Alcatel OmniAccess 4308

The Alcatel OmniAccess 4308 (OAW-4308) signifies a new approach to building, securing, and managing 802.11 networks for enterprises implementing business-critical applications over wireless. For branch office deployments, the OAW-4308 cost effectively delivers high-performance wireless LANs with dynamic radio frequency (RF) management and advanced services such as application-aware security, wireless intrusion protection, seamless user mobility, location tracking, and bandwidth management.

The Alcatel OAW-4308 is a stackable, 1U high, fixed-configuration device that seamlessly integrates into any layer-2/layer-3 wired network without requiring the reconfiguration of the network – logically or physically. The Alcatel OAW-4308 provides eight 10/100 Mbps power over Ethernet (802.3af) ports for connecting to access points, layer-2 switches, servers, or computers. In addition, one Gigabit Ethernet uplink (1000BaseT or 1000BaseSX) allows the OAW-4308 to be connected to the wired network. The Alcatel OAW-4308 supports up to 16 access points (APs), 1 Gbps of full-duplex (clear text) traffic, and 200 Mbps of encrypted throughput.

Features and Benefits

Policy-based network access control - A core feature of the Alcatel OmniAccess 4308 is the ability to separate users into individual roles, and then apply differentiated access and authorization controls to those roles based on policy. In the past, IT managers wrote business policies, requested that users comply, and then reprimanded users who violated the policies. With Alcatel's OmniAccess policy-based access control, business policies are translated into network controls, and violators are detected and then blocked before they ever happen.

Access control decisions are based on configurable policy criteria including user identity, device identity, device integrity, application used, physical location of user, time of day, authentication method, and SSID.

PRELIMINARY INFORMATION

ALCATEL

Universal authentication - Knowing who or what devices are using the network is a cornerstone of every security system. Authentication provides a means to acquire this knowledge. The Alcatel OmniAccess 4308 supports a wide variety of authentication methods ensuring compatibility with the multitude of end-user devices that are common in enterprise networks. With one security system, devices as disparate as industrial sensors, barcode scanners, IP phones, PDAs, and laptop computers are all provided appropriate levels of access.

Multiple industry-standard authentication methods are supported, including 802.1x, Web-based captive portal, RSA SecureID, PPP/L2TP for VPN access, IPSec/XAUTH for VPN access, RADIUS snooping for 802.1x-proxy authentication, and MAC address authentication. Standard authentication databases are supported, including RADIUS, and LDAP. An internal database can also be used.

Adaptive radio management – The Alcatel OmniAccess 4308 allows the network manager to deploy a wireless network as effortlessly as a wired network. The RF spectrum is constantly changing as people, furniture, and equipment are moved around, making automatic control and management of the RF space a critical requirement. Adaptive radio management removes the headaches from old-fashioned manual control of these devices, allowing the administrator to specify performance standards that the radio network will constantly seek to achieve.

The Alcatel OmniAccess 4308 used in conjunction with Alcatel OmniAccess APs includes the following industry-leading radio management capabilities:

- Automatic channel selection

- Automatic power selection

- 3-dimensional access point (AP) location planning tool

- Interference detection and avoidance

- Coverage hole detection

- Configurable performance thresholds

- Self-healing around failed radios

- Radio load balancing

- Wireless RMON statistics

Rogue access point detection – The Alcatel OmniAccess wireless system constantly scans all channels of the RF spec-trum, capturing native 802.11 traffic and learning about all wireless APs. A patent-pending classification algorithms, determines if the detected APs are legitimate APs, rogue APs or interfering APs. An interfering AP is one that has not been authenticated to the corporate network, but is not deemed to be a potential security breach. Rogue APs are those that are deemed hazardous to the network. If rogue APs are detected, the Alcatel OmniAccess wireless system will automatically detect and disable the devices by preventing users from associating with them. Administrators are also notified of the location of rogue APs so that they may be physically removed.

Wireless intrusion protection – The Alcatel OmniAccess wireless intrusion detection capabilities eliminate the need for a separate system of RF sensors and RF security by providing extraordinary capabilities to the Alcatel OmniAccess wireless switching system that gives administrators visibility and the power to thwart malicious wireless attacks. These attacks include wireless probing/discovery, denial of service (DoS), impersonations, man-in-the-middle, and unauthorized intrusions. As new attacks emerge, the system is flexible enough to incorporate new attack signatures while in service.

In addition to attack protection, the Alcatel OmniAccess wireless system enforces wireless security policies, which includes the ability to detect and prevent weak WEP initialization vectors (IVs), AP misconfiguration, ad-hoc networks, unauthorized NIC types, and wireless bridges.

Data encryption – The Alcatel OmniAccess WLAN system is designed to work in environments where the physical media cannot be protected against eavesdropping - such as wireless networks or the Internet. The Alcatel OmniAccess 4308 enables a large number of tested and proven encryption protocols to prevent intruders from eavesdropping on sensitive data. These protocols include AES-CCMP (WPA2), AES-CBC (up to 256 bits), DES, Triple-DES, WEP (64 or 128 bit), TKIP (WPA1), MPPE (PPTP), and SSL (up to 128 bit).

