Alcatel·Lucent
Enterprise

Alcatel-Lucent OmniAccess Wireless Base Software

RELEASE 6.1

The Alcatel-Lucent OmniAccess™ Wireless Base Software is the Operating System (OS) and application engine for all OmniAccess WLAN Switch/Controllers and WLAN access devices. The OmniAccess Wireless Base Software architecture is designed for scalable performance and is built using three core components.

First, a hardened, multicore, multi-threaded supervisory kernel manages administration, authentication, logging and other system-operation functions. Second, an embedded, real-time OS powers dedicated packet-processing hardware, implementing all routing, switching and firewall functions. Third, a programmable encryption and decryption engine, built on dedicated hardware, delivers client-to-core encryption for wireless-user data traffic and software virtual private network (VPN) clients.

OmniAccess Wireless Base Software comes with an extensive set of capabilities. The Alcatel-Lucent OmniAccess WLAN Adaptive Radio Management (ARM) technology employs infrastructure-based controls to optimize Wi-Fi® client behavior and automatically ensures that OmniAccess WLAN access points (APs) remain clear of interference, resulting in a more reliable, high-performance WLAN infrastructure.

In addition to the OmniAccess WLAN ARM, the OmniAccess WLAN Virtual Intranet Access (VIA) agent enables secure IPSec-VPN connectivity to corporate resources for road-warriors and off-site users. Finally, to protect wired network resources from wireless threats, OmniAccess Wireless Base Software delivers the industry's leading integrated rogue-AP classification and containment solution.

Optional software modules are also available for added functionality and are enabled through license keys. Optional modules include the Alcatel-Lucent OmniAccess WLAN Policy Enforcement Firewall (PEF), Alcatel-Lucent OmniAccess Wireless RFProtect™ wireless-security and spectrum-analysis capabilities and xSec advanced Layer 2 encryption.

FEATURES	BENEFITS
802.1x authentication with Wi-Fi Protected Access (WPA), WPA2 and 802.11i	Delivers highly secure authentication, encryption and access control
Web-based captive portal for Secure Sockets Layer (SSL) browser-based authentication	Offers simple Web authentication for guest or visiting employees
EAP off-load with hardware-based	Offers simple Web authentication for guest or visiting employees
acceleration and local processing of	Centrally and securely manage multiple OmniAccess Instant networks using OV3600 Air Manager to operate hundreds of remote locations with real-time visibility into users, mobile device and WLANs
802.1x authentication	Provides high-performance Remote Access Dial-In User Server (RADIUS) authentication
Automatic detection, classification	Provides high-performance Remote Access Dial-In User Server (RADIUS) authentication
and containment of rogue APs	Protects against unauthorized APs connecting to the wireline infrastructure and opening the network to external users
Proxy mobile IP and proxy Dynamic Host Configuration Protocol (DHCP) with roaming cutover times of 2 ms to 3 ms between APs and WLAN switches	Offers ultra-fast handoffs between APs, allowing seamless mobility for users roaming between APs and the WLAN while using real-time delay-sensitive applications such as Voice over WLAN (VoWLAN)
OmniAccess WLAN ARM	Simplifies deployment and operation through self-configuration of all radio frequency (RF) parameters with dynamic-interference avoidance
OmniAccess WLAN VisualRF	Monitors and displays RF coverage and interference in real time
Redundant WLAN switch arrays using Virtual Router Redundancy Protocol (VRRP)	Delivers highly available WLAN infrastructure through WLAN switch redundancy and self-healing capability in case of AP failure
Automatic RF fault-tolerance VRRP	Avoids radio dead spots and provides AP backup
Cooperative control technology	Provides resilient, self-healing, always-on wireless mesh that automatically overcomes a block path or AP failure
Cooperative control technology	Provides resilient, self-healing, always-on wireless mesh that automatically overcomes a block path or AP failure

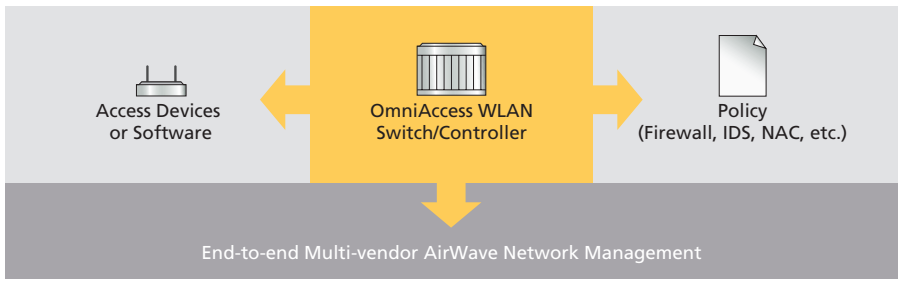
Enabling a unified access architecture

The Alcatel-Lucent OmniAccess WLAN Unified Access Architecture allows any user, regardless of physical location, to securely access the enterprise network with an always-on, consistent experience. Uniform security and access-control policies are applied to users in headquarters and branch or home offices, or on the road. Users and devices join the enterprise network through simple lightweight access devices or software, which securely and automatically connect to an OmniAccess WLAN Switch/Controller installed in the enterprise network core. The OmniAccess WLAN Switch/Controller, powered by OmniAccess Wireless Base Software, directly controls OmniAccess WLAN access devices and software, managing their software image, configuration, user-connection state and policy enforcement. The entire network is managed by the Alcatel-Lucent OmniVista™ 3600 Air Manager, providing IT staff with unmatched visibility and control of network users and infrastructure.

