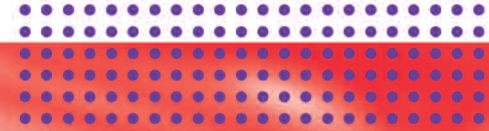


OmniAccess 4504, OmniAccess 4604, OmniAccess 4704

WIRELESS LAN-SWITCHES



Bei den Alcatel-Lucent Switches der Serien OmniAccess™ 4504, 4604 und 4704 (OAW-4504, OAW-4604, OAW-4704) handelt es sich um leistungsfähige, multifunktionale WLAN-Switches, mit deren Hilfe bis zu 32, 64 oder 128 Access Points (APs) an einem Standort zusammengeschaltet werden können. Diese WLAN-Switches bieten optimale Benutzerfreundlichkeit mit Follow Me Connectivity, identitätsbasiertem Zugriff und Application Continuity Services.



LEISTUNGSMERKMALE

- Hohe Leistung
- Skalierbare Architektur
- Zentralisierte WLAN-Switches
- Dynamische Funkfrequenzverwaltung
- Integriertes Funksicherheitssystem (Wireless Intrusion Prevention)
- Benutzerorientierte Sicherheit mit verbindungsorientierter Firewall

VORTEILE

- Plattform, die speziell für die Unterstützung von IEEE 802.11n-Hochleistungsnetzwerke konzipiert sind.
- Ermöglicht durch ein Software-Lizenzmodell wachstumsabhängige Investitionen. Die Access Point Kapazität der WLAN-Switches lässt sich durch Hinzufügen von Software-Lizenzen erweitern.
- Ermöglicht Overlay-Implementierungen ohne Unterbrechung zur bestehenden leitungs-gebundenen Infrastruktur. Vereinfacht Managementaufgaben durch die Minimierung der Anzahl der Netzwerkelemente.
- Ermöglicht die Analyse der WLAN-Umgebung, um die Bereitstellung durch die automatische Optimierung der Access Points zu erleichtern. Vereinfacht den Netzwerkbetrieb durch virtuelle Standortüberwachung in Echtzeit.
- Integriert den Betrieb von Funknetzwerken sowie die Erkennung und Verhinderung von Angriffen auf das Netzwerk; Kosten für kabellose Infrastrukturen und deren Betrieb können damit reduziert werden.
- Verhindert unbefugten Zugriff auf das Unternehmens-WLAN und bietet gleichzeitig Gastnutzern, Lieferanten und Anwendern des Unternehmens sichere Unterstützung. Reduziert durch rollenbasierte Sicherheitsvorkehrungen den Verwaltungsaufwand für ein sicheres Netzwerk.

LEISTUNGSMERKMALE

- Positionsverfolgung in Echtzeit
- Dienstqualität (QoS), verlängerte Akku-Leistung, Application Layer Gateway (ALG) für Sprachprotokolle

VORTEILE

- Ermöglicht die Positionsverfolgung von WLAN-Benutzern in Echtzeit und liefert umfangreiche Präsenzinformationen. Darüber hinaus wird die Positionsverfolgung von WLAN-Geräte-Tags im gesamten Unternehmen unterstützt.
- Verbessert die Sprachqualität durch QoS-Mechanismen wie WMM, DSCP-Kennzeichnung und -Priorisierung, sowie CAC (Connection Admission Control). Darüber hinaus wird das Spracherlebnis für Endbenutzer durch maximierte Akkulebensdauer mit Hilfe von Protokollen wie U-APSD verbessert. Bietet durch integrierte, verbindungsorientierte Firewall unübertroffene Sprachsicherheit.

Der OAW-4504 ist für Systeme in kleinen Unternehmen und Zweigniederlassungen konzipiert, während die Modelle OAW-4604 und OAW-4704 für mittelständische bis große Unternehmen oder eng beieinander liegende Bürobereiche ausgelegt sind. Diese drei WLAN-Switches können problemlos als Overlay implementiert werden, ohne dass das bestehende WLAN beeinträchtigt wird.