Network security – The Alcatel OmniAccess WLAN system was built from the ground up with security in mind, and includes a full ICSA-certified stateful firewall that can process traffic based on user identity as well as other parameters, rather than just simple source/destination addresses.

A number of security features allow the Alcatel OmniAccess 4308 to be installed in the most security-conscious environments, including ICSA-certified internal firewall, system log integrity, hardened OS resistant to known attacks and exploits, control-path encryption of communication between Alcatel OmniAccess WLAN platforms, and access control lists (ACLs).

Availability – The Alcatel OmniAccess WLAN system enables support for business critical applications that cannot tolerate downtime. The Alcatel OmniAccess WLAN system provides a number of features that support high-availability including VRRP-based hot standby, modular software design with protected memory, automatic AP failover.

Seamless user mobility – Mobility is a key requirement in modern enterprise networks, and is more important each day as voice over WLAN (VoWLAN) demands emerge and laptop computers continue to replace stationary desktop computers. Alcatel's mobility services enable users to move freely without the need to restart sessions or re-authenticate each time.

The Alcatel OmniAccess 4308 enables and enhances user mobility through features such as, wireless fast roaming, transparent inter-subnet (L3) roaming, proxy mobile-IP support for roaming between multiple WLAN switches, and proxy DHCP.

Centralized management – Manageability and configuration are top concerns when introducing any type of device to an enterprise data network. The Alcatel OmniAccess WLAN system offers clustering capabilities that allow an OmniAccess WLAN switch to configure and manage up to 32 other WLAN switches. When a policy change is made to the master device, this change is automatically pushed to other devices in the cluster. The intuitive Web-based interface provides logical organization of features, while the industry-standard command line interface allows experienced network managers to be up and running quickly.

The Alcatel OmniAccess WLAN switches are also integrated within Alcatel's OmniVista Enterprise network management application. OmniVista discovery and topology modules enable a network administrator to view both wired and wireless network elements and topologies from a single screen. In addition, OmniVista provides the network administrator with the ability to seamlessly initiate a Web-based management session to a specific OmniAccess WLAN switch.

Seamless wired-wireless integration – The Alcatel OmniAccess WLAN platforms must be able to integrate into wired networks without requiring reconfiguration of existing network components. The Alcatel OmniAccess 4308 (OAW-4308) is built with a number of features typically found in enterprise LAN switches. These features give the OAW-4308 the flexibility to operate in several different modes for maximum ease of integration. These features include 802.1D spanning tree, 802.1Q VLAN tagging, 802.1p prioritization, IP DiffServ/TOS, IP tunnels using GRE or IPSec, DHCP server, and UDP forwarding (DHCP helper).

Endpoint integrity – The Alcatel OmniAccess 4308 provides the ability to limit network access based on client integrity, such as the state of the anti-virus software on the device or operating system patches. It also provides facilities for client remediation, allowing out-of-spec client devices to repair themselves. For endpoint security, industry-leading solutions from Sygate Technologies, Inc. are use. They include Sygate on Demand and Sygate Secure Enterprise.
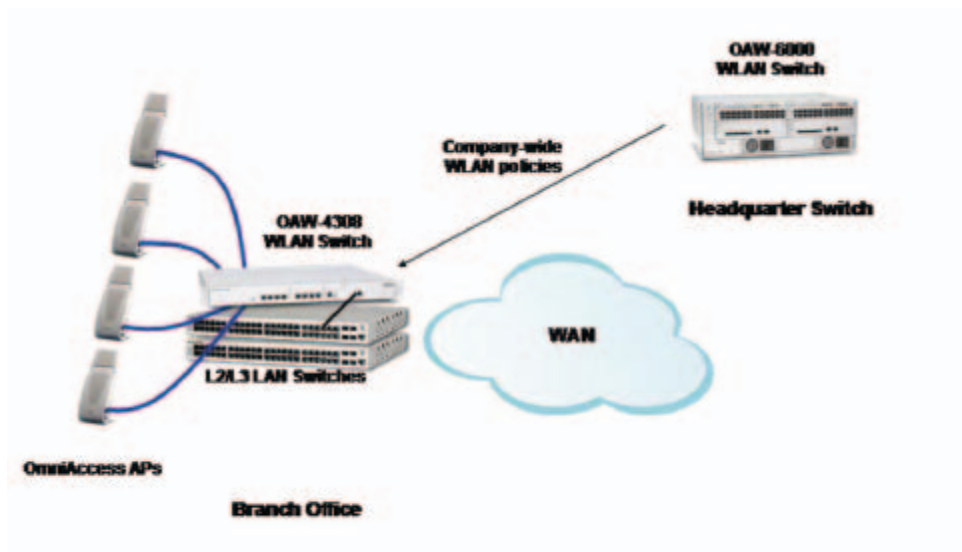
Alcatel OmniAccess 4308 deployed as a WLAN appliance in a branch office

The OAW-4308 is a cost effective WLAN switch for branch office deployment. It offers a fully featured WLAN system that can operate independently or receive company-wide WLAN policies from a central WLAN switch.

