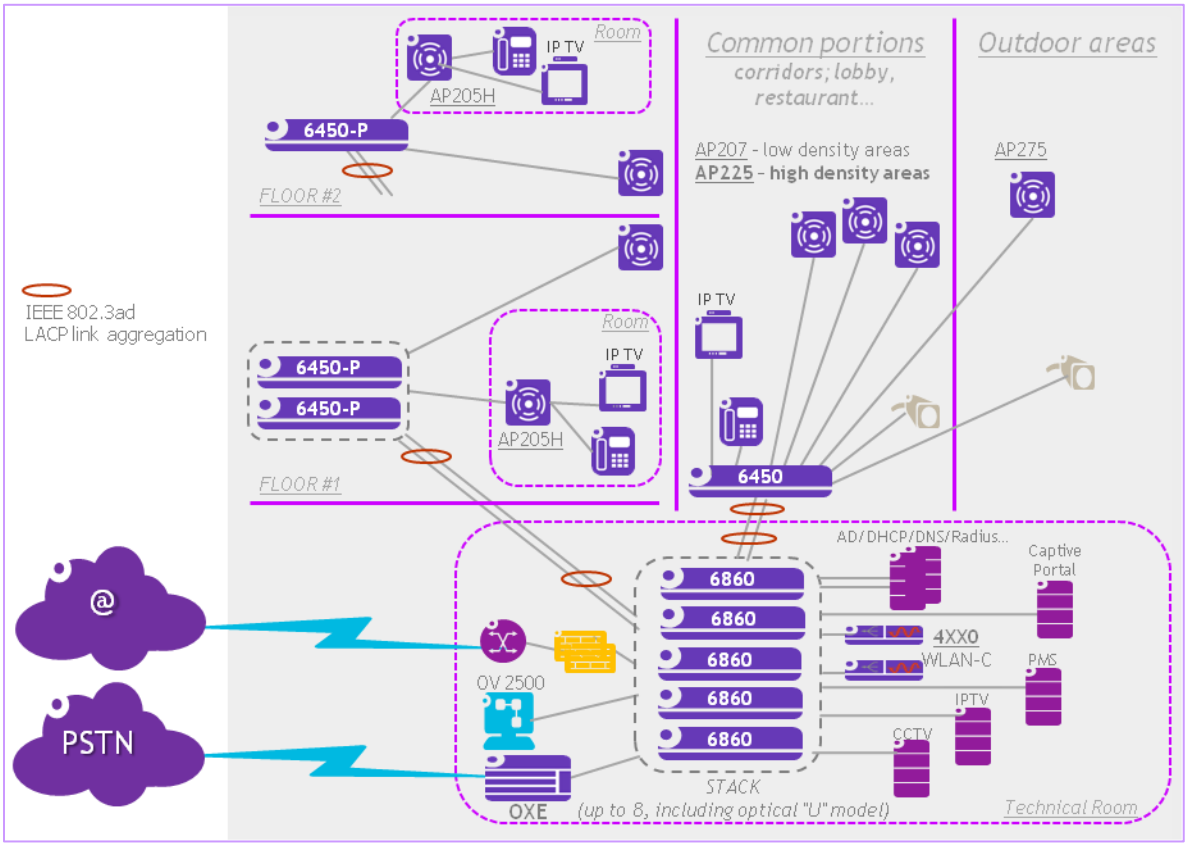


Figure 19: Large or four-star hotel use case

OmniSwitch 6450 switch access switches are connected to the core OS6860 switches (configured as a virtual chassis) in the central technical room with 1Gb/s optical fiber uplinks (>100m) that may be upgraded to 10Gb/s if optical cabling of the hotel can support 10GBASE-F standard (IEEE 802.3ae). Indeed, the OmniSwitch 6450 model gives maximum scalability by offering the possibility to be upgraded from a 10/100Mb/s user ports and 1Gb/s uplinks configuration to a 10/100/1000Mbps user ports and 10Gb/s uplinks configuration with a license upgrade only:

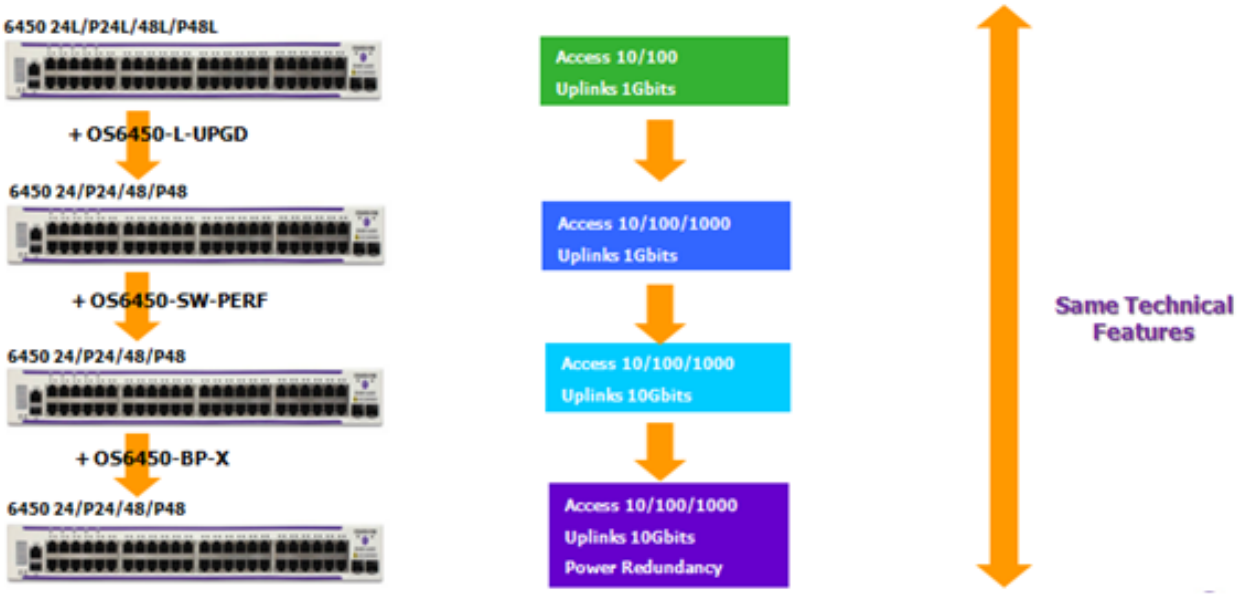


Figure 20: OmniSwitch 6450 scalability

Please note that the OS6860 model in the core layer of the network offers only four 10G ports and connecting the access OS6450 switches would be more relevant with 10G high density ports (OmniSwitch 6900, 10K and 9900) introduced in the next use case.

An answer to the challenge of the high ports density introduced by the various devices (IP phones, IPTVs...) connected to the network and by the size and high number of rooms of the property is the **OmniAccess AP205H** which has been specifically developed for the hospitality market:

Figure 21: Focus on the OmniAccess AP205H

The AP205H is indeed an 802.11ac (wave1) high performance AP with three local Gigabit Ethernet ports are available to securely attach wired devices to the network. One of these ports is also capable of supplying power over Ethernet (PoE) to the attached device. With the AP205H, the hotel makes savings on ports and cabling, and the radio coverage in guests rooms is highly improved and secured leading to maximum guest satisfaction. Additionally, the need for site surveys (and associated costs) is also reduced:

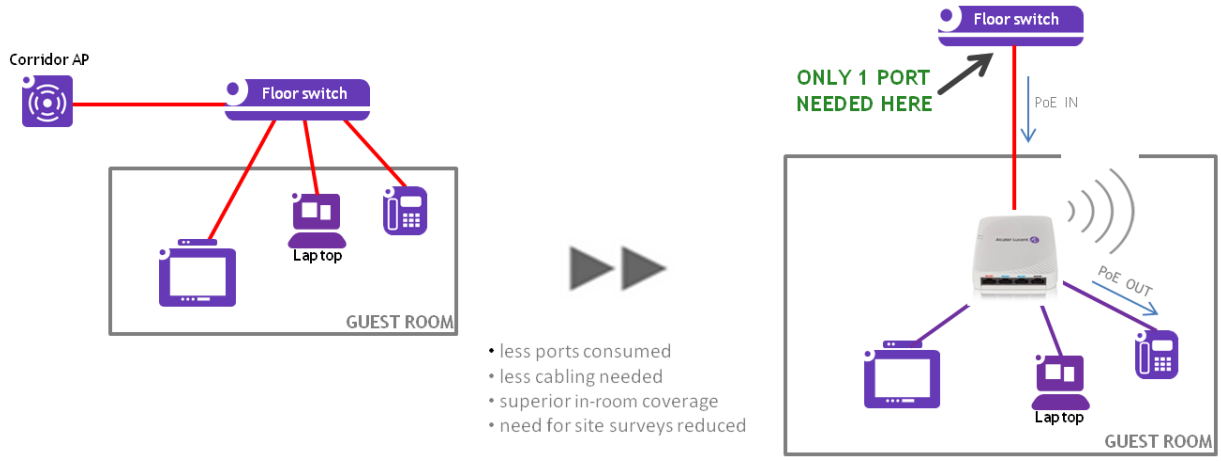


Figure 22: AP205H deployment and benefits

In addition to AP205H APs deployed in a guest's room, AP207 APs in low density areas and AP225 APs in large density areas like a conference room (as well as outdoor ruggedized AP275 access point) are deployed in a controller-based architecture for maximum scalability. The hotel may also decide to go with the latest 802.11ac wave 2 standard and AP305 and AP325 access points.

Such deployment also offers the possibility to rely on the controller embedded captive portal for guests internet access management.

The hotel may be equipped with an OmniVista 2500 server for wired and wireless network management which is free for up to 10 nodes.

