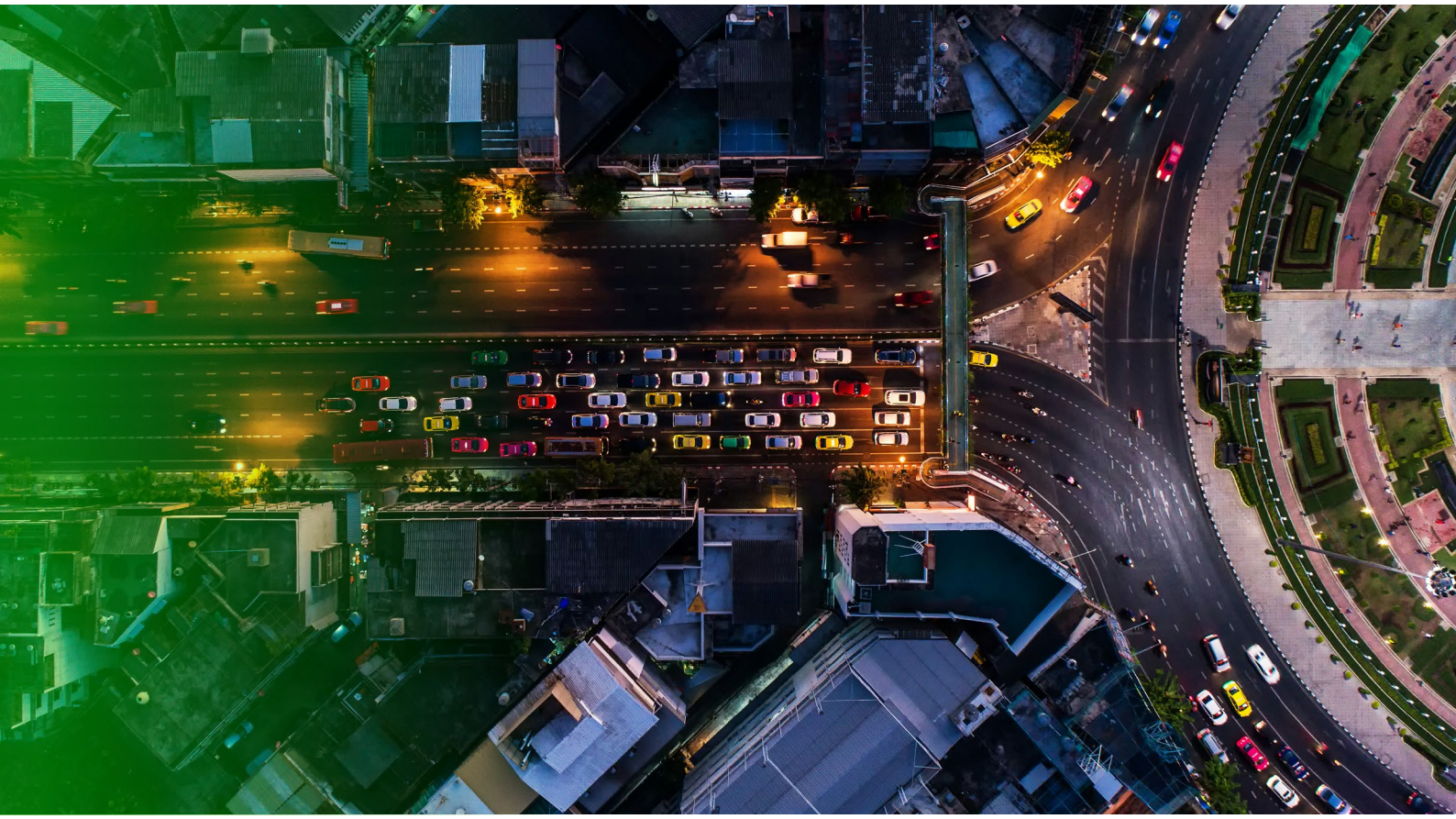
ALE | Where Everything Connects



Alcatel-Lucent Enterprise OmniAccess® Stellar WLAN

GOLDEN RFP
Alcatel-Lucent Enterprise OmniAccess® Stellar WLAN

Alcatel·Lucent Enterprise

Table of Contents

1. Solution and architecture overview

1.	The wireless LAN solution shall be based on IEEE 802.11 and shall be WFA certified for Data and Voice.	C/PC/NC

The Alcatel-Lucent OmniAccess® Stellar WLAN 802.11ac capable access points are Wi-Fi Alliance certified for 802.11a/b/g/n and 802.11ac, ensuring interoperability with other 802.11a/b/g/n/ac products. The Alcatel-Lucent OmniAccess Stellar WLAN solution is also WFA 802.11e WMM certified, ensuring proper prioritization of real-time voice and video traffic and applications.

Alcatel-Lucent Enterprise proposes only standards-based products and solutions and will continue to pursue Wi-Fi certification as new products and standards are introduced:

- IEEE 802.11a/b/g/n/ac wave2
- IEEE 802.11e WMM
- IEEE 802.11h, 802.11i, 802.11e QoS
- 802.11k Radio Resource Management
- 802.11v BSS Transition Management
- 802.11r Fast roaming
- 802.11k OKC

By supporting a solution based on open standards, certifications, and a device-agnostic approach, Alcatel-Lucent Enterprise ensures support for the heterogeneous set of mobile device types common to all environments.

2.	The wireless LAN solution shall propose a distributed control function (no centralized controller) with inherent support for redundancy, elimination of traffic bottlenecks and lowered latency.	C/PC/NC

The Alcatel-Lucent OmniAccess Stellar WLAN solution relies on a distributed control architecture that provides all the functions of a centralized controller and in addition, it eliminates architecture complexity, single points of failure, traffic bottlenecks, latency and high operational costs.

Eliminating the previously required controller from wireless deployment architectures, offers many potential benefits to organizations and their IT departments:

Lower CAPEX

Controller-based architectures involve high upfront capital expenses. They also involve high licensing and maintenance costs. The most obvious benefit of the distributed control architecture is that CAPEX is reduced since no controller is required. The saving is even more significant for deployments that involve multiple controllers for redundancy or load sharing purposes.

Additionally, the Alcatel-Lucent Enterprise licensing model foresees one single license per AP for management. This single license includes all features required today for a state of the art wireless network (intrusion detection, firewalling, deep packet inspection…), thus reducing software and licensing costs. It also brings simplicity and clarity in comparison with traditional licensing models that come with controllers and that charge licensing fees per feature.

Lower OPEX

No controllers mean less equipment to operate and manage, providing several OPEX benefits: Less rack space, less power and cooling requirements, no maintenance fees (especially for unused backup controllers), and less equipment to be monitored by the IT department.

Increased resiliency

In a centralized controller-based architecture, the controller is a single point of failure for the entire wireless network impacting all wireless traffic when the controller fails. The only way to minimize the impact is to add additional redundant controllers, but this comes with a high cost. With a distributed control architecture, that single point of failure does not exist. Indeed, the controller function is no longer centralized but shared by all APs in the domain of management. When an AP fails, the neighboring AP will detect that and react by increasing its transmit power, thus avoiding any hole in the radio coverage. The impact will be purely local: Only clients associated to the failed AP will associate to the neighboring AP and authenticate again.

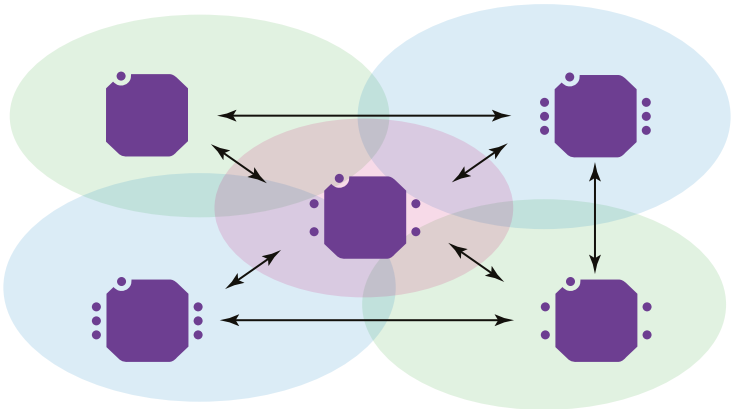
No traffic bottleneck and decreased latency

A WLAN network is now a critical and indispensable asset for an organization. Wi-Fi is no longer only a comfort option. The WLAN is expected today to connect bandwidth-hungry and/or latency sensitive applications (voice or video over IP, video streaming, and more). Over the years, the technology has improved to provide increasing levels of throughput with IEEE standards 802.11a/b/g/n and now 802.11ac that provides more than one Gigabit throughput over the air. To fully leverage the capabilities of 802.11ac APs, such APs can be connected to the LAN with an IEEE 802.3bz 2.5 GBase-T link providing up to 2.5 G connectivity. Tunneling such amounts of traffic from each AP towards the controller will be difficult to sustain and will create a throughput bottleneck in addition to added latency. With a distributed approach, the traffic is no longer tunneled to a centralized equipment but directly bridged into the local Ethernet switch.

Better scalability

When the maximum number of APs that a controller can manage is reached, deploying additional APs requires an additional controller. The distributed control architecture offers much better scalability: No controller equipment is needed, regardless of the size of the deployment.

Figure 1. Stellar WLAN distributed control plane



The control plane of the OmniAccess Stellar WLAN solution relies on communications between neighbor-only APs. Each AP communicates with its adjacent APs with:

- "Over the air" exchanges to discover each other by announcing key information like AP management IP addresses through the *Neighbor Management Protocol*
- "Over the LAN" exchanges (a mix of L2 broadcast/multicast and IP connectivity between AP management IP addresses) to agree on RF parameters (for example, channel use and transmit power) and to share roaming clients' contexts.

Lastly, the distributed control architecture is certainly the shortest route to the next breakthrough in enterprise wireless technology cloud Wi-Fi.

3.	The wireless LAN solution shall rely on a distributed and L2 only data plane.	C/PC/NC

The data plane of the OmniAccess Stellar WLAN solution is fully distributed. Apart from the "guest" traffic, the user traffic is never tunneled to a central point as it is done in the framework of a controller-based WLAN architecture.

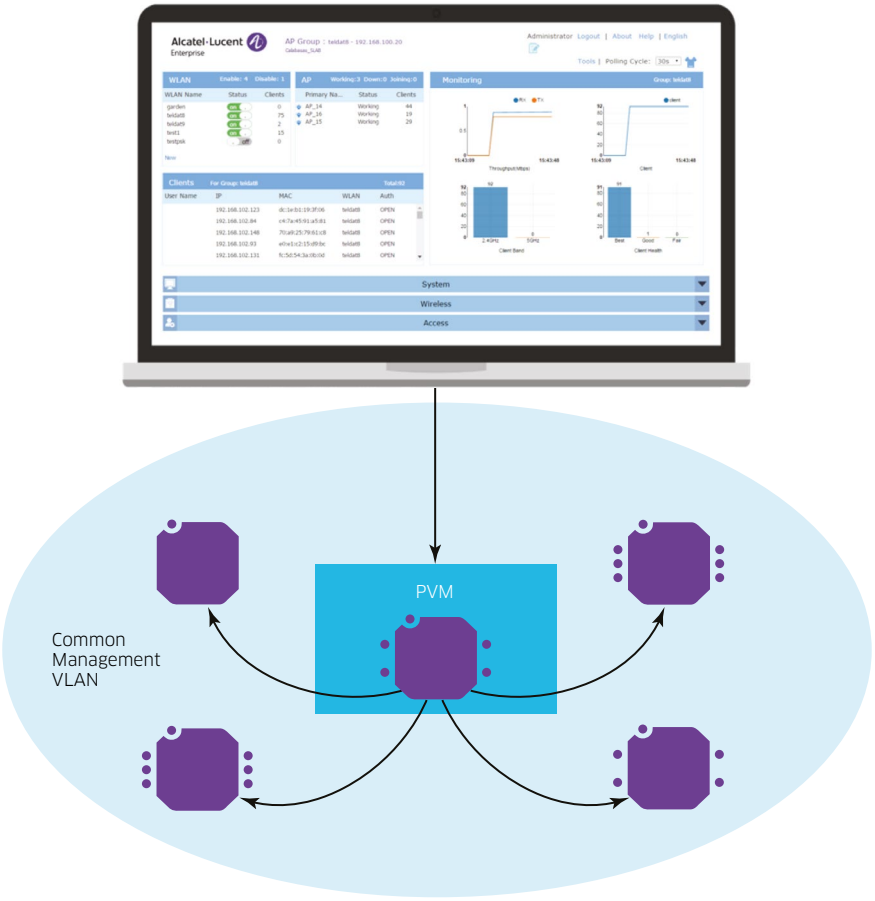
The wireless data (IEEE 802.11) is converted to Ethernet (IEEE 802.3) in the AP and sent to the rest of the network through the AP uplink. The AP does not operate any routing on wireless client data. This L3 function will be handled by the LAN infrastructure. The AP just tags (IEEE 802.1q) traffic at Layer 2 before sending it on the uplink.

4.	The wireless LAN solution shall come in two flavors allowing two deployment types: • "Small deployment" for a mono-site deployment with access points spread over a single broadcast domain (VLAN) and operating in a common RF environment • "Large deployment" for a multi-site deployment with access points spread over multiple broadcast domains (VLAN) that may operate in different RF environment For both deployment types, the solution shall offer advanced features like intrusion detection/prevention or a captive portal to manage guest connections without additional third-party components.	C/PC/NC

The OmniAccess Stellar WLAN solution fully complies with this requirement. Indeed, the OmniAccess Stellar WLAN solution can be deployed in two distinct ways. The first one is called Stellar Wi-Fi *Express* and is meant for smaller deployments with up to 64 APs in a single standalone cluster. The second one is called *Enterprise*, and it can scale up to 512 APs today and many more soon. In the later deployment model, the Alcatel-Lucent Enterprise OmniVista™ 2500 Network Management System (NMS) is deployed on top of the access points infrastructure to take care of management and configuration of all the APs for maximum scalability.

By default, OmniAccess Stellar WLAN access points operate in Wi-Fi *Express* mode, in a cluster architecture that provides simplified plug-and-play deployments. The AP cluster is an autonomous system that consists of a group of OmniAccess APs deployed in a common VLAN and common RF environment (for example, same *Country Code* for all APs) with up to 64 APs of any model in the current Stellar WLAN portfolio (AP1101, AP1220 series, AP1230 series, and the outdoor and ruggedized AP1250 access point). The cluster or "AP-group" is managed and configured through a secure web interface thanks to a wizard driven configuration process and it gives the WLAN network all the power of the distributed intelligence, including the support for an integrated guest management through captive portal and the same advanced radio management or security features like intrusion detection/prevention capabilities. In Wi-Fi *Express* mode, the management web interface is hosted on one of the APs that has been elected (highest model type, then highest MAC address) or manually configured as the *primary virtual manager* (PVM, with an associated *secondary virtual manager* or SVM, for the resiliency of the management plan) that propagates the configuration to all APs that are member of the cluster/ AP-group.

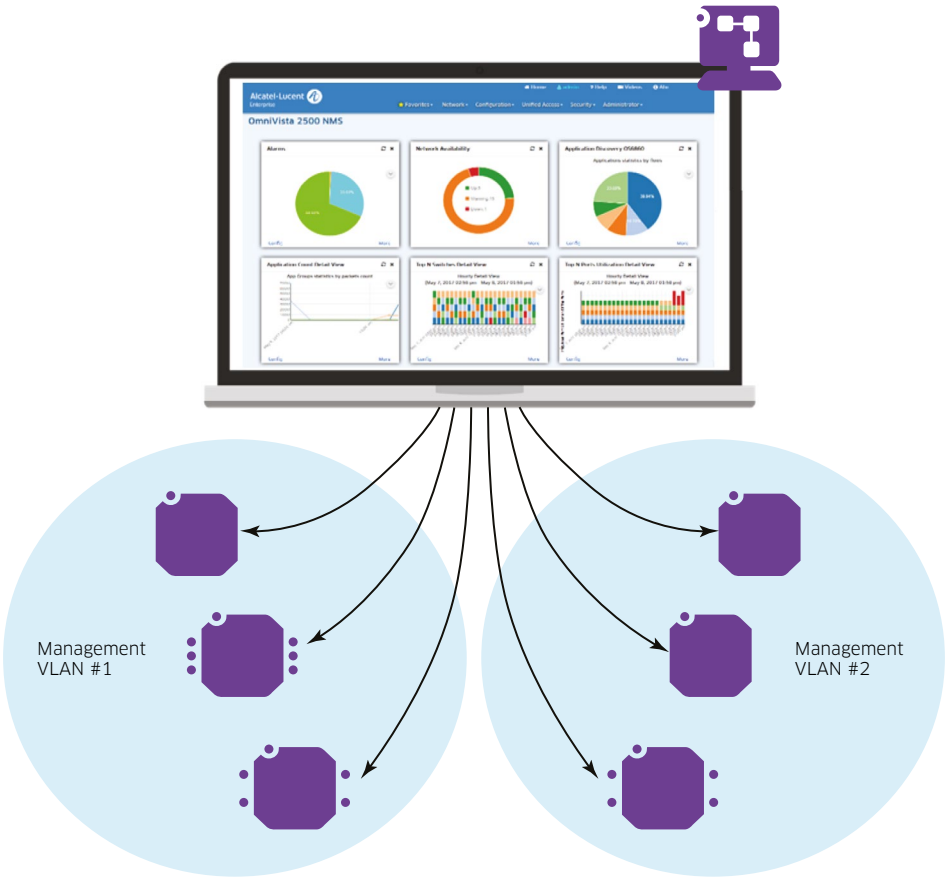
Figure 2. OmniAccess Stellar WLAN *Express*



The OmniAccess Stellar *Express* cluster architecture ensures simplified and quick deployment. Once the first AP is configured using the configuration wizard, the remaining APs in the network will come up automatically with updated configuration. This ensures that the whole network is operational within a few minutes.

In the case where more than 64 APs are needed, or where a multi-site deployment with site specific RF environments (for example, specific *Country Codes* in the case of an international deployment) is envisioned with a centralized management as a requirement, the OmniAccess Stellar Wi-Fi *Enterprise* is the right option. In this mode, the access points are managed as one or more AP-Groups (a logical grouping of one or more Access points with similar settings) by OmniVista 2500 NMS. The OmniVista 2500 embeds a visionary controller-less architecture, providing user friendly workflows for Unified Access together with integrated *Unified Policy Authentication Manager* (UPAM) which helps define authentication strategy and policy enforcement for employees, guest access and BYOD. In addition, the Stellar *Enterprise* mode offers advanced features and capabilities like a “heatmap” feature for WLAN site planning or deep packet inspection capabilities providing real-time classification and control of flows at the application level.

Figure 3. OmniAccess Stellar WLAN *Enterprise*



5.	The wireless LAN solution shall propose a centralized management function, irrespective of the deployment model (“small” or “large”) as described previously [4].	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement for both deployment models (*Express* or *Enterprise*). Please refer to requirement [67].