Technical Specifications

Capacity and performance

- 8 10/100 ports with PoE (802.3af) and SoE capability
- 1 Gigabit uplink ports (1000BaseT or 1000BaseSX)
- Up to 256 users per switch
- Up to 16 APs per switch
- 1Gbps of switch throughput
- 200 Mbps of encrypted traffic (3DES) throughput
- Dedicated crypto processor
- 100W total PoE power
- RS-232 serial console (RJ-45 connector)

Physical specifications

- Height: 1.72 in. (4.4 cm) – 1U
- Width: 17.4 in. (44.2 cm)
- Depth: 13.1 in. (33.3 cm)
- Weight: 10 lbs (4.5 Kg)

Fault tolerance

- VRRP for switch failover
- Automatic AP re-homing
- Multiple uplinks with redundancy (1000BaseX and 10/100 mix)

802.11 Transport, authentication, and encryption

- 802.11a
- 802.11b
- 802.11g
- 802.1x
- WEP, dynamic WEP, TKIP (WPA-1), 3DES, AES-CCMP encryption
- PEAP, TLS, TTLS, LEAP
- MAC address authentication
- Upgradeable to new encryption mechanisms

RF management and control

- Up to 16 ESSIDs per AP
- 3-Dimensional RF site survey
- Distributed and centralized automatic AP calibration
- Self-healing around failed APs
- Load balancing — number of users
- Load balancing — usage-based
- Coverage hole and interference detection
- Wireless RMON/packet capture
- Plug-ins for Ethereal and Airopeek
- Timer-based AP access control

Mobility

- 2–3 msec intra-switch roaming
- 10–15 msec inter-switch roaming
- Intersubnet roaming
- Mobile IP support
- Proxy mobile IP
- Proxy DHCP

VPN and firewall

- 256 concurrent IPSec tunnels
- 16,000 stateful firewall policies (per-user and per-port)
- IPSec, PPTP, XAUTH VPN termination
- VPN dialer
- Customizable Captive Portal
- Network address translation
- Standard and Extended ACLs

Subscriber management

- Per-user or per-role assignments of firewall policies, bandwidth contracts, session prioritization, VLAN assignment
- Role derivation based on authentication, ESSID, encryption, or OUI
- Location based access control

Quality of service

- Per-user and per-role bandwidth contracts
- Application-aware traffic classification and prioritization
- 802.1p support
- TOS support
- DiffServ Control Protocol support (DSCP tagging)

Authentication servers

- Local RADIUS
- External AAA Servers: Microsoft Active Directory, Microsoft IAS Radius Server, Cisco ACS Radius Server, Funk Steel Belted Radius Server, RSA ACEserver, Infoblox, Interlink Radius Server
- LDAP

Environment

- Operating temperature: 32 to 104°F (0 to 40°C)
- Storage temperature: 32 to 122°F (0 to 50°C)
- Humidity: 5% to 95% (non-condensing)

EMC

- FCC Part 15 Class A
- ICES-003 Class A
- VCCI
- 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 Class A

Safety

- UL60950
- CAN/CSA C22.2 No 60950
- IEC/EN60950
- Low Voltage Directive (LVD) 73/23/EEC
- 21 CFR Chapter 1, Subchapter J, Part 1040.10 (Laser Safety)
- IEC/EN 60825-1, EN 60825-2 (Laser Safety)

Ordering Information

Part Number	Description
OAW-4308T	OmniAccess 4308T with adaptive RF management. Provides 8 auto-sensing 10/100 interfaces with Power over Ethernet (PoE) and one 1000BaseT uplink. Supports up to 16 OmniAccess APxx Access Points. Operates directly connected to the Access Points or remotely connected through a Layer 2 or Layer 3 network. Supports auto-sensing 110V/240V AC and includes one accessory kit (installation guide, 19" equipment rack mount hardware, console cable with adapter and full product documentation CD).
OAW-4308SX	OmniAccess 4308SX with adaptive RF management. Provides 8 auto-sensing 10/100 interfaces with Power over Ethernet (PoE) and one 1000BaseSX uplink. Supports up to 16 OmniAccess APxx Access Points. Operates directly connected to the Access Points or remotely connected through a Layer 2 or Layer 3 network. Supports auto-sensing 110V/240V AC and includes one accessory kit (installation guide, 19" equipment rack mount hardware, console cable with adapter and full product documentation CD).
OAW-4308-PEF	Policy Enforcement Firewall Module for the OAW-4308 (single switch license)
OAW-4308-VPN	VPN Server Module for the OAW-4308 (single switch license)
OAW-4308-WIP	Wireless Intrusion Protection Module for the OAW-4308 (single switch license)
OAW-4308-AAA	Advanced AAA Module for the OAW-4308 (single switch license)
OAW-4308-ESI	External Services Interface Module for the OAW-4308 (single switch license)
OAW-4308-CIM	Client Integrity Module for the OAW-4308 (single switch license)

Alcatel OmniAccess 4308

Alcatel

26801 West Agoura Road
Calabasas, CA 91301 USA

Contact Center
(800) 995-2612 US/Canada
(818) 880-3500 Outside US

www.alcatel.com/enterprise

ALCATEL