OmniAccess 6000

WIRELESS LAN SWITCH

The Alcatel-Lucent OmniAccess™ 6000 (OAW-6000) Wireless LAN Switch is a high performance, fully featured modular WLAN switch able to aggregate up to 2,048 campus connected access points (APs). The OAW-6000 provides a true user-centric network experience, delivering follow-me connectivity, identity-based access, and application continuity services.

The OAW-6000 offers a scalable design that supports large deployments and can be easily implemented as an overlay without any disruption to the existing wired network.

Advanced voice-over-WLAN features such as Call Admission Control (CAC), voice-aware RF management and strict over-the-air quality of service (QoS) allow the OAW-6000 to deliver mobile VoIP capabilities. The OAW-6000 is managed via the integrated management capability of the Alcatel-Lucent OmniAccess Wireless Operating System or the Alcatel-Lucent OmniVista™ Mobility Manager.

FEATURES	BENEFITS
• High performance	• Platforms support multiple supervisor engines designed to handle heavy traffic loads generated by IEEE 802.11n access points
• Scalable architecture	• Can control up to 2,048 campus connected access points while offering a pay as you grow model. The OAW-6000 access point capacity can grow by adding supervisor modules and/or adding SW licenses.
• Centralized WLAN switching	• Allows for overlay deployments without disruption to the existing wireline infrastructure. Simplifies management task by minimizing the number of network elements
• Dynamic RF management	• Provides analysis of the RF environment to facilitate deployment with self tuning access points and to facilitates operation of the network with virtual real time site survey
• Integrated wireless intrusion prevention	• Integrates both wireless networking and wireless intrusion detection and prevention thus reducing the cost of wireless infrastructure and cost of operating the wireless network.

FEATURES	BENEFITS
• User-centric security with stateful Firewall	• Prevents unauthenticated users from accessing the corporate wireless network while safely supporting guest users, contractors as well as corporate users. Decreases management burden of security through role-based security.
• Real time location tracking	• Allows for the real time location tracking of wireless users to enrich presence information. Also supports location tracking of wireless asset tags throughout the enterprise.
• Quality of service, extended battery capabilities, application layer gateway (ALG) for voice protocols	• Improves voice quality through support of QoS mechanisms such as WMM, DSCP marking and prioritization, and connection admission control. Also improves voice end user experience by maximizing battery life with protocols such as U-APSD. Provides un-matched voice security through embedded stateful firewall.

The OAW-6000 offers a best in class, user-centric security framework to authenticate wireless users, enforce role-based access control policies and quarantine unsafe endpoints from accessing the corporate wireless network. Guest users can be easily and safely supported with the built-in captive portal server and advanced network services.

The OAW-6000 can create a secure networking environment without requiring additional VPN/firewall devices using integrated site-to-site VPN and NAT capabilities, split-tunneling and an ICSA-certified stateful firewall. Site-to-site VPN support can be integrated with all leading VPN concentrators to provide seamless integration into existing corporate VPNs.

TECHNICAL SPECIFICATIONS

Performance and capacity

- Campus-connected APs: Up to 2,048
- Remote APs: Up to 8,192
- Users: Up to 32,768
- MAC addresses: Up to 256,000
- VLAN IP interfaces: 512
- Fast Ethernet ports (10/100): Up to 72
- Gigabit Ethernet ports (GBIC or SFP): Up to 40
- 10 Gigabit Ethernet ports (XFP): Up to 8
- Active firewall sessions: Up to 2,097,200
- Concurrent IPSec tunnels: Up to 32,768
- Firewall throughput: Up to 80 Gbps
- Encrypted throughput (3DES): Up to 32 Gbps
- Encrypted throughput (AES-CCM): Up to 16 Gbps

Wireless LAN security and control features

- 802.11i security (WFA-certified WPA2 and WPA)
- 802.1X user and machine authentication
- EAP-PEAP, EAP-TLS, EAP-TTLS support
- Centralized AES-CCM, TKIP and WEP encryption
- 802.11i PMK caching for fast roaming applications
- EAP offload for AAA server scalability and survivability
- Stateful 802.1X authentication for standalone APs
- MAC address, SSID and location-based authentication
- Multi-SSID support for operation of multiple WLANs
- SSID-based RADIUS server selection
- Secure AP control and management over IPSec or GRE
- CAPWAP-compatible and upgradeable
- Distributed WLAN mode for remote AP deployments
- Simultaneous centralized and distributed WLAN support

Identity-based security features

- Captive portal, 802.1X and MAC address authentication
- Username, IP address, MAC address and encryption key binding for strong network identity creation
- Per-packet identity verification to prevent impersonation
- RADIUS and LDAP-based AAA server support
- Internal user database for AAA server failover protection
- Role-based authorization for eliminating excess privilege
- Robust policy enforcement with stateful packet inspection
- Per-user session accounting for usage auditing
- Web-based guest enrollment
- Configurable acceptable use policies for guest access
- XML-based API for external captive portal integration
- xSec option for wired LAN authentication and encryption(802.1X authentication, 256-bit AES-CBC encryption)