6.	The wireless LAN solution shall scale up to 512 access points for the “large deployment” model [4], 64 access points for the “small deployment” model [4] and thousands of users while guarantee ease of deployment and expansion (to be described).	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement for both deployment models (*Express* or *Enterprise*). Please refer to requirement [4].

7.	The “small deployment” option previously described [4] shall not require any license fee.	C/PC/NC

Once an Alcatel-Lucent Enterprise OmniAccess Stellar access point is purchased to be deployed in the framework of a Stellar *Express* cluster, no license is required even not for the most advanced features like wireless intrusion detection/protection or for guest management.

8.	The “large deployment” option previously described [4] shall rely on a licensing model that is as simple as possible, with one license per AP including all functions (basic or advanced) handled by the AP.	C/PC/NC

While WLAN solutions proposed by Alcatel-Lucent Enterprise competitors (especially controller-based solutions) rely on a complex and feature-dependent licensing model, the OmniAccess Stellar licensing model in Wi-Fi *Enterprise* mode foresees one single license per AP for management. This single license includes all features required today for a state of the art wireless network (intrusion detection, firewalling, Deep Packet Inspection…), thus reducing software and licensing costs. It also brings simplicity and clarity in comparison with traditional licensing models that come with controllers and that charge licensing fees per feature.

The only additional licenses that may be required based on the deployment requirements are “guest access” and “BYOD” (*bring your own device*) licenses.

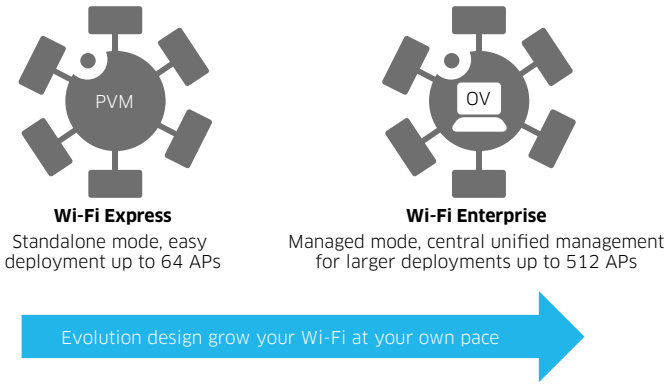
Table 1. Stellar *Enterprise* licensing model description

AP management (1 to 512)	Per AP
RF Management	Included
Floor Pan/Heatmap	Included
wIDS/wIPS	Included
Authentication and policy enforcement	Included
Guest access (20 to 10K)	Per device
BYOD (20 to 10K)	Per device

9.	The “small deployment” (64 AP) option shall allow an easy migration to a “large deployment” (512 AP) when needed.	C/PC/NC

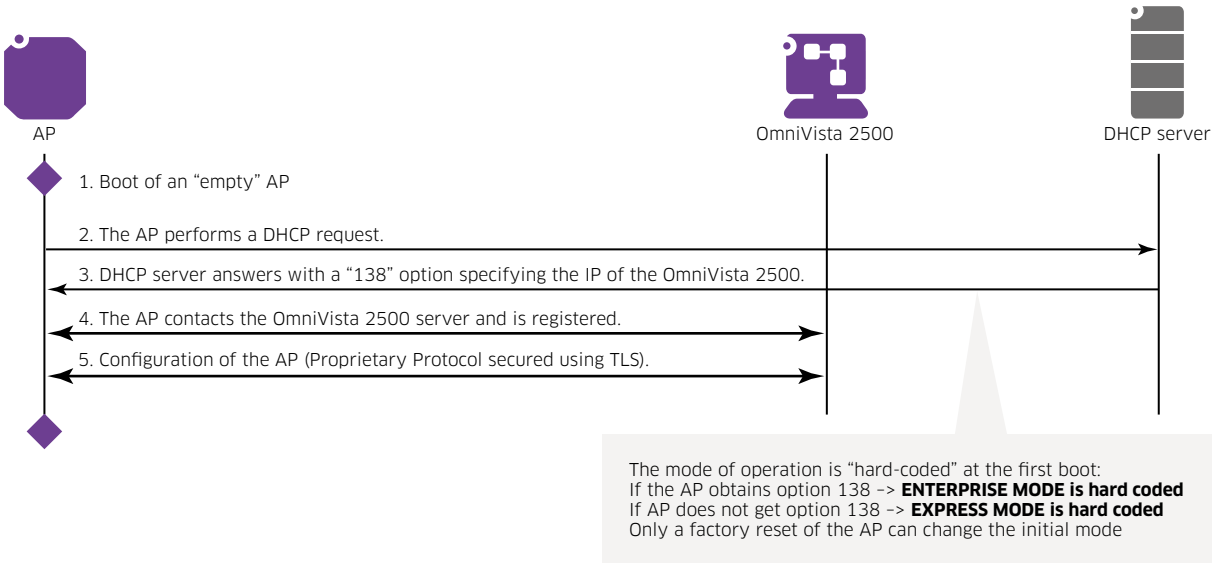
The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution has been planned and designed with future evolution in mind. Indeed, Wi-Fi *Express* and Wi-Fi *Enterprise* mode are mutually exclusive, but moving from a Stellar *Express* architecture to a Stellar *Enterprise* architecture is very easy.

Figure 4. Stellar Wi-Fi *Express* or *Enterprise* - Evolutive design



The operating mode of an AP is hardcoded at first boot: If the AP gets a DHCP lease with option 138 (which gives the IP address of the OmniVista 2500 server), the operating mode of the AP is permanently set to Stellar *Enterprise*. Otherwise (no option 138), the operating mode is permanently set to Stellar *Express*.

Figure 5. Stellar AP boot sequence and DHCP option 138



If a Stellar AP is configured in *Express* mode, it can be easily migrated to Enterprise mode by performing a factory reset after having configured the option 138 in the DHCP server for the management scope. A factory reset can be done manually on each AP by pressing a factory reset button on the back of the AP, or centrally through the centralized WEB GUI.

Figure 6. *Express* to *Enterprise* migration (factory reset button)

10.	The wireless LAN solution shall have been designed with scalability in mind to allow the 512 APs limit to be extended in the future (to be described) without requiring new equipment or deployment design change.	C/PC/NC

The Alcatel-Lucent OmniAccess Stellar WLAN solution fully complies with this requirement. While competitors' controller-based or even controller-less solutions (in that case, an AP is usually elected and handles the control function) rely on a centralized control function, the control function of the OmniAccess Stellar WLAN solution is fully distributed. In theory, the number of APs that the OmniAccess Stellar WLAN solution can support is even unlimited by design. Competitors' solutions rely on a central point that concentrates "control information" for the entire wireless network and which capabilities are physically limited. In Alcatel-Lucent Enterprise's proposal, the "control information" is not concentrated but shared only between neighboring APs to handle some functions like roaming. That allows maximum scalability and investment protection. Alcatel-Lucent Enterprise will regularly proceed to new validation tests to formally validate and announce new maximum number of APs the OmniAccess Stellar WLAN can support.

2. Access control, authentication and encryption

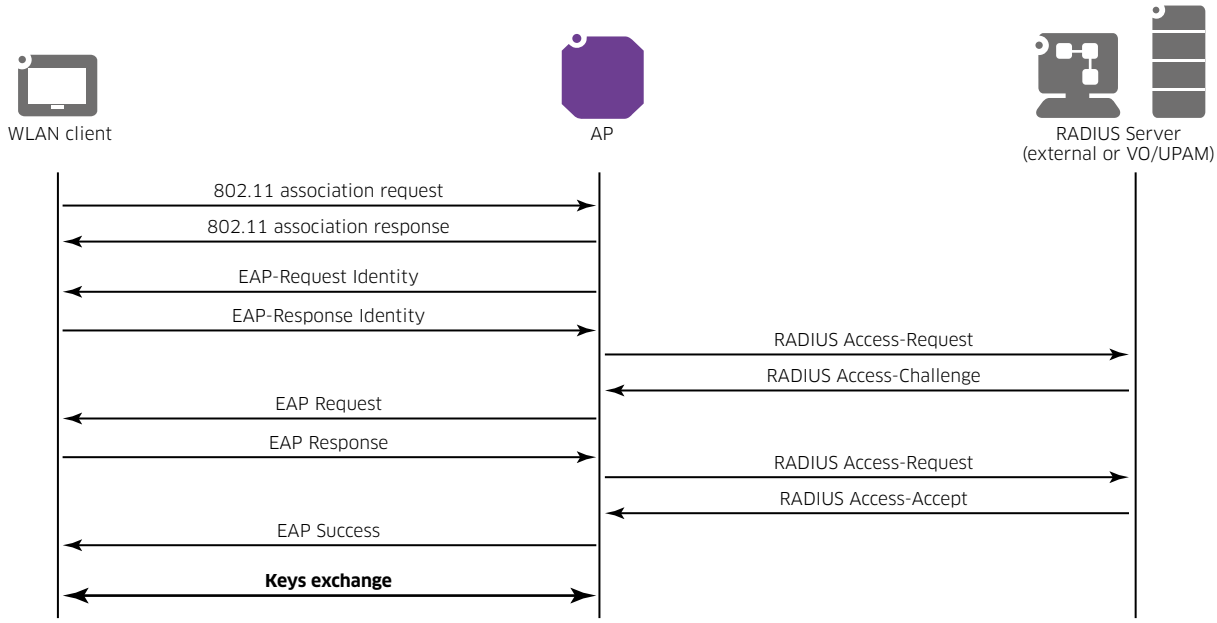
11.	The wireless LAN solution shall support MAC-based authentication.	C/PC/NC

MAC-based authentication, a common authentication method that is used to authenticate devices based on their physical *Media Access Control* (MAC) address, is fully supported with an Alcatel-Lucent Enterprise OmniAccess Stellar solution (*Express* or *Enterprise*). While not the most secure and scalable method, MAC-based authentication implicitly provides an addition layer of security, and is often used to authenticate and allow network access to certain devices while denying access to the rest.

12.	The wireless LAN solution shall support 802.1x based authentication.	C/PC/NC

Alcatel-Lucent Enterprise fully complies with this requirement and recommends indeed using 802.1x for wireless and even wired user authentication. 802.1x authentication involves three parties: A supplicant, an authenticator, and an authentication server. The supplicant is a client device (such as a laptop or a smartphone) that wants to attach to the WLAN. The authentication server is typically a host running software supporting the RADIUS and EAP protocols. In the framework of the OmniAccess Stellar WLAN solution, the authenticator is the OmniAccess Stellar access point itself that acts like a security guard to the protected network. The wireless client device is not allowed access through the authenticator/AP to the protected side of the network until its identity has been validated and authorized.

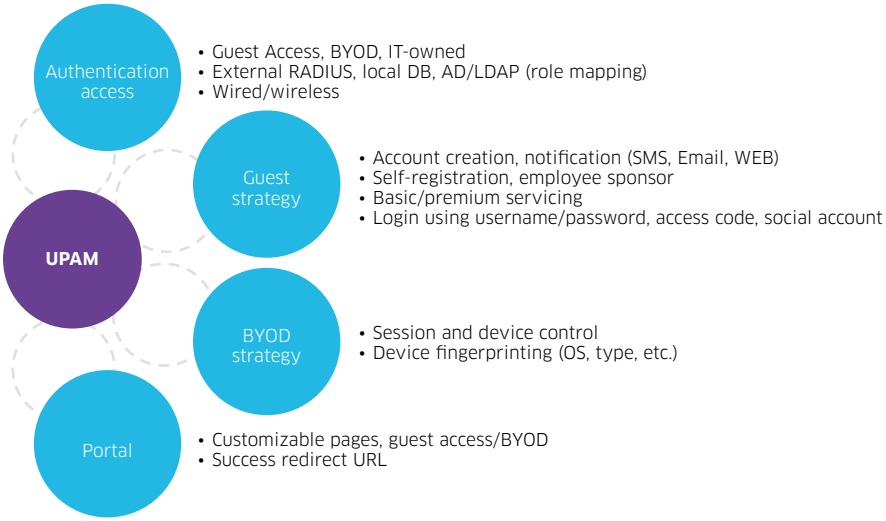
Figure 7. OmniAccess Stellar and 802.1x



13.	At least for a “large deployment” scenario as described previously [4], the WLAN solution shall include a built-in RADIUS server for 802.1x and MAC authentication that shall **not** be proposed as a separate product.	C/PC/NC

As shown in previous figure, the Alcatel-Lucent Enterprise OmniAccess Stellar solution fully complies with this requirement by offering in Wi-Fi *Enterprise* mode an embedded Radius server for 802.1x and MAC authentication. This embedded server is called *Unified Policy Access Manager* (UPAM) and is inherent to the global solution. While ALE’s competitors’ proposals consist of an additional appliance or server/VM, UPAM comes in the form of an integrated software module with the OmniVista 2500 Network Management System.

Figure 8. Unified Policy Access Manager – *Enterprise* mode

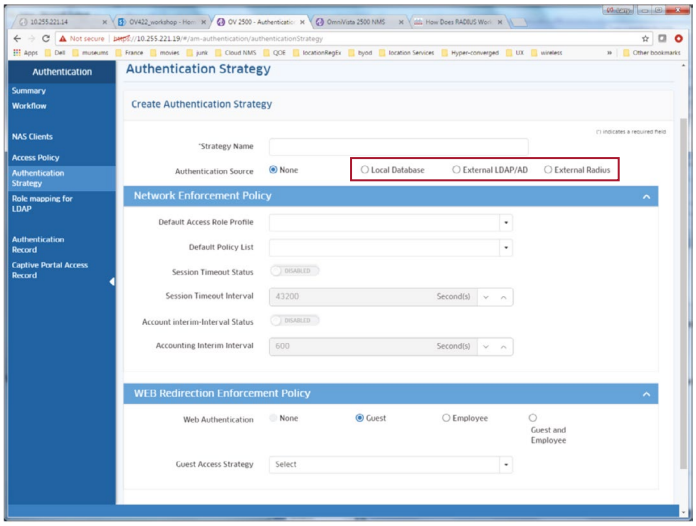


Much more than a built-in RADIUS server, UPAM is a Policy Manager that consists of a Guest Access application for visitor network access and a BYOD access solution for employee device secure on-boarding.

14.	The built-in RADIUS server as described previously (13) shall be able to interface with an external authentication server (Radius, LDAP, Active Directory): FreeRadius, Microsoft NPS Radius Server, Microsoft AD, OpenLDAP…	C/PC/NC

As depicted in Figure 8. Unified Policy Access Manager, the UPAM module can be used as a "local" Radius database but can also interface with an external Radius server or with the company corporate Microsoft Active Directory or LDAP server. Connecting to an external authentication source allows centralized user management with the possibility to assign user or device "role profiles" (VLAN, QoS and security ACL) based on AD/LDAP attributes.

Figure 9. UPAM - Authentication Source options



15.	The built-in RADIUS server as described previously [13] shall support at least following EAP types: EAP-PEAP, EAP-GTC, EAP-TLS, EAP-TTLS.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement.

16.	At least for a “large deployment” scenario as described previously [4], the wireless LAN solution shall have the ability to utilize RADIUS attributes to assign each authenticated user/device to a specific ROLE. A role defines a VLAN and enforces security and QoS using role-based ACLs and QoS policies that can be directly integrated with the roles defined within existing authentication servers.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement and supports role based access control. OmniAccess Stellar APs use radius attributes to assign users or devices to roles. Once the role of the user is learned (accomplished by interfacing with existing backend authentication servers such as RADIUS, LDAP, and Active Directory) authenticated users or devices can be assigned to a specific VLAN. The OmniAccess Stellar APs have firewalling capabilities and the role based access control can even go beyond basic VLAN assignment. A pre-defined profile can be applied to set the VLAN but also security (network ACLs) and Quality of Service (QoS) policies for the authenticated user or device. The AP embedded firewall is identity-aware and can take permit/deny, and QoS decisions (such as setting DSCP/802.1p bits or placing the packet into a priority queue) based on the identity of the user or device and application. By applying granular policies tailored to the role of the specific user, the OmniAccess Stellar WLAN solution restricts network privileges to those appropriate to the user’s role, and greatly decreases exposure if a device or user were compromised by limiting the amount of damage that can be done.

17.	The wireless LAN solution shall support following link layer encryption standards: WPA2_AES, WPA2_TKIP, WPA_AES, WPA_TKIP, DYNAMIC_WEP, WPA_PSK_AES, WPA_PSK_TKIP, WPA_PSK_AES_TKIP, WPA2_PSK_AES, WPA2_PSK_TKIP.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement.

18.	The wireless LAN solution shall support following 802.1x supplicants: Windows 7, 10, MAC OS, IOS, Android, Chromebook…	C/PC/NC

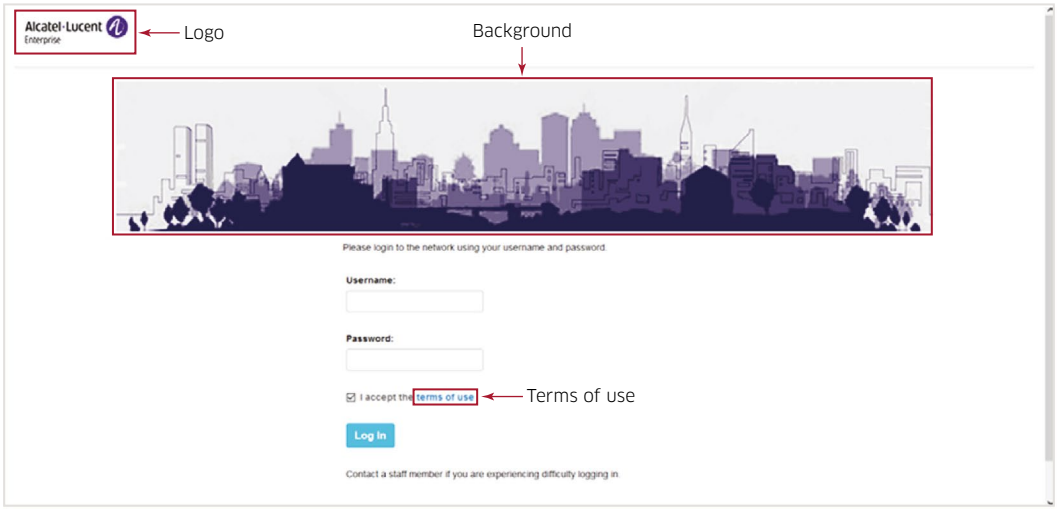
The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement.

19.	Irrespective of the deployment model (“small” or “large”) as described previously [4], the wireless LAN solution shall propose a “Guest” management solution based on an embedded and built-in Captive Portal providing web based authentication for guests and visitors.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement either in *Express* mode or *Enterprise* mode.