OmniSwitch 6450 Access	• Static routing and dynamic RIP routing • Power over Ethernet • Stacking of up to eight units • 1Gb/s uplinks upgradable to 10Gb/s with software license • Backup power supplies
OmniSwitch 6860 Core	• Advanced routing (OSPF, BGP, etc.) • Layer 7 Deep Packet Inspection and webified application recognition (*Facebook*, *SalesForce.com*, etc.) • Power over Ethernet • Stacking of up to eight units and mix of "U" units (24 SFP ports) and non "U" models is possible • Backup power supplies

OmniAccess WLAN controller AP207/225 and 205H 802.11ac wave1	• From 16 (4005 WLC model) to 2048 APs (4750 WLC model) • From 1024 (4005 WLC model) to 32768 (4750 WLC model) concurrent clients • Centralized control functions: Fynamic RF management, rogue AP detection, etc. • Multi broadcast domains deployment • Dynamic IP routing (OSPF) • Specific AP205H AP in rooms, saving cabling and offering optimal radio coverage
OmniVista 2500	• Network management; free for up to 10 nodes

Table 3: Large or four-star hotel – use case 3 technical specifications

4.4. Very large or five-star hotel - Use case 4

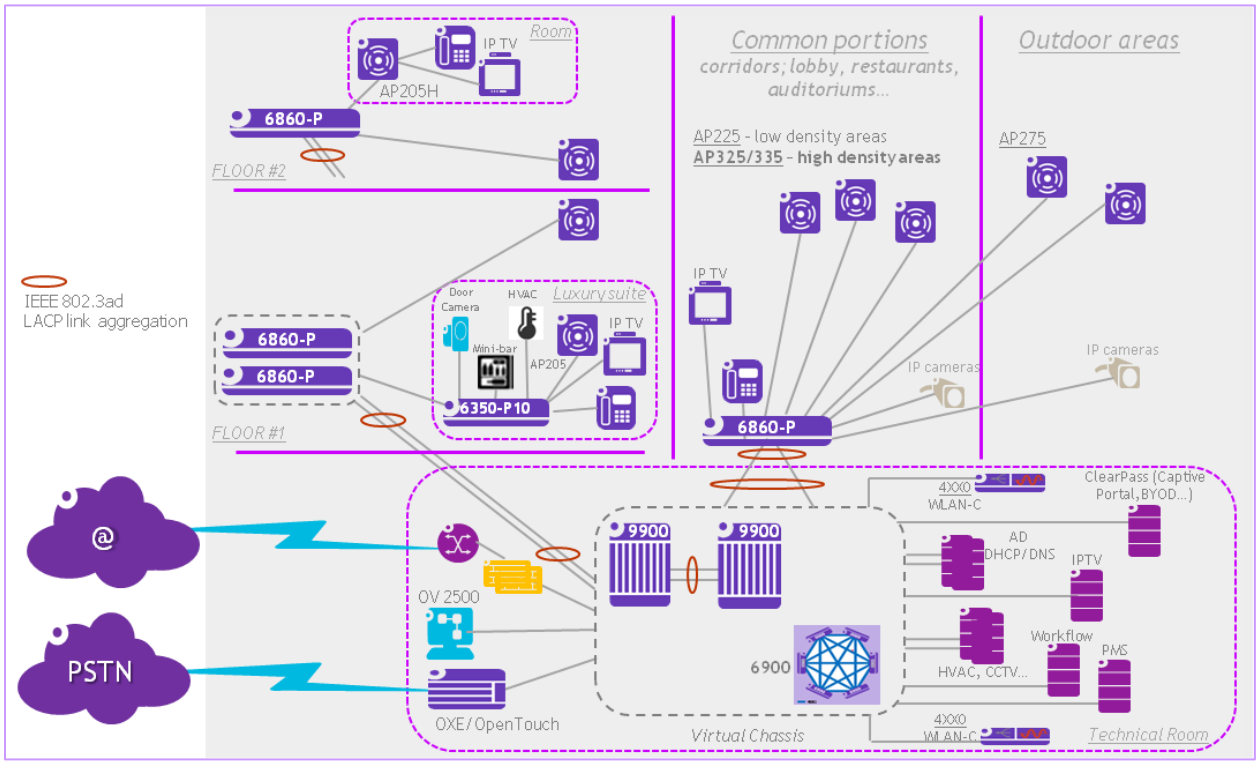


Figure 23: Very large or five-star hotel use case

A network for a very large, or a five-star hotel, which expects high capacity and advanced features will be built with the OmniSwitch 6860 model for the access layer at every floor and in common portions of the property. The OS6860 model is a highly advanced access switch with state of the art features like "Application Visibility" which allows traffic deep packet inspection and makes possible to do application recognition and distinction of "webified" applications (*Facebook*, *SalesForce.com*, online PMS, etc.)

The core layer in the central technical room will be built with the modular OmniSwitch10K or OS9900 switches or the compact OS6900 model, which are all high 10G/40G port density switches. The OmniSwitch 6900 model also offers storage connectivity with Fiber Channel (FC) and Fiber Channel over Ethernet (FCoE) dedicated modules.

Access switches will be doubly connected with IEEE 802.3ad LACP link aggregation to the core layer for additional bandwidth and maximum resiliency. Aggregated links shall be connected to different switch members of a same virtual chassis, for maximum availability.

The 10 port OmniSwitch 6350-10 model (in its PoE version) will also be deployed in some luxury suites that are equipped with many more connected devices like a door camera or the minibar of the suite.

In addition to AP205H APs deployed in guest rooms to save ports, cabling and to provide better and more secured radio coverage, AP225 APs in low density areas and AP325 APs in large density areas like a conference room (as well as outdoor ruggedized AP275 access points) are deployed in a controller-based architecture for maximum scalability. The hotel may also decide to go with the AP335 which supports the IEEE 802.3bz 2.5GBASE-T standard. Indeed, the AP335 is equipped with a 2.5Gb/s Ethernet port which allows with a single Ethernet connection to absorb the maximum 1.733Gb/s wireless throughput that the AP can deliver on the air. Such a connection requires equivalent technology on the connecting access switch and ALE offers the OmniSwitch OS6860-P24Z8 switch which provides eight 1G/2.5G ports that are able to deliver PoE to the attached AP with the same cable:

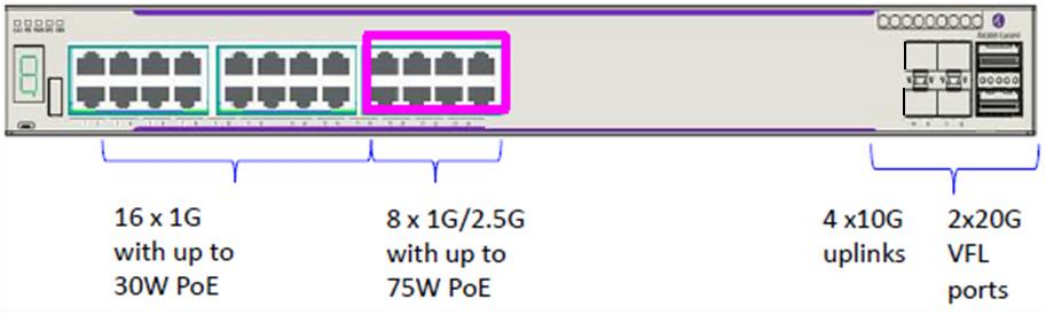


Figure 24: Focus on the OmniSwitch OS6860-P24Z8 multi-gig switch

Providing 75W PoE, the multi-gig ports may also be used to connect “energy-thirsty” devices like PTZ (Pan Tilt Zoom) CCTV cameras that may be deployed by safety departments of some large or luxury properties.

OmniSwitch 6860 and OS6860-P24Z8 Access	• Advanced routing (OSPF, BGP, etc.) • Layer 7 Deep Packet Inspection and webified application recognition (*Facebook*, *SalesForce.com*, etc.) • Power over Ethernet • Stacking of up to eight units and mix of "U" units (24 SFP ports) and non "U" models is possible • Backup power supplies • OS6860-P24Z8 model: Eight IEEE 802.3bz 2.5GBASE-T ports are available, delivering 75W PoE
OmniSwitch 9900/6900/10K Core	• High 10G or 40G port density • FC connectivity (OS6900) • Virtual chassis of two for the OS9000 and 10K models • Virtual chassis of six for the OS6900 model

OmniAccess WLAN controller AP225/325/335 and 205H Outdoor AP275 802.11ac wave1 and wave2	• 802.11ac wave2 APs in high guests density like auditoriums, reducing number of deployed APs • Ruggedized AP275 for outdoor deployment • One IEEE 802.3bz 2.5GBase-T port available on the AP335 AP • Centralized control functions: Dynamic RF management, rogue AP detection, etc. • Multi broadcast domains deployment • Dynamic IP routing (OSPF) • Specific AP205H AP in rooms, saving cabling and offering optimal radio coverage
ClearPass Guest	• Customizable branding and advertising services • Secure guest access (wired and wireless) • PMS integration for automated generation of guests credentials • Interface with payment providers (PayPal, etc.) for premium services
OmniVista 2500	• Network management; free for up to 10 nodes

Table 4: Very large or five-star hotel – use case 4 technical specifications

The multi-gig OmniSwitch 6860-P24Z8 is a member of the OS6860 family with virtual chassis capabilities.

The OS6860 switch supports remote stacking over long distances (several kilometers) if the hotel has several buildings and wishes a single management/control/forwarding plane spreading over all buildings.

The choice of ClearPass offers maximum options for the guest management network (wired and wireless): Built-in advertisement module, PMS integration, customizable billing options (Standard/Premium/VIP)...