Erweiterte WLAN-Sprachübertragungsfunktionen, wie Call Admission Control (CAC), Funkmanagement mit Unterstützung für Sprachanwendungen, sowie eine strikte Funk-QoS ermöglichen den Modellen OAW-4504, OAW-4604 und OAW-4704 die Bereitstellung mobiler VoIP-Funktionen. Die Switches werden über die integrierte Managementfunktion des Alcatel-Lucent OmniAccess Wireless-Betriebssystems oder des Alcatel-Lucent OmniVista™ Mobility Managers verwaltet.

Außerdem bieten die Modelle OAW-4504, OAW-4604 und OAW-4704 ein hervorragendes benutzerorientiertes Sicherheitssystem, um WLAN-Benutzer zu authentifizieren, rollenbasierte Richtlinien für die Zugriffssteuerung zu erzwingen und unsichere Endpunkte so zu isolieren, dass sie nicht auf das Unternehmens-WLAN zugreifen können. Gastbenutzer können mit Hilfe des integrierten Captive-Portal-Servers und der erweiterten Netzwerkdienste problemlos und sicher unterstützt werden.

Dank der integrierten Site-to-Site-VPN- und NAT-Funktionen, des gesplitteten Tunnelings und der verbindungsorientierten Firewall schaffen die Modelle OAW-4504, OAW-4604, OAW-4704 eine sichere Netzwerkumgebung, ohne dass zusätzliche VPN-/Firewall-Geräte bereitgestellt werden müssen. Die Unterstützung von Site-to-Site-VPN kann in alle führenden VPN-Konzentratoren integriert werden, um die nahtlose Integration in bestehende Unternehmens-VPNs zu ermöglichen.

TECHNISCHE DATEN

Leistung und Kapazität (OAW-4504/OAW-4604/OAW-4704)

- Standortgebundene APs: Max. 32/64/128
- Dezentrale APs: Max. 128/256/512
- Benutzer: Max. 512/1024/2048
- MAC-Adressen: Max. 64.000
- VLAN-IP-Schnittstellen: 128
- Gigabit-Ethernet-Ports (RJ-45 oder SFP): 4
- Aktive Firewall-Sitzungen: Max. 128.000
- Gleichzeitige IPSec-Tunnel: Max. 512/1024/2048
- Firewall-Durchsatz: 3/4/4 Gbit/s
- Verschlüsselter Durchsatz (3DES, AESCBC256): 1,6/4/8 Gbit/s
- Verschlüsselter Durchsatz (AES CCM): 0,8/2/4 Gbit/s

Sicherheits- und Steuerungsfunktionen für WLANs

- 802.11i Sicherheitsstandard (WFA-zertifizierter WPA2 and WPA)
- 802.1X Benutzer- und Maschinenauthentifizierung
- EAP-PEAP-, EAP-TLS-, EAP-TTLS-Unterstützung

- Zentralisierte AES-CCM-, TKIP- und WEP-Verschlüsselung
- 802.11i PMK-Cache für schnelle Roaming-Anwendungen
- EAP-Offload für AAA-Serverskalierbarkeit und -stabilität
- Verbindungsorientierte 802.1X-Authentifizierung für eigenständige APs
- MAC-Adresse, SSID- und Multi-SSID-Unterstützung für standortbasierte Authentifizierung für den Betrieb mehrerer WLANs.
- SSID-basierte Radius-Server-Auswahl
- Sichere(s) AP-Steuerung und -Management über IPSec oder GRE
- kompatibel mit und erweiterbar auf CAPWAP
- Modus für verteiltes WLAN für Remote-AP-Implementierungen
- Gleichzeitige Unterstützung von zentralisierten und verteilten WLANs

Identitätsbasierte Sicherheitsfunktionen

- Captive Portal, Authentifizierung über 802.1X oder MAC-Adresse

- Benutzername, IP-Adresse, MAC-Adresse und Encryption Key Binding für leistungsstarke Netzwerkidentitätserstellung
- Identitätsüberprüfung pro Paket zur Vermeidung von Identitätsmissbrauch
- RADIUS- und LDAP-basierte AAA-Serverunterstützung
- Interne Benutzerdatenbank für AAA-Server-Failover-Schutz
- Rollenbasierte Autorisierung zur Vermeidung von zu weit reichenden Zugriffsberechtigungen
- Stabile Umsetzung von Richtlinien durch verbindungsorientierte Paketanalyse
- Sitzungsabrechnung pro Benutzer zur Nutzungsüberwachung
- Web-basierte Gastregistrierung
- Konfigurierbare zulässige Benutzerrichtlinien für den Gastzugriff
- XML-basierte API für die Integration externer Captive Portals
- xSec-Option für WLAN-Authentifizierung und -Verschlüsselung (802.1X-Authentifizierung, 256-Bit-AES-CBC-Verschlüsselung)