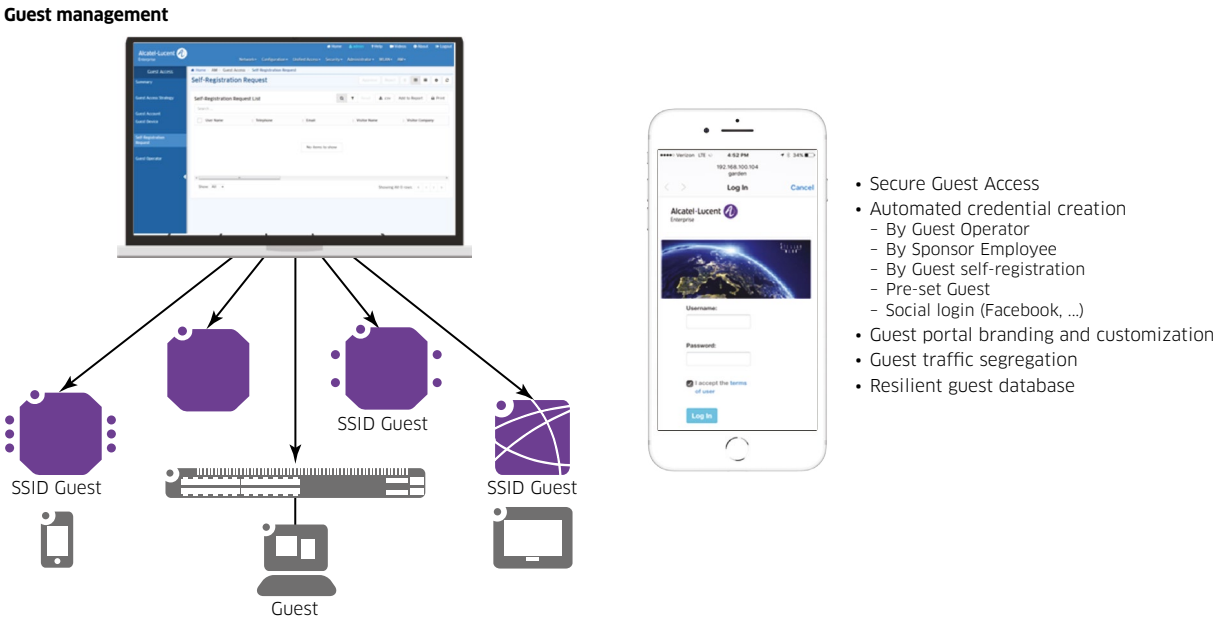
In Wi-Fi *Express* mode, the WLAN access points of the cluster support an embedded and free of charge Captive Portal for guests/visitors controlled and secure access network. Usually, guests can access the Internet only. They use a captive portal authentication (the authentication source being the internal database of the cluster) and a portal page asking for authentication will pop up when they browse any website.

Figure 10. OmniAccess Stellar AP embedded captive portal - *Express* mode



In Wi-Fi Enterprise mode, the guests access function is handled by the UPAM module which provides an advanced and sophisticated captive portal with maximum customization capabilities and various access methods (employee sponsored guest access, guest self-registration…).

Figure 11. OV/UPAM Captive Portal and Guest Access - *Enterprise* mode

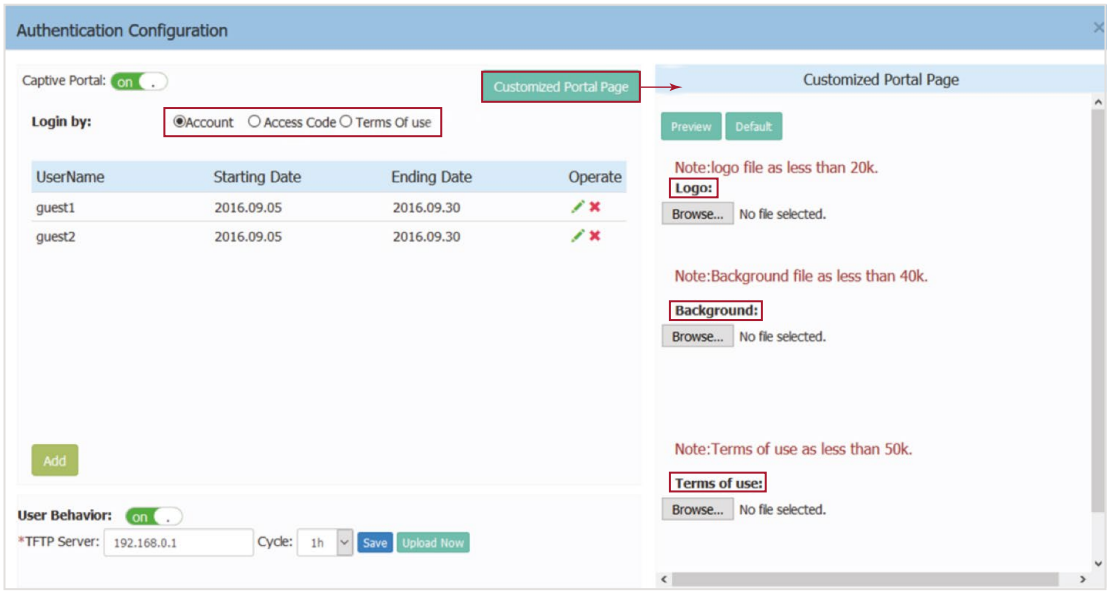


20.	The guests captive portal included in the wireless LAN solution shall allow a customizable look and feel.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement either in *Express* mode or *Enterprise* mode.

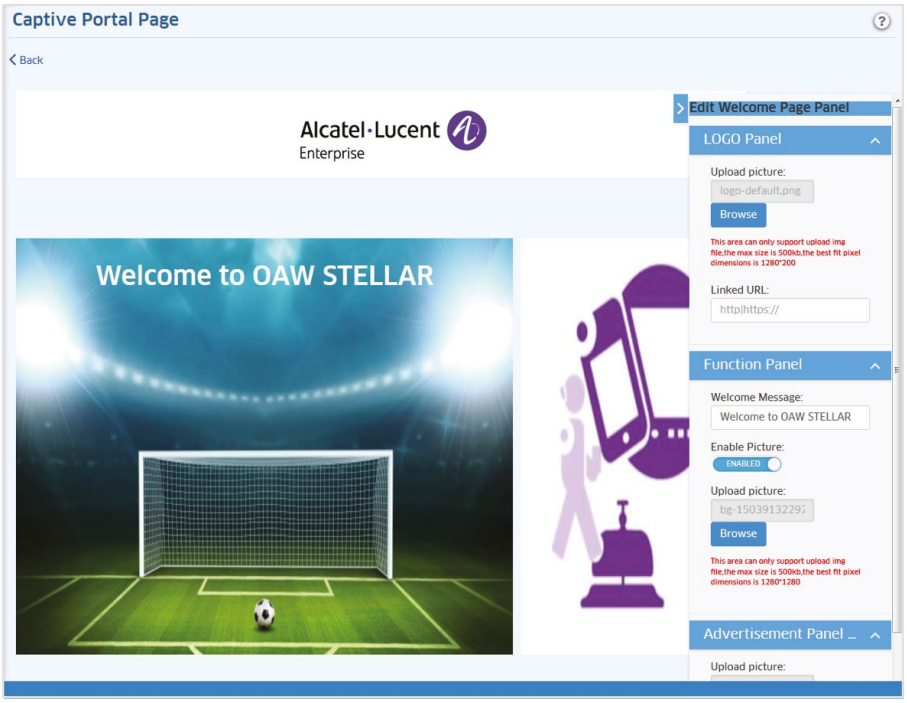
In Wi-Fi *Express* mode, the captive portal can be customized to ask guests to log in with a personal account (previously configured login/password), with an access code (a PIN code), or simply by accepting the “Terms of use”. Moreover, the logo, the background image and the “Terms of use” that are displayed on the landing page are fully customizable:

Figure 12. Stellar AP embedded Captive Portal customization - *Express* mode



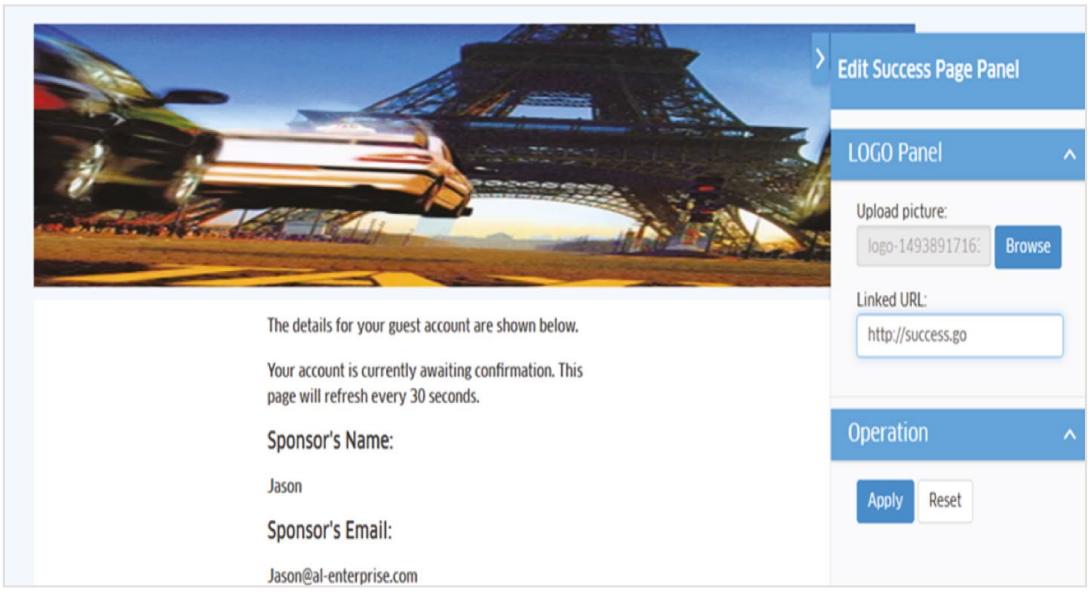
The captive portal provided by UPAM in Wi-Fi *Enterprise* mode is also fully customizable. The logo and background page be personalized and a "welcome" message may also be displayed:

Figure 13. UPAM Captive Portal customization - *Enterprise* mode



Additionally, the “success page” that is displayed after a successful authentication may also be modified for a personal look and feel:

Figure 14. UPAM “success page” customization - *Enterprise* mode



21.	The guest management solution shall allow, at least, following authentication methods: • Username and password • Access code • Simple term and condition acceptance	C/PC/NC

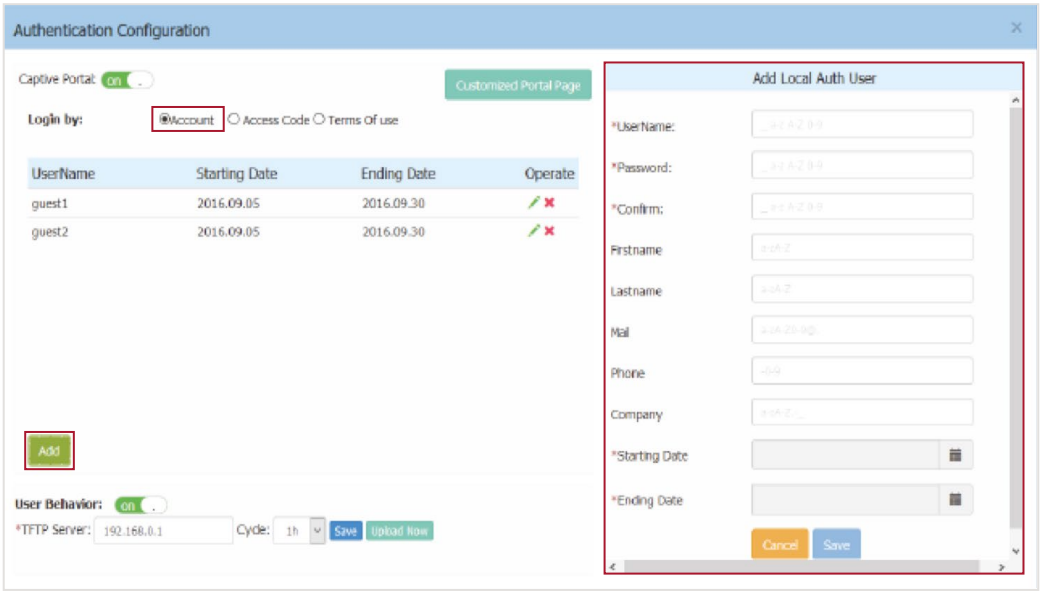
The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement either in *Express* mode or *Enterprise* mode.

22.	The Guest management solution shall allow non-IT staff (for example, a receptionist) to create temporary guest accounts.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement either in *Express* mode or *Enterprise* mode.

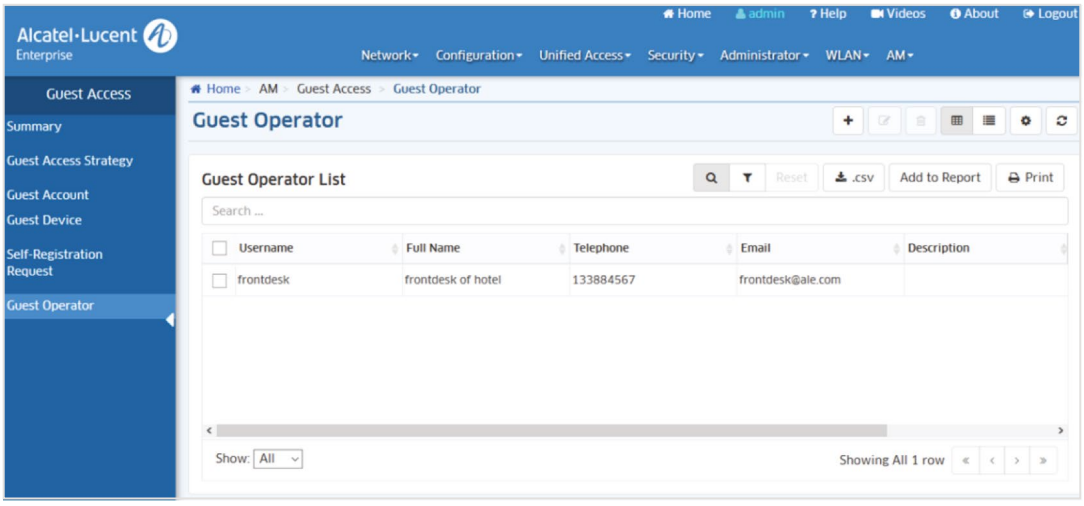
In Wi-Fi *Express* mode, the AP cluster natively supports role based management with a predefined “GuestOperator” for maximum simplification. GuestOperator access simplifies guest account creation and management, and therefore can be used by any non-IT person, such as a front desk or receptionist:

Figure 15. Guests accounts creation – *Express* mode



In Wi-Fi *Enterprise* mode, and from the OmniVista 2500 NMS, the administrator can create multiple "Guest Operators" accounts to manage guests access:

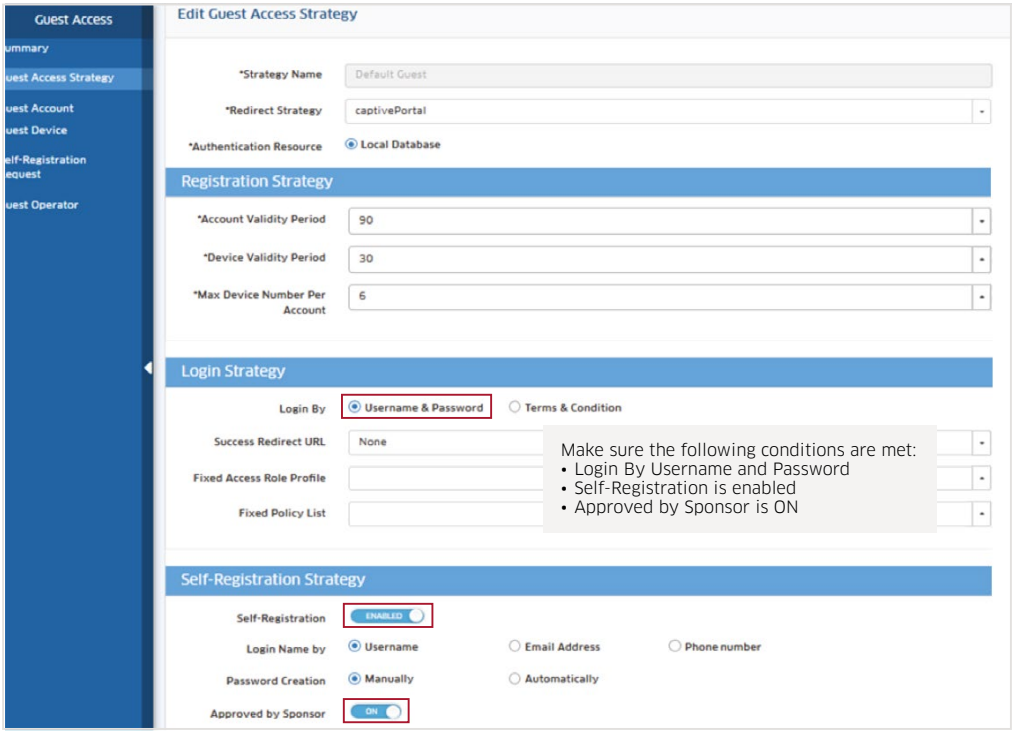
Figure 16. Guests Operator accounts creation – *Enterprise* mode



23.	A least for a "large deployment" scenario as described previously [4], the WLAN solution shall allow guest self-registration and employee sponsored access.	C/PC/NC

Guests accounts can be created by a guest operator as previously described. In addition, and in Wi-Fi *Enterprise* mode, guests accounts can also be self-created by guests when they are redirected to the captive portal if "Self-registration" is enabled in the "Guest Access Strategy":

Figure 17. Guest access strategy for guests self-registration



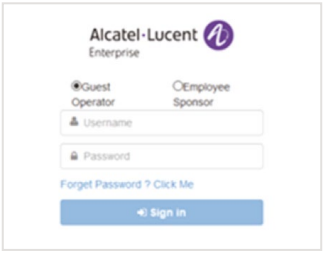
The self-registered guest account will not be usable immediately if "*Approved by Sponsor*" is enabled in the "Guest Access Strategy". The account will be usable after either:

- It is approved by an "Employee Sponsor" which must have been provisioned in the UPAM "Employee" internal database or must "exist" on an external AD/LDAP server interfacing with UPAM.
- Or, it is approved by a Guest Operator.

The self-registered guest account will be usable immediately if "*Approved by Sponsor*" is disabled in the "Guest Access Strategy".

The Guest Operator and the Employee Sponsor can access to the same user interface to approve the self-registered guest account:

Figure 18. Guest Operator and Employee Sponsor UI



24.	For a "large deployment" scenario as described previously [4], the licensing model of the guest management solution shall be based on the number of devices.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement.

25.	For a “small deployment” scenario as described previously [4], the guest management solution shall not require any license fee.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement.