Flexible architecture adapts to unique enterprise requirements

With the OmniAccess WLAN, network design is not a one-size-fits-all approach. Some organizations need pervasive Wi-Fi, while some are purely wired. Branch offices have different requirements than corporate headquarters. And even within a corporate campus, some organizations value a centralized traffic-forwarding model where all network traffic flows to the data center, while other organizations need a more distributed approach. The unparalleled OmniAccess Wireless Base Software flexibility permits all these permutations and more, adapting the network to the requirements of the organization rather than dictating rigid design specifications (see Figure 1).

Figure 1. Alcatel-Lucent OmniAccess WLAN Switch/Controller in network configuration



FEATURE	DESCRIPTION
User-connectivity method	Enterprise-grade secure Wi-Fi
	Wired Ethernet
	VPN remote access
AP-connection method	Private or public IP cloud
	• Ethernet
	• Wireless WAN, including EV-DO and High-Speed Downlink Packet Access (HSDPA) Wi-Fi mesh (point-to-point or point-to-multipoint)
FlexForward™ traffic forwarding	Centralized: All user traffic flows to OmniAccess WLAN Switch/Controller
	Locally bridged: All user traffic bridged by access device to local LAN segment
	Policy-routed: User traffic selectively forwarded to OmniAccess WLAN Switch/Controller or bridged locally, depending on traffic type or policy
Wi-Fi encryption	Centralized: All user traffic encrypted between client device and OmniAccess WLAN Switch/Controller
	Distributed: User traffic encrypted between client device and AP
	Open: No encryption
Integration with existing networks	Layer 2 (L2) or L3 integration: OmniAccess WLAN Switch/Controllers can switch or route traffic on a per-VLAN basis
	Rapid Spanning Tree: Enables fast L2 convergence
	Open Shortest Path First (OSPF): Enables simple integration with existing routing topologies

Enterprise security framework

To secure the enterprise network, OmniAccess Wireless Base Software performs authentication, access control and encryption for users and devices. Network authentication delivers greater access security, but retrofitting authentication onto existing wired networks is often extremely complex and expensive. In the OmniAccess WLAN Unified Access Architecture, authentication is a standard component and can be implemented for both wired and wireless networks. For wired networks, 802.1X is the industry-standard authentication method. For wireless networks, 802.1X authentication is one component of the WPA2 and 802.11i protocols widely recognized as the latest methods for wireless security.

OmniAccess Wireless Base Software uniquely supports AAA FastConnect, allowing the encrypted portions of 802.1X authentication exchanges to be terminated on the controller where the OmniAccess WLAN hardware-encryption engine dramatically increases scalability and performance. Supporting PEAP- MSCHAPv2, PEAP-GTC and EAP-TLS, AAA FastConnect eliminates the requirement for external authentication servers to be 802.1X-capable and increases authentication-server scalability by permitting hundreds of authentication requests per second.

For clients without WPA, VPN or other security software, OmniAccess WLAN supports a web-based captive portal that provides secure browser-based authentication. Captive portal authentication is encrypted using SSL, supporting both registered users with a login and password, and guest users supplying only an e-mail address. Through the integrated Alcatel-Lucent OmniAccess WLAN GuestConnect system, front-desk reception staff can use a customized web-portal page to issue and track authentication credentials for visitors. OmniAccess GuestConnect can also be extended to any user in an enterprise directory system, allowing the guests' sponsors to directly request network-access credentials. Guest credentials can easily be printed or e-mailed.

For enhanced enterprise security, the optional OmniAccess Wireless Base Software PEF license may be added. Without the PEF license, a user or device may be mapped to a particular VLAN based on the port or wireless SSID where the user connects to the network. Once the user has been mapped to a particular VLAN, external firewall systems or routers provide basic access controls. PEF adds full identity-based security with integrated firewall controls, applied on a per-user basis. This allows the OmniAccess Wireless Base Software to create a security perimeter around each user or device, tightly controlling how that user may access enterprise network resources.

FEATURE	AVAILABILITY AND DESCRIPTION
Authentication types	IEEE 802.1X (EAP, LEAP, PEAP, EAP- TLS, EAP-TTLS, EAP-FAST, EAP-SIM, EAP-POTP, EAP-GTC, EAP-TLV, EAP- AKA, EAP-Experimental, EAP-MD5) RFC 2548 Microsoft vendor-specific RADIUS attributes
	RFC 2716 PPP EAP-TLS
	RFC 2865 RADIUS Authentication RFC 3579 RADIUS Support for EAP RFC 3580 IEEE 802.1X RADIUS Guidelines
	RFC 3748 Extensible Authentication Protocol
	MAC address authentication Web-based captive portal authentication
Authentication servers	Internal database
	Lightweight Directory Access Protocol (LDAP)/ SSL Secure LDAP RADIUS
	Terminal Access Concentrator Access Control Server Plus (TACACS+)
	Authentication Server Tested Interoperability: Microsoft Active Directory, Microsoft IAS RADIUS Server, Microsoft NPS RADIUS Server, Cisco ACS Server, Juniper/Funk Steel Belted RADIUS Server, RSA ACEserver, Infoblox, Interlink RADIUS Server and FreeRADIUS
Encryption protocols	CC Mode Protocol (CCMP)/Advanced Encryption Standard (AES)
	Wired Equivalent Privacy (WEP): 64 and 128 bit
	Temporal Key Integrity Protocol (TKIP)
	SSL and Transport Layer Security (TLS): RC4 128-bit and RSA 1024- and 2048-bit
	Layer 2 Tunneling Protocol (L2TP)/IPSec (RFC 3193) XAUTH/IPSec
	Point-to-Point Tunneling Protocol (PPTP): RFC 2637
Programmable encryption engine	Yes: permits future encryption standards to be supported through software updates
Web-based captive portal (SSL)	Yes
Integrated guest access management	Yes
Site-to-site VPN	Yes: IPSec tunnel establishment between OmniAccess WLAN Switch/Controllers and other IPSec-compliant devices. Authentication support for X.509 public key infrastructure (PKI), IKEv2, IKE pre-shared key (PSK,) Internet Key Exchange (IKE) aggressive mode.