Konvergenzmerkmale

- Sprache und Daten über eine SSID für Konvergenzgeräte
- Durchsatzbasierte QoS mit VFC (Voice Flow Classification)
- Alcatel-Lucent NOE, SIP, Spectralink SVP, SCCP und Vocera ALGs
- Strenge Priorisierung für Funk-QoS
- Unterstützung für 802.11e – WMM, U-APSD und T-SPEC
- QoS-Richtlinien zur Vermeidung von Netzwerkmissbrauch über 802.11e
- DiffServ-Markierung und 802.1p-Unterstützung für Netzwerk-QoS
- On-Hook und Off-Hook VoIP-Clients Erkennung
- VoIP-Anrufsteuerung
- Schwellen für Anrufreservierung bei mobilen VoIP-Anrufen
- Funkmanagement mit Unterstützung für Sprachanwendungen zur Sicherstellung der Sprachqualität
- Unterstützung von Fast-Roaming zur Gewährleistung der Tonqualität
- SIP Medien- und Klingeltonerzeugung (RFC 3960)
- Ratenbegrenzung je Nutzer oder Rolle (Bandbreitenverträge)

Adaptive Funkmanagementfunktionen (Adaptive Radio Management, ARM)

- Automatische Kanal- und Leistungseinstellungen für Thin-APs
- Funküberwachung und Endanwenderdienste simultan
- Selbstheilende Reichweite entsprechend den dynamischen Frequenzbedingungen
- Optionen für dichten Einsatz zur Kapazitätsoptimierung
- AP-Lastverteilung je nach Anzahl der Nutzer
- AP-Lastverteilung je nach Bandbreitennutzung
- Erkennung von Funklöchern und Störungen
- 802.11h-Unterstützung für Radarerkennung und -vermeidung
- Automatische Standorterkennung für aktive RFID-Tags
- Integrierte XML-basierte Standort-API für RFID-Anwendungen

WLAN-Sicherheitsfunktionen

- Integration in die WLAN-Infrastruktur
- Simultane und dedizierte Funküberwachungsfunktionen
- Erkennung nicht autorisierter APs und integrierte Positionsvisualisierung
- Automatische Klassifizierung nicht autorisierter, störender und gültiger APs
- Ausschluss nicht autorisierter APs per Funk und Kabel

- Ad-hoc-WLAN-Netzwerkerkennung und -ausschluss
- Erkennung von Windows-Client-Bridging und Funk-Bridging
- Abwehr von Denial-of-Service-Angriffen für APs und Stationen
- Erkennung und Ausschluss falsch konfigurierter eigenständiger APs
- Leistungsüberwachung und Problembehebung von Drittanbieter-APs
- Erstellen flexibler Angriffssignaturen für neue WLAN-Angriffe
- EAP-Handshake- und Sequenznummernanalyse
- Erkennung gültiger AP-Identitätsmissbräuche
- Erkennung von Angriffen durch Frame-Überflutungen, nicht autorisierte APs und Funk
- ASLEAP-, Death Broadcast-, Null-Probe-Reaktionserkennung
- NetStumbler-basiertem Network Probe Detection

Verbindungsorientierte Firewall-Funktionen

- An Benutzeridentität oder Ports gebundene verbindungsorientierte Paketanalyse
- Standort- und tageszeitbezogene Richtliniendefinition
- 802.11-Stationserkennung für WLAN-Firewalls
- Funkrichtliniendurchsetzung und Erstellung schwarzer Listen für Stationen
- Session Mirroring und paketbasierte Protokolle für kriminaltechnische Analysen
- Detaillierte Firewall-Datenverkehrsprotokolle zur Nutzungsüberwachung
- Application Layer Gateway-Unterstützung (ALG) für NOE, SIP, SCCP, RTSP, Vocera, FTP, TFTP, PPTP
- Quell- und Ziel-NAT (Network Address Translation)
- Dedizierte Datenstromverarbeitungs-Hardware für hohe Leistung
- Erkennung und Abwehr von TCP- und ICMP-Denial-of-Service-Angriffen
- Richtlinienbasierte Weiterleitung in GRE-Tunnel für Gastdatenverkehr
- External Service Interface (ESI) für Drittanbieter-Sicherheitsintegration von internen Viren-, Spamschutz- und Inhaltsfilterungsanwendungen
- Funktionsüberprüfung und Lastverteilung für externe Dienste