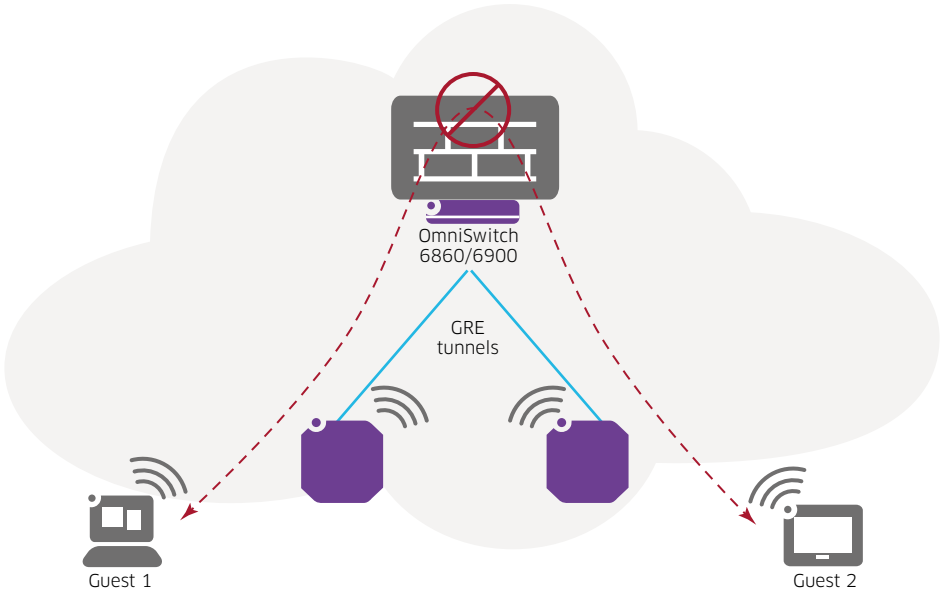
26.	For a “large deployment” scenario as described previously [4], the guest management solution shall allow setting a validity period for an authenticated device, to avoid entering credentials each time a guest access the network.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement.

27.	A least for a “large deployment” scenario as described previously [4], the WLAN solution shall implement strict guests traffic isolation.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. In Wi-Fi *Enterprise* mode, a dedicated Alcatel-Lucent OmniSwitch® 6860 or 6900 switch handles the guest isolation feature. The switch acts, indeed, as a GRE tunnel gateway, terminating the guests GRE tunnels established by the APs and applying firewalling rules for a strict control of the guest traffic, thus blocking traffic between guests even if guests are in the same VLAN:

Figure 19. Guests traffic isolation

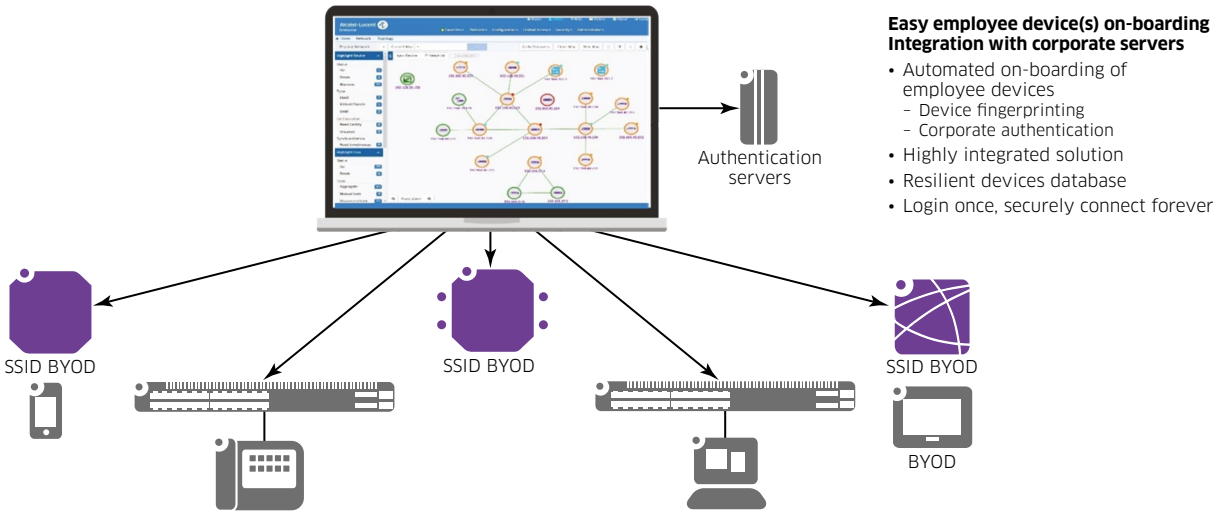


The OmniSwitch 6860 switch (for up to 750 GRE tunnels) and the OmniSwitch 6900 switch (for up to 1000 GRE tunnels) are equipment from the Alcatel-Lucent Enterprise OmniSwitch LAN portfolio and are inherent parts of the OmniAccess WLAN Stellar global solution.

28.	In the framework of a “large deployment” scenario as described previously [4], the WLAN solution shall support BYOD and be able to provide device on-boarding that is as simple as possible and without requiring additional third-party components.	C/PC/NC

As depicted in following figure, the UPAM module of the OmniAccess Stellar WLAN solution (Wi-Fi *Enterprise* mode), includes a BYOD application that allows easy device on-boarding with Captive Portal registration for employees.

Figure 20. OV/UPAM captive portal and BYOD - *Enterprise* mode



29.	The on-boarding process of employee devices shall be based on employee corporate accounts.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. Indeed, the BYOD captive portal asks the employee to provide his corporate login/password to authenticate and on-board his device. This is possible thanks to the capability of the UPAM module to interface with the company corporate authentication server like a LDAP server or a Microsoft Active Directory server. Nevertheless, the employee account can be locally created.

30.	The BYOD application shall allow setting the validity period for the device, and the maximum number of devices per account.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement.

31.	The licensing model of the BYOD application shall be based on the number of on-boarded devices.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement.

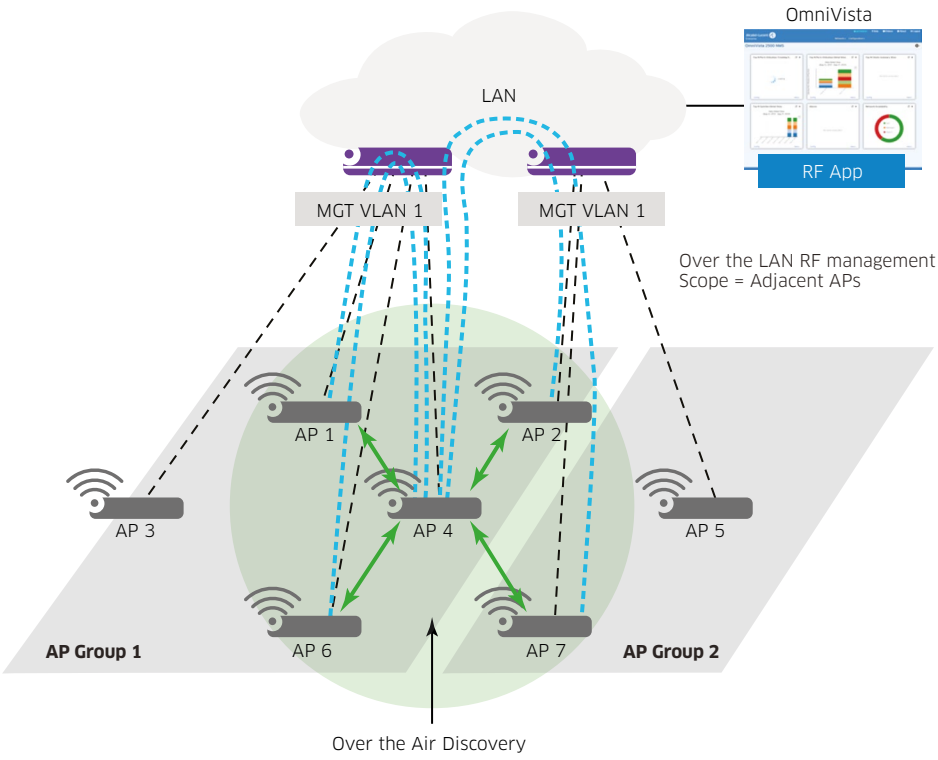
3. RF management

32.	The WLAN solution shall allow automatic and/or manual RF management (channel and power).	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. The OmniAccess Stellar APs implement the *Radio Dynamic Adjustment™* (RDA) technology that automatically assigns channels and power settings, provides DFS/TPC, and ensures that access points stay clear of all radio frequency interference (RFI) sources to deliver reliable, high-performance wireless LANs.

The control plane of the OmniAccess Stellar WLAN solution is fully distributed. The automation (when activated) of the RF parameters settings of the OmniAccess Stellar APs occurs between adjacent/neighbor APs only (even if they belong to different AP-Groups and even if they are in different management VLANs), in a fully distributed manner. Each AP communicates with its neighbor APs with "over the air" exchanges through the *Neighbor Management Protocol* to discover each other and, then, with "over the LAN" exchanges for RF management. This allows RF context sharing (channel use and interference, number or clients per band, radio and AP, power…) and each AP can take RF actions:

Figure 21. Automated RF management between adjacent APs



After the APs have discovered each other, each AP will declare starting auto-channel and auto-power process and, in case of collision, will wait for a while and retry. The AP that can proceed will listen to the RF environment for a while, then choose the best channel based on certain algorithm. After a while, each AP in the neighborhood should have tried once at least, and all APs will be in a channel distribution with as less interference as possible. The auto-channel process will work only when there is no client attached to the radio. Regarding the auto-power process, each AP will send its transmit power setting to its neighbor APs that will compare the RSSI and transmit power to adjust their own transmit power based on certain algorithm. After several rounds of this process, the power of all APs will be adjusted to the most appropriate setting.

The channel width cannot be set automatically and must be set manually for each band. The Channel width is used to control how broad the signal is for transferring data. By increasing the channel width, the speed and throughput can be increased. However, larger channel width brings more unstable transmission in crowded areas with a lot of frequency noise and interference.

Same principles apply in OmniAccess Stellar Wi-Fi *Express* mode where all APs are deployed over a single management VLAN and share same RF characteristics (for example, the Country Code) and, therefore, are not configured in distinct AP-Groups.

Table 2. OmniAccess Stellar WLAN per-band wireless information

Channel and power	• Auto-mode enabled by default • It is recommended to use auto channel and power instead of static setting. • Guidelines for statically setting channels: http://www.revolutionwifi.net/revolutionwifi/2013/03/80211ac-channel-planning.html
Channel width	• Keep default settings • Narrow width for dense AP deployment and large width for sparse AP deployment
Short guard interval	• Enabled by default • If RF environment it not good and clients are crowded, then it should be disabled

33.	The WLAN solution shall support short guard interval.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. In IEEE 802.11 OFDM-based communications, the guard interval is at a very basic level, time spacing between data symbols to prevent inter-symbol interference. The *short guard interval* allows reducing the transmit interval to increase overall throughput, but may also increase packet error rate. The standard guard interval per the 802.11n standard is 800 nanoseconds and has been carried over to 802.11ac. To increase data rate, the optional support for a 400 nanoseconds guard interval has been added providing approximately an 11% increase in data rates, but it results in a higher packet error rate when the delay spread of the channel exceeds the guard interval and/or if timing synchronization between the transmitter and receiver is not precise.

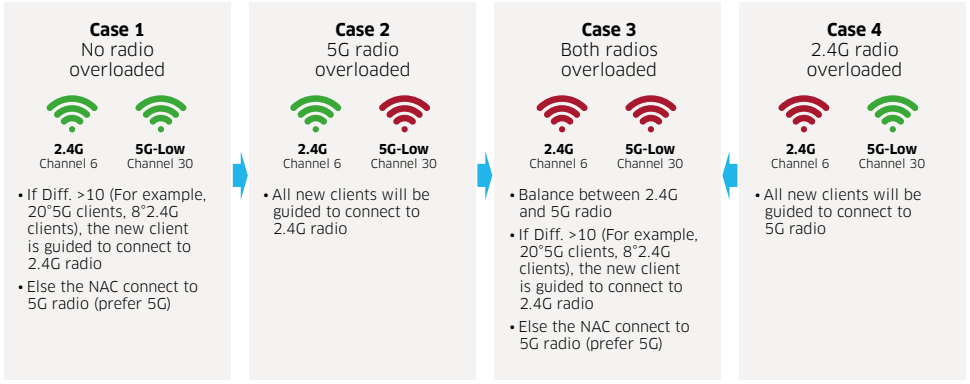
In the framework of the Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution, the *short guard interval* is enabled by default and should be disabled if the RF environment is not good or in clients crowded environments.

34.	The WLAN solution shall be smart enough to guide a new client to the optimal band/channel (2.4GHz/5GHz) considering, at a given time, both the number of associated clients on each band, and the medium utilization.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. Indeed, the OmniAccess Stellar WLAN solution can do smart clients load balancing, including band steering. *Band steering* controls the behavior of dual band clients according to the use of a wireless channel and users connected to the AP and can guide a client accessing the network to the optimal band/channel. Band steering considers, at a given time, two parameters:

- The client count per radio (the difference between the number of 5G band associated clients and the number of 2.4 band associated clients)
- The band/channel load, considering that a channel is overloaded when its average medium use over the span of a minute exceeds 70%

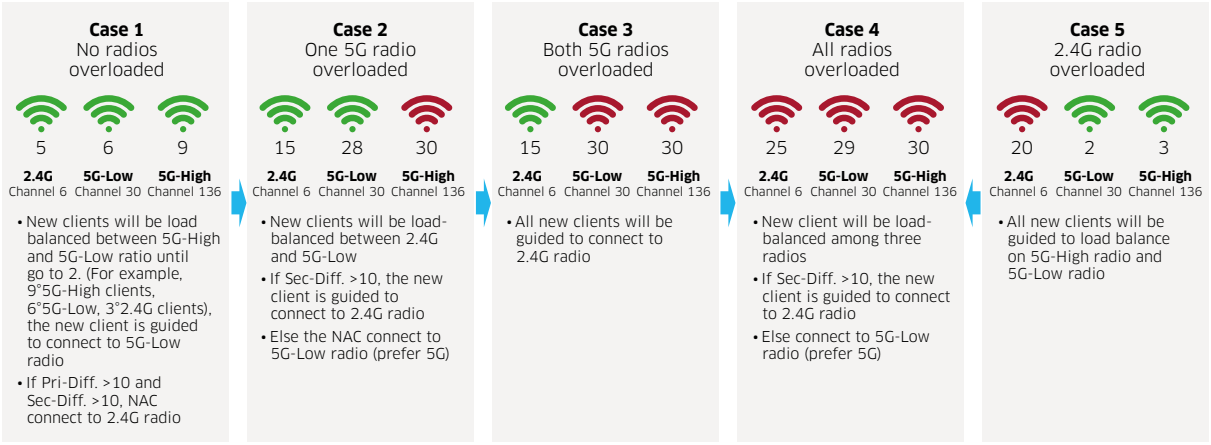
Figure 22. Dual-radio APs band steering



Diff = 5G Client # = 2.4G Client # (Threshold: 10)
Overloaded = A channel is considered overloaded when its average medium utilization over the span of a minute exceeds 70%.

The same principles apply to the Alcatel-Lucent Enterprise OmniAccess Stellar tri-radio AP123X series access points. The band steering feature shall just consider three bands/channels (2.4G, 5G-Low and 5G-High) instead of two:

Figure 23. Tri-radio APs band steering



Pri-Diff = 5G High client # = 2.4G Client # (Threshold: 10)
Sec-Diff = 5G Low client # = 2.4G Client # (Threshold: 10)
Overloaded = A channel is considered overloaded when its average medium utilization over the span of a minute exceeds 70%.

35.	If no band/channel (2.4GHz/5GHz) is overloaded (high medium utilization) or crowded (high client count), an AP shall by default guide a new client to the 5GHz band.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement as depicted on Figure 22. Dual-radio APs band steering and Figure 23. Tri-radio APs band steering (Case1).

36.	Even if the 5GHz band is not overloaded but is crowded (high client count), an AP shall guide a new client to the 2.4GHz band.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement as depicted on Figure 22. Dual-radio APs band steering and Figure 23. Tri-radio APs band steering (Case1).

37.	If a band/channel (2.4GHz/5GHz) is overloaded (high medium utilization) and even if it is not crowded, an AP shall guide a new client to the less loaded band/channel.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement as depicted on Figure 22: Dual-radio APs band steering and Figure 23: Tri-radio APs band steering (Case3 and Case5).

38.	If all bands/channels (2.4GHz/5GHz) are overloaded (high medium utilization) and no band/channel is crowded, an AP shall guide a new client to the 5GHz band.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement as depicted on Figure 22. Dual-radio APs band steering and Figure 23. Tri-radio APs band steering (Case4).

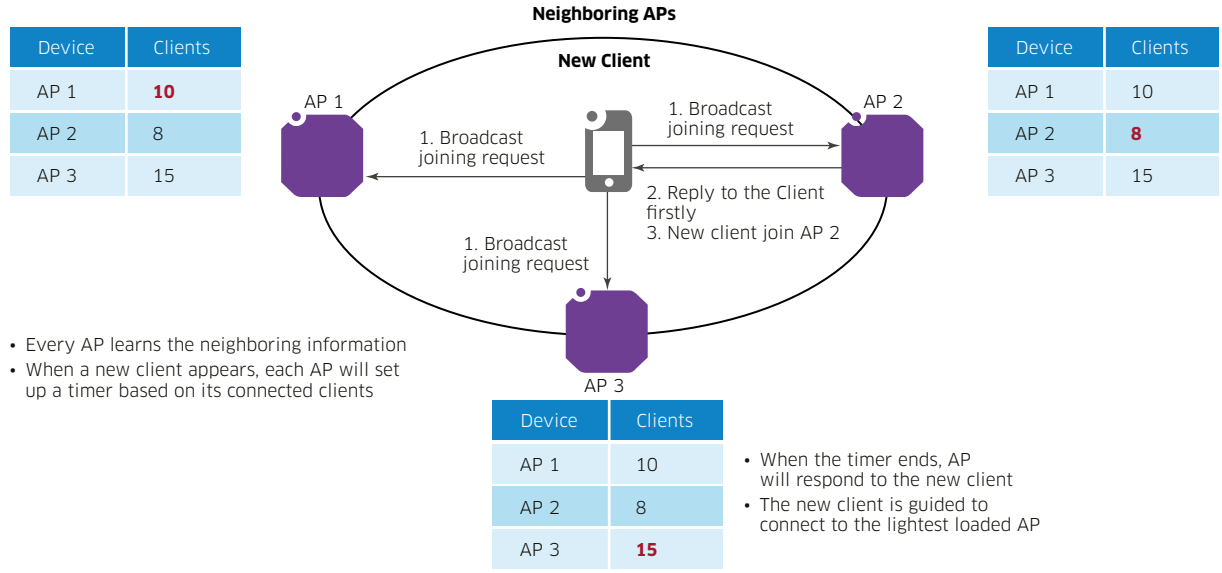
39.	If all bands/channels (2.4GHz/5GHz) are overloaded (high medium utilization) and the 5GHz is crowded, an AP shall guide a new client to the 2.4GHz band.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement as depicted on Figure 22: Dual-radio APs band steering and Figure 23: Tri-radio APs band steering (Case4).