Architecture for seamless mobility

Enterprise users increasingly require network access while moving from location to location, whether from a classroom to a library, a cubicle to a conference room, headquarters to a branch office or the office to home. Mobility should be a seamless experience for the user, whether it is Wi-Fi roaming without loss of voice sessions, or roaming from the office to home with no change in login procedures or access experience. When the access network is unified under the OmniAccess WLAN infrastructure, users experience consistent network services that just work.

For Wi-Fi networks, OmniAccess Wireless Base Software provides seamless connectivity as users move throughout the network. With a roaming handoff time of two milliseconds (ms) to three ms, delay-sensitive and persistent applications, such as voice and video, experience uninterrupted performance. OmniAccess Wireless Base Software integrates proxy mobile IP and proxy DHCP functions, letting users roam between subnets, ports, APs and controllers without special client software. And with VLAN pooling, user membership of VLANs is load balanced to maintain optimal network performance as large groups of users move about the network.

The OmniAccess WLAN Unified Access Architecture also extends the enterprise to remote locations over private WANs or using the public Internet, giving users the same access experience regardless of location. And to address users who are away from the enterprise network infrastructure, OmniAccess WLAN Switch/Controllers also operate as standard VPN concentrators, linking remote users into the same access and security framework as other enterprise users. Using the OmniAccess WLAN eliminates any need to build separate access networks for each work location; the OmniAccess WLAN Unified Access Architecture treats all locations the same.

FEATURE	DESCRIPTION
Fast roaming	Offers 2 ms to 3 ms intracontroller; 10 ms to 15 ms intercontroller
Roaming across subnets and VLANs	Provides sessions that do not drop as clients roam throughout network
Proxy mobile IP	Establishes home-agent or foreign-agent relationship between controllers automatically
Proxy DHCP	Prevents clients from changing IP address when roaming
VLAN pooling	Load balances clients across multiple available VLANs automatically

Enterprise-grade adaptive wireless lans

The OmniAccess WLAN ARM takes the guesswork out of AP deployments. Once APs begin functioning, they immediately begin monitoring their local environment for interference, noise and signals being received from other OmniAccess WLAN APs. This information is reported back to the controller, which then controls the optimal channel assignment and power levels for each AP in the network, even where 802.11n has been deployed with mixed HT20 and HT40 channel types.

Advanced OmniAccess WLAN ARM features dynamically adapt the infrastructure to ensure optimal network performance in today's challenging heterogeneous client environments. With 802.11n in widespread use, users expect high performance, even in crowded areas such as lecture halls. OmniAccess WLAN ARM ensures high performance and multimedia Quality of Service (QoS) through techniques, such as band steering to move dualband clients out of the crowded 2.4 GHz band, and Airtime Performance Protection to prevent slower clients from undermining the entire network's performance. Where dense user populations exist, the OmniAccess WLAN ARM Airtime Fairness provides equal RF access across multiple-client types and OSs. Finally, in areas with dense AP coverage, OmniAccess WLAN ARM ensures the optimal use of each through automatic channel load balancing and cochannel interference mitigation.

OmniAccess WLAN ARM can be used in conjunction with the optional OmniAccess Wireless RFProtect module spectrum analyzer. While OmniAccess WLAN ARM optimizes client behavior and ensures that APs stay clear of interference, the spectrum analyzer uses OmniAccess WLAN 802.11n APs to remotely identify and classify Wi-Fi and non-Wi-Fi interference sources.

Using OmniAccess WLAN 802.11n APs to scan the spectral composition of 2.4-GHz and 5-GHz radio bands, the OmniAccess Wireless RFProtect spectrum analyzer remotely identifies RF interference, classifies its source and provides real-time analysis at the point where the problem occurs.

Data collected by the OmniAccess Wireless RFProtect spectrum analyzer helps to quickly isolate packet-transmission problems, ensure over-the-air QoS and mitigate traffic congestion caused by RF contention with other devices operating in the same band or channel. Appropriate remediation measures can be deployed, to optimize network performance.
Once the network is deployed, the OmniAccess WLAN system provides a real-time, color heatmap display of the RF environment, showing signal strength, coverage and interference. Through tight integration with the Alcatel-Lucent OmniVista 3600 Air Manager VisualRF, WLAN coverage and capacity planning can be automated, avoiding frequent and expensive manual site surveys.

OmniAccess Wireless Base Software collects aggregate and raw wireless statistics on a per-station, per-channel and per-user basis. All statistics can be recorded and analyzed through the OmniVista 3600 Air Manager, and are also available by SNMP for easy integration into third-party management or analysis applications. Live packet capture is available that can turn any OmniAccess WLAN AP or Air Monitor into a packet-capture device able to stream real-time 802.11 frames back to monitoring stations such as Wireshark or WildPackets OmniPeek. With this detailed information, administrators can quickly troubleshoot user problems, identify most-frequent wireless users and diagnose congested APs.