5. Key Features and Differentiators

5.1. Features and use case matrix

Feature	Small or two-star hotel - Use case 1	Medium or three-star hotel - Use case 2	Large or four-star hotel - Use case 3	Very large or five-star hotel - Use case 4
Node virtualization: Network optimization, costs savings, and more	A	A	A	A
Zero-Touch provisioning	A	A	PA	PA
Zero-Touch provisioning *The Alcatel-Lucent Application Fluent Network* approach includes automatic setup capabilities for OmniSwitch switches, OmniAccess AP1101 Access Point (small deployment), OmniAccess Instant Access Points (medium deployment), and even VoIP endpoints. When the network device is added to the network and powered on, it can download its configuration through the network. This can be useful in small properties that do not have highly skilled IT staff or in remote locations when first on site operation needs to be done by non-technical personnel. Indeed, when booting, the switch and the AP1101/IAP can contact a DHCP server on the network in order to initiate the download of a configuration file and a firmware from a file server on the network, thanks to the options 66 and 67 specified in the DHCP lease offered by the DHCP server. A hotel equipped with an OXO IP Telephony server can leverage the OXO server which can handle both DHCP and file server functions:	A	A	A	A

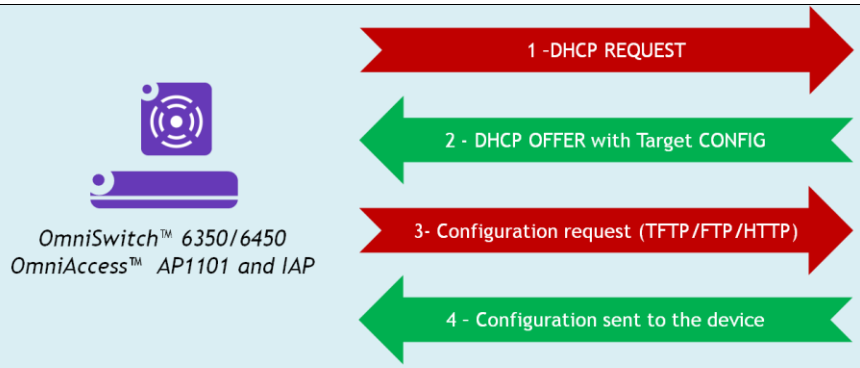


Figure 28: Zero-Touch provisioning

Typical settings defined in default downloaded configuration files from the OXO server include:

- OmniSwitch 6350/6450: PoE activation and QoS
- OmniAccess AP1101 and IAP: Country code, SSIDs ("Employee" with 802.1x authentication, "Guest" and "Voice" with configured QoS), captive portal configuration for guests access (AP1101 only)

For large controller-based deployments, WLAN controllers automatically download configuration information to newly connected wireless access points, integrating them into the existing wireless network infrastructure.

In addition to PoE, and to automate the deployment of IP phones, OmniSwitch switches implement the LLDP-MED protocol that allows to automatically recognize voice devices and insert them in the right voice VLAN with the right voice real-time QoS:

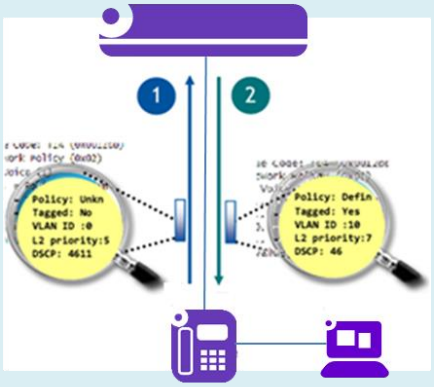


Figure 29: LLDP-MED IP phone auto-configuration

Radio automated and dynamic management

Wireless association optimization: Band and client steering	NA	A	A	A
Role-based profiles: The *User Network Profile*	PA	A	A	A

DPI, uNP, Application Visibility and Enforcement	NA	PA	PA	A
uNP and Unified Access	NA	PA	PA	A
Guest personal network	PA	PA	PA	A
uNP and IoT containment	PA	A	A	A
Guest management and PMS integration	NA	NA	NA	A
Location-based services	*Coming very soon!!*			

(A: available, PA: partially available, NA: not available)

Table 5: Features and use cases matrix

5.2. Node virtualization: Network optimization, costs savings, and more

The Alcatel-Lucent Enterprise solution for node virtualization is based either on the virtual chassis technology (10K/9900/6900/6860 models) or the stacking technology (OS6350/OS6450 models). In both cases, the switches are united into a single logical unit via special stack cables or standard 10/40Gb/s Ethernet cables. The resulting stack or virtual chassis is managed as a single unit by a master switch, which is elected from one of the member switches. It also behaves as a single node at the control and forwarding planes. Each switch in the virtual chassis has the capability to behave as a master or subordinate in the hierarchy. The master switch is elected and serves as the control centre for the virtual chassis. Each stack or virtual chassis has a single IP Network Management address. The Ethernet switches are distributed in a ring topology or in a mesh topology as a chassis with increased redundancy, minimal user configuration and fast convergence upon topology changes. The stacking and the virtual chassis offer the following advantages:

- Simplified administration because the resulting logical equipment is managed as a single piece of equipment (one management IP address only)
- Port members of a logical aggregated link (IEEE 802.3ad LACP) may be ports of distinct switches for maximum resiliency (in case of a switch failure)
- Optimal bandwidth use because node and link (LACP) virtualization avoids spanning-tree blocked ports
- Fast failover in case of link failure (<50ms)
- Scalability because new switches may be added to stack or a virtual chassis (up to the limit)
- Improved fault tolerance because one failed switch will not impact the other switches in the stack or the virtual chassis

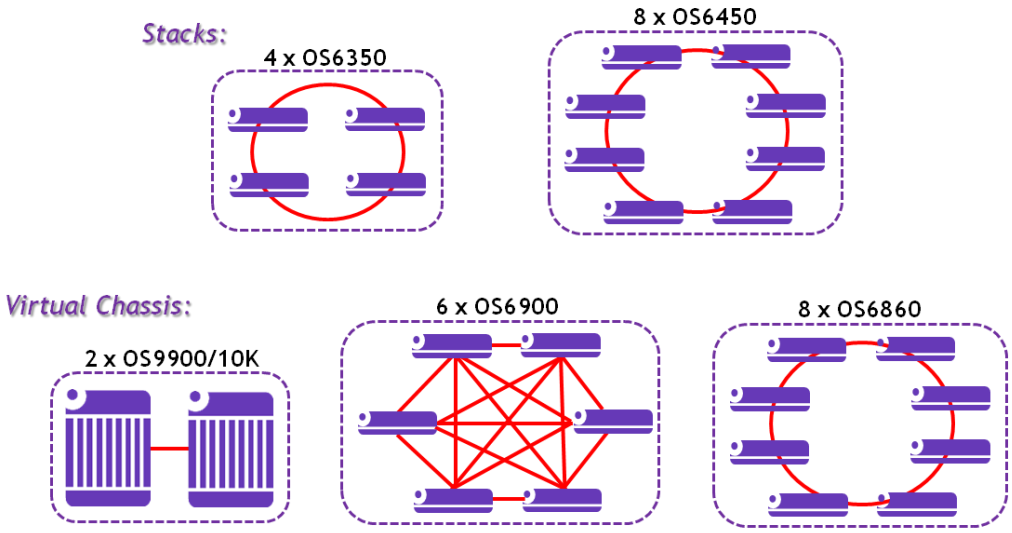


Figure 25: Node virtualization

The stacking technology presents the following characteristics compared to the virtual chassis technology:

- Ports and stacking cables may be proprietary and may need an additional module
- The loop topology leads to weaker performances

Virtualizing network equipment and links optimizes resource utilization, reduces operational complexity, and increases scalability. The virtualization of both switch management and network links, referred to as link aggregation (LACP, 802.3ad), is central to allowing the new two-layer architecture of an application fluent network to operate as a Layer-3 network without requiring the use of the spanning tree protocol, or the VRRP protocol and inherent switchover delay.

Virtualization is also an important component of a flattened and simplified architecture, since it removes spanning tree protocol inefficiencies and enables the network to keep all links active and to fully use all available resources. Traditional methods disable all redundant links, using them only if the main link or switch fails. Technologies such as virtual chassis (VC) enable up to six core switches in the core network or up to eight access switches in the access network to be combined and behave as a single fully redundant unit. In many cases this can replace expensive chassis and require less space and power, and be delivered at lower cost.

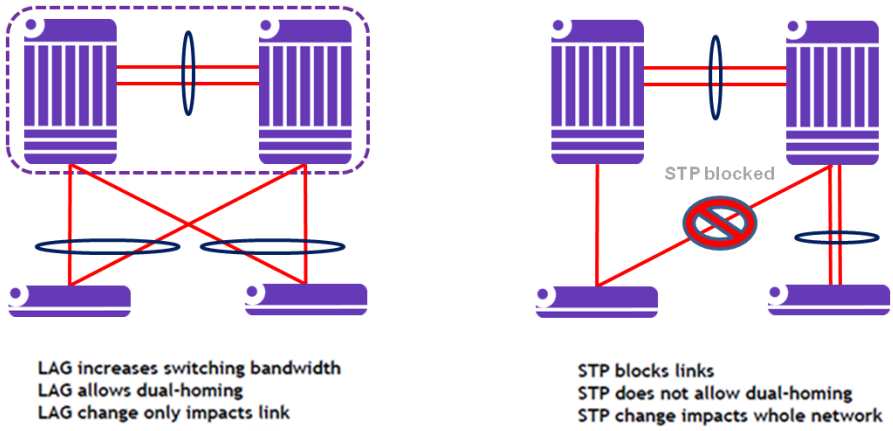


Figure 26: Equipment virtualization and network optimization

As depicted in diagram below, equipment virtualization at the access and the core layers is also an efficient tool to save ports and cabling when connecting access switches deployed at each floor of the hotel, to the core equipment deployed in the technical room of the hotel:

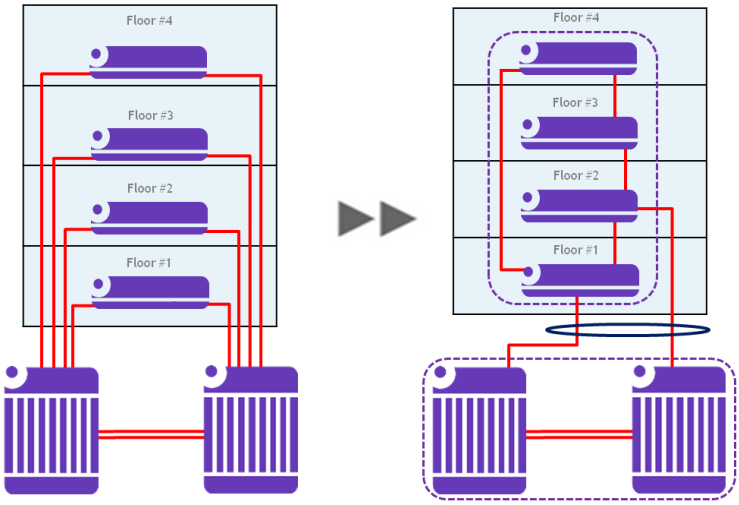


Figure 27: Equipment virtualization and ports and cabling savings

The OS6450 and OS6860 models support remote stacking over long distances (several kilometers) if the hotel has several buildings and wishes a single management / control / forwarding plane spreading over all buildings.