Convergence features

- Voice and data on a single SSID for converged devices
- Flow-based QoS using voice flow classification (VFC)
- Alcatel-Lucent NOE, SIP, Spectralink SVP, SCCP and Vocera ALGs
- Strict priority queuing for over-the-air QoS
- 802.11e support – WMM, U-APSD and T-SPEC
- QoS policing for preventing network abuse via 802.11e
- DiffServ marking and 802.1p support for network QoS
- On-hook and off-hook VoIP client detection
- VoIP call admission control (CAC) using VFC
- Call reservation thresholds for mobile VoIP calls
- Voice-aware RF management for ensuring voice quality
- Fast roaming support for ensuring mobile voice quality
- SIP early media and ringing tone generation (RFC 3960)
- Per-user and per-role rate limits (bandwidth contracts)

Adaptive radio management (ARM) features

- Automatic channel and power settings for thin APs
- Simultaneous air monitoring and end user services
- Self-healing coverage based on dynamic RF conditions
- Dense deployment options for capacity optimization
- AP load balancing based on number of users
- AP load balancing based on bandwidth utilization
- Coverage hole and RF interference detection
- 802.11h support for radar detection and avoidance
- Automated location detection for active RFID tags
- Built-in XML-based Location API for RFID applications

Wireless intrusion protection features

- Integration with WLAN infrastructure
- Simultaneous or dedicated air monitoring capabilities
- Rogue AP detection and built-in location visualization
- Automatic rogue, interfering and valid AP classification
- Over-the-air and over-the-wire rogue AP containment
- Adhoc WLAN network detection and containment
- Windows client bridging and wireless bridge detection
- Denial of service attack protection for APs and stations
- Misconfigured standalone AP detection and containment
- Third party AP performance monitoring and troubleshooting
- Flexible attack signature creation for new WLAN attacks
- EAP handshake and sequence number analysis
- Valid AP impersonation detection
- Frame floods, Fake AP and Airjack attack detection
- ASLEAP, death broadcast, null probe response detection
- Netstumbler-based network probe detection

Stateful firewall features

- Stateful packet inspection tied to user identity or ports
- Location and time-of-day aware policy definition
- 802.11 station awareness for WLAN firewalling
- Over-the-air policy enforcement and station blacklisting
- Session mirroring and per-packet logs for forensic analysis
- Detailed firewall traffic logs for usage auditing
- Application Layer Gateway (ALG) support for NOE, SIP, SCCP, RTSP, Vocera, FTP, TFTP, PPTP
- Source and destination Network Address Translation (NAT)
- Dedicated flow processing hardware for high performance
- TCP, ICMP denial of service attack detection and protection
- Policy-based forwarding into GRE tunnels for guest traffic
- External service interface for third-party security integration for inline anti-virus, anti-spam and content filtering apps
- Heath checking and load balancing for external services

VPN server features

- Site-to-site VPN support for branch office deployments
- Site-to-site interoperability with third-party VPN servers
- VPN server emulation for easy integration into WLAN
- L2TP/IPSec VPN termination for Windows VPN clients
- XAUTH/IPSec VPN termination for third-party clients
- PPTP VPN termination for legacy VPN integration
- RADIUS and LDAP server support for VPN authentication
- PAP, CHAP, MS-CHAP and MS-CHAPv2 authentication
- Hardware encryption for DES, 3DES, AES, MPPE
- Secure point-to-point xSec tunnels for L2 VPNs

Networking features and advanced services

- L2 and L3 switching over-the-air and over-the-wire
- VLAN pooling for easy, scalable network designs
- VLAN mobility for seamless L2 roaming
- Proxy mobile IP and proxy DHCP for L3 roaming
- Built-in DHCP server and DHCP relay
- VRRP-based N+1 WLAN switch redundancy (L2)
- AP provisioning-based N+1 WLAN switch redundancy (L3)
- Etherchannel support for link redundancy
- 802.1d Spanning Tree Protocol (STP)
- 802.1Q VLAN tags

WLAN switch-based management features

- RF Planning and AP Deployment Toolkit
- Centralized AP provisioning and image management
- Live coverage visualization with RF heat maps
- Detailed statistics visualization for monitoring
- Remote packet capture for RF troubleshooting
- Interoperable with Ethereal and Airopeek analyzers
- Multi-WLAN switch configuration management
- Location visualization and device tracking
- System-wide event collection and reporting

Administration features

- Web-based user interface access over HTTP and HTTPS
- Quickstart screens for easy WLAN switch configuration
- CLI access using SSH, Telnet and console port
- Role-based access control for restricted admin access
- Authenticated access via RADIUS, LDAP or Internal DB
- SNMPv3 and SNMPv2 support for WLAN switch monitoring
- Standard MIBs and private enterprise MIBs
- Detailed message logs with syslog event notification