To protect against unsanctioned wireless devices, the OmniAccess WLAN rogue AP classification algorithms allow the system to accurately differentiate between threatening rogue APs connected to the network and nearby interfering APs.

Once classified as rogue, these APs can be automatically disabled through the wireless and wired network. Administrators are also notified of the rogue device's presence and precise physical location on a floorplan, so it can be promptly removed from the network. Rogue-AP classification and containment is available within base OmniAccess Wireless Base Software and does not require additional OmniAccess WLAN Switch/Controller licensing.

FEATURE	AVAILABILITY AND DESCRIPTION
OmniAccess WLAN ARM	Automatically manages all RF parameters to achieve maximum performance
802.11n HT20 and HT40 support	Manages spectrum for all 802.11n networks
Client band steering	Keeps dual-band clients on optimal RF band
Self-healing around failed APs	Automatically adjusts power levels to compensate for failed APs
Airtime Fairness	Guarantees performance in high-density environments
RF-spectrum load balancing	Evenly distributes clients across all available channels
Airtime performance protection	Prevents low-speed clients from slowing down high-speed clients
Single-channel coordinated access	Ensures optimal performance even with nearby APs on the same channel
RF plan	Automatically predeploys modeling, planning and placement of APs and RF monitors based on capacity, coverage and security requirements
Coverage-hole and interference detection	Detects clients that cannot associate due to coverage gaps
Timer-based AP access control	Shuts off APs outside of defined operating hours
Remote wireless packet capture	Remotely captures raw 802.11 frames and streams to protocol analyzer
Plug-ins for third-party analysis tools	WireShark, OmniPeek and Air Magnet
Rogue AP detection and containment	Detects unauthorized APs and automatically shuts them down
RTLS tracking and monitoring	Yes
Location-tracking API for external integration	Yes

For comprehensive Wireless Intrusion Protection (WIP), the OmniAccess WLAN Switch/Controller RFProtect module protects against ad hoc networks, man-in-the-middle attacks, Denial-of-Service (DoS) attacks and many other threats while enabling wireless-intrusion signature detection.

TotalWatch™, an essential part of the OmniAccess Wireless RFProtect WIP capability, delivers the industry's most-effective WLAN threat mitigation. It provides visibility into all 802.11 Wi-Fi channels at 5-MHz increments, monitors the 4.9-GHz frequency band and automatically adapts wireless-security scanning intervals on APs based on data availability.

Tarpit containment is another vital OmniAccess Wireless RFProtect WIP feature where OmniAccess WLAN APs deliver fake BSSIDs or channels in response to probe requests from rogue devices. The rogue device then associates with that fake information and fails to push any traffic. User interaction is then required to reconnect the rogue device.

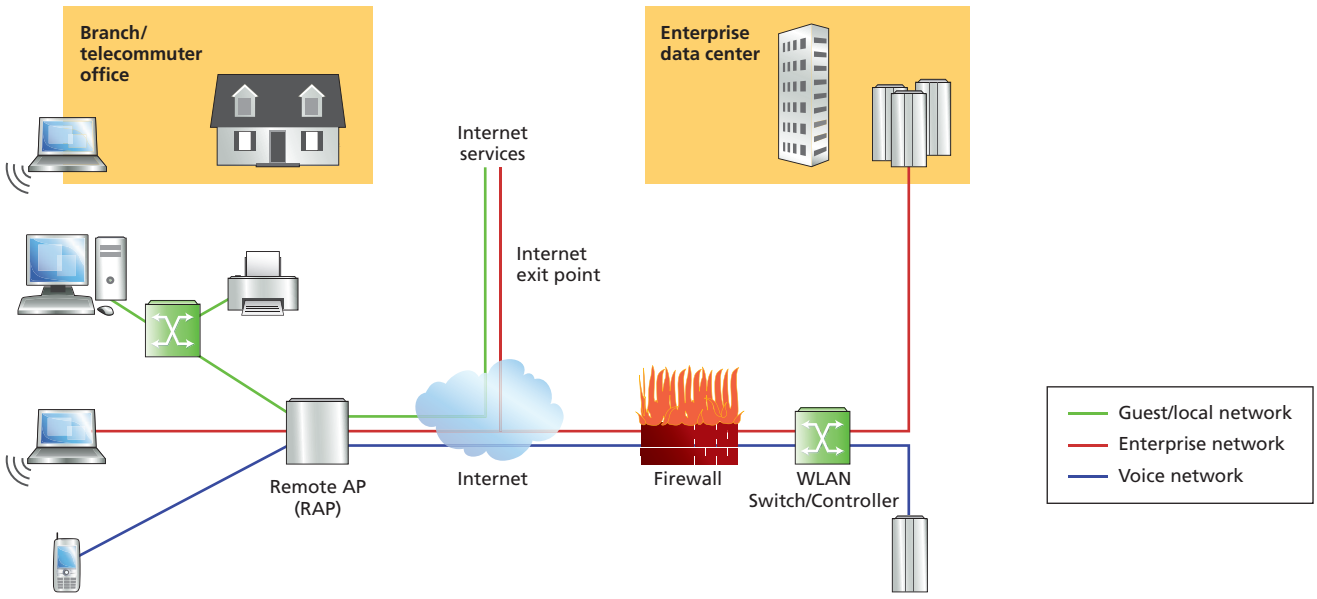
OmniAccess Wireless Base Software includes advanced location visualization and tracking of 802.11 devices. RF signature-based location triangulation allows administrators to accurately locate any 802.11 user or device within one meter. With the OmniAccess WLAN real-time locating system (RTLS) tracking capabilities, multiple devices can be continuously located and tracked simultaneously. The devices' locations can be displayed on building floorplans to network administrators through the Alcatel-Lucent OmniVista 3600 Management Platform, or linked to outside systems through a simple application programming interface (API).