5.3. Zero-Touch provisioning

The Alcatel-Lucent *Application Fluent Network* approach includes automatic setup capabilities for OmniSwitch switches, OmniAccess AP1101 Access Point (small deployment), OmniAccess Instant Access Points (medium deployment), and even VoIP endpoints.
When the network device is added to the network and powered on, it can download its configuration through the network. This can be useful in small properties that do not have highly skilled IT staff or in remote locations when first on site operation needs to be done by non-technical personnel. Indeed, when booting, the switch and the AP1101/IAP can contact a

DHCP server on the network in order to initiate the download of a configuration file and a firmware from a file server on the network, thanks to the options 66 and 67 specified in the DHCP lease offered by the DHCP server.

A hotel equipped with an OXO IP Telephony server can leverage the OXO server which can handle both DHCP and file server functions:

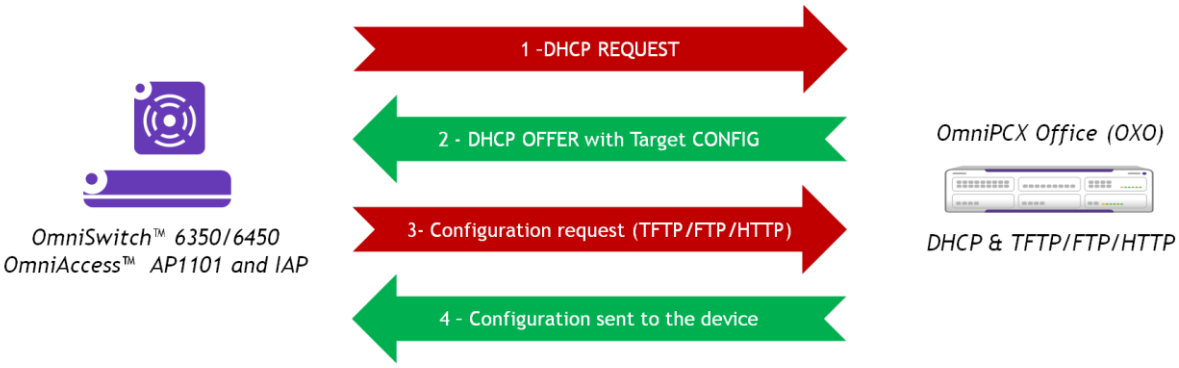


Figure 28: Zero-Touch provisioning

Typical settings defined in default downloaded configuration files from the OXO server include:

- OmniSwitch 6350/6450: PoE activation and QoS
- OmniAccess AP1101 and IAP: Country code, SSIDs ("Employee" with 802.1x authentication, "Guest" and "Voice" with configured QoS), captive portal configuration for guests access (AP1101 only)

For large controller-based deployments, WLAN controllers automatically download configuration information to newly connected wireless access points, integrating them into the existing wireless network infrastructure.

In addition to PoE, and to automate the deployment of IP phones, OmniSwitch switches implement the LLDP-MED protocol that allows to automatically recognize voice devices and insert them in the right voice VLAN with the right voice real-time QoS:

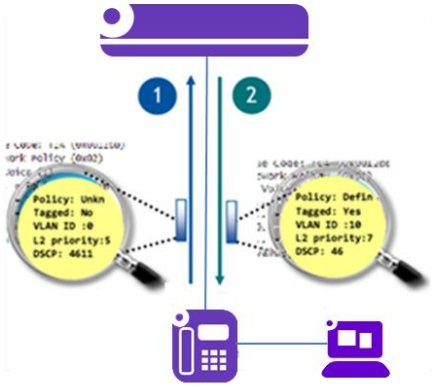


Figure 29: LLDP-MED IP phone auto-configuration

5.4. Radio automated and dynamic management

Wireless networks operate in environments with electrical and radio frequency devices that can interfere with network communications. Microwave ovens, cordless phones, and even adjacent Wi-Fi networks are all potential sources of continuous or intermittent interference.
The OmniAccess series supports dynamic management of the radio frequency (RF) spectrum using, on one hand, *Adaptive Radio Management* (ARM) feature for the controller-based and instant-based deployment options (large and medium deployments) and, on the other hand, *radio dynamic adjustment* (RDA) feature available with the AP1101 access point (small deployment).

Both features work in background and allow each AP to figure out its own best channel and power settings. The system will detect changes in the RF environment and dynamically react to maintain the most optimized RF system possible. This also enables the AP to automatically self-heal in the event of an AP failure or to detect coverage holes. ARM and RDA are a continuous process, using APs to constantly scan channels, gathering usage data and SNR statistics. Channels are switched as necessary to provide minimal channel contention, with dampening used to prevent flapping. Similarly, power levels are dynamically calibrated to avoid interference with other APs.

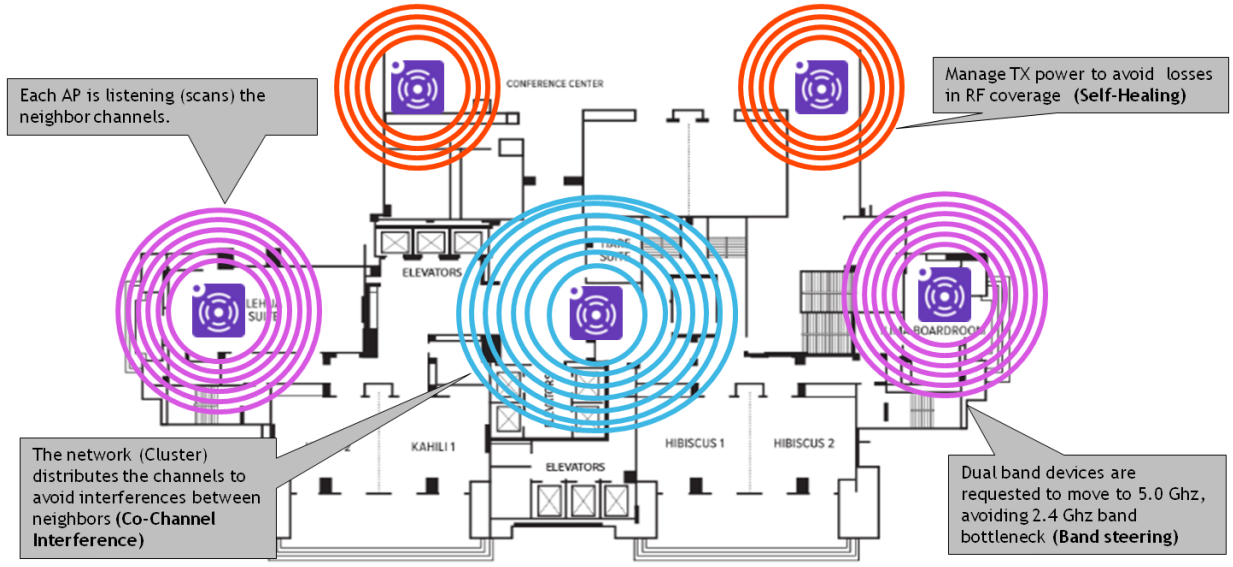


Figure 30: Radio automated and dynamic management

ALE recommends a procedure that involves deploying APs in a relatively dense configuration every 20 to 30 meters and then allowing the OmniAccess wireless active RF management and monitoring features, ARM or RDA, to automatically adjust each AP to the environment.

5.5. Wireless association optimization: Band and client steering

Ensuring that all wireless network clients get the service they need is a major challenge, especially when smartphones, tablets, and other clients control their own connectivity and roaming decisions. Clients are typically in control of connectivity decisions, such as which AP

to associate with, what speed they send and receive data, and when to change APs as they roam.

Unfortunately, clients do not have a system view of the network and often make poor decisions such as connecting to the first AP they hear, regardless of whether it matches their needs. For example, a dual band 2.4Ghz and 5GHz capable smartphone may attach itself to the 2.4GHz band, even if it is crowded, reducing the client's throughput by half despite the availability of a 5GHz-capable AP within that client's range. Another example is that once attached to an AP, clients tend to stay attached even when guests begin to roam and the WLAN signal weakens. Because clients tend to attach to the strongest AP they hear, a given AP can become overloaded and clients will continue to attach to an already overloaded AP simply because it is the first or strongest signal they detect. As a result of this stickiness, performance for mobile guests often degrades, dragging down overall network throughput. Even a client capable of fast data rates must drop back to a slower rate if its user moves far from the AP
This is a common problem in lobbies, conference rooms and other locations where guests congregate in a hotel. Clients attached to an overloaded AP experience poor performance and, due to client "stickiness", performance can degrade even as users leave the area.