40.	When a new client discovers multiple APs to associate to, the new client shall be guided to the AP that has the fewest associated clients, thus allowing smart/dynamic load balancing.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. Clients are typically in control of connectivity decisions such as which AP to associate with. 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. The OmniAccess Stellar WLAN solution allows smart load balancing of clients between APs. The client information like the client count per AP is shared between APs so that an AP can know the load of its neighbor AP and decide whether to permit client access based on a timer set up according to its current associated client count:

Figure 24. WLAN clients load-balancing



41.	The WLAN solution shall deny connection to an AP when the signal of the client becomes too weak and disconnect a client when the signal becomes too weak.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. Indeed, the OmniAccess Stellar WLAN solution allows to set SNR (*Signal to Noise Ratio*) thresholds in decibels (default values: 2.4G =18db, 5G = 12db) to optimize connectivity by forbidding client access to the network when the signal is too weak or by disconnecting a client when the signal becomes too weak. The thresholds are set for each radio band, considering also the 5GHz-low and 5GHz-high bands supported by the OmniAccess Stellar 123X series tri-radio access points:

Figure 25. Per-band signal strength threshold

42.	The WLAN solution shall propose APs that can scan the air to provide interfering/rogue APs and wireless attacks detection, and shall not rely on dedicated scanning equipment.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. Indeed, all OmniAccess Stellar access points have background scanning capabilities and the OmniAccess Stellar WLAN solution does not require any specific and dedicated scanning equipment.

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 or even attacks.

Background scanning is used to examine the *Radio Frequency* (RF) environment in which the wireless network is operating, discover neighbor APs, and identify interference and attacks. Background scanning is the basis of some advanced features such as wIDS/wIPS (*wireless intrusion detection/protection system*) or RDA (*radio dynamic adjustment*). When background scanning is turned off, the foreign AP detection and rogue containment will stop and the precision of the RDA feature may be affected.

By default, background scanning is enabled with default scanning interval (5 seconds, with a 5 to 10 second range) and a default scanning duration (20 ms, with a 20 to 110 ms range).

Table 3. Background scanning information

Background scanning	Enabled by default
Scanning interval	Keep default settings
Scanning duration	Keep default settings Higher scanning interval or lower scanning duration means intrusions are less likely being detected but client performance will be better Lower scanning interval or higher scanning duration means intrusions are more likely being detected but client performance will be lower
Voice and video awareness	Enabled by default

43.	The scanning function of the APs shall not impact active voice or video calls (SIP and H.323).	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. During scanning, wireless clients are impacted and the access points cannot process 802.11 data. Background scanning needs to be aware of existing traffic on the AP. If there is an ongoing voice/video session (SIP or H.323), scanning must not be performed to ensure uninterrupted traffic; and scanning must resume when there is no active voice/video session. As mentioned on Table 3: Background scanning information, the “voice and video awareness” feature is enabled by default.

4. Intrusion detection and prevention

44.	The WLAN solution have wIDS/wIPS capabilities with no additional and dedicated equipment nor additional license.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. Indeed, OmniAccess Stellar access points integrate *wireless intrusion detection and prevention* (wIDS/wIPS) capabilities and reduce deployment and management costs by using access points to simultaneously serve clients and contain wireless threats.

With OmniAccess Stellar, there is no need for a costly overlay IDS with dedicated sensors. Automatic threat mitigation protects the network from unauthorized clients or APs and attacks. Integrated wIDS/wIPS capabilities allow to protect the WLAN better than an overlay deployment by being able to analyze and correlate 802.11 frames inline. It is possible to monitor the wireless radio spectrum for the presence of unsafe access points or unsafe clients, and countermeasures can be taken to mitigate the impact of foreign intrusions.

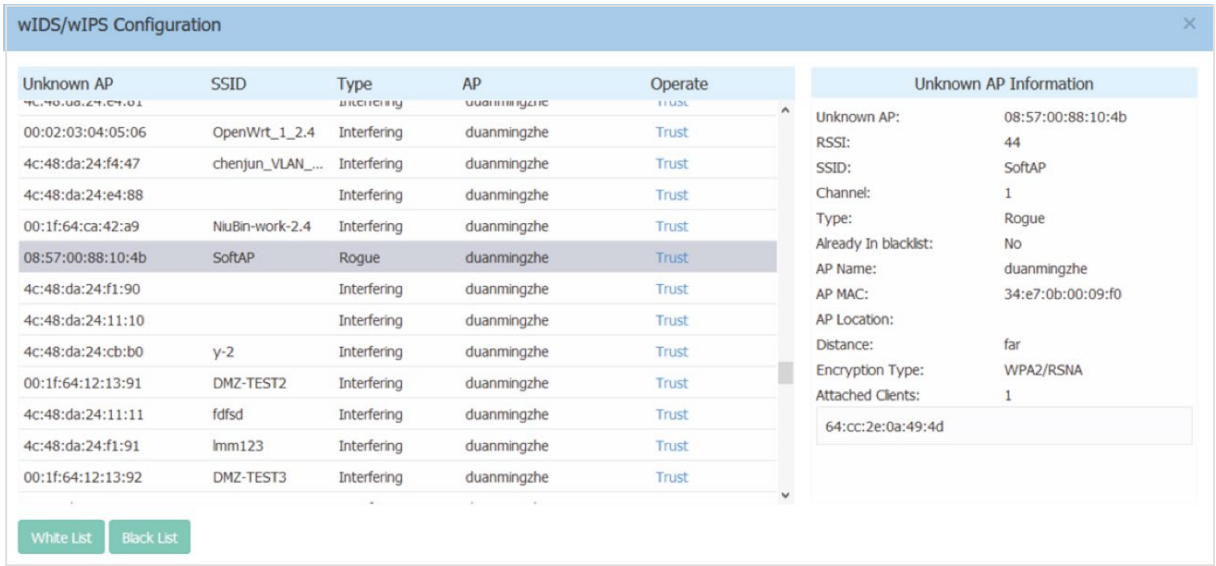
Lastly, either in Wi-Fi *Express* mode or in Wi-Fi *Enterprise* mode, the OmniAccess Stellar APs embedded wIDS/wIPS capabilities do not require any additional license to protect the wireless network.

45.	The WLAN solution shall be able to identify Interfering APs.	C/PC/NC

A wireless network is a borderless network and always works in an open environment which can be interfered with and attacked. It is useful to discover the surrounding wireless conditions, and based on that, provide instructions and tools to help administrators improve the quality of the wireless network. Usually there are two types of foreign unknown APs having a negative effect on the wireless network; they are interfering APs and rogue APs.

An **interfering AP** is an AP seen in the wireless environment but not connected to the wired network. The interfering AP can provide RF interference potentially, but, it is not considered a direct security threat, because it is not connected to the wired network. However, some interfering APs may have an impact on network quality and can interfere with valid clients accessing the network.

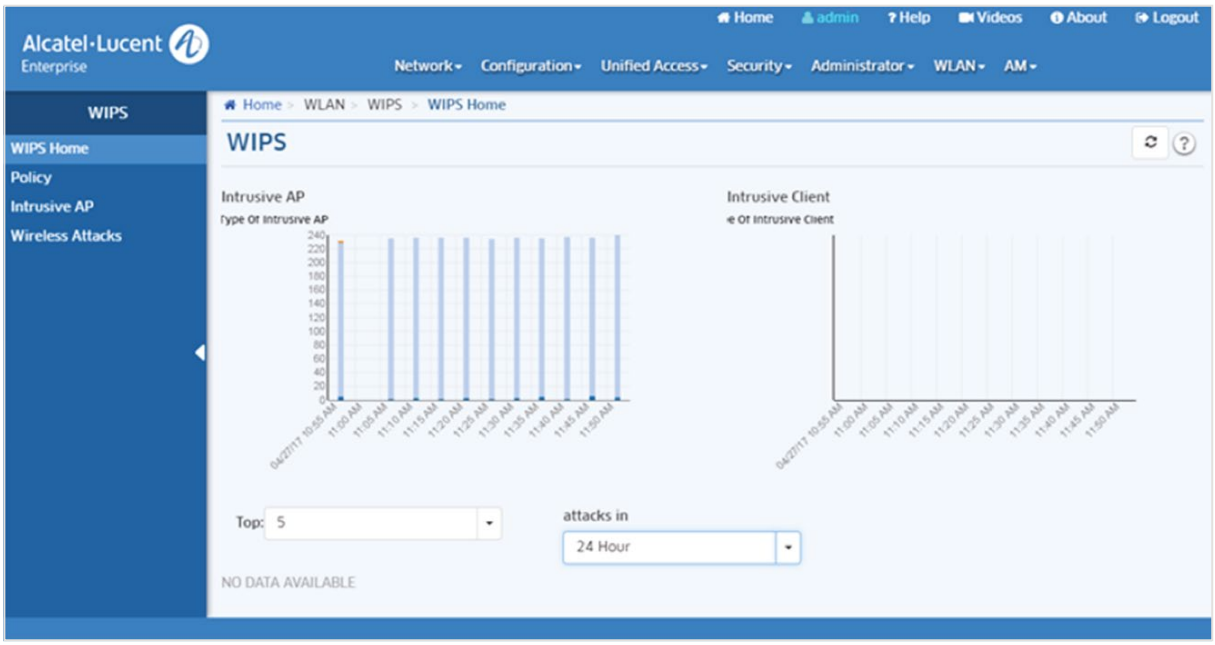
Figure 26. wIDS/wIPS - *Express* mode



46.	The WLAN solution shall be able to identify and contain rogue APs.	C/PC/NC

Beyond potential RF interference it can cause, a **rogue AP** is considered as a security threat to the WLAN network. This is typically the case of an unauthorized AP plugged into the wired side of the network (in that case, the MAC address of the scanned interfering AP is identified in the forwarding database of the scanning AP) or a foreign interfering AP broadcasting a SSID that is configured and set in the WLAN network.

Figure 27. wIDS/wIPS - *Enterprise* mode



When an AP is classified as a rogue AP and when containment is enabled (disabled by default), the detecting AP (the one that detected the rogue AP) will send DEAUTH frames to clients that have associated to the rogue AP, keeping the clients away from the unsafe wireless network.

47.	The WLAN solution shall allow the definition of flexible policies to classify an AP as a rogue AP.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. Indeed, beyond the detection of a valid SSID, and as described in table below, the OmniAccess Stellar WLAN solution can consider several other parameters for rogue AP classification:

Table 4. Rogue AP policy

Rogue AP policy	Description	Wi-Fi *Express*	Wi-Fi *Enterprise*
Unauthorized AP detected on LAN	• When an intrusive AP is plugged into the wired side of the network	Y	Y
Detect valid SSID	• When an intrusive AP plugged on the wired network is advertising a SSID that is already configured and set in the WLAN network • When an intrusive AP not plugged on the wired network is advertising a SSID that is that is already configured and set in the WLAN network and a known station MAC is detected associating with it.	Y	Y
Signal strength threshold	• The detected AP signal in dBm is too strong and above the threshold • Default: – 70 dBm (Range: -95 to -50 dBm)	N	Y
Detect rogue SSID keyword	• The detected AP is advertising a SSID name that matches one of the string set in this policy (SSID blacklist)	N	Y
Rogue OUI	• The detected AP is having a OUI that matches one of the OUI set in this policy	N	Y

48.	A least for a “large deployment” scenario as described previously [4], the WLAN solution shall allow the definition of flexible AP attacks detection policies.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. In Wi-Fi *Enterprise* mode, the OmniAccess Stellar solution allows to create flexible policies to detect and react to AP wireless attacks. When an attack is detected based on the policy, the detected AP is displayed with details for review and action. An AP attack detection policy detects multiple attacks originating from foreign APs. The following detection methods are available:

Table 5. AP attack policy - *Enterprise* mode

AP spoofing	An AP spoofing attack involves an intruder sending forged frames that are made to look like they are from a valid AP.
AP impersonation	In AP impersonation attacks, an AP assumes the BSSID and ESSID of a valid AP. AP impersonation attacks can be done for man-in-the-middle attacks, a rogue AP attempting to bypass detection, or a Honeypot attack.
Broadcast de-authentication	A de-authentication broadcast attempts to disconnect all clients in range. Rather than sending a spoofed de-authentication frame to a specific MAC address, this attack sends the frame to a broadcast address.
Broadcast disassociation	By sending disassociation frames to the broadcast address (FF:FF:FF:FF:FF:FF), an intruder can disconnect all stations on a network for a widespread DoS.
Ad hoc networksusing a valid SSID	If an unauthorized ad hoc network is using the same SSID as an authorized network, a valid client may be tricked into connecting to the wrong network. If a client connects to a malicious ad hoc network, security breaches or attacks can occur.
Long SSID	802.11 allows a maximum of 32 bytes for the SSID. Over-sized SSIDs are indicative of an attack attempting to exploit vulnerabilities in several drivers
Ad hoc networks	An ad hoc network is a collection of wireless clients that form a network among themselves without the use of an AP. If the ad hoc network does not use encryption, it may expose sensitive data to outside eavesdroppers. If a device is connected to a wired network and has bridging enabled, an ad hoc network may also function like a rogue AP. Additionally, ad hoc networks can expose client devices to viruses and other security vulnerabilities.
Wireless bridge	Wireless bridges are normally used to connect multiple buildings together. However, an intruder could place (or have an authorized person place) a wireless bridge inside the network that would extend the corporate network somewhere outside the building. Wireless bridges are somewhat different from rogue APs in that they do not use beacons and have no concept of association. Most networks do not use bridges. In these networks, the presence of a bridge is a signal that a security problem exists.
Null probe response	A null probe response attack has the potential to crash or lock up the firmware of many 802.11 NICs. In this attack, a client probe-request frame will be answered by a probe response containing a null SSID. Many popular NIC cards will lock up upon receiving such a probe response.
Invalid address combination	In this attack, an intruder can cause an AP to transmit de-authentication and disassociation frames to its clients. Triggers that can cause this condition include the use of broadcast or multicast MAC address in the source address field.
Reason code invalid of de-authentication	The 802.11 specification defines valid reason codes for disconnect and de-authenticate events. De-authentication packets with invalid reason code will be classified as an attack.
Reason code invalid of disassociation	The 802.11 specification defines valid reason codes for disconnect and de-authenticate events. Disassociation packets with invalid reason code will be classified as an attack.

49.	A least for a “large deployment” scenario as described previously [4], the WLAN solution shall allow the definition of flexible client attacks detection policies.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. In Wi-Fi *Enterprise* mode, the OmniAccess Stellar solution allows to create flexible policies to detect and react to client wireless attacks. When an attack is detected based on the policy, the detected client is displayed and can be automatically blacklisted (its MAC address is not allowed to associate to any AP of the WLAN). The following detection methods are available:

Table 6. Client attack policy - *Enterprise* mode

Valid station mis-association	This feature does not detect attacks, but monitors authorized (valid) or innocent wireless clients associated to a rogue AP.	Not blacklisted
Omerta attack	Omerta is an 802.11 DoS tool that sends disassociation frames to all stations on a channel in response to data frames. The Omerta attack is characterized by disassociation frames with a reason code of 0x01. This reason code is "unspecified" and is not be used under normal circumstances.	Blacklisted
Unencrypted valid client	This feature does not detect attacks, but monitors authorized (valid) or innocent wireless clients associated to an open (no encryption) SSID. A valid client that is passing traffic in unencrypted mode is a security risk. An intruder can sniff unencrypted traffic (also known as packet capture) with software tools known as sniffers. These packets are then reassembled to produce the original message.	Not blacklisted
802.11 40Mhz intolerance setting	When a client sets the HT capability "intolerant bit" to indicate that it is unable to participate in a 40MHz BSS, the AP must use lower data rates with all its clients. Network administrators often want to know if there are devices that are advertising 40MHz intolerance, as this can impact the performance of the network.	Blacklisted
Active 802.11n greenfield mode	When 802.11 devices use the HT operating mode, they can't share the same channel as 802.11a/b/g clients. Not only can they not communicate with legacy devices, the way they use the transmission medium is different, which would cause collisions, errors and retransmissions.	Blacklisted
DHCP client ID	A client which sends a DHCP DISCOVER packet containing a client-ID tag (tag 61) which doesn't match the source MAC of the packet may be doing a DHCP denial-of-service to exhaust the DHCP pool.	Blacklisted
DHCP conflict	Clients which receive a DHCP address and continue to use a different IP address may indicate a mis-configured or spoofed client.	Blacklisted
DCHP name change	The DHCP configuration protocol allows clients to optionally put the hostname in the DHCP discover packet. This value should only change if the client has changed drastically (such as a dual-boot system). Changing values can often indicate a client spoofing/MAC cloning attack.	Blacklisted
Malformed frame association request	A null probe response attack has the potential to crash or lock up the firmware of many 802.11 NICs. In this attack, a client probe-request frame will be answered by a probe response containing a null SSID. Many popular NIC cards will lock up upon receiving such a probe response.	Blacklisted
Sticky client	Client keep trying to authenticate with too much authentication failure.	Blacklisted
Detect long SSID in client detection	The 802.11 specification allows a maximum of 32 bytes for the SSID. Over-sized SSIDs also in probe request frame or associate request frame are indicative of an attack attempting to exploit vulnerabilities in several drivers.	Blacklisted
Detect Reason Code Invalid	The 802.11 specification defines valid reason codes for disconnect and de-authenticate events. Invalid reason code in disassociation frames and de-authentication frames indicates an attack attempt.	Blacklisted

50.	A least for a "large deployment" scenario as described previously [4], the WLAN solution shall be able to blacklist a WLAN client, either manually or automatically after a client attack has been detected.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. In Wi-Fi *Enterprise* mode, the OmniAccess Stellar solution allows to manually or automatically blacklist a client. If a wireless attack has been detected the intruder identified (MAC address) by the wIDS/wIPS application is prevented from associating with the network.

51.	A least for a “large deployment” scenario as described previously [4], the WLAN solution shall allow to configure a blacklist duration.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution (in Wi-Fi *Enterprise* mode) fully complies with this requirement.

52.	A least for a “large deployment” scenario as described previously [4], the WLAN solution shall allow to configure an authentication failure times threshold.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution (in Wi-Fi *Enterprise* mode) fully complies with this requirement. When a client fails to pass the authentication in the associated phase for too many times in a brief period, it will be classified as an intruder and added into the “Client Blacklist”. (Ranges: 3 - 10 times per 5 - 3600 seconds, Default: 10 times per 60 seconds).

5. Quality of service

53.	At least for a “large deployment” scenario as described previously [4], the WLAN solution shall offer WLAN access points that shall support fine-tuned Quality of Service (QoS) allowing following actions based on the identity of the connecting user: • ACL based (source/destination IP address and TCP/UDP ports) permit/ deny decision • QoS priority marking and queuing	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. Each time a user connects to the WLAN network, a role is assigned to that user and connection. That role assigns a VLAN to the user. It also defines and applies network security ACLs and a QoS policy to the user connection. The security ACLs (based on source/destination IP address and TCP/UDP ports) allow to restrict the resources the user can access like critical financial servers.