Virtual branch networking for branch offices and teleworkers

The Alcatel-Lucent OmniAccess WLAN Virtual Branch Networking (VBN) solution provides a simple, secure and cost-effective way to extend the corporate network to branch offices, clinics, SOHOs, stores and telecommuters. Traditional remote networking solutions replicate routing, switching, firewall and other services at each remote location. Managing and controlling user access to network services, applications and resources requires proliferating ports, subnets and VLANs, effectively creating multiple networks at each site. This proliferation is costly and complex to deploy and maintain.

Whether supporting branch offices serving one or one-hundred users, the OmniAccess WLAN VBN solution delivers full-service networking without compromises. As the head-end component of the OmniAccess WLAN VBN solution, data-center-based OmniAccess WLAN Switch/Controllers handle all complex configuration, management, software-updates, authentication, intrusion-detection and remote-site-termination tasks. Branch-office network services are virtualized in the data-center controllers and then extended over any public or private IP network to affordable Remote Access Points (RAPs) that provide secure connectivity and services to end users (see Figure 2).

Figure 2. OmniAccess WLAN RAPs are ideally suited for providing secure mobile connectivity to branch and home offices



FEATURE	DESCRIPTION
Zero-touch provisioning	Administrators can deploy RAPs without any preconfiguration; simply ship it to end user (RAP-2, RAP-5 series only)
Wired and wireless	Users connect to RAPs by wired Ethernet, Wi-Fi or both
Flexible authentication	802.1X, Captive Portal, move, add and change (MAC) address authentication, per-port and per-user
Centralized management	No local configuration is performed on APs, all configuration and management done by OmniAccess WLAN Switch/Controller
Third-Generation (3G) wireless WAN (WWAN)	RAP-5 series support Universal Serial Bus(USB) wireless WAN adapters, such as EV-DO and HSDPA, for primary or backup Internet connection
FlexForward traffic forwarding	Centralized: All user traffic flows to OmniAccess WLAN Switch/Controller Locally bridged: All user traffic bridged by access device to local LAN segment Policy-routed: User traffic selectively forwarded to OmniAccess WLAN Switch/Controller or bridged locally, depending on traffic type and policy: Requires PEF license
Enterprise-grade security	RAPs authenticate to WLAN Switch/Controller using X.509 certificates, then establish secure IPSec tunnels
Uplink bandwidth reservation	Reserved bandwidth definition for loss-sensitive application protocols such as voice
Local diagnostics	In the event of a call to the help desk, local users can browse to a pre-defined URL to access full RAP diagnostics
Remote mesh portal	Each RAP may also act as a mesh portal, providing wireless links to downstream APs (except RAP-2WG)
Supported APs	RAP-2WG, RAP-5WN, RAP-5, AP-105, AP-120/121, AP-124/125, AP-60/61, AP-65, AP-70, AP-85
Minimum required link speed	64 kb/s per SSID
Encryption Protocol: RAP to OmniAccess WLAN Switch/Controller	AES-CBC-256: Inside IPSec External Security Password (ESP)

Integrating offsite workers into a single access architecture

Users who need access to enterprise resources while away from their office typically rely on VPN client software, which connects to a VPN concentrator located in an enterprise DMZ.

With OmniAccess WLAN, remote VPN users are treated just like any other user. They leverage the same access policies and service definitions used on a campus Wi-Fi network or a branch-office RAP deployment. Because any OmniAccess WLAN Switch/Controller can act as a VPN concentrator, a parallel access infrastructure need not be deployed or maintained.

OmniAccess Wireless Base Software is compatible with several popular VPN clients and the VPN clients built into major client OSs. In addition, OmniAccess Wireless Base Software also provides the optional OmniAccess WLAN VIA agent, which can be installed on Windows or Apple MacBook laptops and is ordered by the PEF-V license for the corresponding OmniAccess WLAN Switch/Controller. By merging access networks together, policy and access configuration is unified, the user experience is improved, help-desk calls are reduced and IT expenses are lowered.

FEATURE	DESCRIPTION
Tested client support	Alcatel-Lucent VIA agent on Windows Cisco, Nortel VPN clients OpenVPN, Apple/Windows native client
VPN protocols	L2TP/IPSec (RFC 3193) XAUTH/IPSec PPTP: RFC 2637
Authentication	Username and password, X.509 PKI, RSA SecurID, Smart Card, multi-factor