In contrast, the WLAN infrastructure, with its system level view of the network and ability to monitor clients, is ideally suited to manage client connectivity:

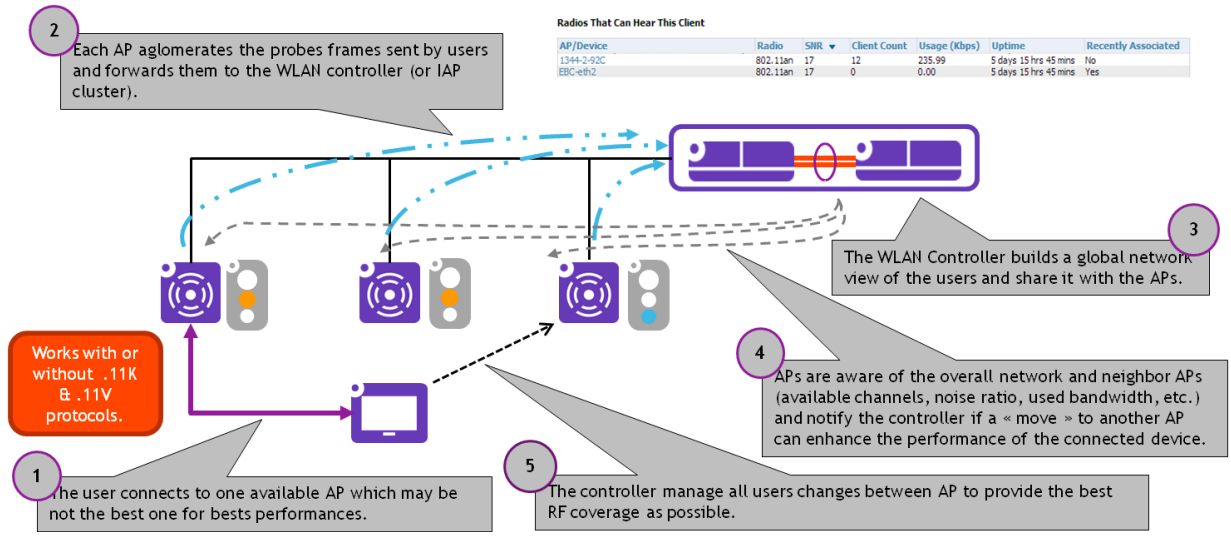


Figure 31: Wireless clients association optimization

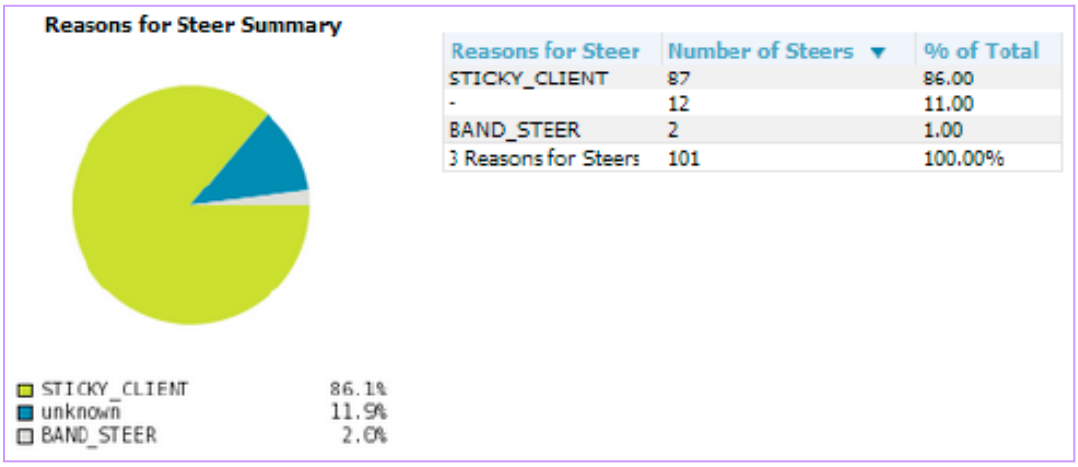
The controller-based and Instant-based deployment models (large and medium deployments) benefit from the ClientMatch feature handled by the WLAN controller or the elected virtual controller in an Instant-based cluster. The ClientMatch feature allows monitoring of each client's capabilities and connection on a WLAN, matching every client to the best radio on the best AP. By consistently monitoring each client, ClientMatch can react to client behavior at the time of connection and as client and network conditions change.

For example, if a client moves into another AP's coverage area or interference causes performance to drop, the feature will automatically move the client to an AP or channel that can deliver better performance. All standard-based clients work with ClientMatch; no proprietary software is required.

ClientMatch features a number of capabilities that enable it to pair clients and APs including:

- **Band steering**: If a dual-band capable client attempts to connect to a 2.4GHz radio on an AP with a 20-MHz, ClientMatch will steer the client to an available 5-GHz radio with a 40-MHz channel and good signal strength, taking advantage of the client's capabilities to double its throughput
- **Client steering**: When a client attempts to connect to an AP that provides sub-optimal performance, ClientMatch uses client steering to direct that client to a better AP. For example, if a client connects to an AP with a weak signal, ClientMatch will steer that client to an AP with a stronger signal
- **Dynamic load-balancing**: ClientMatch addresses client density and stickiness problems by dynamically distributing clients across available APs and channels, ensuring that individual APs are not overtaxed and client performance is continually maximized, even in dense environments.

Hereunder picture depicts a ClientMatch report showing sticky clients that were steered, how many times they were steered and why there were steered:



Reasons for Steer	Number of Steers	% of Total
STICKY_CLIENT	87	86.00
-	12	11.00
BAND_STEER	2	1.00
3 Reasons for Steers	101	100.00%

Figure 32: ClientMatch steering report

5.6. Role-based profiles: The *User Network Profile*

More than ever before, security needs to be built in from the ground up and applied universally across all methods of access for the network, wired or wireless. Network edge security services provided with the Alcatel-Lucent Enterprise solution are applied to each individual or device, rather than fixed to the switch port.

Using role-based profiles, a user (staff or guest) connecting to the network is authenticated and then a user profile is assigned that specifies all the network security behavior including access control lists (ACLs) and QoS rules. With this capability, wherever the user goes unique security rules will follow. Indeed, embedded in the access layer switches and APs is a feature unique to ALE: The Alcatel-Lucent **User Network Profile (uNP)**.

The following figure shows the uNP conceptually, where the users are surrounded by the information required to support them. The uNP enables the network to follow the user and automatically adjust its configuration depending on where the user is connected, instead of the traditional approach of static configurations based on switch port, AP or service set identifier (SSID). The uNP feature minimizes IT effort by eliminating the need to manually adjust the network, it improves mobile application delivery performance by fine-tuning the network so users have the same experience wherever they are connected and it provides consistent security throughout the network:

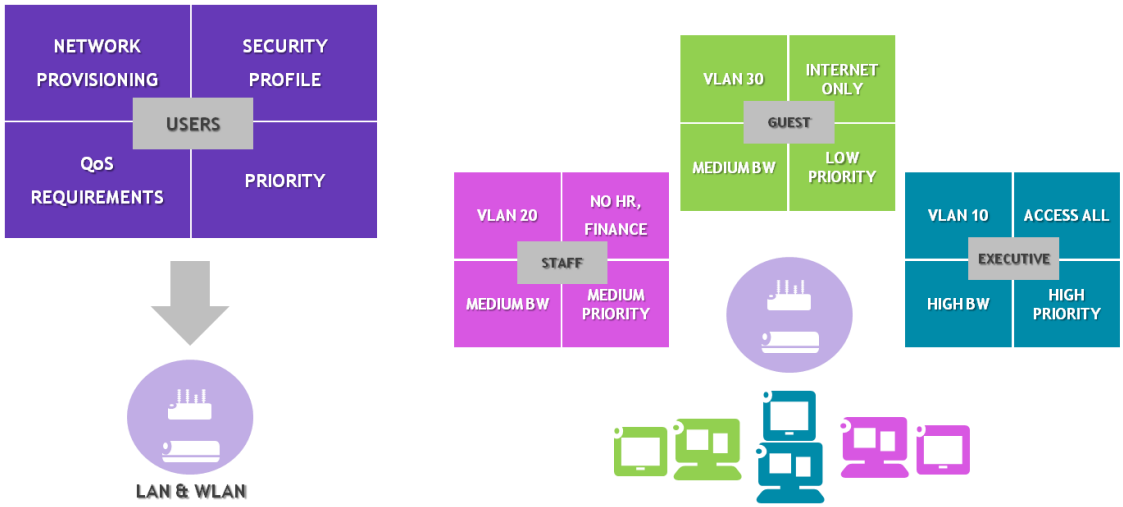


Figure 33: User Network Profile

5.7. DPI, uNP, Application Visibility and Enforcement

There are several solutions available to IT and network administrators to evolve and improve network performance. The most common is to increase available bandwidth, along with defining a system of QoS for given types of traffic. The downside with just “throwing” more bandwidth at a problem is that it is expensive, invasive (that is, redesigning the network, rip-and-replacing existing equipment) which consumes time and resources, which can be put to better use improving the business. Without properly controlling, or indeed just knowing, what traffic flows over a network, the performance increase brought by adding bandwidth is short term, with network traffic just using whatever bandwidth is available.