The QoS policy defined in the user role allows to assign the QoS markings (802.1p/DSCP on the wired side, and WMM over the air) within the AP based on the user identity to apply user specific treatment to the traffic originating from or destined for that user, thus providing appropriate QoS for each application such as voice, video and desktop sharing.

54.	The wireless LAN solution shall comply with the 802.11e WMM standard and shall allow for custom QoS tag (802.1p/DSCP) to WMM queue mapping.	C/PC/NC

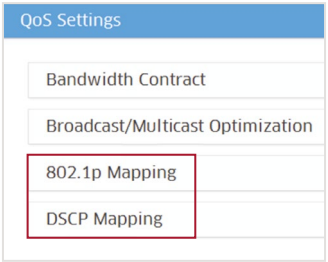
The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. The OmniAccess Stellar solution and access points are indeed WFA 802.11e WMM certified, ensuring proper prioritization of real-time voice and video traffic and applications according to four categories: “Voice”, “Video”, “Best Effort” and “Background”.

In the downstream portion of the WLAN network (AP to the device), prioritization is handled in the AP. Delay sensitive traffic is identified by the AP based on the 802.1p MAC header field or the DSCP IP header field of the inbound traffic. Upon receiving priority-tagged frames, the AP places these frames into a high-priority queue. Frames are transmitted using a strict queuing method, ensuring that high priority frames are always transmitted before low-priority frames.

In the upstream portion of the WLAN network (device to the AP), devices transmitting priority-sensitive traffic can use WMM (Wi-Fi Multimedia) - a derivative of IEEE 802.11e -to provide preferential access to the wireless media. WMM also provides a mechanism for client devices to tag frames with a relative priority, allowing the AP to recognize the relative priority of the received frame.

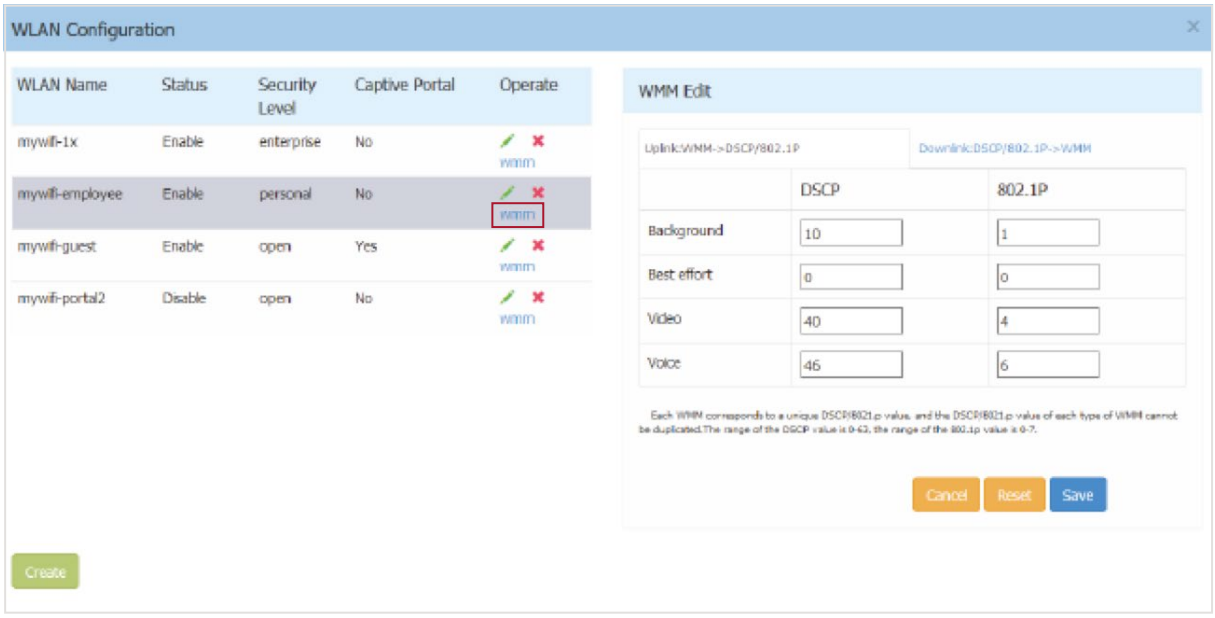
The OmniAccess Stellar solution, both in Wi-Fi *Express* mode and Wi-Fi *Enterprise* mode, allows for use of customized DSCP/802.1p to WMM queue mapping to accommodate already existing assignments used within the wired LAN. The OmniVista 2500 NMS allows granular WMM-802.1p/DSCP mapping:

Figure 28. WMM/802.1p-DSCP mapping - *Enterprise* mode



Such a mapping is also possible in OmniAccess Stellar Wi-Fi *Express* mode:

Figure 29. WMM/802.1p-DSCP mapping - *Express* mode



The recommended WMM/802.1p-DSCP mapping settings are described in following table:

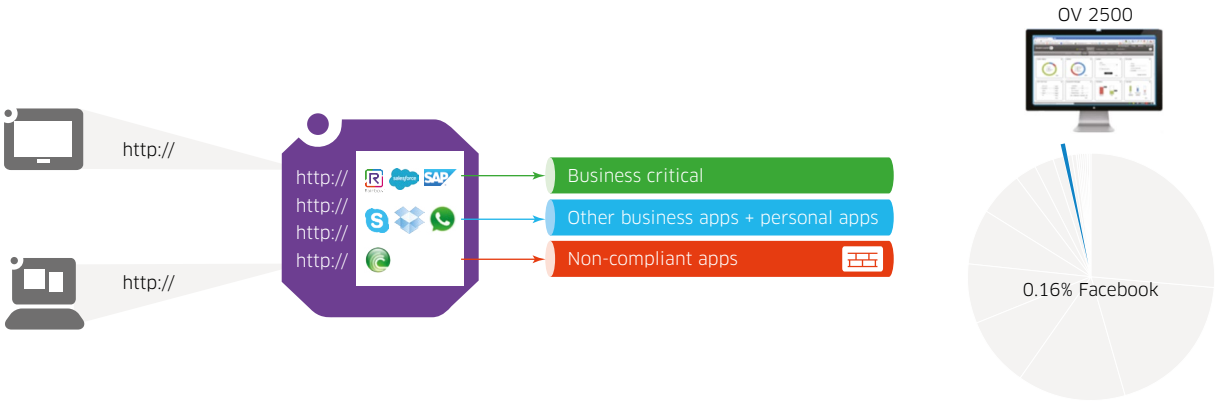
Table 7. WMM/802.1p-DSCP recommended mapping

WMM	802.1p	DSCP
Best Effort	0	0
Background	2	18 – AF 21
Voice	5	46 - EF
Video	4	34 - AF41

55.	A least for a “large deployment” scenario as described previously [4], the WLAN solution shall have traffic *deep packet inspection* (DPI) capabilities allowing an administrator to take control of applications (even if they all run on top of the HTTP or HTTPs protocols), including not only blocking applications, but also allowing to prioritize and rate-limit applications.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution in Wi-Fi *Enterprise* mode fully complies with this requirement. Indeed, the AP122X, AP123X and 125X series have a built-in DPI technology that provides real-time applications classification and role-based control capabilities: The *Application Visibility and Enforcement* feature. With OmniVista 2500, the network administrator can obtain a comprehensive view of applications running in the network and apply adequate control to optimize the performance of the network for business-critical applications. It is also possible to prevent harmful or non-compliant applications from being utilized and create a space for employees to explore new applications and also use personal apps, harmonizing the coexistence of both business and personal applications.

Figure 30. Application visibility and enforcement - *Enterprise* mode



Application visibility and enforcement is an answer to the challenge of application "webification". More and more applications - even corporate application - 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) and apply different prioritization and QOS (with QoS policy lists defined in the applied user/device role) to critical applications like Salesforce, SAP, Rainbow and IP telephony against some personal services like Facebook, YouTube…

56.	The wireless LAN solution shall be able to define and guarantee bandwidth based on the SSID. At least for a "large deployment" scenario as described previously [4], it shall also be to define and guarantee bandwidth based on the user/device role.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. Indeed, in Wi-Fi *Enterprise* mode, a "bandwidth contract" may be defined and set at user/device role level based on the QoS policy list defined within the role. Moreover, the policy list can embed an application/DPI rule as previously introduced [55]. As depicted in Figure 31: SSID bandwidth contract below, a "bandwidth contract may also be set at SSID level (the bandwidth is then shared for all users, per radio) by specifying:

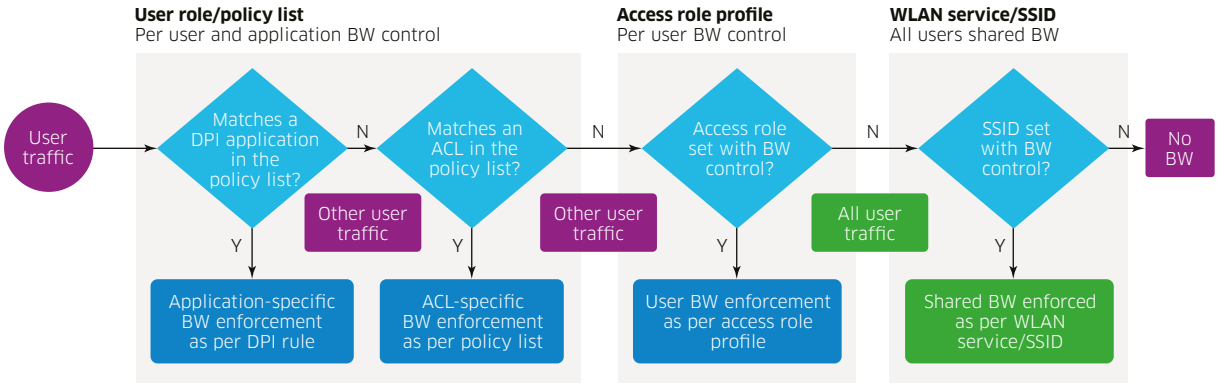
- The upstream (Ingress) bandwidth (and depth) for the SSID
- The downstream (Egress) bandwidth (and depth) for the SSID

Figure 31. SSID bandwidth contract

Such a bandwidth contract may also be set at SSID level in Wi-Fi *Express* mode.

In Wi-Fi *Enterprise* mode, a WLAN service or SSID is always configured with an associated "Access Role Profile" that defines a default role that will be applied to a user if the authentication process for that user has succeeded but has not returned a role. In that case the connected user will be assigned the VLAN, the security ACLs and the QoS policy list defined in the SSID "access role profile":

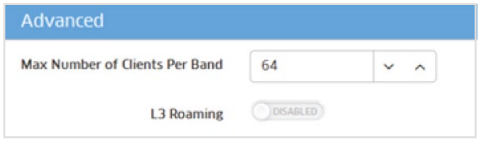
Figure 32. User bandwidth control precedence



57.	At least for a "large deployment" scenario as described previously [4], the WLAN solution shall allow to set the maximum number of clients per band/ radio and per AP for a specific SSID.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement.

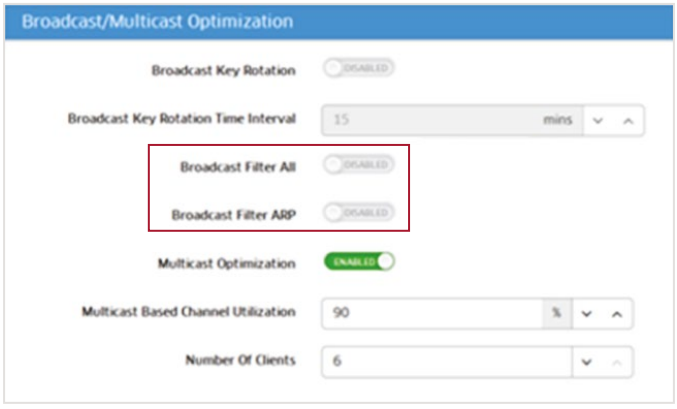
Figure 33. Maximum number of clients per band per SSID



58.	The wireless LAN solution shall propose broadcast traffic optimization mechanisms (including broadcast filtering and broadcast/multicast key rotation).	C/PC/NC

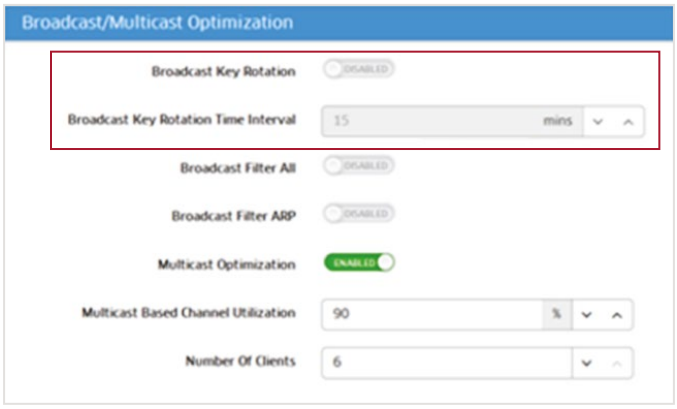
The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. As depicted in Figure 34: Broadcast filtering - Enterprise mode below, the OmniAccess Stellar WLAN solution, in Wi-Fi *Enterprise* mode, allows to filter broadcast traffic by dropping all multicast packets except DHCP and ARP. It allows also to convert multicast ARP to unicast:

Figure 34. Broadcast filtering - *Enterprise* mode



The OmniAccess Stellar WLAN solution allows to activate "*Broadcast Key Rotation*" (with WPA, WPA2 or Dynamic WEP encryption only) and set the broadcast key rotation time (default value: 15 min, Range: 1 min – 24 hours):

Figure 35. Broadcast Key Rotation - *Enterprise* mode

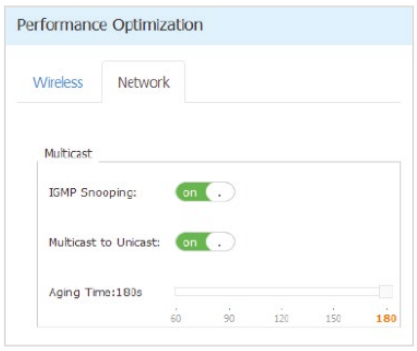


When "*Broadcast Key Rotation*" is enabled, encryption keys constantly rotate, making them much harder for hackers to sniff with a protocol analyzer. But, the faster the keys rotate, the more potential there is for transmission latency while the key resets. It is recommended to start with a small value, and, if performance issues are encountered, increase it until the performance issues stop.

59.	Leveraging its IGMP snooping capabilities, the wireless LAN solution shall be able to optimize multicast traffic by converting multicast traffic to unicast traffic.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. In an OmniAccess Stellar deployment, multicast traffic is appropriately controlled to ensure that proper bandwidth exists for all connected devices/users. IGMP snooping, enabled on the APs (either in Wi-Fi *Express* or in Wi-Fi *Enterprise* mode) allows to reduce the amount of traffic replication within the network infrastructure. IGMP Snooping is enabled by default and ensures that the wired infrastructure sends multicast traffic, such as video traffic, only to those APs that have active subscribers.

Figure 36. Multicast optimization - *Express* mode



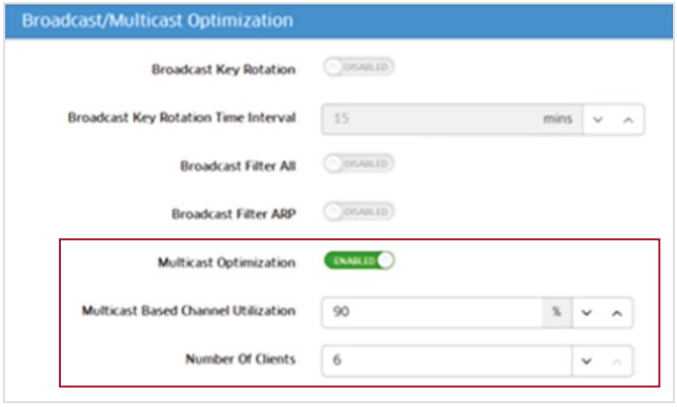
Wireless multicast transmissions occur at broadcast rates. Broadcast and multicast frames are not acknowledged, so these transmission methods use lower (slower) data rates to provide a better chance of reception. The 802.11 standard states that multicast over WLAN must be transmitted at the lowest supported rate so that all clients can decode it. The low transmission rate results

in increased airtime utilization, and therefore decreased overall throughput for transmissions. Because of the slower speed, it is desirable to transform multicast traffic to unicast when a few clients have subscribed to a multicast stream. Transforming multicast traffic to unicast increases the speed of wireless transmissions by using the higher unicast rates.

60.	At least for a “large deployment” scenario as described previously [4], multicast optimization shall stop on high load.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. In general, unicast traffic can be transmitted at higher transmission rates and an acknowledgement ensures consistent delivery. However, after a certain number of clients have been reached, it is more efficient to revert to multicast transmissions.

Figure 37. Multicast optimization - Enterprise mode



Two parameters can be considered to stop multicast optimization on high load:

- Channel use (RF environment too poor to have optimization): The default value is 90% (range: 85% to 95%)
- Number of Clients (CPU load too high to support optimization): The default value is 32 (range: 16 to 64)

61.	The wireless LAN solution shall propose the WMM *Automatic Power Save delivery* (APSD) feature to allow clients conserve battery life.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution and access points fully comply with this requirement, allowing mobile WLAN client (especially devices like phones running real time applications) to save more battery while connected to the WLAN network by entering standby or sleep mode. The WMM APSD feature allows smooth transition in and out of sleep mode by allowing the client to signal the AP of its status. Whenever the clients enter power saving mode or “sleep” mode, the AP can buffer data and hold it for the client. The client chooses the time to wake up and receive data packets to maximize power conservation without sacrificing quality of service.

62.	The wireless LAN solution shall by default identify voice and video (SIP and H323) calls and provide appropriate treatment.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. It is indeed SIP and H323 voice and video over IP aware, and can dynamically classify real-time traffic in appropriate class of service. In addition, this level of voice awareness enables OmniAccess Stellar APs to know that a voice/video call is taking place and not to scan channels for RF management or intrusion detection purposes until the call is terminated.

6. Mobility

63.	The WLAN solution shall support Layer 2 roaming capabilities across APs with no special client-side software required.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement, either in Wi-Fi *Express* or in Wi-Fi *Enterprise* mode. Mobility and roaming is a given. In an Alcatel-Lucent Enterprise Stellar deployment, roaming is always transparent and seamless to both the client and the network (the end goal is that the client's view of the network does not change, and the network's view of the client does not change). With very high roaming performances, delay-sensitive and persistent applications such as voice and video experience no interruption.

L2 roaming between APs means the roaming client remains in the same VLAN when associating to the new AP and its IP address does not change. Roaming between APs occurs on the same subnet and all traffic goes through standard Layer 2 learning to allow a WLAN client to move from one AP to another. L2 roaming is always enabled.