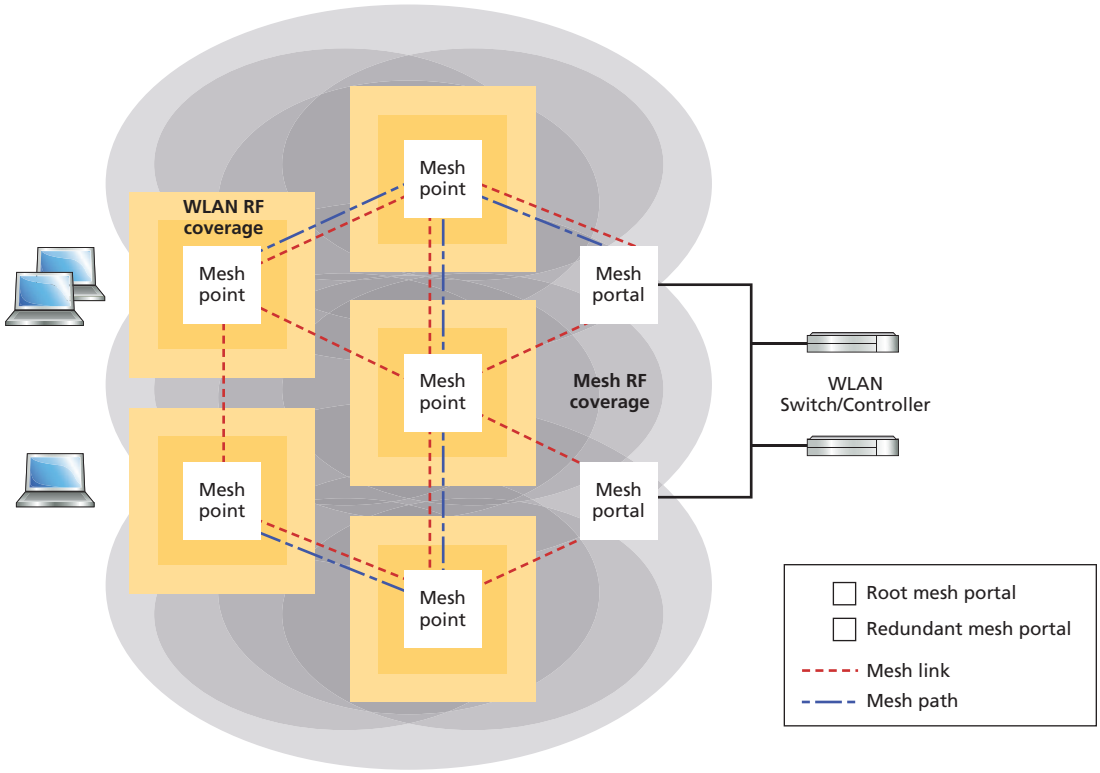
Secure enterprise mesh

The OmniAccess WLAN Secure Enterprise Mesh solution provides a flexible, wireless design, allowing APs to be placed wherever they are needed, indoors or outdoors. The absence of fiber or cable runs significantly reduces network-installation costs and requires fewer Ethernet ports. The solution fully integrates with the OmniAccess WLAN Unified Access Architecture, enabling a single, enterprise-wide network wherever users may roam. The OmniAccess WLAN Secure Enterprise Mesh is based on programmable software and does not require specialized hardware; virtually any OmniAccess WLAN indoor or ruggedized outdoor access can function as a mesh AP.

The OmniAccess Secure Enterprise Mesh can support all enterprise wireless needs, including Wi-Fi access, concurrent Wireless Intrusion Protection, wireless backhaul, LAN bridging and point-to-multipoint connectivity, all with a single common infrastructure, the OmniAccess WLAN Secure Enterprise Mesh. This is an excellent solution for connectivity applications, including interbuilding connectivity, outdoor campus mobility, wireless offices and wireline backup; security applications, such as video and audio monitoring, alarms and duress signals; and industrial applications and sensor networks.

Through cooperative control technology, the OmniAccess WLAN mesh uses an intelligent-link management algorithm to optimize traffic paths and links. Mesh APs communicate with their neighbors and broadcast a number of RF and link attributes, for example, link, path and node cost and loading, that allow these APs to intelligently select the best path for the application. Mesh paths and links automatically adjust for high loads or interference. Further, application tags for voice and video traffic are shared to ensure latency-sensitive traffic is prioritized over data. The cooperative-control technology also provides self-healing functionality for the mesh network in the event of a blocked path or AP failure (see Figure 3).

Figure 3. OmniAccess WLAN Secure Enterprise Mesh



FEATURE	DESCRIPTION
Broad application support	Wi-Fi access, concurrent WIP, wireless backhaul, LAN bridging and point-to-multipoint connectivity
OmniAccess WLAN Unified Access Architecture	Integrates mesh networks with campus WLAN and branch-office networks; users seamlessly roam between campus Wi-Fi and mesh networks
Cooperative control	Intelligent RF link management determines optimal performance path and allows the network to self-organize
Self-healing	Resilient self-healing mesh automatically overcomes a block path or AP failure
Mesh clustering	Scalability support by allowing a large mesh to be segmented into highly available clusters
Centralized encryption	End-to-end data encryption, from client to core, protecting the network even if a mesh AP is stolen
Centralized management	All mesh nodes are configured and controlled centrally by OmniAccess WLAN Switch/Controllers, no local management required
Extensive graphical support tools	Full network visualization includes coverage heatmaps, automatic link budget calculation, floorplans and maps with network topology
Standards-based design	OmniAccess WLAN Secure Enterprise Mesh is designed using principles from draft IEEE 802.11s and will be able to easily migrate to this standard once it is ratified

Network management and high-availability

OmniAccess WLAN Switch/Controller configuration, management and troubleshooting are provided through a browser-based GUI and a command line interface familiar to any network administrator. OmniAccess Wireless Base Software also integrates seamlessly with the Alcatel-Lucent OmniVista 3600 Wireless Management Suite (AWMS), which eases management during all stages of the WLAN life cycle, from planning and deploying to monitoring, analyzing and troubleshooting. The OmniVista 3600 AWMS provides long-term trending and analysis, help-desk integration tools and extensive customizable reporting.

All APs and controllers, even those distributed in branch or regional offices, can be centrally configured and managed from a single console.