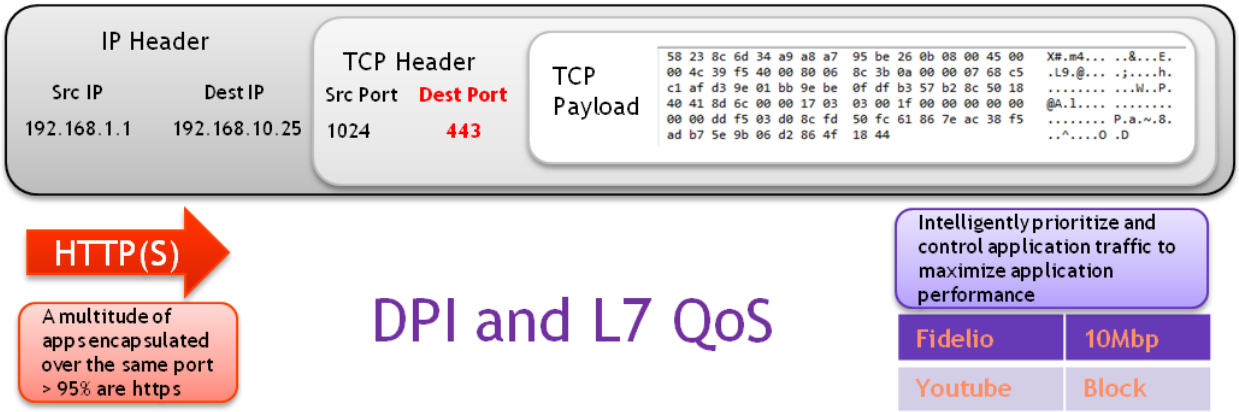


Figure 34: Deep Packet Inspection - Application Visibility and Enforcement

The Alcatel-Lucent OmniSwitch 6860 and the OmniAccess series (whether controller-based or Instant-based) provide application visibility and analytics using integrated deep packet inspection (DPI) technology. DPI provides IT with detailed visibility into the applications being used (by monitoring application signatures) and bandwidth consumed, and with the ability to immediately enforce policies at user level to control prioritization, QoS and security of these applications right at the edge of the network, both wired and wireless.

Application Visibility and Enforcement is an answer to the challenge of application "webification". More and more applications - even corporate applications like online PMS in the cloud - use the same port to communicate and appear as HTTP(S) traffic. Based on a signature application file and its DPI capability, the Application Visibility and Enforcement feature allows identifying unique applications (even when encrypted) like *Facebook*, *Twitter*, *and SalesForce.com*. After applications are identified, access controls and policies can be applied with uNPs to prioritize the performance of enterprise applications over personal ones. Shown below are Application Visibility reports samples that are provided by OmniVista 2500 NMS for an OS6860 switch (right) on one hand, and by the controller or virtual controller embedded GUI (left) on the other hand:

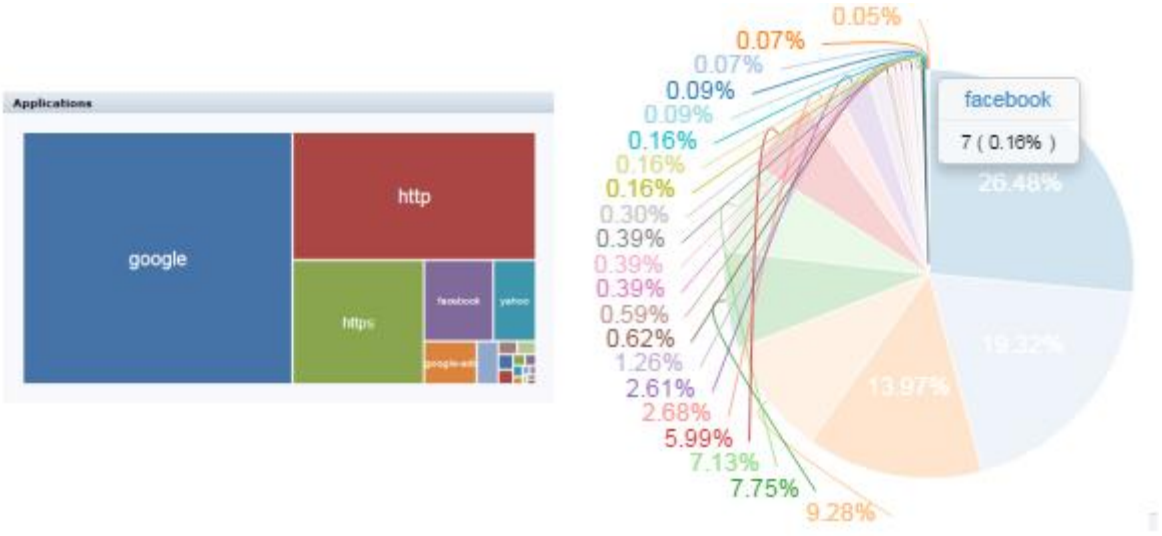


Figure 35: Application Visibility reports samples

5.8. uNP and Unified Access

Deploying an ALE converged network solution (wired and wireless) with Unified Access ensures staff and guests can fully exploit the benefits of mobility. Users can experience the same level of high-quality application delivery, the same policies and the same network services whether they are using a wired or wireless connection. With IEEE 802.11n and 802.11ac access points, even the performance is similar between wired and wireless, providing proper support for the increased speeds needed for real-time applications.

A Unified Access approach also provides simplification for the IT team. They can now offer a common set of policies on both wired and wireless access and the same level of security. Indeed, Alcatel-Lucent OmniVista 2500 NMS has the functionality to define unified security and QoS rules which can then be used, with User Network Profiles, to provision the switch or the WLAN controller with the correct access details for each user or type of user that will connect to the network, for a seamless user experience, wired or wireless.

Figure 36: Context-based and unified security

The diagram below describes the one-step unified wired and wireless access provisioning from the OV2500 NMS and requires an OS6860 switch at the access layer of the wirer network. This option eliminates the possibility of any errors being introduced (by having to repeat the process twice) and saves time and money by reducing the steps needed to provision the same network access rules to all equipment on the network:

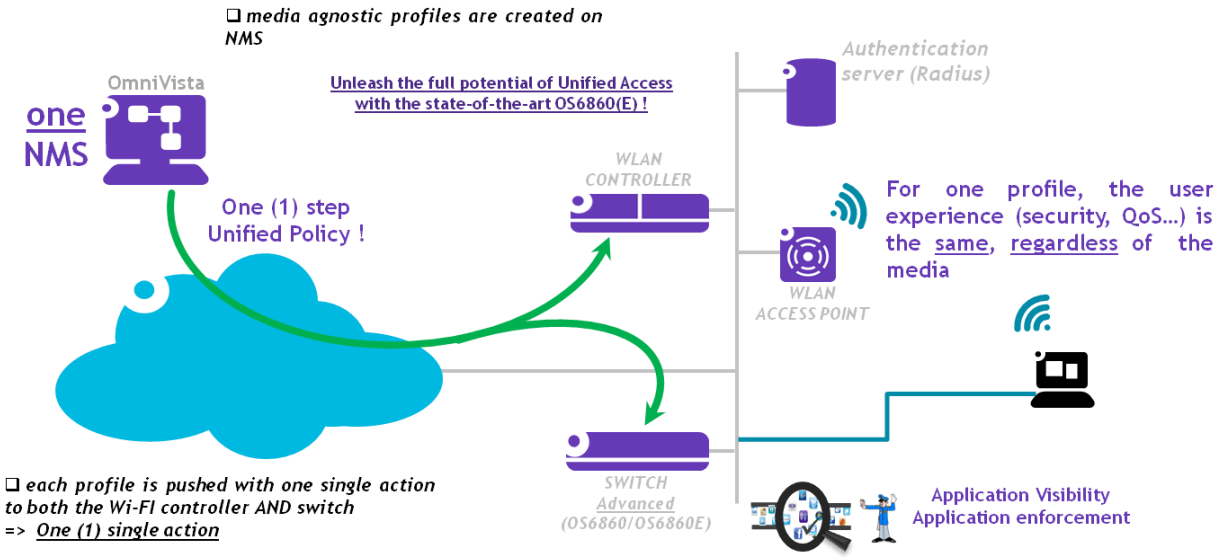


Figure 37: one-step unified wired and wireless access provisioning (6860)

The diagram below describes the two-step unified wired and wireless access provisioning from the OV2500 NMS in a scenario where the wired access layer of the network is built with OmniSwitch 6350/6450 switches:

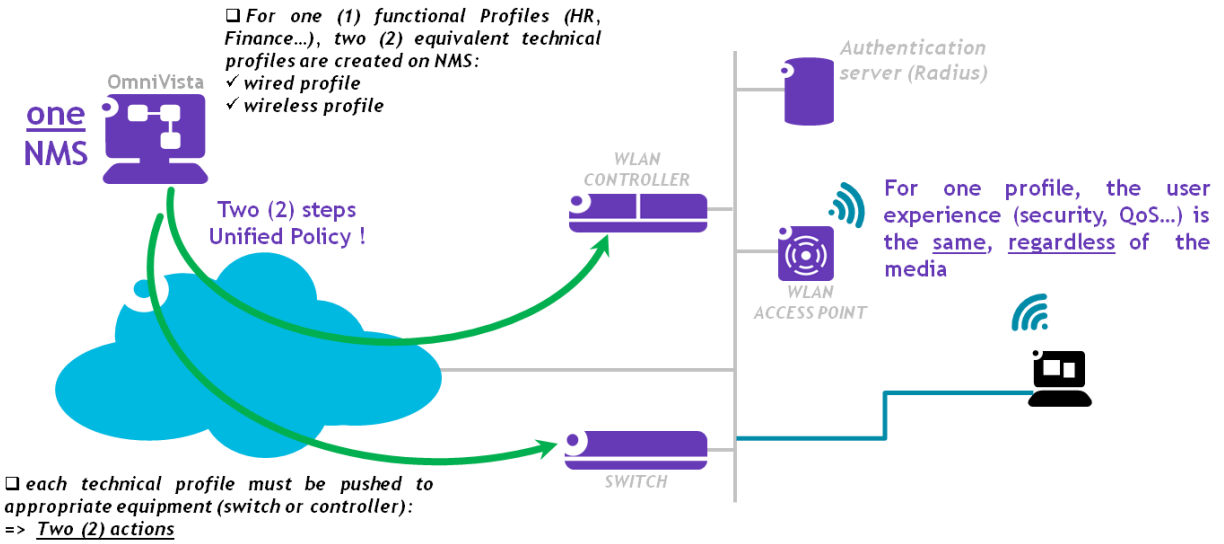


Figure 38: two-steps unified wired and wireless access provisioning (6350/6450)

Mobility and Unified Access is essential in a context where he management of a hotel is now done by employees from the front desk (with a wired connection) but also while on the move with tablets: Housekeeping staff equipped with a workflow management tool notifying that the mini-bar is lacking products, restaurant waiters equipped with a mobile POS system, and so forth. Moreover, a wired connection is still expected and required by guests who do not trust the wireless access that is offered to them. The user experience cannot be different whether wired or wireless.