VPN-Serverfunktionen

- Unterstützung von Site-to-Site-VPN für den Einsatz in Zweigniederlassungen
- Site-to-Site-Interoperabilität mit VPN-Servern von Drittanbietern
- VPN-Server-Emulation zur einfachen Integration in WLANs
- L2TP/IPsec-VPN-Terminierung für Windows-VPN-Clients
- XAUTH/IPsec-VPN-Terminierung für Drittanbieter-Clients

- PPTP-VPN-Terminierung zur Integration bereits bestehender VPNs:
- RADIUS- und LDAP-Serverunterstützung zur VPN-Authentifizierung
- PAP-, CHAP-, MS-CHAP- und MS-CHAP V.2-Authentifizierung
- Hardwareverschlüsselung für DES, 3DES, AES, MPPE
- Sichere Point-to-Point-xSec-Tunnel für L2 VPN

Netzwerkfunktionen und erweiterte Dienste

- L2- und L3-Switching per Funk und Kabel
- VLAN-Pooling für einfache, skalierbare Netzwerkdesigns
- VLAN-Mobilität für nahtloses L2-Roaming
- Proxy Mobile IP und Proxy-DHCP für L3-Roaming
- Integrierter DHCP-Server und integriertes DHCP-Relais
- VRRP-basierte N+1-WLAN-Switch-Redundanz (L2)
- Auf AP-Bereitstellung basierte N+1-WLAN-Switch-Redundanz (L3)
- Etherchannel-Unterstützung für Verbindungsredundanz
- 802.1d-STP (Spanning Tree Protocol)
- 802.1Q-VLAN-Tags

WLAN-Switch-basierte Managementfunktionen

- Toolkit für Funkplanung und AP-Bereitstellung
- Zentrales AP-Bereitstellungs- und Image-Management
- Live Coverage Visualization mit RF Heat Maps
- Detaillierte Statistikvisualisierung zur Überwachung
- Remote-Paketerfassung für RF-Fehlerbehebung
- Interoperabel mit Ethereal- und Airopack-Analysen
- Konfigurationsmanagement für mehrere WLAN-Switches
- Positionsvisualisierung und Geräteverfolgung
- Systemweite Protokollierung und Berichterstellung von Ereignissen

Administrationsfunktionen

- Web-basierter Zugang zur Benutzerschnittstelle über HTTP und HTTPS.
- Schnellstart-Bildschirme zur einfachen WLAN-Switch-Konfiguration
- CLI-Zugang über SSH, Telnet und Konsolen-Port
- Rollenbasierte Zugangskontrolle für eingeschränkten Admin-Zugang
- Authentifizierungszugang über RADIUS, LDAP oder interne DB
- Unterstützung von SNMPv3 und SNMPv2 zur WLAN-Switch-Überwachung
- Standard-MIBs und MIBs für private Unternehmen
- Detaillierte Meldungsprotokolle mit Syslog zur Ereignisbenachrichtigung

Stromverbrauch

- OAW-4504: max. 35 W
- OAW-4604: max. 45 W
- OAW-4704: max. 60 W

Leistungsdaten (AC-Eingangsanforderungen)

OAW-4504

- AC-Eingangsspannung: 90 - 264 V~, Universaleingang
- AC-Eingangsstrom: 1,5 A
- AC-Eingangsfrequenz: 47 - 63 Hz

OAW 4604 und OAW 4704

- AC-Eingangsspannung: 90 - 264 V~, Universaleingang
- AC-Eingangsstrom: 2,2 A
- AC-Eingangsfrequenz: 47 - 63 Hz