To ease configuration of common tasks, intuitive task-based wizards guide the network administrator through every step of the process.

Controllers can be deployed in 1:1 and 1:n VRRP-based redundant configurations with redundant data-center support. When deployed in Layer-3 topologies, the OSPF routing protocol enables automatic route learning and route distribution for fast convergence.

FEATURE	AVAILABILITY AND DESCRIPTION
Web-based configuration	Management by any administrator with a standard web browser
Command line	Console, SSH
Syslog	Yes: Supports multiple servers, multiple levels, and multiple facilities
SNMP v2c	Yes
SNMP v3	Yes: Enhances standard SNMP with cryptographic security
Centralized configuration of controllers	Designated master controller can configure and manage several downstream local controllers
VRRP	High availability between multiple controllers support
Redundant data-center support	Yes: Access devices can be configured with IP addresses for backup controllers
OSPF	Yes: Stub-mode support for learning default route or injecting local routes into an upstream router
Rapid Spanning Tree Protocol	Yes: Provides fast L2 convergence

IPV6 support

With the depletion of available IPv4 addresses, organizations are now planning for, or have already begun deployments of, IPv6 within their networks. While IPv4 and IPv6 both define how data is transmitted over networks, IPv6 adds a much larger address space than IPv4 and can support billions of unique IP addresses.

As organizations transition from IPv4 to IPv6, network equipment must support dual-stack interoperability of IPv6 within an IPv4 network or full deployments within a pure IPv6 environment. OmniAccess Wireless Base Software supports deploying OmniAccess WLAN Switch/Controllers and APs in today's IPv6 and dual-stack environments.

Management over IPV6

- Secure Shell (SSH)
- Telnet
- Service Control Point (SCP)
- Web user interface (UI)
- FTP
- Trivial File Transfer Protocol (TFTP)
- Syslog

FEATURE	AVAILABILITY
Captive portal over IPv6	Yes
Support IPv6 VLAN interface address on OmniAccess WLAN Switch/Controller	Yes
Support AP-controller communication over IPv6	Yes
ICSA IPv6 certified firewall	Yes
USGv6 certified firewall	Yes

Context-aware controls for mission-critical networking

Support for 802.11e and Wi-Fi Multimedia (WMM) ensures wireless QoS for delay-sensitive applications with mapping between WMM tags and internal hardware queues. OmniAccess WLAN Switch/Controllers enable mapping of 802.1p and IP DiffServ tags to hardware queues for wired-side QoS and can be instructed to apply certain 802.1p and IP DiffServ tags to different applications on-demand.
With the addition of the OmniAccess WLAN PEF module, Voice-over-IP (VoIP) protocols, including Session Initiation Protocol (SIP), SVP, Alcatel-Lucent NOE, Vocera and SCCP, are followed within the OmniAccess WLAN Switch/Controller. The OmniAccess WLAN Application Fingerprinting technology enables OmniAccess WLAN Switch/Controllers to follow encrypted signaling protocols.

Once these streams are identified, OmniAccess WLANs can prioritize them for delivery on the wireless channel as well as trigger voice-related features such as OmniAccess WLAN ARM-scanning postponement for the duration of a call and roaming prioritization for clients engaged in an active call. These capabilities are critical for enabling the large-scale deployment of enterprise voice communications over Wi-Fi.

Additionally, OmniAccess Wireless Base Software now includes Device Fingerprinting technology, allowing network administrators to assign network policies on device types in addition to applications and users. OmniAccess WLAN Device Fingerprinting delivers greater control over which devices are allowed to access the network and how these devices can be used. OmniAccess Wireless Base Software can accurately identify and classify mobile devices such as the Apple iPad, iPhone or iPod, as well as devices running the Android or BlackBerry OSs. This information can be shared with the OmniVista 3600 Management Platform for enhanced network visibility for all users, regardless of location or mobile device.

FEATURE	AVAILABILITY OR DESCRIPTION
802.1p support	Yes
802.11e support	Yes
T-SPEC/TCLAS	Yes
WMM	Yes
WMM priority mapping	Yes
Unscheduled Automatic Power Save Delivery (U-APSD)	Yes
802.11k	Improves call quality and rapid handoff for voice and other quality-sensitive devices
Internet Group Management Protocol (IGMP) snooping for efficient multicast delivery	Yes
Application and OmniAccess WLAN Device Fingerprinting	Yes

CERTIFICATIONS
Wi-Fi Alliance Certified: 802.11a/b/g/n/d/h, WPA™ Personal, WPA™ Enterprise, WPA2™ Personal, WPA2™ Enterprise, WMM™, WMM Power Save
ICSA Firewall, Corporate v4.1 (with optional PEF module), ICSA IPv6 Firewall
FIPS 140-2 validated (when operated in FIPS mode)
Common criteria EAL-2
RSA certified
Polycom/Spectralink VIEW certified
USGv6 Firewall

Technical specifications

Standards supported

General switching and routing

- RFC 1812 Requirements for IP Version 4 Routers
- RFC 1519 CIDR
- RFC 1256 IPv4 ICMP Router Discovery (IRDP)
- RFC 1122 Host Requirements
- RFC 768 UDP
- RFC 791 IP
- RFC 792 ICMP
- RFC 793 TCP
- RFC 826 ARP
- RFC 894 IP over Ethernet
- RFC 1027 Proxy ARP
- RFC 2236 IGMPv2
- RFC 2328 OSPFv2
- RFC 2338 VRRP
- RFC 2460 Internet Protocol version 6 (IPv6)
- RFC 2516 Point-to-Point Protocol over Ethernet (PPPoE)
- RFC 3220 IP Mobility Support for IPv4 (partial support)
- RFC 4541 IGMP and MLD Snooping
- IEEE 802.1D-2004 – MAC Bridges
- IEEE 802.1Q – 1998 Virtual Bridged Local Area Networks
- IEEE 802.1w – Rapid Spanning Tree Protocol