5.9. Guest personal networks

Guests expect today a “home” experience with no possible interference with other guests. Deploying guests’ dedicated and segregated networks that would isolate guests from each other’s is the foundation of that “home” experience.

One option would be to configure one VLAN for each guest. That VLAN would connect all devices, wired or wireless, belonging to the guest, including permanent connected devices installed in the room: IPTV, mini bar, door camera, and more. But this would dramatically add complexity to the global network architecture and the IP addressing plan: Guests dedicated subnets, IP gateways explosion, etc. ALE has therefore developed the *Private VLAN* (PVLAN) feature.

A standard VLAN usually represents a single broadcast domain, but a PVLAN divides a VLAN (Primary) into sub-VLANs (Secondary). The single broadcast domain is partitioned into smaller broadcast sub-domains while keeping the existing Layer-3 configuration. When a VLAN is configured as a PVLAN, the PVLAN is referred to as the primary VLAN, and any subsequent VLANs that are associated with the primary VLAN are referred to as secondary VLANs.
To isolate the guests from each other, Secondary VLANs can be created for each guest under the primary VLAN. The following diagram represents the scenario where Guest-1 and Guest-2 are sharing the same primary VLAN. To isolate them from communicating with each other, they are assigned to individual secondary VLANs. These secondary VLANs are assigned “community” ports. Community ports cannot exchange traffic if they are assigned to different secondary VLANs. Secondary VLANs can communicate with the primary VLAN through the promiscuous port that is assigned to the primary VLAN and that can communicate with any community port of any secondary VLAN:

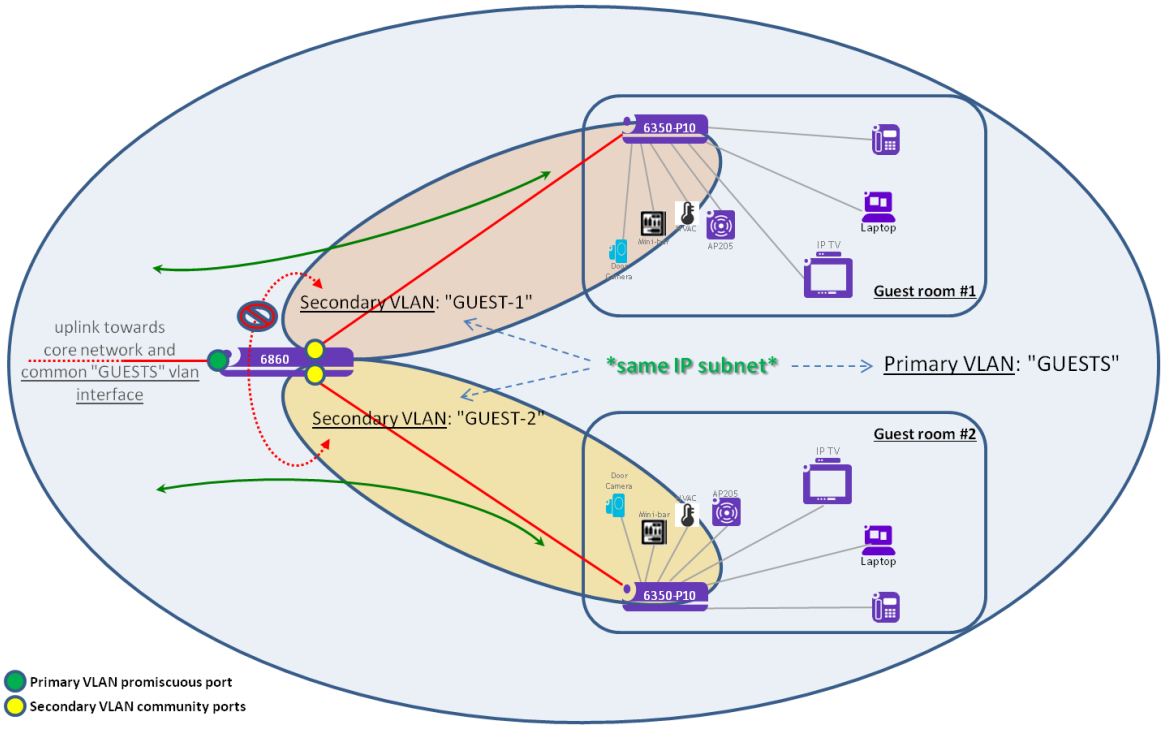


Figure 39: Private VLAN and guest personal networks

When wireless connected, in-between guest isolation is inherent to the nature of the ALE controller-based or Instant-based wireless architecture, even if both guests are in the same

VLAN. Indeed, both architectures have been designed to force guest traffic to go through the native firewalling function that is embedded in any ALE WLAN controller or virtual controller:

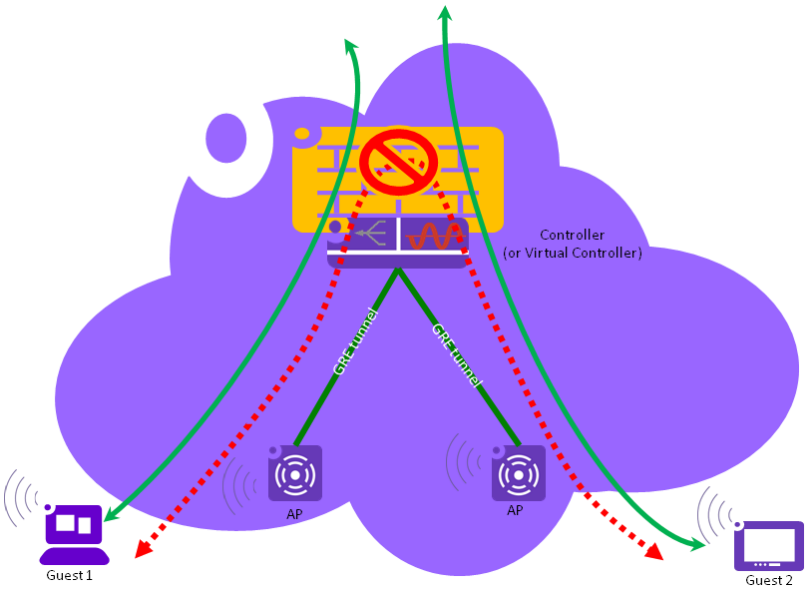


Figure 40: In-between wireless connected guest isolation

User traffic is applied user based firewall policies that block by default traffic between users even if both guests are in the same VLAN, with some exceptions like peer-to-peer RTP media that is established between IP phones during an internal phone conversation.

5.10. uNP and IoT containment

As discussed in chapter 2.9, IoT is a phenomenon that any hotel would consider today. Indeed, IoT application is almost infinite in the hospitality industry including:

- Remote-management systems
- Instant notification of failures
- Surveillance and access control
- Lighting and HVAC regulation
- Motion and humidity detection

But, deploying connected devices also introduces new security risks.

ALE helps hotels adopt IoT with an innovative IoT containment technology that provides the security and the right resources to make connected devices run successfully. This is done by leveraging the key “User/Machine network Profile” or **uNP** concept.

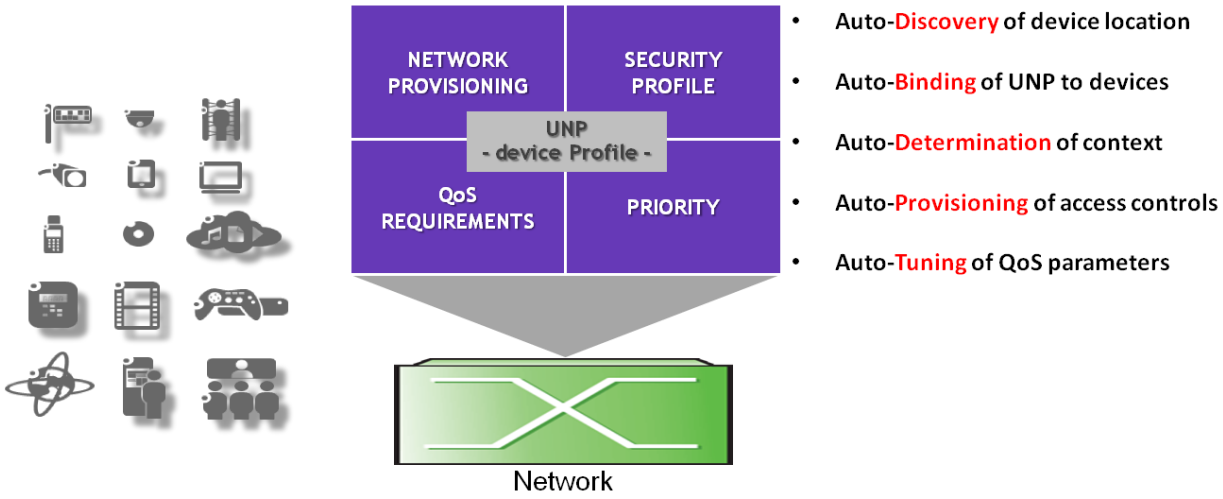


Figure 41: uNP and IoT containment

With this technology, we force every single device to be authorized or classified before it can connect to the network. Once it is authorized, which could be as simple as using local (within the switch) classification of the device (based on its MAC address, IP address or IEEE 802.1q VLAN-id) or using 802.1x authentication, the device is classified and put in a certain profile. In the profile we have information that define in which container this device is going to participate, what quality of service it is going to be applied, and what level of security. In other words, we associate a device with a virtual dedicated and segregated environment.