Betriebsdaten und Abmessungen

- Betriebstemperaturbereich 0 °C bis 40 °C
- Lagertemperaturbereich 10 °C bis 70 °C
- Luftfeuchtigkeit, nicht kondensierend 5 bis 95 %
- Höhe 44 mm
- Breite 351 mm
- Tiefe 297 mm

Gewicht

- OAW-4504: 3,2 kg (ohne Verpackung)
- OAW-4604/OAW-4704: 3,4 kg (ohne Verpackung)

Behördliche Vorgaben und Sicherheitsbestimmungen

- FCC Teil 15 Klasse A CE
- Industry Canada Klasse A
- VCCI Klasse A (Japan)
- EN 55022 Klasse A (CISPR 22 Klasse A), EN61000-3, 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-Kennzeichen, cTUVus, GS, CB, C-Tick, Anatel, NOM, MIC, IQC

BESTELLINFORMATIONEN

TEILENUMMER	BESCHREIBUNG
OAW-4504-0	OmniAccess 4504 - 4x 10/100/1000BaseT (RJ-45) oder 1000BaseX (SFP) Dual Personality Ports (ohne AP-Lizenz). Kann bis zu 32 APs unterstützen (zusätzliche AP-Lizenzen erforderlich).
OAW-4504-8	OmniAccess 4504 - 4x 10/100/1000BaseT (RJ-45) oder 1000BaseX (SFP) Dual Personality Ports, umfasst 8 AP-Lizenzen. Kann bis zu 32 APs unterstützen (zusätzliche AP-Lizenzen erforderlich).
OAW-4604-0	OmniAccess 4604 - 4x 10/100/1000BaseT (RJ-45) oder 1000BaseX (SFP) Dual Personality Ports (ohne AP-Lizenz). Kann bis zu 64 APs unterstützen (zusätzliche AP-Lizenzen erforderlich).
OAW-4604-32	OmniAccess 4604 - 4x 10/100/1000BaseT (RJ-45) oder 1000BaseX (SFP) Dual Personality Ports, umfasst 32 AP-Lizenzen. Kann bis zu 64 APs unterstützen (zusätzliche AP-Lizenzen erforderlich).
OAW-4704-0	OmniAccess 4704 - 4x 10/100/1000BaseT (RJ-45) oder 1000BaseX (SFP) Dual Personality Ports (ohne AP-Lizenz). Kann bis zu 128 APs unterstützen (zusätzliche AP-Lizenzen erforderlich).
OAW-4704-64	OmniAccess 4704 - 4x 10/100/1000BaseT (RJ-45) oder 1000BaseX (SFP) Dual Personality Ports, umfasst 64 AP-Lizenzen. Kann bis zu 128 APs unterstützen (zusätzliche AP-Lizenzen erforderlich).
OAW-SFP-SX	OmniAccess Wireless SFP - 1000BaseSX, LC-Anschluss
OAW-SFP-LX	OmniAccess Wireless SFP - 1000BaseLX, LC-Anschluss
OAW-SFP-TX	OmniAccess Wireless SFP - 1000Base-T, RJ-45-Anschluss

Wenn Sie weitere Informationen wünschen, wenden Sie sich an Ihren zuständigen Alcatel-Lucent-Ansprechpartner, autorisierten Wiederverkäufer oder Verkäufer. Oder besuchen Sie unsere Website unter www.alcatel-lucent.com.

Dieses Dokument wird nur zu Planungszwecken zur Verfügung gestellt und begründet, ändert oder ergänzt keinerlei Garantien, die von Alcatel-Lucent in Bezug auf die hierin beschriebenen Produkte und/oder Services gewährt werden können. Die Publikation der in diesem Dokument enthaltenen Informationen impliziert keine Aufgabe von Patentrechten oder anderer Schutzrechte von Alcatel-Lucent oder Dritten.

www.alcatel-lucent.com

Alcatel, Lucent, Alcatel-Lucent und das Alcatel-Lucent-Logo sind Marken von Alcatel-Lucent. Alle anderen Marken sind Eigentum ihrer jeweiligen Besitzer. Alcatel übernimmt keine Verantwortung für die Richtigkeit der hier enthaltenen Informationen. Änderungen behalten wir uns ohne Ankündigung vor.
© 2007 Alcatel-Lucent. Alle Rechte vorbehalten. P/N 4288700 - DE - 5/08