Power supply options

- Power consumption: Max. 466 Watts per PSU

OAW-6000-PS200: AC power supplies deliver 200 W of power

- AC input voltage 90-132 VAC, 170-264 VAC
- AC input frequency 47-63 Hz
- AC input current 5 A @ 110 VAC

OAW-6000-PS400: AC power supplies deliver 400W of power

- AC input voltage 85-264 VAC, Auto-sensing
- AC input frequency 47-63 Hz
- AC input current 5 A @ 110 VAC

Operating specifications and dimensions

- Operating temperature range: 0° to 40° C
- Storage temperature range: 10° to 70° C
- Humidity, non-condensing: 5 to 95%
- Height: 5.75″ (146 mm)
- Width: 17.4″ (444 mm)
- Depth: 12.5″ (317.5 mm)
- Weight: 30 lbs. (unboxed)

TECHNICAL SPECIFICATIONS

Regulatory and safety compliance

- FCC part 15 Class A CE
- Industry Canada Class A
- VCCI Class A (Japan)
- EN 55022 Class A (CISPR 22 Class A), EN 61000-3
- EN 61000-4-2, EN 61000-4-3, EN 61000-4-4
- EN 61000-4-5, EN 61000-4- 6, EN 61000-4-8
- EN 61000-4-11, EN 55024, AS/NZS 3548
- UL 60950, EN60950
- CAN/CSA 22.2 #60950
- CE mark, cTUVus, GS, CB, C-tick, Anatel, NOM, MIC, IQC

ORDERING INFORMATION

PART NUMBER	DESCRIPTION
OAW-6000-PS2	Alcatel-Lucent OmniAccess 6000 chassis for non PoE configurations. Includes one modular 4-Slot 19" chassis, one fan tray, two 200 watt auto-sensing 110V/240V AC PSU, and one accessory kit.
OAW-6000-PS4	Alcatel-Lucent OmniAccess 6000 chassis for PoE configurations. Includes one modular 4-slot 19" chassis, one fan tray, two 400 watt auto-sensing 110V/240V AC PSU, and one accessory kit.
OAW-SC-1-48	OmniAccess Supervisor Card I with adaptive RF management and support for up to 48 access points. One OAW-6000 chassis can accommodate one or two Supervisor Cards.
OAW-SC-1-128	OmniAccess Supervisor Card I with adaptive RF management and support for up to 128 access points. One OAW-6000 chassis can accommodate one or two Supervisor Cards.
OAW-SC-2-256	OmniAccess Supervisor Card II with adaptive RF management and support for up to 256 access points. One OAW-6000 chassis can accommodate one or two Supervisor Cards.
OAW-S3-C-2X10G	OmniAccess Supervisor Card III, 10x 1000BaseX (SFP), 2x 10GBaseX (XFP), bundled with license to support 128 AP. One OAW-6000 chassis can accommodate up to four (4) Supervisor Card III.
OAW-S3-0-2X10G	OmniAccess Supervisor Card III, 10x 1000BaseX (SFP), 2x 10GBaseX (XFP), (no AP license included). One OAW-6000 chassis can accommodate up to four (4) Supervisor Card III.
OAW-LC-2G	OmniAccess 2GE Line Card with support for two GBIC uplinks. GBIC adapters shall be ordered separately.
OAW-LC-2G24F	OmniAccess 2GE24F Line Card with support for 24 auto-sensing 10/100 interfaces and two GBIC uplinks. GBIC adapters shall be ordered separately.
OAW-LC-2G24FP	OmniAccess 2GE24FP Line Card with support for 24 auto-sensing 10/100 interfaces with power-over-Ethernet (PoE) and two GBIC uplinks. GBIC adapters shall be ordered separately. Requires an OAW-6000-PS4 chassis.
OAW-GBIC-T	OmniAccess GBIC Interface Adapter - T
OAW-GBIC-SX	OmniAccess GBIC Interface Adapter - SX
OAW-GBIC-LX	OmniAccess GBIC Interface Adapter - LX
OAW-XFP-SR	OmniAccess Wireless XFP - 850nm serial pluggable XFP optic (LC), target range 300m over MMF
OAW-XFP-LR	OmniAccess Wireless XFP - 1310nm serial pluggable XFP optic (LC) for up to 10km over SMF
OAW-SFP-TX	OmniAccess Wireless SFP - 1000BaseT, RJ45
OAW-SFP-SX	OmniAccess Wireless SFP - 1000BaseSX, LC Connector
OAW-SFP-LX	OmniAccess Wireless SFP - 1000BaseLX, LC connector

To learn more, contact your dedicated Alcatel-Lucent representative, authorized reseller, or sales agent. You can also visit our Web site at www.alcatel-lucent.com.

www.alcatel-lucent.com

Alcatel·Lucent