Roaming relies on "client contexts" sharing between adjacent APs and L2 or L3 roaming decision is based on client VLAN between the "home" and the "foreign" AP. All APs learn about their neighboring APs through "over-the-air" exchanges allowing to announce to each other their respective IP management on the wired side of the network. The adjacent APs can then share dynamically clients' contexts that contain client specific information allowing the APs to handle roaming properly:

Table 8. Clients contexts

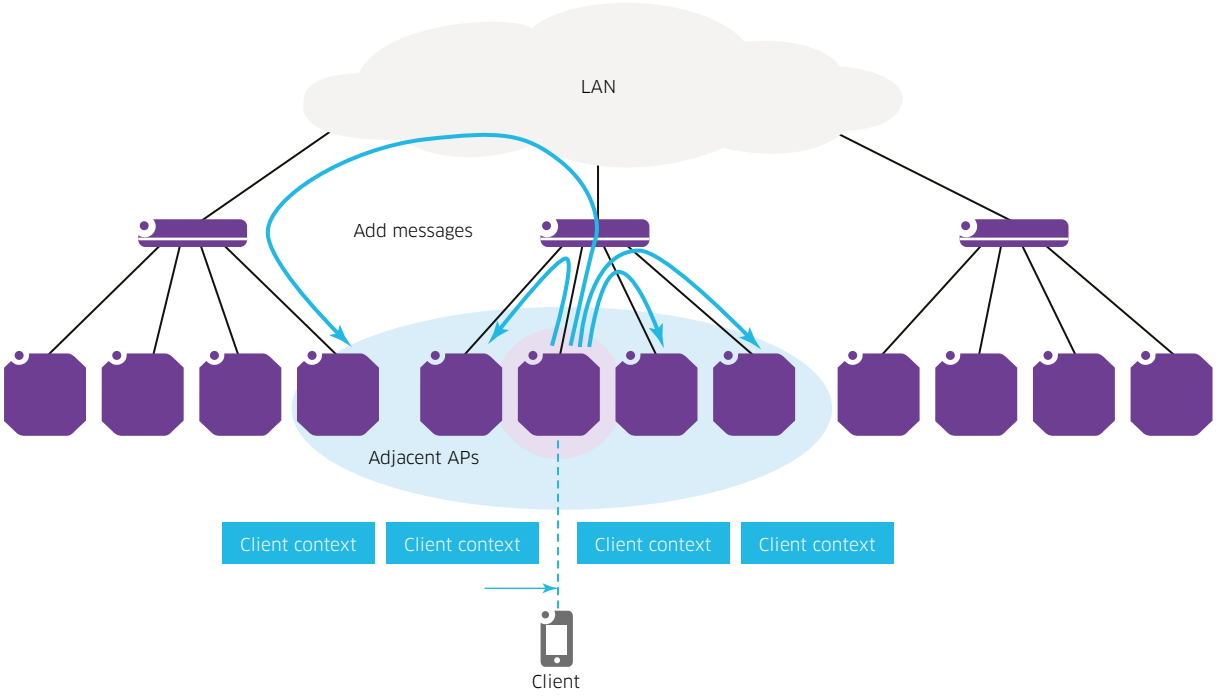
Client network context	AP context	Fast roaming

• SSID and WLAN service
• MAC address
• IP address
• Currently assigned:
  ¬ VLAN ID
  ¬ Access role profile
  ¬ Policy list
  ¬ Redirect-URL
  ¬ Captive portal status
	• MAC address
	• IP address
	• OV IP address
		• PMKSA cache
		• FT PMK R0/R1 cache

Upon roaming, the adjacent AP implement a client context removal mechanism. On client association, the new AP sends an *add message* to all adjacent APs, and, on client dis-association, the AP sends a *delete message* to all adjacent APs. On a receiving AP, *add/delete* messages are discarded when the AP is not managed by the same OV, or when the AP does not have the WLAN service (SSID).

The following figure illustrates the *add* messages that are sent by an AP to its adjacent APs upon association of a client on the move (*delete* messages are not depicted):

Figure 38. Client context sharing



The roaming conditions may be summarized as follows:

Table 9. Client roaming conditions

Client context exists on the new AP?	Client context WLAN service and access role profile exist on new AP?	Client context VLAN ID = VLAN ID mapped to the access role profile on new AP?	Roaming results
No	-	-	No roaming, new client
Yes	No	-	No roaming, new client
Yes	Yes	Yes	L2 roaming
Yes	Yes	No	L3 roaming

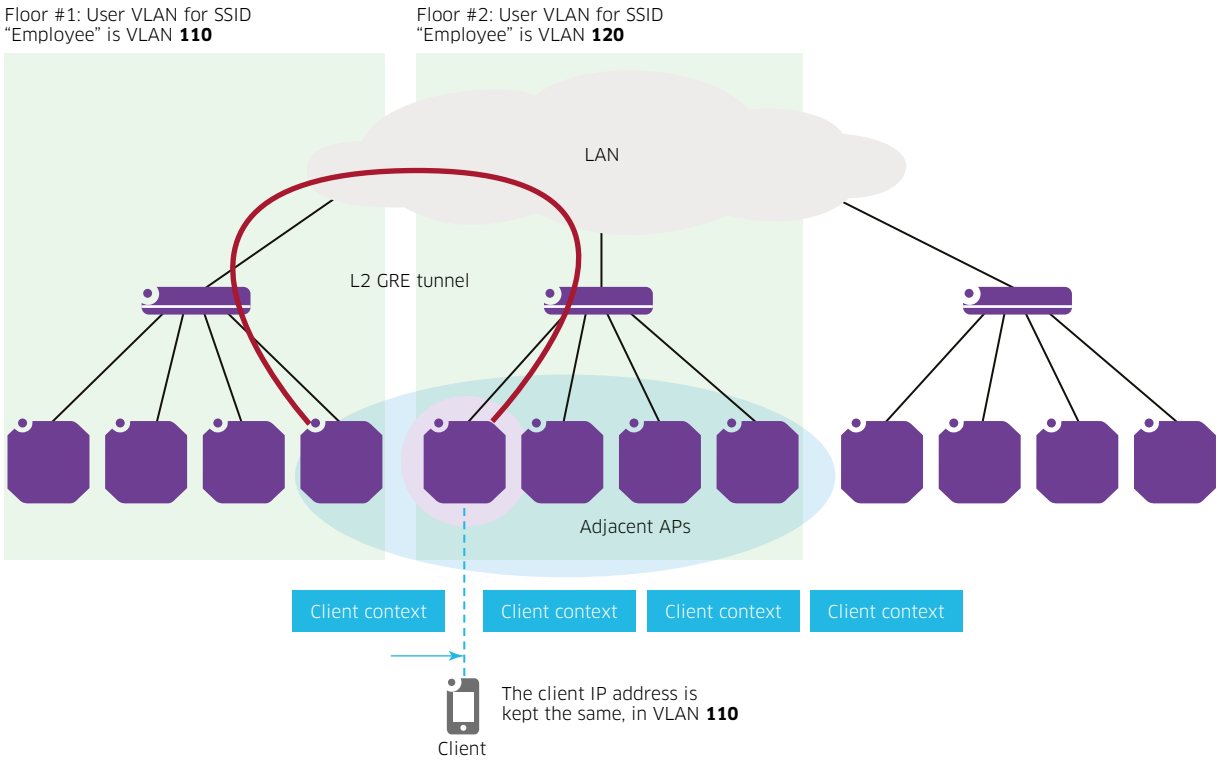
64.	At least for a “large deployment” scenario as described previously [4], the WLAN solution shall support Layer 3 roaming across APs with no special client-side software required.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution, in Wi-Fi *Enterprise* mode, fully complies with this requirement.

In campus WLAN deployments, there must be multiple user VLANs that need to be provisioned since the number of IP addresses available per VLAN are restricted by the subnet size (for instance, 255 for 255.255.255.0 or/24 address space) and there are more mobile users in a WLAN deployment than the provisioned address space. WLAN deployment hence require provisioning of different APs, supporting the same SSID, assigned with different user VLANs. A wireless user that roams across APs that are assigned with different user VLANs is regarded as performing L3 roaming – as it is roaming across different user VLANs. The *Enterprise* mode of the OmniAccess Stellar WLAN solution allows to automatically tunnel the traffic of a roaming client from the “foreign” AP (the new associating AP) to the “home” AP (the former associating AP). A L2 GRE tunnel is indeed established by the foreign AP to the home AP at early stage of roaming and the client traffic is transparently tunneled to the home AP where it is then processed locally.

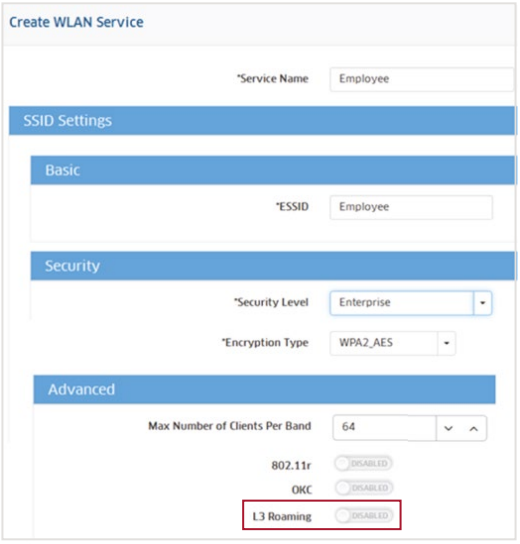
This allows users to roam the enterprise without a change of IP address as depicted in following figure where the same SSID is broadcasted in two floors of a same building but with specific user VLANs per floor:

Figure 39. L3 roaming



All policies including QoS and security ACLs, are maintained as the user roams and L3 roaming (disabled by default) shall be enabled at SSID ("WLAN service") level:

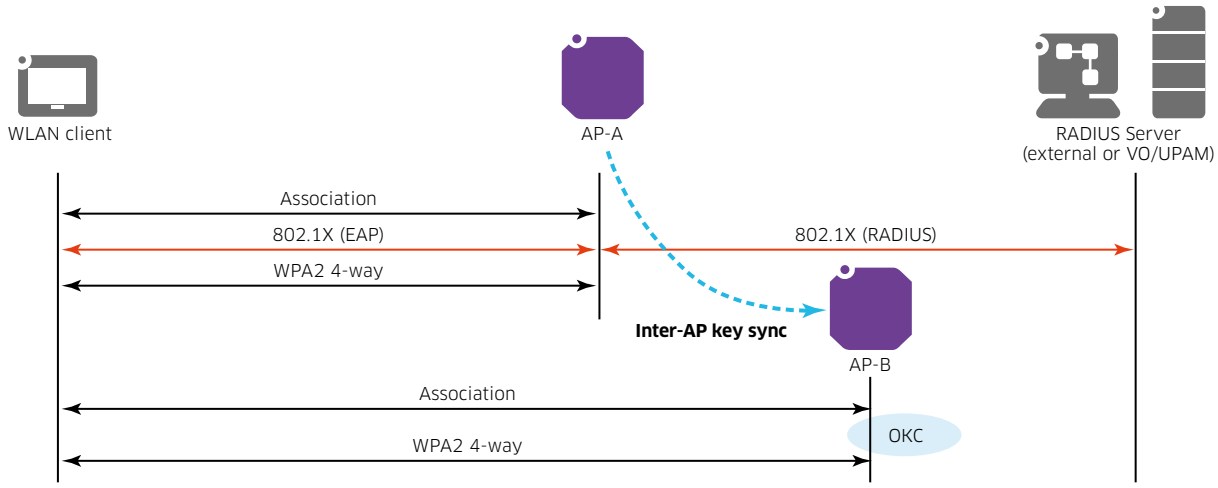
Figure 40. L3 roaming activation



65.	The WLAN solution shall support both *Opportunistic Key Caching* (802.11k).	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution, fully complies with this requirement. *Opportunistic key caching* (OKC, 802.11k), which is supported on WPA2 Enterprise SSIDs only, helps reduce the time needed for authentication. When OKC is used, multiple APs can share *pairwise master keys* (PMKs, resulting from the initial 802.1X client authentication) among themselves, and the WLAN client can roam to a new AP that has not visited before and reuse a PMK that was established with the current AP. OKC allows the client to roam quickly to an AP it has never authenticated to, without having to perform pre-authentication. OKC is available specifically on WPA2 SSIDs only. OKC helps stations to roam faster by caching the PMK. When the PMK is cached, WPA2 stations can bypass 802.1X authentication and derive new encryption keys when they roam between APs.

Figure 41. OKC (802.11k) fast roaming



66.	The WLAN solution shall comply to the 802.11r standard.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. Like 802.11k, 802.11r has been designed to create a more seamless roaming experience for WLAN clients. This is particularly useful for VoIP or other real-time applications where long roaming times can result in a very noticeable impact on performance. 802.11r uses *Fast Basic Service Set Transition* (FT) to allow encryption keys to be stored on all the APs in a network. This way, a client doesn't need to perform the complete authentication process to an authentication backend server every time it roams to a new AP within the network. Thus, avoiding a significant amount of latency that would have previously delayed network connectivity.

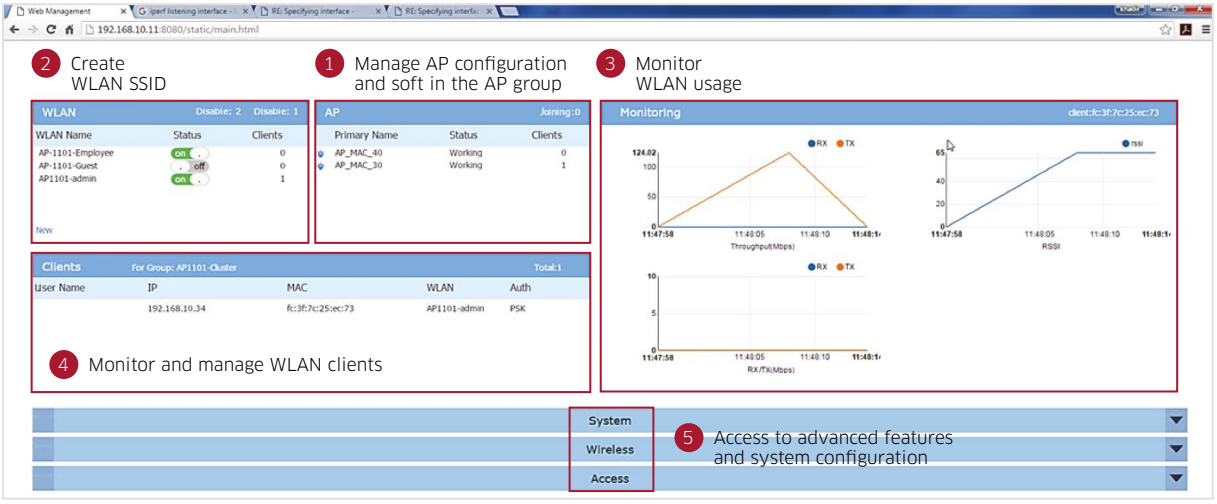
7. Management

67.	The wireless LAN solution shall propose a centralized management function based on an embedded and secure WEB GUI, irrespective of the deployment model (“small” or “large”) as described previously [4].	C/PC/NC

Both deployment models (Wi-Fi *Express* or Wi-Fi *Enterprise*) allowed by the OmniAccess Stellar solution offer a secure (HTTPS) web based centralized management function relying on:

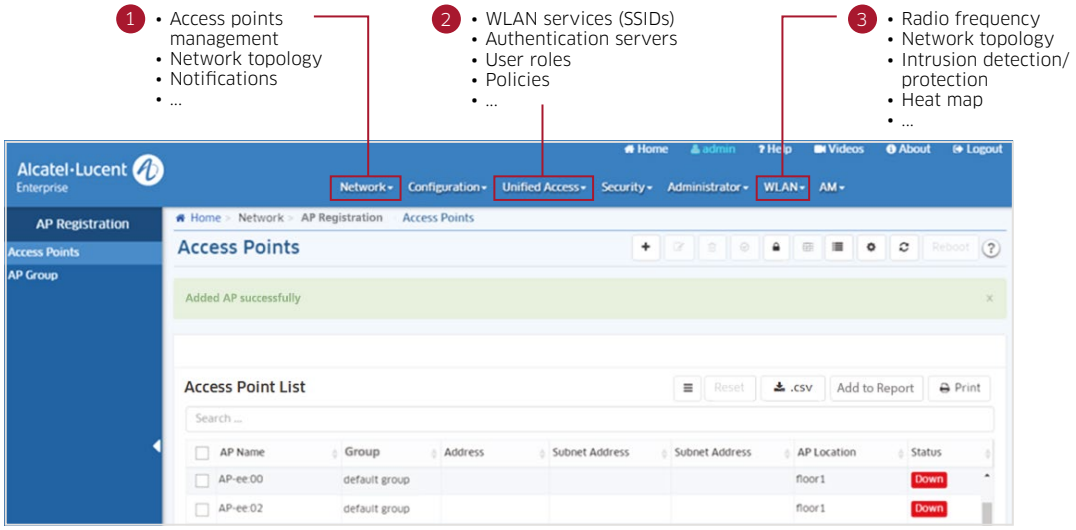
- AA web server embedded in the PVM/SVM (Primary/Secondary Virtual Manager) access point in the Stellar Wi-Fi *Express* mode

Figure 42. Centralized management - *Express* mode



- The Alcatel-Lucent Enterprise OmniVista 2500 unified (wired and wireless) Network Management System in the Stellar Wi-Fi *Enterprise* mode

Figure 43. Centralized management (OmniVista) - *Enterprise* mode



68.	If the centralized management function requires the deployment of a dedicated application, this one shall be in the form of a Virtual Appliance that can be installed on top of any of following hypervisors: VMware ESXi, Microsoft HyperV and Oracle VirtualBox.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. Indeed, the OmniVista 2500 NMS that is part of the OmniAccess Stellar WLAN solution in Wi-Fi *Enterprise* mode is available as a virtual appliance (for example, OVF file) that may be installed on top of a VMware ESXi, Oracle VirtualBox, or Microsoft HyperV hypervisor. The management function in Wi-Fi *Express* mode is handled by the *primary virtual manager* (PVM) access point.

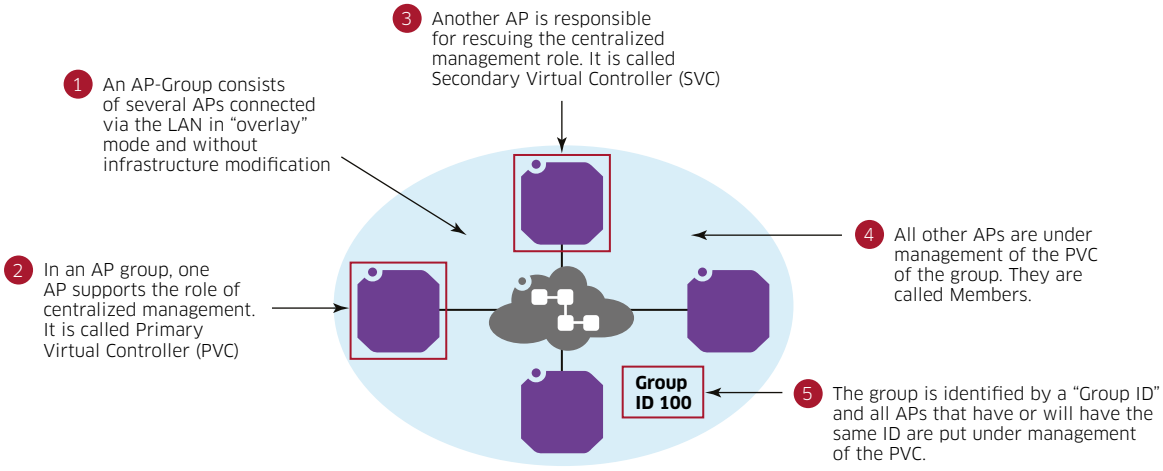
69.	At least for a "large deployment" scenario as described previously [4], the centralized management function shall be able to handle wired equipment (switches) management for a "unified management" approach.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. Indeed, the OmniVista 2500 NMS that is part of the OmniAccess Stellar WLAN solution in Wi-Fi *Enterprise* mode, provides unified management of your whole network with Alcatel-Lucent switches and third-party network equipment. That "unified management" approach provides a single pane of glass for the entire network (wired/wireless), with a single management platform, same cohesive (wired or wireless) workflows and applications for maximum operational value.