The pictures below describes some of the thirty different IoT device types that have been securely deployed on one single Ethernet/Wi-Fi network designed by ALE for a five-star luxury hotel in Paris (France):

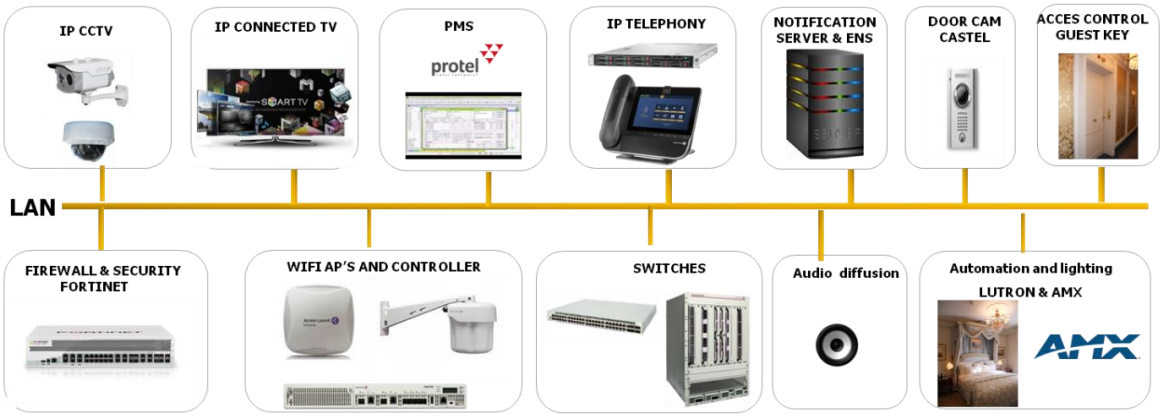


Figure 42: IoT luxury hotel use case

5.11. Guest management and PMS integration

For the hospitality sector, ClearPass integrates with leading property management systems such as Micros Fidelio and *HTNG Agilisys*. With this integration, hotel guests only need to provide their room number and surname to register on to the Wi-Fi system.

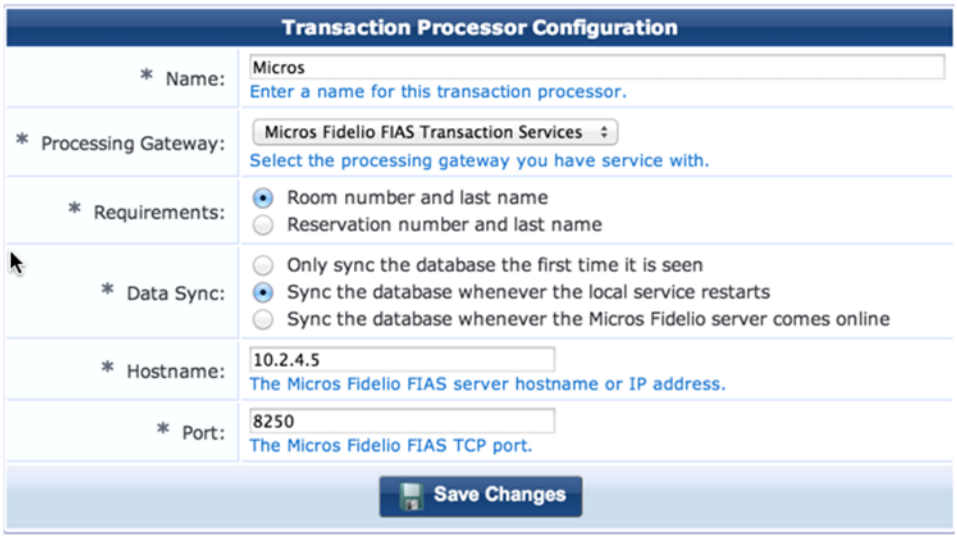


Figure 43: ClearPass and PMS integration

After a successful transaction ClearPass will allow the guest on to the network and inform the PMS system of the transaction event, should the property want to charge for access, etc.

5.12. Location-based services

Indoor location-based services provide a unique and differentiated service in the competitive hospitality industry.

Figure 44: Location-based services within a hotel

With personalized marketing, way finding, behavioral insights and other services will enhance customer satisfaction and motivate spending:

- **Location based marketing and services**: Welcome and farewell greetings, recognize loyalty guest members with special offers, provide real time promotions to increase

sales as guests pass by amenities such as restaurants and gift shops, cross-sell and upsell services such as upgraded rooms, valet parking or food specials at the point of decision, enable to find the closest staff member who can answer or deliver service.

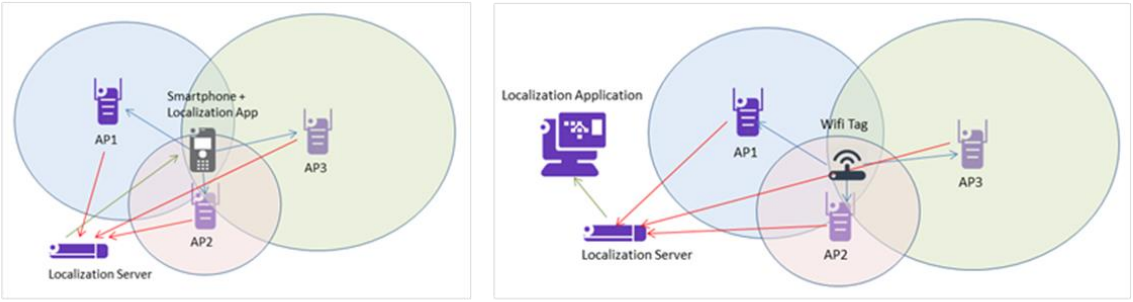
- **Indoor navigation**: Provide step-by-step directions to points of interest in hotels or on tradeshow floors, offer accessibility routes and services for guests with special mobility needs, provide exit maps and directions in the event of an emergency, enable guests to share their location and find friends, family, and colleagues at large venues and conferences quickly and easily.

- **Data analytics and business results**: With "heat maps" and footfall analysis, hotel management can analyze consumer behavior and add services where guests congregate, Increase guest satisfaction with the hospitality or event experience, drive facility and time-limited event revenues with real-time offers, increase guest per-visit revenues with mobile marketing, improve staff efficiency by streamlining guest interactions, provide enhanced security and crowd control to increase guest comfort and security.

Location-based services may be built using two technologies:

Wi-Fi technology:

The localization technique used for positioning with wireless access points is based on measuring the intensity of the received signal on several Wi-Fi access points (AP) and the method of "fingerprinting".



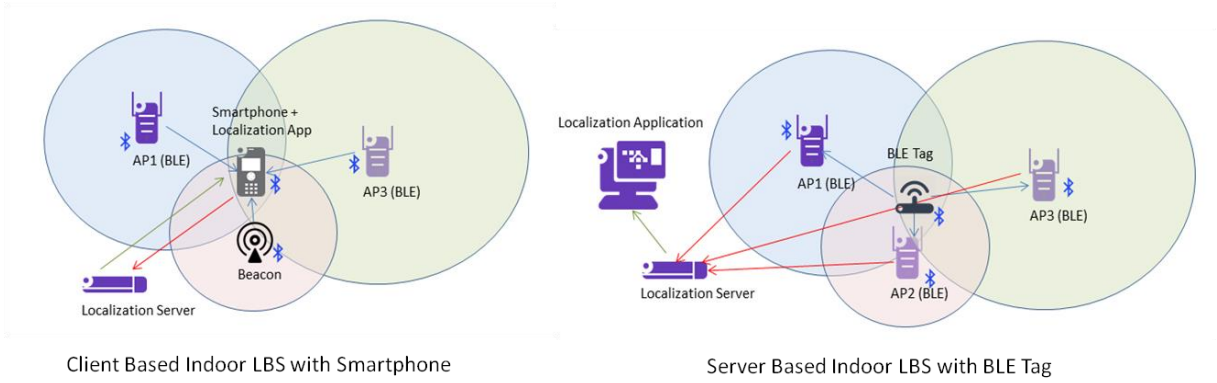
Server Based Indoor LBS with Smartphone Server Based Indoor LBS with Wi-Fi Tag

Figure 45: Wi-Fi based location-based services

Typical parameters useful to geo-locate the Wi-Fi access point includes SSID and MAC address. The accuracy depends on multiple factors, for example the number of available networks, reflections for example in corridors and last but not least shielding through walls, ceilings and your own body. The accuracy of Wi-Fi used for indoor positioning varies from three to ten meters – depending on the conditions, number of APs, etc.

Bluetooth Low Energy (BLE) technology:

This technology is today widely used for indoor positioning and indoor navigation. Most Bluetooth beacons are able to send out signals, but they can't receive them. They are relatively cheap and most beacons do not require any connectivity and are often very small. They are battery or USB powered or integrated into Wi-Fi APs and have a maximum range of 30 meters indoors. Their accuracy is sub-meter. On the one hand they are used in client based solutions, that is to say, positioning via app on the smartphone itself. In this case, Bluetooth must be activated on the device. On the other hand server based tracking solutions using mobile beacons (tags, bracelets, badges, etc.) are possible as well. For turn-by-turn direction services, in client based applications, several beacons are required. They send out unique signals with which the app determines the position by means of fingerprinting. Based on beacons, it is possible to trigger an action, for example displaying a coupon or information on a smartphone.



Client Based Indoor LBS with Smartphone

Server Based Indoor LBS with BLE Tag

Figure 46: BLE-based location-based services