QoS and policies

- IEEE 802.1D – 2004 (802.1p) Packet Priority
- IEEE 802.11e – Quality of Service Enhancements
- RFC 2474 Differentiated Services

Wireless

- IEEE 802.11a/b/g 5GHz, 2.4GHz
- IEEE 802.11d Additional Regulatory Domains
- IEEE 802.11e Quality of Service
- RFC 2863 The Interfaces Group MIB
- RFC 3418 Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
- RFC 959 File Transfer Protocol (FTP)
- RFC 2660 The Secure Hypertext Transfer Protocol (HTTPS)
- RFC 1901 1908 SNMP v2c SMIv2 and Revised MIB-II
- RFC 2570 2575 SNMPv3 user based security, encryption and authentication
- RFC 2576 Coexistence between SNMP Version 1, Version 2 and Version 3
- RFC 2233 Interface MIB
- RFC 2251 Lightweight Directory Access Protocol (v3)
- RFC 1492 An Access Control Protocol, TACACS+
- RFC 2865 Remote Access Dial In User Service (RADIUS)
- RFC 2866 RADIUS Accounting
- RFC 2869 RADIUS Extensions
- RFC 3576 Dynamic Authorization Extensions to Remote RADIUS
- RFC 3579 RADUIS Support For Extensible Authentication Protocol (EAP)
- RFC 3580 IEEE 802.1X Remote Authentication Dial In User Service (RADIUS)
- RFC 2548 Microsoft RADUIS Attributes
- RFC 1350 The TFTP Protocol (Revision 2)
- RFC 3164 BSD System Logging Protocol (Syslog)

Security/encryption

- IEEE 802.1X Port-Based Network Access Control
- RFC 1661 The Point-to-Point Protocol (PPP)
- RFC 2406 IP Encapsulating Security Payload (ESP)
- RFC 2661 Layer Two Tunneling Protocol "L2TP"
- RFC 3193 Securing L2TP using IPSec
- RFC 2451 The ESP CBC-Mode Cipher Algorithms
- RFC 2403 The Use of HMAC-MD5-96 within ESP and AH
- IEEE 802.11h Spectrum and TX Power Extensions for 5 GHz in Europe
- IEEE 802.11i MAC Security Enhancements
- IEEE 802.11k Radio Resource Management (partial support) IEEE 802.11n Draft 2.0 Enhancements for Higher Throughput IEEE 802.11v Wireless Network Management (partial support)

Management and traffic analysis

- RFC 2030 SNTP, Simple Network Time Protocol v4
- RFC 854 Telnet client and server
- RFC 783 TFTP Protocol (revision 2)
- RFC 951,1542 BootP
- RFC 2131 Dynamic Host Configuration Protocol
- RFC 1591 DNS (client operation)
- RFC 1155 Structure of Mgmt Information (SMIv1)
- RFC 1157 SNMPv1
- RFC 1212 Concise MIB definitions.
- RFC 1213 Management Information Base for Network Management of TCP/IP-based internets – MIB-II
- RFC 1215 Convention for defining traps for use with the SNMP
- RFC 1286 Bridge MIB
- RFC 3414 User-based Security Model (USM) for v.3 of the Simple Network Management
- RFC 1573 Evolution of Interface
- RFC 2011 SNMPv2 Management Information Base for the Internet Protocol using SMIv2
- RFC 2012 SNMPv2 Management Information
- RFC 2013 SNMPv2 Management Information
- RFC 2578 Structure of Management Information Version 2 (SMIv2)
- RFC 2579 Textual Conventions for SMIv2
- RFC 2401 Security Architecture for the Internet Protocol
- RFC 2404 The Use of HMAC-SHA-1-96 within ESP and AH
- RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 2409 The Internet Key Exchange (IKE)
- RFC 2405 ESP DES-CBC cipher algorithm with explicit IV
- RFC 2403 Use of HMAC-SHA1-96 with ESP and AH
- RFC 3602 The AES-CBC Cipher Algorithm and Its Use with IPSec
- RFC 4017 Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs
- RFC 3706 A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
- RFC 3748, 5247 Extensible Authentication Protocol (EAP)
- RFC 3079 Deriving Keys for use with Microsoft Point-to-Point Encryption (MPPE)
- RFC 4137 State Machines for Extensible Authentication Protocol (EAP) Peer and Authenticator
- RFC 2716 PPP EAP TLS Authentication Protocol
- RFC 2246 The TLS Protocol (SSL)
- RFC 2407 Internet IP Security Domain of Interpretation for ISAKMP
- RFC 3948 UDP encapsulation of IPSec packets
- RFC 4793 EAP-POTP
- Internet Draft draft-ietf-ipsec-nat-t-ike-00
- Internet Draft draft-ietf-ipsec-nat-t-ike-01
- Internet Draft draft-ietf-ipsec-nat-t-ike-02
- Internet Draft EAP-TTLS
- Internet Draft EAP-PEAPv0
- Internet Draft XAuth for ISAKMP
- RFC 2819 Remote Network Monitoring (RMON) MIB

EMG3105110401 (06)

Alcatel·Lucent
Enterprise