70.	The WLAN solution shall be able to automatically discover new APs added to the network.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. In Wi-Fi *Express* mode, all APs are connected to the same VLAN and build together a cluster or AP-Group if they share the same "Group ID". They are then put under the management of the PVM (supported by the SVM) for the AP-group. An AP that is not configured with the right "Group ID" will not be added to the cluster and will work in standalone mode:

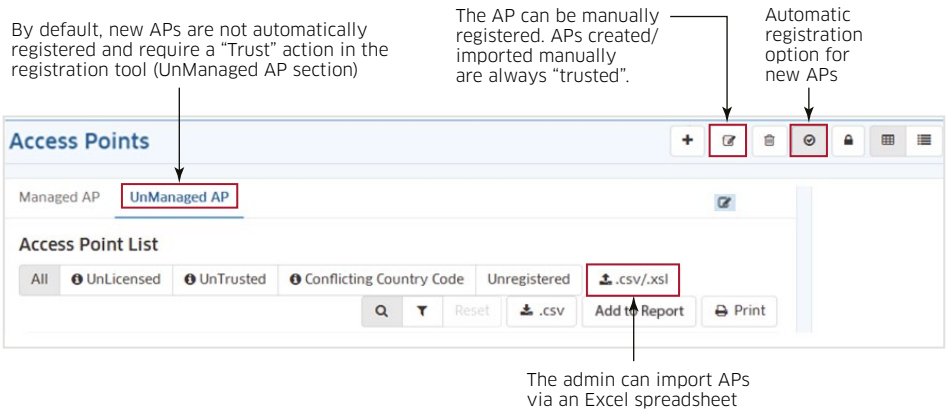
Figure 44. APs automatic discovery - *Express* mode



When the AP has joined the AP-group, it is not yet operational but in "joining" state until it is authorized by the network administrator to join the AP-group through the PVM embedded administration web GUI.

In Wi-Fi *Enterprise* mode, the APs contact the OmniVista 2500 server according to the Option 138 inserted in the DHCP lease they have received (please refer to requirement [9]). They can then "register". By default, for security reasons, new APs are not automatically registered and require a "Trust" action in the registration tool. An untrusted AP will have the radios turned off. But the OmniVista 2500 NMS offers the possibility to configure "automatic registration" for new APs:

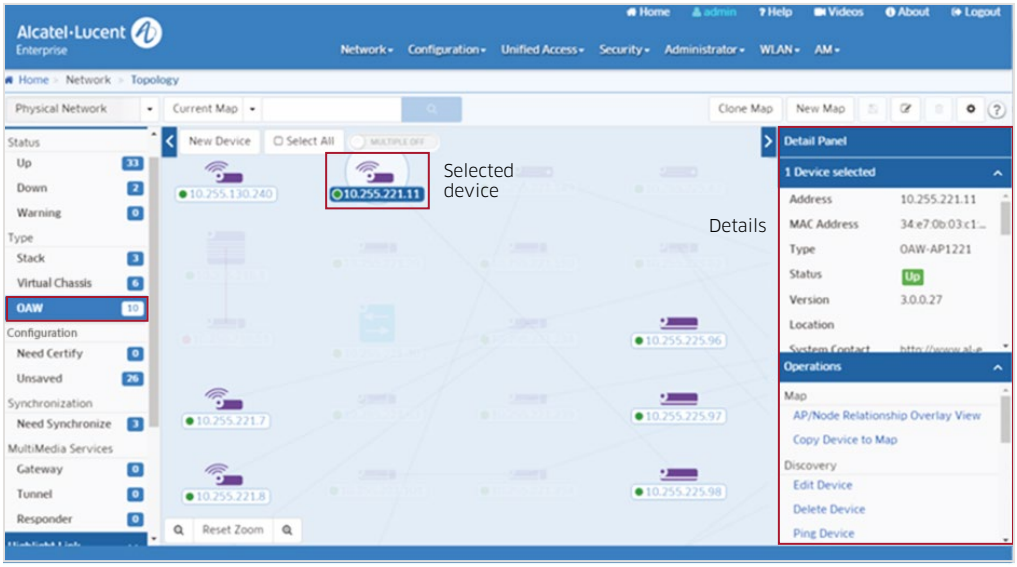
Figure 45. APs Automatic discovery - *Enterprise* mode



71.	At least for a "large deployment" scenario as described previously [4], the centralized management function shall allow to display the physical topology of the network.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. The OmniVista 2500 NMS, as a unified management platform (wired and wireless), automatically builds a topology of the network, displaying the wireless access points and the switches that connect them. The links in-between are also displayed:

Figure 46. Network topology - *Enterprise* mode



The network administrator can easily display only the wireless devices, and clicking on a device allows the administrator to see more detailed information about any device.

72.	The centralized management function shall allow per equipment configuration and software backup and restore, and bulk backup and restore.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement, either in Wi-Fi *Express* or in Wi-Fi *Enterprise* mode as depicted in following pictures.

Figure 47. Backup and restore - *Express* mode

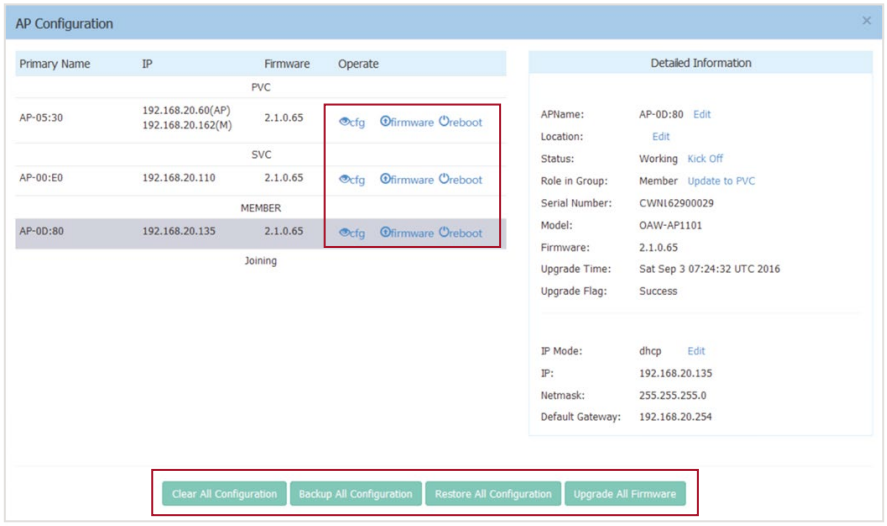
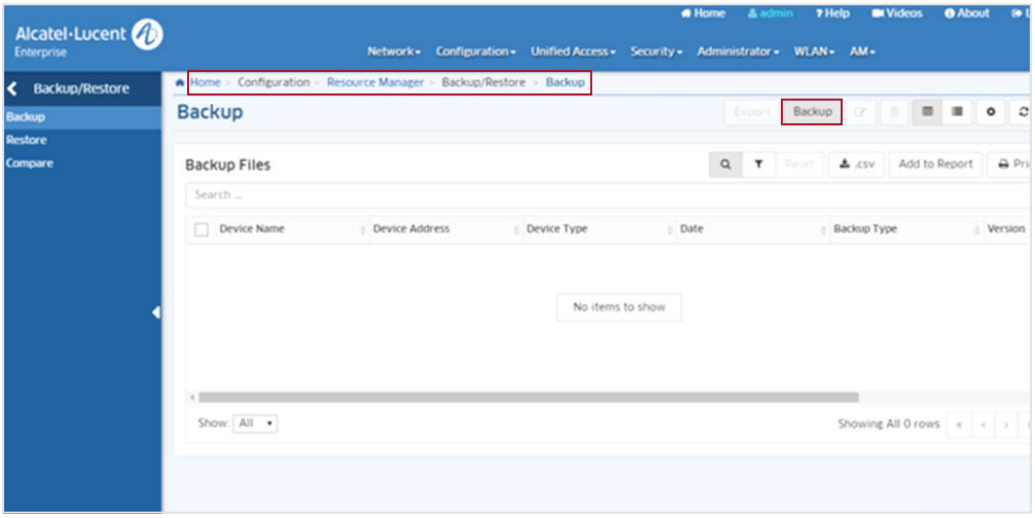


Figure 48. Backup and restore - *Enterprise* mode



73.	The centralized management function shall allow access to all wIPS/wIDS features.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement, either in Wi-Fi *Express* or in Wi-Fi *Enterprise* mode. Please refer to chapter 5.

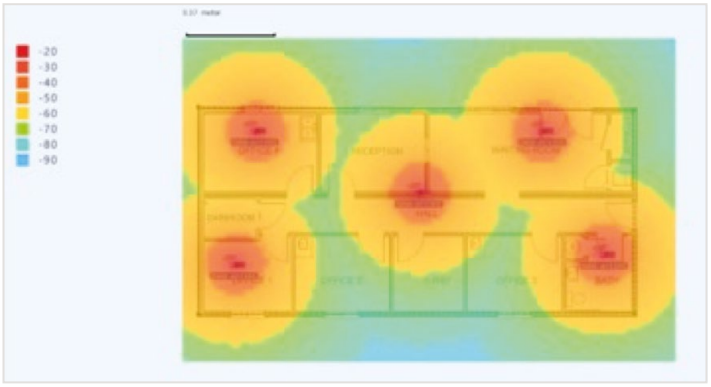
74.	At least for a “large deployment” scenario as described previously [4], the centralized management function shall offer, based on an application signature file, insight at application layer (for example, *facebook.com*, *youtube.com*, *salesforce.com*…) even if the applications run on top of the HTTP or HTTPs protocols. It shall also allow control of those applications.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. Please refer to requirement [55].

75.	At least for a “large deployment” scenario as described previously [4], the centralized management function shall allow to display the Wi-Fi coverage quality within a given area (“Heat Map”).	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. Indeed, the OmniVista 2500 NMS allows to use the “h*eat map*” application which is a design, verification, troubleshooting tool for installed Stellar Wi-Fi networks. The application provides a way to create and organize heat maps from multiple locations, from campus level to building level and floor level to give a comprehensive view of Wi-Fi coverage:

Figure 49. Heat map - *Enterprise* mode



After creating a heat map, the map displays the Wi-Fi coverage quality. Wi-Fi coverage areas are displayed by color depending on the quality of the coverage.

76.	At least for a “large deployment” scenario as described previously [4], the centralized management function shall allow, before deployment, to determine optimal placement of access points (APs) in a location (RF Planning).	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. Indeed, the OmniVista 2500 NMS allows to use the “*Floor Plan*” application which is a design, verification, troubleshooting tool for Stellar Wi-Fi networks. Floor Plan can be used to determine optimal placement of APs in a location. The application can also automatically determine AP placement and configurations for optimal set-up.

The application enables to create a floor plan for a location and manually place Stellar APs on the floor plan to view the effective Wi-Fi coverage within the floor plan. An expected coverage area on the floor plan can also be set up and the application will automatically identify the optimal number and location of APs within the floor plan to use as a guide when installing APs on site.

77.	At least for a “large deployment” scenario as described previously [4], the centralized management function shall be collocated with the Guest and BYOD management applications.	C/PC/NC

The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement by collocating the three functions on the OmniVista 2500 Network Management System. Please refer to chapter 3 and requirement [13].

8. Access points specific requirements

8.1. Indoor access point – Type A

78.	The WLAN solution shall propose an 802.11ac wave1 indoor dual-radio AP (2GHz, 5GHz) Access Point: “Type A”.	C/PC/NC

With the OmniAccess Stellar AP1101 wave1 and dual-radio AP, the Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement.

Figure 50. OmniAccess Stellar AP1101 access point

79.	The “Type A” access point shall have integrated omnidirectional antennas.	C/PC/NC
80.	The “Type A” access point shall support up to 16 SSIDs (8 per radio).	C/PC/NC
81.	The “Type A” access point shall offer up to 867Mbps throughput on the 5Ghz band and up to 300Mbps throughput on the 2.4GHz band.	C/PC/NC
82.	The “Type A” access point shall support up to 128 clients.	C/PC/NC
83.	The “Type A” access point shall have one 1 GbE port.	C/PC/NC
84.	The “Type A” access point shall support 802.3af/at PoE with 10W maximum consumption.	C/PC/NC
85.	The MTBF for the “Type A” access point shall be at least 525600h (60 Years).	C/PC/NC
86.	The “Type A” access point shall propose a factory reset button.	C/PC/NC
87.	The “Type A” access point shall propose a console port.	C/PC/NC

8.2 Indoor access point – Type B

88.	The WLAN solution shall propose an 802.11ac wave2 MU-MIMO indoor dual-radio AP Access Point: “Type B”.	C/PC/NC

With the OmniAccess Stellar AP1220 series wave2 and dual-radio APs, the Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement.

Figure 51. OmniAccess Stellar AP1220 series

89.	The “Type B” access point shall have integrated omni-directional antennas or may be equipped with external antennas.	C/PC/NC

As depicted on previous figure, The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. Indeed, the Stellar AP1220 series includes the AP1220 access point with omni-directional antennas and the AP1221 access point with connectors to connect external antennas.

90.	The “Type B” access point shall offer BLE radio support through USB port (BLE dongle).	C/PC/NC
91.	The “Type B” access point shall support up to 16 SSIDs (8 per radio).	C/PC/NC
92.	The “Type B” access point shall offer up to 1733Mbps throughput on the 5Ghz band and up to 400Mbps throughput on the 2.4GHz band.	C/PC/NC
93.	The “Type B” access point shall support up to 512 clients.	C/PC/NC
94.	The “Type B” access point shall have one 1 GbE port.	C/PC/NC
95.	The “Type B” access point shall propose deep packet inspection (DPI) capabilities providing real-time classification of flows at the application level.	C/PC/NC

The OmniAccess Stellar AP1220 series access points fully comply to this requirement. Please refer to requirement [55].

96.	The “Type B” access point shall support 802.3af/at PoE with 18.5W maximum consumption.	C/PC/NC

97.	The “Type B” access point shall support 802.3af/at PoE with 18.5W maximum consumption.	C/PC/NC

98.	The MTBF for the “Type B” access point shall be at least 525600h (60 Years).	C/PC/NC

99.	The “Type B” access point shall propose a factory reset button.	C/PC/NC

100.	The “Type B” access point shall propose a console port.	C/PC/NC

8.3 Indoor access point – Type C

101.	The WLAN solution shall propose an 802.11ac wave2 MU-MIMO indoor tri-radio AP access point (2.4, 5G low, 5G high): “Type C”.	C/PC/NC

With the OmniAccess Stellar AP1230 series wave2 and tri-radio APs, the Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement.

Figure 52. OmniAccess Stellar AP1230 series

102.	The “Type C” access point shall have integrated omni-directional antennas or may be equipped with external antennas.	C/PC/NC

As depicted on previous figure, The Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement. Indeed, the Stellar AP1230 series includes the AP1230 access point with omni-directional antennas and the AP1231 access point with connectors to connect external antennas.

103.	The “Type C” access point shall offer native BLE radio support.	C/PC/NC

104.	The “Type C” access point shall support up to 24 SSIDs (8 per radio).	C/PC/NC

105.	The “Type C” access point shall offer up to 1733 Mb/s throughput on the 5 GHz band (low and high bands) and up to 800 Mb/s throughput on the 2.4 GHz band.	C/PC/NC

106.	The “Type C” access point shall support up to 768 clients.	C/PC/NC

107.	The “Type C” access point shall have one 1 GbE port and one 2.5 GbE (IEEE 802.3bz Multi-rate Gigabit Ethernet).	C/PC/NC

108.	The “Type C” access point shall propose deep packet inspection (DPI) capabilities providing real-time classification of flows at the application level.	C/PC/NC

The OmniAccess Stellar AP1230 series access points fully comply to this requirement. Please refer to requirement [55].

109.	The “Type C” access point shall support 802.3af/at PoE with 31W maximum consumption.	C/PC/NC

110.	The MTBF for the “Type C” access point shall be at least 525600h (60 years).	C/PC/NC

111.	The “Type C” access point shall propose a factory reset button.	C/PC/NC

112.	The “Type C” access point shall propose a console port.	C/PC/NC

8.4 Outdoor access point

113.	The WLAN solution shall propose an 802.11ac wave2 MU-MIMO outdoor ruggedized dual-radio AP access point.	C/PC/NC

With the OmniAccess Stellar AP1251 series wave2 and dual-radio AP, the Alcatel-Lucent Enterprise OmniAccess Stellar WLAN solution fully complies with this requirement.

Figure 53. OmniAccess Stellar AP1251 access point

114.	The outdoor ruggedized access point shall have integrated omni-directional antennas or may be equipped with external antennas.	C/PC/NC

115.	The outdoor ruggedized access point shall support up to 16 SSIDs (8 per radio).	C/PC/NC

116.	The outdoor ruggedized access point shall offer up to 1733 Mb/s throughput on the 5 GHz band and up to 400 Mb/s throughput on the 2.4 GHz band.	C/PC/NC

117.	The outdoor ruggedized access point shall support up to 512 clients.	C/PC/NC

118.	The outdoor ruggedized access point shall have two (2) 1Gb Ethernet port.	C/PC/NC

119.	The outdoor ruggedized access point shall propose *deep packet inspection* (DPI) capabilities providing real-time classification of flows at the application level.	C/PC/NC

The OmniAccess Stellar AP1251 access point fully complies with this requirement. Please refer to requirement [55].

120.	The outdoor ruggedized access point shall be IP66/67 certified.	C/PC/NC

121.	The outdoor ruggedized access point shall support persistent moisture and precipitation, and high and low temperatures: -40°C to 65°C.	C/PC/NC

122.	The outdoor ruggedized access point shall support 802.3af/at PoE with 40W maximum consumption.	C/PC/NC

123.	The MTBF for the outdoor ruggedized access point shall be at least 525600h (60 years).	C/PC/NC

124.	The outdoor ruggedized access point shall propose a factory reset button.	C/PC/NC

125.	The outdoor ruggedized access point shall propose a console port.	C/PC/NC